

# ЗАКОН

## О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

### І. ОСНОВНЕ ОДРЕДБЕ

#### Предмет уређивања

##### Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности субјеката приликом управљања и коришћења информационо-комуникационих система, поступци и мере за постизање високог општег нивоа информационе безбедности и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите, праћење правилне примене прописаних мера заштите, као и надлежности субјеката за надзор над спровођењем овог закона.

#### Значење појединих термина

##### Члан 2.

Поједини термини у смислу овог закона имају следеће значење:

1) *информационо-комуникациони систем* (ИКТ систем) је технолошко-организациона целина која обухвата:

- (1) *електронске комуникационе мреже и услуге* у смислу закона који уређује електронске комуникације;
- (2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
- (3) податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;
- (4) организациону структуру путем које се управља ИКТ системом;
- (5) све типове системског и апликативног софтвера и софтверске развојне алате;

2) *оператор ИКТ система* је физичко лице у својству регистрованог субјекта, правно лице, орган или организациона јединица органа који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) *информациона безбедност* представља способност информационо-комуникационих система и мрежа да се одупру и/или ублаже, уз одређени степен поузданости, сваки догађај који би могао да угрози расположивост, интегритет, аутентичност, непорецивост и поверљивост података који се чувају, преносе или обрађују, као и услуга које се пружају или су доступне путем тог ИКТ система;

4) *интегритет* је својство које осигурава да подаци или информације нису промењени или уништени на неовлашћени начин од када су креирани, пренети или ускладиштени;

5) *расположивост* је својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан;

6) *аутентичност* је својство којим се осигурава могућност да се провери и потврди да је информацију створио или послао онај за кога се тврди да је ту радњу извршио;

7) *поверљивост* је својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима;

8) *непорецивост* представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

9) *ризик* представља могућност губитка или поремећаја изазваног инцидентом и изражава се као комбинација величине таквог губитка или поремећаја и вероватноће настанка инцидента;

10) *рањивост* представља слабост или недостатак у ИКТ производима или услугама који се могу искористити за реализацију једне или више претњи;

11) *управљање ризиком* је скуп систематичних активности идентификације, процене и успостављање система контроле ризика који омогућава планирање, организовање и усмеравање мера заштите како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

12) *избегнути инцидент* представља идентификовани догађај у ИКТ систему који је могао довести до значајног угрожавања расположивости, аутентичности, интегритета, непорецивости или поверљивости података, услуга или система, али је правовременом интервенцијом или заштитним мерама спречено остваривање штетних последица;

13) *претња* представља сваку околност, догађај или радњу која може да угрози, поремети или на други начин штетно утиче на ИКТ систем, кориснике система и друга лица са јасном вероватноћом настајања штете у случају да изостане реакција;

14) *озбиљна претња* представља претњу по информациону безбедност за коју се, с обзиром на њена техничка својства, може претпоставити да има потенцијал да изазове значајне негативне последице по ИКТ систем, његовог оператора или кориснике услуга тог оператора узрокујући значајну материјалну или нематеријалну штету;

15) *инцидент* је сваки догађај који угрожава расположивост, интегритет, аутентичност, непорецивост или поверљивост података који се чувају, преносе или обрађују или услуге које се пружају, односно које су доступне путем ИКТ система;

16) *злонамерни софтвер* је софтвер намерно креиран са циљем да оштети, поремети, онемогући или неовлашћено приступи информационо-комуникационим системима и обухвата различите типове штетних програма, укључујући вирусе, тројанце, црве, рансомвер и шпијунски софтвер;

17) *јединствени систем за пријем обавештења о инцидентима* је информациони систем у који се уносе подаци о инцидентима и избегнутим инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

18) *управљање инцидентом* подразумева предузимање свих радњи и поступака чији је циљ спречавање, откривање, анализа и прекид инцидента, као

и предузимање других мера ради одговора на инцидент и отклањања његових последица;

19) *криза информационе безбедности* је догађај или стање које угрожава, омета рад или онемогућује рад ИКТ система од посебног значаја и при том изазива ризике, претње или последице по становништво, материјална добра или животну средину изузетно великог обима и интензитета које није могуће спречити или отклонити редовним деловањем надлежних органа и служби, а одговор на такав догађај или стање захтева учешће више надлежних органа, као и примену одговарајућих мера;

20) *мере заштите ИКТ система* су техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система;

21) *тајни податак* је податак који је, у складу са прописима о тајности података, одређен и означен одређеним степеном тајности;

22) *ИКТ систем за рад са тајним подацима* је ИКТ систем који је у складу са законом одређен за рад са тајним подацима;

23) *орган* је државни орган, орган аутономне покрајине, јединица локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења;

24) *служба безбедности* је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије;

25) *самостални оператори ИКТ система* су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове, службе безбедности и Народна банка Србије;

26) Центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: ЦЕРТ) је функционална целина у оквиру органа или правног лица која обухвата скуп послова који се односе на превенцију и заштиту од инцидентата;

27) *компромитујуће електромагнетно зрачење (КЕМЗ)* представља ненамерне електромагнетне емисије приликом преноса, обраде или чувања података, чијим пријемом и анализом се може открити садржај тих података;

28) *криптобезбедност* је компонента информационе безбедности која обухвата криптозаштиту, управљање криптоматеријалима и развој метода криптозаштите;

29) *криптозаштита* је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима;

30) *криптографски производ* је софтвер или уређај путем кога се врши криптозаштита;

31) *криptomатеријали* су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

32) *безбедносна зона* је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци, као и простор или просторија која је од кључног значаја за очување информационе безбедности ИКТ система;

33) *информациона добра* обухватају информације које се обрађују у складу са функцијом и наменом ИКТ система; електронске записе о конфигурацији уређаја и електронске комуникационе мреже; електронске записе о интеракцијама у ИКТ системима, приступу и употреби ИКТ система (тзв. log записе); програмски код; техничку и корисничку документацију; електронске записе о интеракцијама у електронској комуникационој мрежи (тзв. мрежни саобраћај); информације којима се регулишу намена и коришћење ИКТ система, процеси, мере заштите и сл;

34) *услуга информационог друштва* је услуга у смислу закона којим се уређује електронска трговина;

35) *пружалац услуге информационог друштва* је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина;

36) *мрежа за испоруку садржаја (Content Delivery Network – CDN)* означава мрежу географски распоређених сервера која је осмишљена да обезбеди високу доступност, приступачност и брзу испоруку дигиталног садржаја и услуга корисницима интернета, у име пружалаца садржаја и услуга;

37) *тачка за размену интернет саобраћаја (енгл. internet exchange point)* је мрежна структура која пружа могућност повезивања две или више независних мрежа (аутономних система) првенствено у сврху олакшавања размене интернет саобраћаја, и која омогућује међуповезивање аутономних система, у ком случају није потребно да интернет саобраћај између аутономних система прође кроз трећи аутономни систем, те која такав саобраћај не мења и не утиче на њега на други начин;

38) *систем назива домена (ДНС)* је дистрибуирани, хијерархијски организован систем који повезује називе домена са одговарајућим ИП адресама које се користе за усмеравање и повезивање корисничких уређаја са услугама и ресурсима на интернету;

39) *пружалац услуге ДНС-а* је субјекат који пружа услуге разрешавања ДНС упита корисницима интернета или пружа услугу ауторитативних сервера имена за називе домена које користе трећа лица, са изузетком коренских (енгл. root) сервера имена;

40) *услуга од поверења* је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

41) *пружалац услуге од поверења* је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

42) *квалификована услуга од поверења* је услуга у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

43) *пружалац квалификоване услуге од поверења* је пружалац у смислу закона којим се уређује електронски документ, електронска идентификација и услуге од поверења у електронском пословању;

44) *услуге рачунарства у клауду (енгл. „cloud computing service“)* су дигиталне услуге које омогућавају управљање на захтев и широки даљински приступ надоградивом и еластичном скупу дељивих рачунарских ресурса, укључујући и ситуације када су такви ресурси распоређени на неколико локација;

45) *услуга центра за управљање и чување података* је услуга која се пружа коришћењем структура или група структура намењених за централизовано смештање, међуповезивање и функционисање рачунарске и мрежне опреме ради чувања, обраде и преноса података, укључујући све објекте и инфраструктуру за дистрибуцију електричне енергије и контролу утицаја на животну средину;

46) *научноистраживачка организација* је организација у смислу закона којим се уређују наука и истраживање;

47) *јавна електронска комуникациона мрежа* је електронска комуникациона мрежа у смислу закона којим се уређују електронске комуникације;

48) *електронска комуникациона услуга* је услуга у смислу закона којим се уређују електронске комуникације;

49) *пужалац управљаних услуга* је субјект који пружа услуге у вези са постављањем, управљањем, радом и одржавањем ИКТ производа, мрежа, инфраструктуре, апликација или друге мреже и информационог система путем пружања помоћи или активног управљања које се спроводи у просторијама корисника услуге или на даљину;

50) *пужалац управљаних безбедносних услуга* је пужалац управљаних услуга који спроводи или пружа помоћ у спровођењу активности у вези са управљањем ризиком у области безбедности;

51) *регистар назива домена највишег нивоа (енгл. TLD name registry)* означава субјекта којем је додељен одређени домен највишег нивоа и који је одговоран за управљање доменом највишег нивоа, укључујући регистрацију домена под доменом највишег нивоа и техничко функционисање домена највишег нивоа, што обухвата рад његових серверских имена, одржавање база података и дистрибуцију зона домена највишег нивоа преко серверских имена, без обзира на то да ли се те активности обављају од стране самог субјекта или су поверене трећим лицима, осим у ситуацијама када називе домена највишег нивоа регистар користи искључиво за сопствене потребе;

52) *пужалац услуге регистрације назива домена* је регистратор назива домена или други субјект који делује у име регистратора или за рачун регистратора;

53) *ИКТ производ* је елемент или група елемената у оквиру информационо-комуникационог система;

54) *ИКТ услуга* је услуга која се у потпуности или у већој мери састоји из преноса, чувања, преузимања или обраде података коришћењем ИКТ система;

55) *ИКТ процес* је скуп активности који се обавља у циљу израде, развоја, коришћења и одржавања ИКТ производа или ИКТ услуге;

56) *TLP (Traffic Light Protocol)* представља стандард за дељење информација у области информационе безбедности, који је успостављен у циљу обезбеђивања ефективне сарадње и дељења информација од извора информације до једног или више прималаца. Протокол пружа једноставну и интуитивну шему од четири ознаке за упућивање на то са ким се потенцијално осетљиве информације могу поделити;

57) *податак о личности* је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим

мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета;

58) *администратор* је лице које је овлашћено и одговорно за одржавање, управљање и обезбеђивање функционалности и безбедности ИКТ система од посебног значаја, у складу са одредбама овог закона и другим важећим прописима.

