ЗАКОН

о информационој безбедности

"Службени гласник РС", бр. 6 од 28. јануара 2016, 94 од 19. октобра 2017, 77 од 31. октобра 2019.

I. ОСНОВНЕ ОДРЕДБЕ

Предмет уређивања

Члан 1.

Овим законом се уређују мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређују се надлежни органи за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите.

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 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 правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) *информациона безбедност* представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података,

да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

4) тајност је својство које значи да податак није доступан неовлашћеним лицима;

5) интегритет значи очуваност изворног садржаја и комплетности податка;

6) расположивост је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;

7) аутентичност је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;

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 значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;

10) управљање ризиком је систематичан скуп мера који укључује планирање, организовање и усмеравање активности како би се обезбедило да ризици остану у прописаним и прихватљивим оквирима;

11) *инцидент* је сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система;

11а) *јединствени систем за пријем обавештења о инцидентима* је информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности;

12) мере заштите ИКТ система су техничке и организационе мере за управљање безбедносним ризицима ИКТ система;

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

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

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

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

17) самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности;

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

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

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

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

22) криптоматеријали су криптографски производи, подаци, техничка документација криптографских производа, као и одговарајући криптографски кључеви;

23) безбедносна зона је простор или просторија у којој се, у складу са прописима о тајности података, обрађују и чувају тајни подаци;

24) *информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично;

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

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

Начела

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.

Обрада података о личности

Члан 3а

У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог закона поступа се у складу са прописима који уређују заштиту података о личности.

Надлежни орган

Члан 4.

Орган државне управе надлежан за безбедност ИКТ система је министарство надлежно за послове информационе безбедности (у даљем тексту: Надлежни орган).

Тело за координацију послова информационе безбедности

Члан 5.

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, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе Народне банке Србије, Центра за безбедност ИКТ система у органима власти и Националног центра за превенцију безбедносних ризика у ИКТ системима.

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

II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ИКТ системи од посебног значаја

Члан 6.

ИКТ системи од посебног значаја су системи који се користе:

1) у обављању послова у органима власти;

2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности;

3) у обављању делатности од општег интереса и другим делатностима и то у следећим областима:

(1) енергетика:

- производња, пренос и дистрибуција електричне енергије;
- производња и прерада угља;
- истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата;
- истраживање, производња, прерада, транспорт и дистрибуција природног и течног гаса;

(2) саобраћај:

- железнички, поштански, водни и ваздушни саобраћај;

(3) здравство:

- здравствена заштита;

(4) банкарство и финансијска тржишта:

- послови финансијских институција;
- послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;
- послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;

(5) дигитална инфраструктура:

- размена интернет саобраћаја;
- управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи);

(6) добра од општег интереса:

- коришћење, управљање, заштита и унапређивање добара од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја);

(7) услуге информационог друштва:

- услуге информационог друштва у смислу члана 2. тачка 25) овог закона;

(8) остале области:

- електронске комуникације;
- издавање службеног гласила Републике Србије;
- управљање нуклеарним објектима;
- производња, промет и превоз наоружања и војне опреме;

- управљање отпадом;
- комуналне делатности;
- производња и снабдевање хемикалијама;

4) у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности из тачке 3) овог става.

Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу делатности из става 1. тачка 3) овог члана.

Обавезе оператора ИКТ система од посебног значаја

Члан 6а

Оператор ИКТ система од посебног значаја у складу са овим законом у обавези је да:

1) упише ИКТ систем од посебног значаја којим управља у евиденцију оператора ИКТ система од посебног значаја;

2) предузме мере заштите ИКТ система од посебног значаја;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то 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 трећим лицима;

6) доставља обавештења о инцидентима који значајно угрожавају информациону безбедност ИКТ система;

7) достави тачне статистичке податке о инцидентима у ИКТ систему.

Евиденција оператора ИКТ система од посебног значаја

Члан 6б

Надлежни орган успоставља и води евиденцију ИКТ система од посебног значаја (у даљем тексту: Евиденција) која садржи:

1) назив и седиште оператора ИКТ система од посебног значаја;

2) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора ИКТ система од посебног значаја;

3) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја;

4) податак о врсти ИКТ система од посебног значаја, у складу са чланом 6. овог закона.