59) *техничка спецификација* је документ којим се утврђују технички захтеви које треба да испуни производ, процес или услуга, у складу са законом којим се уређује стандардизација.

Термини који се користе у овом закону и прописима који се доносе на основу њега, а који имају родно значење, изражени у граматичком мушком роду, подразумевају природни женски и мушки пол лица на која се односе.

### **Начела информационе безбедности**

#### **Члан 3.**

Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима:

1) начело управљања ризиком – избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;

2) начело свеобухватне заштите – мере се примењују на свим организационим, физичким и техничко-технолошким нивоима, као и током целокупног животног циклуса ИКТ система;

3) начело стручности и добре праксе – мере се примењују у складу са стручним и научним сазнањима и искуствима у области информационе безбедности;

4) начело свести и оспособљености – сва лица која својим поступцима ефективно или потенцијално утичу на информациону безбедност треба да буду свесна ризика и поседују одговарајућа знања и вештине;

5) начело континуираног побољшања – мере заштите и управљања информационом безбедношћу треба редовно процењивати и унапређивати како би се осигурала њихова ефикасност и прилагодљивост новим претњама и технолошким променама;

6) начело равноправности и недискриминације – мере заштите ИКТ система морају се спроводити на начин који осигурава једнак третман свих корисника, без дискриминације по било ком основу, у складу са законом.

### **Обрада података о личности**

#### **Члан 4.**

На обраду података о личности која је неопходна за вршење надлежности и испуњење обавеза из овог закона примењују се одредбе овог закона, одредбе посебних закона којима се уређују одређене области, као и одредбе закона којим се уређује заштита података о личности.

## **II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА**

### **ИКТ системи од посебног значаја**

#### **Члан 5.**

ИКТ системи од посебног значаја су ИКТ системи који су од кључног значаја за одржавање критичних друштвених и економских активности чији би

прекид или поремећај у пружању услуга имао или могао да има значајан утицај на јавну безбедност, јавно здравље, функционисање других сектора или би створио односно могао да створи значајан системски ризик.

ИКТ системи од посебног значаја су:

- 1) приоритетни ИКТ системи;
- 2) важни ИКТ системи.

Оператори приоритетних ИКТ система су:

1) правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:

(1) Енергетика и рударство

- производња електричне енергије, изузев производње коју обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика;
- комбинована производња електричне и топлотне енергије;
- снабдевање електричном енергијом;
- пренос електричне енергије и управљање преносним системом;
- дистрибуција електричне енергије и управљање дистрибутивним системом, као и дистрибуција електричне енергије и управљање затвореним дистрибутивним системом;
- складиштење електричне енергије, изузев складиштења које обављају крајњи купци у смислу закона којим се уређује коришћење обновљивих извора енергије и закона којим се уређује енергетика;
- управљање организованим тржиштем електричне енергије;
- производња, дистрибуција и снабдевање топлотном енергијом;
- транспорт нафте нафтоводима, транспорт деривата нафте продуктоводима и транспорт нафте и деривата нафте другим облицима транспорта;
- истраживање и производња нафте и природног гаса;
- производња деривата нафте;
- складиштење нафте и деривата нафте;
- транспорт и управљање транспортним системом за природни гас;
- складиштење и управљање складиштем природног гаса;
- дистрибуција и управљање дистрибутивним системом за природни гас;
- снабдевање и јавно снабдевање природним гасом;
- производња и прерада угља;

- производња и прерада бакра, злата, олова, цинка, литијума и бора;
- производња, складиштење и пренос водоника;

(2) Саобраћај

- обављање јавног авио-превоза уз важећу оперативну дозволу;
- управљање аеродромом;
- услуге контроле летења;
- управљање јавном железничком инфраструктуром;
- послови железничких предузећа;
- обављање превоза путника и терета унутрашњим водама;
- управљање лукама;
- сервис за управљање бродским саобраћајем (VTS);
- речни информациони сервиси (RIS);
- управљање путном инфраструктуром;
- управљање интелигентним транспортним системима (ИТС);

(3) Банкарство и финансијска тржишта

- послови финансијских институција и институција тржишта капитала, које су под надзором Народне банке Србије односно Комисије за хартије од вредности;
- послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;
- послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;
- послови клиринга односно салдирања финансијских инструмената, у смислу закона којим се уређује тржиште капитала;
- послови пружалаца услуга повезаних с дигиталном имовином, у смислу закона којима се уређује дигитална имовина;

(4) Здравство

- пружање здравствене заштите;
- рад националних референтних лабораторија;
- истраживање и развој лекова;
- производња фармацеутских лекова и препарата намењених за здравствену употребу;
- производња лекова и других производа намењених употреби у здравству, укључујући производе који су од виталног значаја током ванредног стања у области јавног здравља;
- обрада генетских, биомедицинских података и других података од значаја за истраживање и развој у области



биотехнологије, биоинформатике, биоекономије, генетике и медицине;

(5) Вода за пиће

- снабдевање и дистрибуција воде намењене за људску потрошњу, изузев дистрибутера којима наведени послови нису претежни део њихове делатности;

(6) Отпадне воде

- сакупљање, одвођење или пречишћавање комуналних отпадних вода, отпадних вода насеља и привреде, изузев привредних субјеката којима наведени послови нису претежни део њихове делатности;

(7) Дигитална инфраструктура

- пружање услуга рачунарства у клауду;
- пружање услуге центра за чување и складиштење података;

(8) Управљање ИКТ услугама које се пружају операторима приоритетних ИКТ система

- пружање управљаних услуга;
- пружање управљаних безбедносних услуга;

(9) Остале области

- управљање нуклеарним објектима;
- пружање услуга од поверења, укључујући квалификоване услуге од поврења, пружање услуга система домена (DNS), управљање регистром домена највишег нивоа и пружање услуга регистрације домена са изузетком оператора коренских сервера имена;
- пружање услуга мреже за испоруку садржаја;
- обављање делатности електронских комуникација;
- тачка за размену интернет саобраћаја;
- издавање Службеног гласника Републике Србије и вођење Правно-информационог система Републике Србије;
- области у којој у Републици Србији постоји само један пружалац услуге и која је неопходна за обављање критичних друштвених и привредних делатности;

2) органи;

3) субјекти који су одређени као оператори критичне инфраструктуре у складу са прописима којима се уређује критична инфраструктура.

Поред субјеката из става 3. овог члана, као оператори приоритетних ИКТ система могу се одредити субјекти код којих прекид рада ИКТ система или поремећај у раду ИКТ система:

1) може имати значајан утицај на јавну безбедност, националну безбедност или јавно здравље;

2) може изазвати значајан системски ризик, а посебно у секторима где поремећај може имати прекогранични утицај.

Субјекте из става 4. овог члана одређује министарство надлежно за послове информационе безбедности, а по прибављеном мишљењу органа у чијој је надлежности област у којој субјект обавља делатности.

На операторе приоритетних ИКТ система од посебног значаја који обављају делатност у сектору банкарства и финансијских тржишта из става 3. тачка 1) подтачка (3) алинеје прва, друга и пета овог члана примењују се посебни, секторски прописи којима се ближе, односно на друкчији начин уређују поједина питања из овог закона, а којима се обезбеђује најмање исти ниво делотворности мера управљања безбедносним ризицима тих оператора сходно мерама из члана 10. овог закона, при чему се обезбеђује и извештавање о инцидентима који представљају кризу информационе безбедности у складу са овим законом.

Народна банка Србије, као надлежни надзорни орган над пословањем оператора приоритетних ИКТ система од посебног значаја који обављају делатност у сектору банкарства и финансијских тржишта из става 3. тачка 1) подтачка (3) алинеје прва, друга и пета овог члана (субјекти надзора Народне банке Србије), у складу са овим законом и одредбама посебних закона којима се уређује пословање тих субјеката доноси прописе којима се уређују питања информационе безбедности за те субјекте, и то мере заштите ИКТ система, доношење аката о процени ризика и акта о безбедности ИКТ система, класификација инцидента, достављање обавештења о инциденту, поступање у вези са инцидентима, извештавање током и након инцидента, достављање статистичких података о инциденту и друга питања од значаја за безбедност информационог система ових субјеката, као и надзора који врши над њима.

### **Оператори важних ИКТ система**

#### **Члан 6.**

Оператори важних ИКТ система су:

1) правна лица и физичка лица у својству регистрованог субјекта, која обављају послове и делатности у следећим областима:

- поштанске услуге у смислу закона којим се уређује област поштанских услуга;
- управљање отпадом, у смислу закона којим се уређује управљање отпадом, изузев привредних субјеката којима наведени посао није претежни део њихове делатности;
- управљање амбалажним отпадом, у смислу закона којим се уређује управљање амбалажним отпадом;
- производња и снабдевање хемикалијама, у складу са законом којим се уређују хемикалије;
- производња, прерада и дистрибуција хране у сегменту veleprodaje и индустријске производње и прераде;
- производња рачунара, електронских и оптичких производа;
- производња електричне опреме;
- производња машина и уређаја;
- производња моторних возила, приколица и полуприколица и производња остале опреме за превоз;
- производња медицинских уређаја и производња *in vitro* дијагностичких медицинских средстава;

- услуге информационог друштва у смислу закона о електронској трговини;
- производња, промет и превоз наоружања и војне опреме;
- свемирске услуге које се ослањају на земаљску инфраструктуру, нарочито активности управљања контролним центрима, објектима за праћење и комуникацију и пружање услуга лансирања;

2) научноистраживачке институције;

3) правна и физичка лица у својству регистрованог субјекта и органи из члана 5. овог закона, а који не спадају у операторе приоритетних ИКТ система према критеријумима за одређивање оператора.