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

Оператор ИКТ система од посебног значаја дужан је да ИКТ систем од посебног значаја којим управља упише у евиденцију из става 1. овог члана.

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

Надлежни орган ставља на располагање Националном центру за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) ажурну евиденцију из става 1. овог члана.

Мере заштите ИКТ система од посебног значаја

Члан 7.

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 инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

1) успостављање организационе структуре, са утврђеним пословима и одговорностима запослених, којом се остварује управљање информационом безбедношћу у оквиру оператора ИКТ система;

2) постизање безбедности рада на даљину и употребе мобилних уређаја;

3) обезбеђивање да лица која користе ИКТ систем односно управљају ИКТ системом буду оспособљена за посао који раде и разумеју своју одговорност;

4) заштиту од ризика који настају при променама послова или престанка радног ангажовања лица запослених код оператора ИКТ система;

5) идентификовање информационих добара и одређивање одговорности за њихову заштиту;

6) класификовање података тако да ниво њихове заштите одговара значају података у складу са начелом управљања ризиком из члана 3. овог закона;

7) заштиту носача података;

8) ограничење приступа подацима и средствима за обраду података;

9) одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа;

10) утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију;

11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности и интегритета података;

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

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

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

15) заштиту података и средства за обраду података од злонамерног софтвера;

16) заштиту од губитка података;

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

18) обезбеђивање интегритета софтвера и оперативних система;

19) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

20) обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система;

21) заштиту података у комуникационим мрежама укључујући уређаје и водове;

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

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

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

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

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

27) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;

28) мере које обезбеђују континуитет обављања посла у ванредним околностима.

Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

Акт о безбедности ИКТ система од посебног значаја

Члан 8.

Оператор ИКТ система од посебног значаја дужан је да донесе акт о безбедности ИКТ система.

Актом из става 1. овог члана 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 из става 1. овог члана мора да буде усклађен с променама у окружењу и у самом ИКТ систему.

Оператор ИКТ система од посебног значаја је дужан да самостално или уз ангажовање спољних експерата врши проверу усклађености примењених мера ИКТ система са актом из става 1. овог члана и то најмање једном годишње и да о томе сачини извештај.

Ближи садржај акта из става 1. овог члана, начин провере ИКТ система од посебног значаја и садржај извештаја о провери уређује Влада на предлог Надлежног органа.

Поверавање активности у вези са ИКТ системом од посебног значаја трећим лицима

Члан 9.

Оператор ИКТ система од посебног значаја може поверити активности у вези са ИКТ системом трећим лицима, у ком случају је обавезан да уреди однос са тим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом.

Активностима из става 1. овог члана (у даљем тексту: поверене активности) сматрају се све активности које укључују обраду, чување, односно могућност приступа подацима којима располаже оператор ИКТ система од посебног значаја, а односе се на његово пословање, као и активности развоја, односно одржавања софтверских и хардверских компоненти од којих непосредно зависи његово исправно поступање приликом вршења послова из надлежности, односно пружања услуга.

Под трећим лицем из става 1. овог члана сматра се и привредни субјекат који је имовинским и управљачким односима (лица са учешћем, чланице групе друштава којој тај привредни субјект припада и др.) повезан са оператором ИКТ система од посебног значаја.

Поверавање активности врши се на основу уговора закљученог између оператора ИКТ система од посебног значаја и лица коме се те активности поверавају или посебним прописом.

Члан 10.

Изузетно од одредаба члана 9. овог закона, уколико су активности у вези са ИКТ системом поверене прописом, тим прописом се могу другачије уредити обавезе и одговорности оператора ИКТ система од посебног значаја у вези поверених активности.

Обавештавање о инцидентима

Члан 11.

Оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко веб странице Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима којег одржава Надлежни орган.

Уколико органи из става 1. овог члана буду обавештени о инциденту на други начин, податке о инциденту уносе у систем из става 1. овог члана.

Изузетно од става 1. овог члана, обавештење о инцидентима се упућује:

1) Народној банци Србије, у случају инцидената у ИКТ системима из члана 6. став 1. тачка 3) подтачка (4) алинеје прва и друга овог закона;

2) регулаторном телу за електронске комуникације у случају инцидената у ИКТ системима из члана 6. став 1. тачка 3) подтачка 8) алинеја прва овог закона.

Народна банка Србије и регулаторно тело за електронске комуникације обавештења из става 3. овог члана достављају у јединствени систем за пријем обавештења о инцидентима на начин из става 1. овог члана.