Поред субјеката из става 1. овог члана, као оператори важних ИКТ система могу се одредити субјекти код којих прекид рада ИКТ система или поремећај у раду ИКТ система:

1) може имати значајан утицај на јавну безбедност, националну безбедност или јавно здравље;

2) може изазвати значајан системски ризик, а посебно у секторима где поремећај може имати прекогранични утицај.

Субјекте из става 2. овог члана одређује министарство надлежно за послове информационе безбедности, а по прибављеном мишљењу органа у чијој је надлежности област у којој субјект обавља делатности.

Подзаконски акт којим се ближе уређују услови, општи и секторски критеријуми укључујући и критеријуме у погледу величине привредних субјеката, за одређивање оператора приоритетних и важних ИКТ система доноси Влада, на предлог министарства надлежног за послове информационе безбедности.

Министарства у чијим надлежностима су области у којима оператори приоритетних и важних ИКТ система обављају делатности и Народна банка Србије, дужни су да у поступку израде подзаконског акта из става 4. овог члана, доставе министарству надлежном за послове информационе безбедности предлоге секторских критеријума ради одређивања оператора ИКТ система од посебног значаја.

### **Обавезе оператора ИКТ система од посебног значаја**

#### **Члан 7.**

Оператор ИКТ система од посебног значаја, сходно овом закону, у обавези је да:

1) поднесе пријаву за упис у евиденцију ИКТ система од посебног значаја;

2) предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидената;

3) изврши процену ризика и донесе акт о процени ризика;

4) донесе акт о безбедности ИКТ система од посебног значаја;

5) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система и то најмање једном годишње;

6) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја трећим лицима;

7) доставља обавештења, без одлагања, о сваком инциденту који значајно нарушава безбедност ИКТ система од посебног значаја;

8) пријави избегнуте инциденте који представљају озбиљну претњу у складу са овим законом;

9) доставља статистичке податке о инцидентима и избегнутим инцидентима у ИКТ системима.

### **Обавезе самосталних оператора**

#### **Члан 8.**

Самостални оператор дужан је да:

1) поднесе пријаву за упис у евиденцију ИКТ система од посебног значаја;

2) предузме одговарајуће техничке, оперативне, организационе и физичке мере заштите ИКТ система од посебног значаја, управљање ризицима и превенцију и смањење штетних последица инцидента;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености мера заштите ИКТ система које се примењују са актом о безбедности ИКТ система у складу са сопственим правилима за проверу усклађености мера заштите, а најмање једном годишње;

5) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико поверава активности у вези са ИКТ системом од посебног значаја са трећим лицима;

6) формира сопствени ЦЕРТ ради управљања инцидентима у својим системима.

Самостални оператори могу да међусобно размењују информације о инцидентима са Канцеларијом за информациону безбедност, а по потреби и са другим организацијама.

На самосталне операторе не примењују се одредбе овог закона о пријављивању инцидента који значајно угрожавају информациону безбедност, одредбе о достављању статистичких података о инцидентима и одредбе о проактивном скенирању мреже оператора ИКТ система од посебног значаја.

Самостални оператори, могу самостално и у координацији са Канцеларијом за информациону безбедност, ради откривања рањивости да врше проактивно скенирање сопствених ИКТ система повезаних на Јединствену информационо-комуникациону мрежу електронске управе.

Самостални оператори ИКТ система одредиће посебна лица, односно организационе јединице за интерну контролу сопствених ИКТ система.

Лица за интерну контролу самосталних оператора ИКТ система извештају о извршеној интерној контроли подносе руководиоцу самосталног оператора ИКТ система.

## **Евиденција оператора ИКТ система од посебног значаја**

### **Члан 9.**

Министарство надлежно за послове информационе безбедности (у даљем тексту: Министарство) успоставља и води евиденцију приоритетних и важних ИКТ система (у даљем тексту: Евиденција) која садржи:

- 1) назив, матични број и седиште оператора ИКТ система од посебног значаја;
- 2) име и презиме, службену адресу за пријем електронске поште и службени контакт телефон администратора задуженог за одржавање и управљање ИКТ системом од посебног значаја;
- 3) име и презиме, службену адресу за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја;
- 4) податак о врсти ИКТ система од посебног значаја, односно да ли ИКТ систем од посебног значаја потпада под приоритетан или важан;
- 5) податак о делатности оператора ИКТ система од посебног значаја;
- 6) адресни опсег интернет протокола (енгл. „IP address range“) који припадају ИКТ систему од посебног значаја, а који обухвата податке о јавним статичким ИП адресама;
- 7) веб презентацију оператора ИКТ система од посебног значаја;
- 8) број локација на којима се ИКТ систем од посебног значаја налази.

Поред података из става 1. овог члана, евиденција може да садржи и друге допунске податке о ИКТ систему од посебног значаја.

Самостални оператори ИКТ система изузети су од обавезе достављања података из става 1. тач. 4), 5), 6) и 8) овог члана.

Подзаконски акт којим се ближе уређује садржај и структура евиденције, као и начин подношења захтева за унос и промену података у Евиденцији доноси Министарство.

Оператор ИКТ система од посебног значаја дужан је да Министарству достави податке из ст. 1. и 2. овог члана најкасније 90 дана од дана усвајања прописа из става 4. овог члана, односно 90 дана од дана успостављања ИКТ система од посебног значаја.

Оператор ИКТ система од посебног значаја дужан је да у случају промене података из става 1. овог члана о томе обавести Министарство у року од 15 дана од дана настанка промене.

Подаци из става 1. тач. 2) и 3) овог члана обрађују се у сврху извршења одредби овог закона у погледу достављања обавештења и упозорења значајних за безбедност ИКТ система од посебног значаја, као и ради успостављања комуникације и остваривања сарадње у циљу отклањања штетних последица инцидената и превентивног деловања.

Подаци из става 1. тач. 2) и 3) овог члана обрађују се у складу са законом којим се уређује заштита података о личности и чувају се до тренутка престанка сврхе обраде или до извршене промене података у складу са ставом 6. овог члана.

Министарство ставља на располагање ажурну Евиденцију Канцеларији за информациону безбедност ради извршења одредби овог закона у погледу прикупљања и размене информација о претњама, рањивостима и инцидентима

и пружања подршке, упозоравања и саветовања лица која управљају ИКТ системима.

Евиденција представља тајни податак у смислу закона којим се уређује тајност података.

### **Мере заштите ИКТ система од посебног значаја**

#### **Члан 10.**

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидента, односно превенција и смањење штете од инцидента који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите примењују се у свим ИКТ системима оператора из става 1. овог члана.

Мере заштите ИКТ система се односе на:

- 1) успостављање организационе структуре, са утврђеним пословима, знањима, компетенцијама, искуством и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;
- 2) прикупљање података о претњама по информациону безбедност ИКТ система;
- 3) постизање безбедности рада на даљину и употребе мобилних уређаја;
- 4) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност, односно да обезбеди одржавање основних и по потреби напредних информатичких обука за све запослене и ангажована лица која имају приступ ИКТ системима, обука за руководиоце односно органе управљања оператора ИКТ система од посебног значаја, као и специјализоване стручне обуке за запослене одговорне за управљање информационом безбедношћу, ради обезбеђивања континуиране едукације;
- 5) обезбеђивање довољно ресурса за адекватно управљање информационом безбедношћу;
- 6) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;
- 7) идентификовање информационих добара и одређивање одговорности за њихову заштиту;
- 8) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;
- 9) заштиту носача података;
- 10) ограничење приступа подацима и средствима за обраду података;
- 11) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;
- 12) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;

13) предвиђање употребе криптографских контрола и других техника за сакривање података ради заштите поверљивости, аутентичности и интегритета података;

14) примена мера заштите ради спречавања отицања података;

15) физичку заштиту објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему;

16) заштиту од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем;

17) обезбеђивање исправног и безбедног функционисања средстава за обраду података;

18) примену одговарајућих процедура и мера заштите приликом коришћења услуге рачунарства у клауду;

19) праћење ИКТ система у циљу откривања рањивости и претњи;

20) ограничење приступа веб презентацијама које могу потенцијално да наруше безбедност ИКТ система;

21) заштиту података и средстава за обраду података од злонамерног софтвера;

22) заштиту од губитка података редовном израдом резервних копија података, софтвера и система путем одговарајућих средстава за размену података;

23) чување података о догађајима који могу бити од значаја за безбедност ИКТ система;

24) обезбеђивање интегритета софтвера и оперативних система;

25) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

26) обезбеђивање заштите ИКТ система приликом спровођења ревизорског тестирања;

27) заштиту података у комуникационим мрежама, укључујући уређаје и водове;

28) безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система;

29) испуњење захтева за информациону безбедност у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

30) заштиту података који се користе за потребе тестирања ИКТ система односно делова система;

31) процедуре за чување и брисање информација у ИКТ системима, у складу са прописима;

32) заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга;

33) одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга;

34) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама, као и примену мера санације последица инцидента;

35) мере које обезбеђују континуитет обављања посла у ванредним околностима које се дефинишу Планом континуитета обављања посла;

36) усвајање докумената којима се дефинишу процедуре за проверу адекватности мера заштите;

37) употребу мултифакторске аутентикације или решења континуиране провере аутентичности, заштићене гласовне, видео и текстуалне комуникације, те безбедних комуникационих система у хитним случајевима унутар оператора ИКТ система.

Подзаконски акт којим се ближе уређују мере заштите приоритетних и важних ИКТ система уважавајући начела из члана 3. овог закона, националне и међународне стандарде, и стандарде који се примењују у одговарајућим областима рада и релевантне техничке спецификације доноси Влада, на предлог Министарства.

### **Акт о процени ризика ИКТ система од посебног значаја**

#### **Члан 11.**

Оператор ИКТ система од посебног значаја дужан је да донесе акт о процени ризика за ИКТ системе (у даљем тексту: акт о процени ризика) којима управља.

Актом о процени ризика врши се процена ризика за ИКТ систем од посебног значаја с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај.

Акт о процени ризика ревидира се најмање једном годишње.

Акт о процени ризика израђује се у складу са општом методологијом за процену ризика у приоритетним и важним ИКТ системима од посебног значаја коју доноси орган, односно организација у којој се обављају послови Националног ЦЕРТ-а.

Оператор ИКТ система од посебног значаја није у обавези да донесе акт из става 1. овог члана у случају када има дефинисану процену ризика у другим постојећим интерним актима, која обухвата захтеве из опште методологије из става 4. овог члана.

### **Акт о безбедности ИКТ система од посебног значаја**

#### **Члан 12.**

Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система (у даљем тексту: акт о безбедности).

Актом о безбедности одређују се мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја.

Акт о безбедности ИКТ система од посебног значаја заснива се на Акту о процени ризика из члана 11. овог закона. Примена мера заштите ИКТ система мора бити у складу са процењеним ризицима, како би се обезбедила адекватна заштита система и минимизирао утицај потенцијалних инцидентата.



Акт о безбедности мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

Оператор ИКТ система од посебног значаја дужан је да, самостално или уз ангажовање спољних експерата, врши проверу из претходног става најмање једном годишње и да о томе сачини извештај.

Подзаконски акт којим се ближе уређује садржај акта о безбедности, начин провере ИКТ система од посебног значаја и садржај извештаја о провери, као и достављање извештаја надлежном органу, доноси Влада на предлог Министарства.

### **Обавеза обавештавања о инцидентима који значајно нарушавају информациону безбедност**

#### **Члан 13.**

Оператори ИКТ система од посебног значаја дужни су да доставе обавештење о инциденту који може да има значајан утицај на нарушавање информационе безбедности, без одлагања, а најкасније у року од 24 сата од када су сазнали за инцидент.

Инциденти који могу да имају значајан утицај на нарушавање информационе безбедности су:

- 1) инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;
- 2) инциденти који утичу на велики број корисника услуга, или трају дужи временски период;
- 3) инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;
- 4) инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;
- 5) инциденти који доводе до неовлашћеног приступа подацима чије откривање може угрозити права и интересе оних на које се подаци односе;
- 6) инциденти који су настали као последица инцидента у ИКТ систему оператора приоритетних ИКТ система који обављају делатности у области дигиталне инфраструктуре, из члана 5. став 3. тачка 1) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге у области дигиталне инфраструктуре;
- 7) инциденти који изазивају или могу да изазову знатну материјалну или нематеријалну штету оператору ИКТ система од посебног значаја и другим физичким и правним лицима.

Оператори ИКТ система од посебног значаја дужни су да пријаве и избегнуте инциденте који представљају озбиљну претњу и који би могли довести до околности сличних онима описаним у ставу 2. овог члана. У случају инцидента у ИКТ системима за рад са тајним подацима оператори тих ИКТ система поступају у складу са прописима којима се уређује област заштите тајних података.

## **Достављање обавештења о инцидентима**

### **Члан 14.**

Оператори ИКТ система од посебног значаја дужни су да обавештења о инцидентима доставе у јединствени систем за пријем обавештења о инцидентима путем веб презентације Министарства или Канцеларије за информациону безбедност.

Оператори приоритетних ИКТ система од посебног значаја који обављају делатности у области банкарства и финансијских тржишта из члана 5. став 3. тачка 1) подтачка (3) овог закона дужни су да обавештење о инциденту доставе Народној банци Србије, а ако су оператори приоритетних ИКТ система у области финансијских тржишта који су под надзором Комисије за хартије од вредности, обавештење достављају и Комисији за хартије од вредности.

Оператори приоритетних ИКТ система који обављају делатности електронских комуникација из члана 5. став 3. тачка 1) подтачка (9) алинеја четврта овог закона и оператори важних ИКТ система од посебног значаја који обављају делатност поштанских услуга из члана 6. став 1. тачка 1) алинеја прва овог закона, дужни су да обавештење о инциденту доставе Регулаторном телу за електронске комуникације и поштанске услуге.

Народна банка Србије, Регулаторно тело за електронске комуникације и поштанске услуге и Комисија за хартије од вредности дужни су да добијена обавештења из ст. 2. и 3. овог члана проследе у јединствени систем за пријем обавештења о инцидентима.

Оператори ИКТ система од посебног значаја, осим оператора ИКТ система из ст. 2. и 3. овог члана, дужни су да путем одговарајућих канала комуникације обавесте о инциденту кориснике којима пружају услуге, без одлагања, у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга, као и о мерама које корисници могу да предузму и употребе у циљу умањења или елиминације штетних последица инцидента.

Оператори ИКТ система од посебног значаја из ст. 2. и 3. овог члана обавештавају кориснике о инцидентима у складу са посебним прописима.

Орган коме је у складу са овим законом упућено обавештење о инциденту, уколико је реч о ИКТ систему од посебног значаја који је одређен као критична инфраструктура у складу са законом којим се уређује критична инфраструктура, информацију о томе прослеђује министарствима надлежним за секторе критичне инфраструктуре.

Органи из ст. 1–3. овог члана, којима је упућено обавештење о инциденту, дужни су да, у случају инцидента који је настао у ИКТ систему оператора критичне инфраструктуре утврђеног у складу са законом којим се уређује критична инфраструктура, добијену информацију без одлагања проследе надлежним министарствима за секторе критичне инфраструктуре, у складу са прописима о заштити тајних података.

### **Садржај обавештења о инциденту**

### **Члан 15.**

Обавештење о инциденту мора да садржи следеће податке:

- 1) податке о подносиоцу пријаве;
- 2) врсту и опис инцидента и процену да ли је инцидент последица кривичног дела;

- 3) датум и време почетка инцидента, односно сазнања о инциденту и трајање инцидента;
- 4) последице које је инцидент изазвао;
- 5) предузете активности ради ублажавања последица инцидента;
- 6) иницијалну процену нивоа опасности и утицаја инцидента на ИКТ систем од посебног значаја, као и индикаторе компромитације;
- 7) информацију о евентуалном прекограничном дејству инцидента;
- 8) податке о претходно пријављеним сличним инцидентима, ако су постојали, укључујући време и природу тих инцидентата, као и мере које су том приликом предузете;
- 9) друге релевантне информације, по потреби.

### **Значај инцидентата према нивоу опасности**

#### **Члан 16.**

Инциденти у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности сврставају се према нивоу опасности, имајући у виду последице инцидента, у следеће нивое опасности:

- 1) низак;
- 2) средњи;
- 3) висок;
- 4) веома висок.

Подзаконски акт којим се уређује поступак обавештавања о инцидентима, обрасци за обавештавање, листа инцидентата према врстама и класификација инцидентата према нивоу опасности доноси Влада, на предлог Министарства.

### **Оперативни тим за реаговање на инциденте**

#### **Члан 17.**

У циљу координисане реакције на инциденте високог и веома високог нивоа Канцеларија за информациону безбедност образује стални оперативни тим.

Канцеларија за информациону безбедност ближе уређује критеријуме за именовање чланова, као и вршење послова и задатке сталног оперативног тима.

Канцеларија за информациону безбедност може да, зависно од природе и последица инцидента, затражи укључивање других органа у рад оперативног тима у оквиру њихових надлежности.

По потреби, састанцима оперативног тима могу присуствовати и представници самосталних оператора, лица укључена у рад Тела за координацију послова информационе безбедности, као и представници посебних ЦЕРТ-ова.

Лица која учествују у раду сталног оперативног тима дужна су да се сертификају за рад са тајним подацима.

## **План за реаговање у случају инцидента високог нивоа и криза информационе безбедности**

### **Члан 18.**

Влада доноси План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности, на предлог Канцеларије за информациону безбедност.

План из става 1. овог члана обухвата:

- 1) циљеве мера и активности за реаговање у случају инцидента високог нивоа и криза информационе безбедности;
- 2) деловање надлежних органа у циљу спровођења плана;
- 3) опис процедура у случају инцидента високог нивоа и криза информационе безбедности;
- 4) активности за унапређење способности реаговања на инциденте, а пре свега планове одговарајућих вежби и обука;
- 5) моделе сарадње са приватним, невладиним и академским сектором;
- 6) међусобну сарадњу надлежних органа.

Приликом израде плана из става 1. овог члана успоставља се сарадња са органима и правним лицима чије су надлежности, односно послови и делатности повезани са планираним активностима.

План из става 1. овог члана се периодично мења и допуњује у складу са потребама и новим околностима, а у целини се поново израђује и доноси сваке треће године, а уколико су се околности у значајној мери промениле и раније.

### **Поступање по пријему обавештења о инциденту**

### **Члан 19.**

По пријему обавештења о инциденту у ИКТ систему од посебног значаја, Канцеларија за информациону безбедност поступа у складу са надлежностима утврђеним законом, односно прикупља, анализира и размењује информације о ризицима за безбедност ИКТ система, као и инциденту, и у вези са тим обавештава, пружа подршку, упозорава и саветује оператора ИКТ система од посебног значаја и врши друге послове из своје надлежности.

Канцеларија за информациону безбедност, након извршене анализе, утврђује ниво опасности инцидента.

Када је неопходно да јавност буде упозната са инцидентом или када је инцидент такав да је од интереса за јавност, Канцеларија за информациону безбедност објављује информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио.

Изузетно од става 3. овог члана, Канцеларија за информациону безбедност може објавити информацију о инциденту који се догодио у оператору приоритетног ИКТ система од посебног значаја који обавља делатност у области банкарства и финансијских тржишта из члана 5. став 3. тачка 1) подтачка (3) овог закона, уз претходно прибављену сагласност Народне банке Србије односно Комисије за хартије од вредности.

Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске комуникације и поштанске услуге дужни су да обавештења о инцидентима проследе:

1) надлежном јавном тужилаштву, односно министарству надлежном за унутрашње послове, у случају да је инцидент везан за извршење кривичних дела која се гоне по службеној дужности,

2) органу надлежном за безбедносне и контраобавештајне послове од значаја за одбрану Републике Србије или органу надлежном за послове националне безбедности, у случају да је инцидент повезан са значајним нарушавањем информационе безбедности које има или може имати за последицу угрожавање одбране или националне безбедности Републике Србије.

Приликом управљања инцидентом Канцеларија за информациону безбедност, Народна банка Србије, Комисија за хартије од вредности и Регулаторно тело за електронске комуникације и поштанске услуге означавају обавештење о инциденту, односно информације о инциденту у складу са прописима и TLP (енг. „traffic light protocol“) протоколом.

#### **Поступање у случају инцидента нивоа опасности „низак”**

##### **Члан 20.**

У случају инцидента којима је у складу са класификацијом утврђен ниво опасности „низак” Канцеларија за информациону безбедност по потреби даје препоруке за поступање оператору ИКТ система од посебног значаја.

#### **Поступање у случају инцидента нивоа опасности „средњи”**

##### **Члан 21.**

У случају инцидента којима је у складу са класификацијом утврђен ниво опасности „средњи” Канцеларија за информациону безбедност даје препоруке за поступање оператору ИКТ система од посебног значаја.

#### **Поступање у случају инцидента нивоа опасности „висок”**

##### **Члан 22.**

У случају инцидента којима је у складу са класификацијом утврђен ниво опасности „висок” Канцеларија за информациону безбедност је дужна да о томе обавести Министарство.

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, припрема препоруке и мере за решавање инцидента.

Министарство након пријема обавештења из става 1. овог члана сазива седницу Тела за координацију послова информационе безбедности.

Након завршетка инцидента Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, сачињава завршни извештај који доставља Министарству у року од 30 дана након завршеног инцидента.

#### **Поступање у случају инцидента нивоа опасности „веома висок”**

##### **Члан 23.**

У случају инцидента којем је у складу са класификацијом утврђен ниво опасности „веома висок” и који представља кризу информационе безбедности, руковођење и координацију спровођења мера и задатака предузима Влада.

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, израђује предлог за проглашавање кризе информационе безбедности, у складу са Планом за реаговање у случају инцидента високог нивоа и кризе информационе безбедности, који садржи:

- 1) податке о инциденту;
- 2) информације о предузетим мерама;
- 3) разлоге за проглашење кризе информационе безбедности;
- 4) задужење органа за поступање у складу са својим надлежностима;
- 5) мере за решавање кризе.

Предлог за проглашење кризе информационе безбедности упућује се Министарству, које по пријему предлога без одлагања сазива седницу Тела за координацију послова информационе безбедности.

Влада на предлог Министарства доноси одлуку о проглашењу кризе информационе безбедности и задужује органе да поступају према предложеним мерама у складу са својим надлежностима.

Канцеларија за информациону безбедност, у сарадњи са оперативним тимом, координира решавањем кризе информационе безбедности и најмање једном недељно извештава Министарство и Владу о свим активностима.

Предлог за проглашење завршетка кризе информационе безбедности упућује се Министарству.

Одлуку о проглашењу завршетка кризе информационе безбедности доноси Влада на предлог Министарства.

Након завршетка кризе информационе безбедности Канцеларија за информациону безбедност сачињава завршни извештај који доставља Министарству и Влади у року од 30 дана након завршетка кризе.

### **Извештавање током и након инцидента**

#### **Члан 24.**

Оператори ИКТ система од посебног значаја дужни су да:

1) достављају извештај о инциденту, током трајања инцидента, са описом мера које су предузете за решавање инцидента, у јединствени систем за пријем обавештења о инцидентима и то:

- (1) на свака три дана у случају инцидента средњег нивоа;
- (2) на свака 24 сата у случају инцидента високог и веома високог нивоа;

2) достављају обавештења и додатне извештаје о битним догађајима у вези са инцидентом и активностима које предузимају, на захтев Канцеларије;

3) достављају завршни извештај о инциденту у року од 15 дана од дана престанка инцидента, који садржи следеће податке:

- (1) врсту и детаљан опис инцидента;
- (2) врсту претње и узрок који је довео до инцидента;
- (3) време и трајање инцидента;
- (4) обим и степен утицаја инцидента (остварени ризик), односно последице које је инцидент изазвао;
- (5) информацију о евентуалном прекограничном дејству инцидента;
- (6) предузете активности ради отклањања последица инцидента и, по потреби, друге информације од значаја за евидентирање инцидента и статистичку обраду.

Након завршеног инцидента Канцеларија за информациону безбедност припрема препоруке и савете за заштиту од потенцијалних ризика, на основу спроведене анализе извршеног инцидента.

### **Достављање статистичких података о инцидентима**

#### **Члан 25.**

Оператор ИКТ система од посебног значаја дужан је да, поред обавештавања о инцидентима из члана 13. овог закона, достави органу, односно организацији надлежној за послове Националног ЦЕРТ-а статистичке податке о свим инцидентима у ИКТ систему, укључујући и избегнуте инциденте, у претходној години најкасније до 28. фебруара текуће године.

Орган, односно организација из става 1. овог члана извештаје о статистичким подацима доставља Министарству и објављује на својој веб презентацији.

Врсту, форму и начин достављања статистичких података из става 1. овог члана утврђује орган, односно организација из става 1. овог члана.

### **III. ОРГАНИ НАДЛЕЖНИ ЗА ПРЕВЕНЦИЈУ И ЗАШТИТУ ОД БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ**

#### **Надлежни орган**

#### **Члан 26.**

Орган државне управе надлежан за информациону безбедност је министарство надлежно за послове информационе безбедности.

У оквиру својих надлежности Министарство:

- 1) припрема и предлаже прописе и планска документа из области информационе безбедности у складу са овим законом;
- 2) води евиденцију оператора ИКТ система од посебног значаја;
- 3) врши надзор над радом Канцеларије за информациону безбедност у вршењу послова за које је надлежна у складу са овим законом;
- 4) врши инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима;
- 5) остварује међународну сарадњу у оквиру својих надлежности.

#### **Тело за координацију послова информационе безбедности**

#### **Члан 27.**

У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности, Влада оснива Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, послове правосуђа, представници служби безбедности, Канцеларије за информациону безбедност, Канцеларије за информационе технологије и електронску управу, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Народне банке Србије и Регулаторног тела за електронске комуникације и поштанске услуге.

У функцији унапређења појединих области информационе безбедности формирају се стручне радне групе Тела за координацију у које се укључују и представници других органа, привреде, академске заједнице и невладиног сектора.

Одлуком којом оснива Тело за координацију Влада одређује и његов састав, задатке, рок у коме оно подноси извештаје Влади и друга питања која су везана за његов рад.

### **Канцеларија за информациону безбедност**

#### **Члан 28.**

Ради обављања послова превенције и заштите од безбедносних ризика и инцидената у ИКТ системима у Републици Србији оснива се Канцеларија за информациону безбедност (у даљем тексту: Канцеларија), као посебна организација у смислу закона којим се уређује положај државне управе.

Канцеларија има својство правног лица.

Радом Канцеларије руководи директор који мора да буде лице одговарајуће стручности са најмање пет година радног искуства у области информационе безбедности и кога именује Влада, у складу са законом којим се уређује положај државних службеника.

Канцеларија има заменика директора, који мора бити лице одговарајуће стручности са најмање пет година радног искуства у области информационе безбедности, који се поставља у складу са прописима којим се уређује положај државних службеника и има овлашћења у складу са прописима о државној управи.

### **Надзор над радом Канцеларије**

#### **Члан 29.**

Надзор над радом Канцеларије у вршењу послова спроводи Министарство, у складу са законом којим се уређује државна управа.

### **Надлежности Канцеларије**

#### **Члан 30.**

Канцеларија у оквиру своје надлежности обавља следеће послове, и то:

- 1) врши превенцију и заштиту од безбедносних ризика на националном нивоу у складу са овим законом (послови Националног ЦЕРТ-а);
- 2) предузима превентивне и реактивне мере у циљу заштите Јединствене информационо-комуникационе мреже електронске управе у складу са овим законом (послови ЦЕРТ-а органа власти);
- 3) обавља сарадњу на националном нивоу у области информационе безбедности;
- 4) врши послове јединствене тачке контакта;
- 5) врши послове сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга, изузев система, производа, процеса и услуга за потребе одбране и безбедности и ИКТ система за рад са тајним подацима;
- 6) прописује минималне мере заштите ИКТ система органа, уважавајући начела из члана 3. овог закона, мере заштите из члана 10. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада;



7) у сарадњи са надлежним органима и другим субјектима из јавног, академског, привредног и невладиног сектора учествује у развоју и спровођењу програма обука и стручног усавршавања лица која раде на пословима информационе безбедности;

8) обавља сарадњу и размену информација на међународном нивоу у области информационе безбедности у циљу праћења и усаглашавања са међународним прописима и стандардима;

9) врши стручни надзор над радом оператора ИКТ система од посебног значаја;

10) води базу рањивости ИКТ производа и ИКТ услуга;

11) извештава Министарство на кварталном нивоу о предузетим активностима;

12) обавља друге послове у складу са овим законом.

Подзаконски акт којим се ближе уређује начин вршења сертификације ИКТ система, ИКТ производа, ИКТ процеса и ИКТ услуга из става 1. тачка 5) овог члана доноси Влада, на предлог Министарства.

### **Послови превенције и заштите од безбедносних ризика на националном нивоу (Национални ЦЕРТ)**

#### **Члан 31.**

У оквиру послова превенције и заштите од безбедносних ризика и инцидентата Канцеларија врши послове Националног ЦЕРТ-а, и то:

1) прикупља и размењује информације о претњама, рањивостима, избегнутим инцидентима и инцидентима и пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност;

2) прати стање о инцидентима у Републици Србији;

3) пружа рана упозорења, узбуне и најаве и информише релевантна лица о претњама, рањивостима и инцидентима;

4) реагује без одлагања по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања;

5) на захтев оператора ИКТ система од посебног значаја, пружа помоћ у праћењу стања безбедности ИКТ система у реалном времену или приближно реалном времену;

6) на захтев оператора ИКТ система од посебног значаја, врши проактивно скенирање ИКТ система у циљу утврђивања рањивости које могу да потенцијално знатно наруше безбедност ИКТ система, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;

7) поступа као координатор за потребе координираног откривања рањивости, у складу са овим законом;

8) учествује у развоју и коришћењу технолошких алата за размену информација са операторима ИКТ система од посебног значаја и других субјеката са којима сарађује;

9) континуирано израђује анализе ризика и инцидентата, на основу прикупљених информација;

10) подиже свест код грађана, привредних субјеката и органа о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести;

11) води Евиденцију посебних ЦЕРТ-ова;

12) припрема извештаје на кварталном нивоу о предузетим активностима;

13) пружа подршку у прикупљању и анализирању форензичких података и пружа динамичке анализе ризика и инцидената у складу са прописима;

14) сарађује са ЦЕРТ-овима страних држава и на њихов захтев пружа узајамну помоћ у складу са својим капацитетима и надлежностима.

Канцеларија подстиче примену и коришћење прописаних и стандардизованих процедура за:

1) управљање инцидентима;

2) класификацију информација о инцидентима, односно класификацију према нивоу опасности инцидената;

3) управљање кризним ситуацијама;

4) координирано откривање рањивости.

Канцеларија је овлашћена да врши обраду података о лицу које пријави инцидент, при чему обрада података о лицу обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Канцеларија обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације.

У оквиру обављања послова Националног ЦЕРТ-а потребно је обезбедити следеће захтеве:

1) висок ниво доступности комуникационих канала избегавањем јединствених тачака прекида и коришћење више средстава за двосмерно контактирање;

2) просторије Националног ЦЕРТ-а и информациони системи за подршку треба да буду смештени на сигурним локацијама;

3) употребу одговарајућег система за управљање захтевима и њихово усмеравање, посебно како би се олакшала ефикасна и ефективна размена информација;

4) обезбеђивање поверљивости и поузданости својих активности;

5) постојање адекватних кадровских капацитета;

6) опремљеност редундантним системима и резервним радним простором како би се осигурао континуитет услуга.

Подзаконски акт којим се ближе уређује поступак проактивног скенирања ИКТ система из става 1. тачка 6) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјекат који непосредно врши скенирање, као и процедура којом се утврђују услови у циљу заштите безбедности система, мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

**Превентивне и реактивне мере у циљу заштите Јединствене  
информационо-комуникационе мреже електронске управе  
(ЦЕРТ органа власти)**

**Члан 32.**

У оквиру предузимања превентивних и реактивних мера у циљу заштите Јединствене информационо-комуникационе мреже електронске управе (у даљем тексту: мрежа еУправе) Канцеларија обавља следеће послове:

- 1) врши заштиту мреже еУправе;
- 2) обавља координацију и сарадњу са операторима ИКТ система које повезује мрежа еУправе у превенцији инцидената;
- 3) активно учествује у откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;
- 4) врши проактивно скенирање мреже оператора ИКТ система од посебног значаја који су корисници мреже, при чему такво скенирање не сме имати штетан утицај на послове и делатности оператора;
- 5) у случају откривене рањивости:
  - (1) обавештава операторе ИКТ система који су корисници мреже еУправе о томе;
  - (2) налаже операторима ИКТ система од посебног значаја који су корисници мреже да предузму адекватне мере заштите у циљу спречавања, смањења и отклањања последица инцидента;
- 6) издаје стручне препоруке за заштиту ИКТ система органа, осим ИКТ система за рад са тајним подацима;
- 7) доноси акт којим се уређује поступање оператора ИКТ система од посебног значаја који користе мреже у случају инцидента;
- 8) у сарадњи са надлежним органима врши процену потребе за стручним усавршавањем запослених у операторима ИКТ система од посебног значаја који користе мрежу;
- 9) планира и организује процедуралне и практичне вежбе у области информационе безбедности за запослене у операторима ИКТ система од посебног значаја који користе мрежу;
- 10) израђује предлоге за унапређење безбедносних карактеристика мреже еУправе;
- 11) израђује анализе ризика и инцидената у оквиру мреже еУправе;
- 12) обавља друге послове у складу са законом у циљу унапређења информационе безбедности мреже еУправе.

Подзаконски акт којим се ближе уређује поступак проактивног скенирања ИКТ система из става 1. тачка 4) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјекат који непосредно врши скенирање, као и процедура којом се утврђују услови у циљу заштите безбедности система, мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

## **Сарадња на националном нивоу**

### **Члан 33.**

Канцеларија непосредно сарађује са Министарством, Регулаторним телом за електронске комуникације и поштанске услуге, Посебним ЦЕРТ-овима у Републици Србији, са јавним и привредним субјектима и ЦЕРТ-овима самосталних оператора ИКТ система.

ЦЕРТ-ови могу, у складу са својим надлежностима и безбедносним протоколима, самостално успостављати сарадњу са релевантним актерима из јавног и приватног сектора, уз обавезу обавештавања Канцеларије ради координације и размене информација од значаја за национални систем информационе безбедности.

Канцеларија и ЦЕРТ-ови самосталних оператора ИКТ система одржавају међусобне састанке у организацији Канцеларије најмање три пута годишње, као и по потреби у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Састанцима из става 3. овог члана присуствују и представници Министарства, а по позиву могу да присуствују и представници посебних ЦЕРТ-ова, као и друга лица.

Приликом сарадње са субјектима из става 1. овог члана Канцеларија је дужна да обезбеди ефективну, ефикасну и безбедну размену информација уз примену адекватних процедура, укључујући „traffic light protocol” (TLP), и поштујући прописе о заштити података о личности.

### **Међународна сарадња и послови јединствене тачке контакта**

### **Члан 34.**

Канцеларија остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

- 1) брзо расту или имају тенденцију да постану високоризични;
- 2) превазилазе или могу да превазиђу националне капацитете;
- 3) могу да имају негативан утицај на више од једне државе.

Приликом размене података из става 1. овог члана, Канцеларија је дужна да поступа тако да се не угрози поверљивост података, као и да таква размена података не утиче на потенцијално нарушавање безбедности ИКТ система.

Размена података из става 1. овог члана подразумева пренос или обраду података који су неопходни за процену и реаговање на безбедносне ризике и инциденте у складу са овим законом. У случају да се размена односи на податке о личности, Канцеларија је дужна да обезбеди да такав пренос или обрада буду усклађени са прописима којима се уређује заштита података о личности, укључујући и правила која се односе на пренос података у друге државе или међународне организације.

Уколико је инцидент у вези са извршењем кривичног дела које се гони по службеној дужности, Канцеларија ће о томе обавестити надлежно јавно тужилаштво, које ће самостално или преко министарства надлежног за унутрашње послове у званичној процедури проследити пријаву у складу са потврђеним међународним уговорима.

Канцеларија обавља послове јединствене тачке контакта за информациону безбедност у случају прекограничних безбедносних претњи и инцидената и сарађује са јединственим тачкама контакта других држава.

### **Посебни центри за превенцију безбедносних ризика у ИКТ системима**

#### **Члан 35.**

Посебан центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Посебан ЦЕРТ) обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

Посебан ЦЕРТ је правно лице или организациона јединица у оквиру правног лица са седиштем на територији Републике Србије, које је уписано у евиденцију посебних ЦЕРТ-ова коју води орган, односно организација надлежна за послове Националног ЦЕРТ-а и објављује је јавно.

Упис у евиденцију посебних ЦЕРТ-ова, коју води Канцеларија, врши се на основу пријаве правног лица у оквиру кога се налази посебан ЦЕРТ.

Евиденција посебних ЦЕРТ-ова од података о личности садржи податке о одговорним лицима, и то: име, презиме, функцију и контакт податке као што су адреса, број телефона и адреса електронске поште, а у сврху ангажовања посебних ЦЕРТ-ова у случају безбедносних ризика и инцидената у ИКТ системима.

Орган, односно организација из става 2. овог члана прописује садржај, начин уписа и вођења евиденције из става 3. овог члана.

### **База рањивости**

#### **Члан 36.**

Орган, односно организација надлежна за послове Националног ЦЕРТ-а успоставља и одржава базу рањивости ИКТ производа и ИКТ услуга у Републици Србији и омогућава физичким и правним лицима, као и произвођачима, добављачима и пружаоцима услуге у ИКТ систему, да на добровољној бази пријаве рањивости у ИКТ производима или ИКТ услугама, а које се могу пријавити анонимно.

База рањивости ИКТ производа и ИКТ услуга садржи:

- 1) податке о рањивости;
- 2) податке о рањивостима ИКТ производа или ИКТ услуга.

Влада, на предлог Министарства, прописује садржај, процедуре верификације рањивости, процедуре за управљање техничким рањивостима ИКТ производа и ИКТ услуга, начин уписа и вођења регистра.

### **База података о регистрацији домена**

#### **Члан 37.**

Организација која је овлашћена за управљање регистром домена највишег нивоа води списак овлашћених регистара за регистрацију домена у Републици Србији.

Списак из става 1. овог члана обавезно садржи следеће податке:

- 1) назив овлашћеног регистра;
- 2) седиште и ажурне контакт податке овлашћеног регистра (адресу електронске поште, службени телефон);

3) адресни опсег интернет протокола (енгл. „IP address range“) који припада овлашћеном регистру, а који обухвата податке о јавним статичким ИП адресама.

Овлашћени регистар дужан је да у случају промене података из става 2. овог члана о томе обавести организацију која је овлашћена за управљање регистром домена највишег нивоа у року од 15 дана од дана настанка промене.

Организације које су овлашћене за управљање регистром домена највишег нивоа и пружање услуга ДНС-а обавезне су да прикупљају, чувају и одржавају тачне и потпуне податке о регистрацији домена у посебној бази података, уз дужну пажњу и уз примену техничких, организационих и безбедносних мера за заштиту података, у складу са прописима о заштити података о личности.

База података из става 4. овог члана мора да садржи најмање следеће податке:

- 1) назив домена;
- 2) датум регистрације домена;
- 3) податке о регистранту, и то: име и презиме физичког лица, односно назив правног лица, контакт адресу електронске поште и број телефона;
- 4) контакт адресу електронске поште и број телефона лица задуженог за администрацију домена, уколико се разликују од података регистранта.

Организације из става 4. овог члана дужне су да усвоје и примене акте и процедуре за верификацију тачности и потпуности података у бази података. Ове процедуре морају бити јавно доступне.

Организације из става 4. овог члана дужне су да обезбеде јавну доступност података који не представљају податке о личности одмах по регистрацији домена, а у складу са правилима и условима регистрације назива националних интернет домена.

Организације из става 4. овог члана обавезне су да омогуће приступ подацима о регистрацији домена који нису јавно доступни на основу законитих и образложених захтева овлашћених лица или органа, у складу са овлашћењима додељеним прописима који уређују делокруг њиховог рада и у складу са прописима који уређују заштиту података о личности.

Одговор на захтев из става 7. овог члана мора бити достављен без одлагања, а најкасније у року од 72 сата од пријема захтева.

Организације из става 4. овог члана дужне су да донесу и јавно објаве политике и процедуре за поступање по захтевима за откривање података о регистрацији домена, у складу са овим законом и прописима о заштити података о личности. У складу са овим чланом, прикупљање података о регистрацији домена не сме довести до дуплирања података. Организације из става 4. овог члана дужне су да сарађују ради избегавања дуплирања и осигурања усклађености са законом.

Министар надлежан за информациону безбедност прописује ближе услове за прикупљање, чување, верификацију и објављивање података из овог члана, а у складу са најбољом праксом регистара националних интернет домена из Европске Уније, као и Интернет корпорације за додељене називе и бројеве (ICANN).

### **Заштита деце при коришћењу информационо-комуникационих технологија**

#### **Члан 38.**

Министарство предузима превентивне мере за безбедност и заштиту деце на интернету, као активности од јавног интереса, путем едукације и информисања деце, родитеља и наставника о предностима, ризицима и начинима безбедног коришћења интернета, као и путем јединственог места за

пружање савета и пријем пријава у вези безбедности деце на интернету и упућује пријаве надлежним органима ради даљег поступања.

Оператор електронских комуникација који пружа јавно доступне телефонске услуге дужан је да омогући свим претплатницима услугу бесплатног позива према јединственом месту за пружање савета и пријем пријава у вези безбедности деце на интернету.

У случају да наводи из пријаве упућују на постојање кривичног дела, на повреду права, здравственог статуса, добробити и/или општег интегритета детета, на ризик стварања зависности од коришћења интернета, пријава се прослеђује надлежном органу ради поступања у складу са утврђеним надлежностима.

Министарство је овлашћено да врши обраду података о лицу које се обрати Министарству у складу са законом који уређује заштиту података о личности и другим прописима.

Обрада података о лицу из става 4. овог члана обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Подаци о личности из става 5. овог члана чувају се у роковима предвиђеним прописима који уређују канцеларијско пословање.

Подзаконски акт којим се ближе уређује начин спровођења мера за безбедност и заштиту деце на интернету из ст. 1. и 3. овог члана доноси Влада на предлог Министарства.

#### **IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА**

##### **Надлежност**

##### **Члан 39.**

Министарство надлежно за послове одбране је надлежно за послове информационе безбедности који се односе на одобравање криптографских производа који се користе за заштиту преноса и чувања података који су одређени као тајни, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења и послове и задатке у складу са законом и прописима донетим на основу закона.

##### **Послови и задаци**

##### **Члан 40.**

У складу са овим законом, министарство надлежно за послове одбране:

- 1) организује и реализује научноистраживачки рад у области криптографске безбедности и заштите од КЕМЗ;
- 2) развија, имплементира, верификује и класификује криптографске алгоритме;
- 3) истражује, развија, верификује и класификује сопствене криптографске производе и решења заштите од КЕМЗ;
- 4) верификује и класификује домаће и стране криптографске производе и решења заштите од КЕМЗ;

5) дефинише процедуре и критеријуме за евалуацију криптографских безбедносних решења;

6) врши функцију националног органа за одобрења криптографских производа и обезбеђује да ти производи буду одобрени у складу са одговарајућим прописима;

7) врши функцију националног органа за заштиту од КЕМЗ;

8) врши проверу ИКТ система са аспекта криптобезбедности и заштите од КЕМЗ;

9) врши функцију националног органа за дистрибуцију криптоматеријала и дефинише управљање, руковање, чување, дистрибуцију и евиденцију криптоматеријала у складу са прописима;

10) планира и координира израду криптопараметара (параметара криптографског алгоритма), дистрибуцију криптоматеријала и заштите од компромитујућег електромагнетног зрачења у сарадњи са самосталним операторима ИКТ система;

11) формира и води централни регистар верификованог и дистрибуираног криптоматеријала;

12) формира и води регистар издатих одобрења за криптографске производе;

13) израђује електронске сертификате за криптографске системе засноване на инфраструктури јавних кључева (Public Key Infrastructure – PKI);

14) предлаже доношење прописа из области криптобезбедности и заштите од КЕМЗ на основу овог закона;

15) врши послове стручног надзора у вези криптобезбедности и заштите од КЕМЗ;

16) пружа стручну помоћ носиоцу инспекцијског надзора информационе безбедности у области криптобезбедности и заштите од КЕМЗ;

17) пружа услуге уз накнаду правним и физичким лицима, изван система јавне власти, у области криптобезбедности и заштите од КЕМЗ према пропису Владе на предлог министра одбране;

18) сарађује са домаћим и међународним органима и организацијама у оквиру надлежности уређених овим законом.

Средства остварена од накнаде за пружање услуга из става 1. тачка 17) овог члана су приход буџета Републике Србије.

### **Компромићујуће електромагнетно зрачење**

#### **Члан 41.**

Мере заштите од КЕМЗ у ИКТ системима за руковање са тајним подацима примењују се у складу са прописима којима се уређује заштита тајних података.

Мере заштите од КЕМЗ могу примењивати на сопствену иницијативу и оператори ИКТ система којима то није законска обавеза.

За све техничке компоненте система (уређаје, комуникационе канале и просторе) код којих постоји ризик од КЕМЗ, а што би могло довести до нарушавања информационе безбедности из става 1. овог члана, врши се провера заштићености од КЕМЗ и процена ризика од неовлашћеног приступа тајним подацима путем КЕМЗ.



Проверу заштићености од КЕМЗ врши министарство надлежно за послове одбране.

Самостални оператори ИКТ система могу вршити проверу КЕМЗ за сопствене потребе.

Подзаконски акт којим се ближе уређују услови за проверу КЕМЗ и начин процене ризика од отицања података путем КЕМЗ доноси Влада, на предлог министарства надлежног за послове одбране.

### **Мере криптозаштите**

#### **Члан 42.**

Мере криптозаштите за руковање са тајним подацима у ИКТ системима примењују се у складу са прописима којима се уређује заштита тајних података.

Мере криптозаштите се могу применити и приликом преноса и чувања података који нису означени као тајни у складу са законом који уређује тајност података, када је на основу закона или другог правног акта потребно применити техничке мере ограничења приступа подацима и ради заштите интегритета, аутентичности и непорецивости података.

Подзаконски акт којим се уређују технички услови за криптографске алгоритме, параметре, протоколе и информациона добра у области криптозаштите који се у Републици Србији користе у криптографским производима ради заштите тајности, интегритета, аутентичности, односно непорецивости података доноси Влада, на предлог министарства надлежног за послове одбране.

### **Одобрење за криптографски производ**

#### **Члан 43.**

Криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни, у складу са законом, морају бити верификовани и одобрени за коришћење.

Подзаконски акт којим се ближе уређују услови које морају да испуњавају криптографски производи из става 1. овог члана доноси Влада, на предлог министарства надлежног за послове одбране.

### **Издавање одобрења за криптографски производ**

#### **Члан 44.**

Одобрење за криптографски производ издаје министарство надлежно за послове одбране, на захтев оператора ИКТ система, произвођача криптографског производа или другог заинтересованог лица.

Одобрење за криптографски производ се може односити на појединачни примерак криптографског производа или на одређени модел криптографског производа који се серијски производи.

Одобрење за криптографски производ може имати рок важења.

Министарство надлежно за послове одбране решава по захтеву за издавање одобрења за криптографски производ у року од 45 дана од дана подношења уредног захтева, који се може продужити у случају посебне сложености провере највише за још 60 дана.

Против решења из става 4. овог члана жалба није допуштена, али може да се покрене управни спор.

Министарство надлежно за послове одбране води регистар издатих одобрења за криптографски производ.

Регистар из става 6. овог члана од података о личности садржи податке о одговорним лицима, и то: име, презиме, функција и контакт податке као што су адреса, број телефона и адреса електронске поште. Министарство надлежно за послове одбране објављује јавну листу одобрених модела криптографских производа за све моделе криптографских производа за које је у захтеву за издавање одобрења наглашено да модел криптографског производа треба да буде на јавној листи и ако је захтев поднео произвођач или лице овлашћено од стране произвођача предметног криптографског производа.

Министарство надлежно за послове одбране претходно издато одобрење за криптографски производ може повући или променити услове из ст. 2. и 3. овог члана из разлога нових сазнања везаних за техничка решења примењена у производу, а која утичу на оцену степена заштите који пружа производ.

Подзаконски акт којим се ближе уређује садржај захтева за издавање одобрења за криптографски производ, услове за издавање одобрења за криптографски производ, начин издавања одобрења и вођења регистра издатих одобрења за криптографски производ доноси Влада, на предлог министарства надлежног за послове одбране.

### **Опште одобрење за коришћење криптографских производа**

#### **Члан 45.**

Самостални оператори ИКТ система имају опште одобрење за коришћење криптографских производа.

Оператор ИКТ система из става 1. овог члана самостално оцењује степен заштите који пружа сваки појединачни криптографски производ који користи, а у складу са прописаним условима.

### **Регистри у криптозаштити**

#### **Члан 46.**

Самостални оператори ИКТ система који имају опште одобрење за коришћење криптографских производа устројавају и воде регистре криптографских производа, криптоматеријала, правила и прописа и лица која обављају послове криптозаштите.

Регистар лица која обављају послове криптозаштите од података о личности садржи следеће податке о лицима која обављају послове криптозаштите: презиме, име оца и име, датум и место рођења, матични број, телефон, адресу електронске поште, школску спрему, податке о завршеном стручном оспособљавању за послове криптозаштите, назив радног места, датум почетка и завршетка рада на пословима криптозаштите.

Регистар криптоматеријала за руковање са страним тајним подацима води Канцеларија Савета за националну безбедност и заштиту тајних података, у складу са ратификованим међународним споразумима.

Подзаконски акт којим се ближе уређује вођење регистара из става 1. овог члана доноси Влада, на предлог министарства надлежног за послове одбране.

## **V. НАДЛЕЖНОСТИ И ОДГОВОРНОСТИ СУБЈЕКТА ЗА НАДЗОР НАД СПРОВОЂЕЊЕМ ОВОГ ЗАКОНА**

### **Инспекција за информациону безбедност**

#### **Члан 47.**

Инспекција за информациону безбедност врши инспекцијски надзор над применом овог закона и радом оператора ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима, а у складу са законом којим се уређује инспекцијски надзор.

Послове инспекције за информациону безбедност обавља Министарство преко инспектора за информациону безбедност.

У оквиру инспекцијског надзора рада оператора ИКТ система, инспектор за информациону безбедност утврђује да ли су испуњени услови прописани овим законом и прописима донетим на основу овог закона.

### **Овлашћења инспектора за информациону безбедност**

#### **Члан 48.**

Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом:

- 1) наложи отклањање утврђених неправилности и за то утврди разуман рок;
- 2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок;
- 3) захтева од оператора ИКТ система од посебног значаја да изврши скенирање, конфигурацију и пенетрационо тестирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости, а у складу са проценом ризика;
- 4) наложи да надзирани субјект учини доступним јавности информације које се тичу непоштовања одредби овог закона, а за које постоји оправдан интерес јавности на утврђени начин;
- 5) наложи да надзирани субјект одреди лице са тачно утврђеним овлашћењима које ће у утврђеном временском периоду надзирати и пратити усаглашеност са одредбама овог закона и наложеним мерама;
- 6) предложи надлежном органу, телу за оцењивање усаглашености или другом надлежном телу да привремено суспендује или повуче издат сертификат, дозволу или други акт којим се потврђује испуњеност услова, уколико надзирани субјект не отклони неправилности у остављеном року;
- 7) покрене поступак пред надлежним судом или другим надлежним органом ради утврђивања привремене мере забране обављања управљачких функција лицу које у име надзираног субјекта врши руководеће послове, ако је његовим поступањем онемогућено усаглашавање са овим законом и наложеним мерама.

Подзаконски акт којим се ближе уређује поступак скенирања, конфигурација и пенетрационо тестирање ИКТ система у циљу утврђивања евентуалних безбедносних рањивости из става 1. тачка 3) овог члана, заштитни, технички и безбедносни услови и мере које мора да испуни субјект који непосредно врши активности из става 1. тачка 3) овог члана, као и процедура којом се утврђују услови у циљу заштите безбедности система,

мрежа и података којима се приступа и начин извештавања надлежног органа, доноси Влада на предлог Министарства.

### **Стручни надзор**

#### **Члан 49.**

Стручни надзор над применом овог закона и радом оператора ИКТ система од посебног значаја, осим самосталних оператора ИКТ система и ИКТ система за рад са тајним подацима, врши Канцеларија, а у складу са законом којим се уређује инспекцијски надзор.

Послове стручног надзора обавља овлашћено лице запослено у Канцеларији (у даљем тексту: овлашћено лице).

У поступку стручног надзора овлашћено лице има право и обавезу да контролише:

- 1) адекватност процењених ризика с обзиром на степен изложености ризику, величину оператора и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај;
- 2) ниво безбедности технолошких поступака и техничких средстава које оператор ИКТ система од посебног значаја употребљава ради примена мера заштите;
- 3) одговарајуће спровођење процеса провере усклађености примењених мера ИКТ система са актом о безбедности;
- 4) примену препорука и мера у случају инцидента који значајно угрожавају информациону безбедност.

Ако у вршењу стручног надзора Канцеларија утврди неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, о томе обавештава надзираног субјекта и одређује му рок у коме је дужан да их отклони.

Рок из става 4. овог члана не може бити краћи од осам дана од дана пријема обавештења, осим у случајевима који захтевају хитно поступање.

Ако Канцеларија утврди да надзирани субјект није, у остављеном року, отклонио утврђене неправилности, недостатке или пропусте у примени овог закона и прописа донетих на основу њега, подноси пријаву инспекцији.

Канцеларија је дужна да по захтеву инспектора за информациону безбедност обави стручни надзор и достави информацију о утврђеном чињеничном стању.

Образац легитимације и начин издавања легитимације овлашћеног лица утврђује Канцеларија.

Легитимација овлашћеног лица обавезно садржи: грб Републике Србије и назив Канцеларије, име и презиме овлашћеног лица, фотографију овлашћеног лица, службени број легитимације, датум издавања легитимације, печат Канцеларије, потпис директора Канцеларије, као и одштампани текст следеће садржине: „Ималац ове легитимације има овлашћења у складу са одредбама члана 49. ст. 3. и 4. Закона о информационој безбедности.”

## **VI. КАЗНЕНЕ ОДРЕДБЕ**

#### **Члан 50.**

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система ако:

- 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. овог закона;
- 2) не донесе Акт о процени ризика из члана 11. став 1. овог закона;
- 3) не донесе Акт о безбедности ИКТ система из члана 12. став 1. овог закона;
- 4) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 12. став 2. овог закона;
- 5) не изврши проверу усклађености примењених мера из члана 12. став 5. овог закона;
- 6) не достави статистичке податке из члана 25. став 1. овог закона;
- 7) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 48. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 500.000,00 динара.

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

#### **Члан 51.**

Новчаном казном у износу од 50.000,00 до 1.000.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система ако:

- 1) не поступи у складу са одредбама о упису у евиденцију из члана 9. овог закона;
- 2) не донесе Акт о процени ризика из члана 11. став 1. овог закона;
- 3) не донесе Акт о безбедности ИКТ система из члана 12. став 1. овог закона;
- 4) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 12. став 2. овог закона;
- 5) не изврши проверу усклађености примењених мера из члана 12. став 5. овог закона;
- 6) не достави статистичке податке из члана 25. став 1. овог закона;
- 7) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 48. став 1. тачка 1) овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор важног ИКТ система новчаном казном у износу од 10.000,00 до 250.000,00 динара.

За прекршај из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор важног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

#### **Члан 52.**

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор приоритетног ИКТ система ако:

- 1) о инцидентима у ИКТ систему из члана 13. став 2. овог закона не обавести органе из члана 14. ст. 1. до 3. овог закона;

2) не обавести кориснике којима пружају услуге у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга у складу са чланом 14. став 5. овог закона;

3) не доставља обавештења и извештаје током и након завршетка инцидента из члана 24. овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 500.000,00 динара.

За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу који је оператор приоритетног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Изузетно од ст. 1–3. овог члана, ако оператор приоритетних ИКТ система од посебног значаја из члана 14. став 2. овог закона не обавести Народну банку Србије о инцидентима у ИКТ систему од посебног значаја или не обавести кориснике о инцидентима у складу са чланом 14. став 6. овог закона, Народна банка Србије изриче том субјекту мере и казне у складу са законом којим се уређује његово пословање.

### **Члан 53.**

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај правно лице које је оператор важног ИКТ система ако:

1) о инцидентима у ИКТ систему из члана 13. став 2. овог закона не обавести органе из члана 14. ст. 1. до 3. овог закона;

2) не обавести кориснике којима пружају услуге у случају инцидента који може да изазове или изазива штетан утицај на пружање и коришћење услуга у складу са чланом 14. став 5. овог закона;

3) не доставља обавештења и извештаје током и након завршетка инцидента из члана 24 овог закона.

За прекршај из става 1. овог члана казниће се физичко лице у својству регистрованог субјекта које је оператор приоритетног ИКТ система новчаном казном у износу од 10.000,00 до 250.000,00 динара.

За прекршаје из става 1. овог члана казниће се и одговорно лице у правном лицу или органу које је оператор важног ИКТ система новчаном казном у износу од 5.000,00 до 50.000,00 динара.

## **VII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ**

### **Рокови за доношење подзаконских аката**

#### **Члан 54.**

Подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона.

План за реаговање у случају инцидента високог нивоа и кризе информационе безбедности из члана 18. овог закона доноси се у року од 18 месеци од дана ступања на снагу овог закона.

#### **Члан 55.**

Оператори ИКТ система од посебног значаја који су одређени Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) настављају да поступају у складу са обавезама утврђеним чл. 6а-11б тог закона до 31. децембра 2025. године.

На операторе ИКТ система од посебног значаја који су одређени Законом о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) до датума из става 1. овог члана примењују се казнене одредбе из чл. 30. и 31. тог закона.

Оператори ИКТ система од посебног значаја дужни су да донесу акт из члана 11. став 1. овог закона у року од 18 месеци од дана ступања на снагу овог закона.

Орган, односно организација у којој се обављају послови Националног ЦЕРТ-а дужна је да, у року од девет месеци од дана ступања на снагу овог закона, донесе општу методологију за процену ризика у ИКТ системима од посебног значаја из члана 11. став 4. овог закона.

Оператор ИКТ система од посебног значаја дужан је да донесе акт из члана 12. овог закона у року од 18 месеци од дана ступања на снагу овог закона.

#### **Члан 56.**

Канцеларија за информациону безбедност се успоставља и почиње да обавља послове из своје надлежности прописане овим законом од 1. јануара 2027. године.

Послове Канцеларије за информациону безбедност прописане овим законом, изузев послова Националног ЦЕРТ-а, обављаће Канцеларија за информационе технологије и електронску управу у периоду који почиње даном наступања 6 месеци од дана ступања на снагу овог закона и који траје до 1. јануара 2027. године.

Регулаторно тело за електронске комуникације и поштанске услуге обавља послове Националног ЦЕРТ-а утврђене овим законом до успостављања Канцеларије за информациону безбедност односно до 1. јануара 2027. године.

Канцеларија за информациону безбедност преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Регулаторног тела за електронске комуникације и поштанске услуге насталу у обављању послова Националног ЦЕРТ-а потребне за вршење стручних послова утврђених овим законом.

Канцеларија за информациону безбедност почев од датума из става 1. овог члана преузима права, обавезе, запослене, предмете, опрему, средства за рад и архиву од Канцеларије за информационе технологије и електронску управу насталу у обављању послова прописаних овим законом из надлежности Канцеларије за информациону безбедност.

### **Престанак важења Закона о информационој безбедности**

#### **Члан 57.**

Даном ступања на снагу овог закона престаје да важи Закон о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19), изузев одредби чл. 6а-11б и чл. 30. и 31. које важе до 31. децембра 2025. године.

Подзаконски акти донети на основу Закона о информационој безбедности („Службени гласник РС”, бр. 6/16, 94/17 и 77/19) примењиваће се до ступања на снагу подзаконских аката који се доносе у складу са овим законом.

**Ступање на снагу****Члан 58.**

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”, изузев члана 29. овог закона који почиње да се примењује од 1. јануара 2027. године.