Након пријаве инцидента, уколико је инцидент и даље у току, оператори ИКТ система од посебног значаја достављају обавештења о битним догађајима у вези са инцидентом и активностима које предузимају до престанка инцидента органу коме су у складу са овим законом пријавили инцидент.

Оператори ИКТ система од посебног значаја достављају завршни извештај о инциденту органу кога су у складу са овим законом обавештавали о инциденту у року од 15 дана од дана престанка инцидента, а који обавезно садржи врсту и опис инцидента, време и трајање инцидента, последице које је инцидент изазвао, предузете активности ради отклањања последица инцидента и, по потреби, друге релевантне информације.

У случају инцидената у ИКТ системима за рад са тајним подацима оператори тих ИКТ система поступају у складу са прописима којима се уређује област заштите тајних података.

Одредбе ст. 1. и 7. овог члана не односе се на самосталне операторе ИКТ система.

Влада, на предлог Надлежног органа, уређује поступак обавештавања о инцидентима, листу, врсте и значај инцидената према нивоу опасности, поступање и размену информација о инцидентима између органа из члана 5. овог закона.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 3. овог члана коме се упућују обавештења о инцидентима, може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио.

Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, орган коме је упућено обавештење о инциденту, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Ако је инцидент повезан са значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање одбране Републике Србије, орган коме је упућено обавештење о инциденту обавештава Војнобезбедносну агенцију.

Ако је инцидент повезан са значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање националне безбедности, орган коме је упућено обавештење о инциденту обавештава Безбедносно-информативну агенцију.

У случају наступања околности угрожавања, ометања рада или уништења ИКТ система од посебног значаја руковођење и координацију спровођења мера и задатака у наведеним околностима предузима Републички штаб за ванредне ситуације, у складу са законом.

Инциденти у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности

Члан 11а

Оператор ИКТ система од посебног значаја дужан је да пријави следеће инциденте који могу да имају значајан утицај на нарушавање информационе безбедности:

1) инциденте који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;

2) инциденте који утичу на велики број корисника услуга, или трају дужи временски период;

3) инциденте 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) инциденте који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;

5) инциденте који доводе до неовлашћеног приступа заштићеним подацима чије откривање може угрозити права и интересе оних на које се подаци односе;

6) инциденте који су настали као последица инцидента у ИКТ систему из члана 6. став 1. тачка 3) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге ИКТ система из члана 6. став 1. тачка 3) подтачка (7) овог закона.

Оператор ИКТ система од посебног значаја дужан је да пријави и инциденте који су довели до значајног повећања ризика од наступања последица из става 1. овог члана.

Достављање статистичких података о инцидентима

Члан 11б

Оператор ИКТ система од посебног значаја дужан је да, поред обавештавања о инцидентима из члана 11. овог закона, достави Националном ЦЕРТ-у статистичке податке о свим инцидентима у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.

Национални ЦЕРТ обједињене статистичке податке из става 1. овог члана доставља Надлежном органу и објављује их на веб страници Националног ЦЕРТ-а.

Врсту, форму и начин достављања статистичких података из става 1. овог члана утврђује Национални ЦЕРТ.

Међународна сарадња и рана упозорења о ризицима и инцидентима

Члан 12.

Надлежни орган 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.

Уколико је инцидент у вези са извршењем кривичног дела, по добијању обавештења од Надлежног органа, министарство надлежно за унутрашње послове ће у званичној процедури проследити пријаву у складу са потврђеним међународним уговорима.

Самостални оператори ИКТ система

Члан 13.

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

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

Сходна примена одредаба о самосталним операторима ИКТ система

Члан 13а

На Народну банку Србије као оператора ИКТ система сходно се примењују одредбе чл. 13, 15, 15а, 19, 22, 26, 27. и 28. овог закона које се односе на самосталне операторе ИКТ система.

На Народну банку Србије као оператора ИКТ система сходно се примењују и одредбе чл. 11. и 11а овог закона које се односе на операторе ИКТ система од посебног значаја.

III. ПРЕВЕНЦИЈА И ЗАШТИТА ОД БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ

Национални ЦЕРТ

Члан 14.

Национални ЦЕРТ обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.

За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.

Делокруг Националног ЦЕРТ-а

Члан 15.

Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно:

1) прати стање о инцидентима на националном нивоу;

2) пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима;

3) реагује 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;

4) континуирано израђује анализе ризика и инцидената;

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

6) води евиденцију Посебних ЦЕРТ-ова;

7) извештава Надлежни орган на кварталном нивоу о предузетим активностима.

Национални ЦЕРТ је овлашћен да врши обраду података о лицу које се обрати Националном ЦЕРТ-у у складу са законом који уређује заштиту података о личности и другим прописима.

Обрада података о лицу из става 1. тачка 3) 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.

Национални ЦЕРТ обезбеђује непрекидну доступност својих услуга путем различитих средстава комуникације.

Просторије и информациони системи Националног ЦЕРТ-а морају да се налазе на безбедним локацијама.

У циљу обезбеђивања континуитета рада, Национални ЦЕРТ треба да:

1) буде опремљен са одговарајућим системима за обављање послова из свог делокруга;

2) има довољно запослених како би се осигурала доступност у свако доба;

3) обезбеди инфраструктуру чији је континуитет осигуран, односно да обезбеди редундантне системе и резервни радни простор.

Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом органа власти.

Национални ЦЕРТ промовише усвајање и коришћење прописаних и стандардизованих процедура за:

1) управљање и санирање ризика и инцидената;

2) класификацију информација о ризицима и инцидентима, односно класификацију према нивоу инцидената и ризика.

Сарадња ЦЕРТ-ова у Републици Србији

Члан 15а

Национални ЦЕРТ, ЦЕРТ органа власти и ЦЕРТ-ови самосталних оператора ИКТ система одржавају континуирану сарадњу.

ЦЕРТ-ови из става 1. овог члана одржавају међусобне састанке у организацији Националног ЦЕРТ-а најмање три пута годишње, као и по потреби у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Састанцима ЦЕРТ-ова из става 1. овог члана присуствују и представници Надлежног органа.

Састанцима ЦЕРТ-ова из става 1. овог члана могу, по позиву, да присуствују и представници посебних ЦЕРТ-ова, као и друга лица.

Надзор над радом Националног ЦЕРТ-а

Члан 16.

Надзор над радом Националног ЦЕРТ-а у вршењу послова поверених овим законом врши Надлежни орган, који периодично, а најмање једном годишње, проверава да ли Национални ЦЕРТ располаже одговарајућим ресурсима, врши послове у складу са чланом 15. овог закона и контролише учинак успостављених процеса за управљање сигурносним инцидентима.

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 17.

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 Национални ЦЕРТ.

Упис у евиденцију посебних ЦЕРТ-ова 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.

Национални ЦЕРТ прописује садржај, начин уписа и вођења евиденције из става 3. овог члана.

Центар за безбедност ИКТ система у органима власти (ЦЕРТ органа власти)

Члан 18.

ЦЕРТ органа власти обавља послове који се односе на заштиту од инцидената у ИКТ системима органа власти, изузев ИКТ система самосталних оператора.

Послове ЦЕРТ-а органа власти обавља орган надлежан за пројектовање, развој, изградњу, одржавање и унапређење рачунарске мреже републичких органа.

Послови ЦЕРТ-а органа власти обухватају:

1) заштиту Јединствене информационо-комуникационе мреже електронске управе;

2) координацију и сарадњу са операторима ИКТ система које повезује јединствена мрежа из тачке 1) овог става у превенцији инцидената, откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;

3) издавање стручних препорука за заштиту ИКТ система органа власти, осим ИКТ система за рад са тајним подацима.

ЦЕРТ самосталног оператора ИКТ система

Члан 19.

Самостални оператори ИКТ система су у обавези да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима.

Центри из става 1. овог члана међусобно размењују информације о инцидентима, као и са националним ЦЕРТ-ом и са ЦЕРТ-ом органа власти, а по потреби и са другим организацијама.

Делокруг центра за безбедност ИКТ система, као организационе јединице самосталног оператора ИКТ система, поред послова из ст. 1. и 2. овог члана, може обухватати:

1) израду интерних аката у области информационе безбедности;

2) избор, тестирање и имплементацију техничких, физичких и организационих мера заштите, опреме и програма;

3) избор, тестирање и имплементацију мера заштите од КЕМЗ;

4) надзор имплементације и примене безбедносних процедура;

5) управљање и коришћење криптографских производа;

6) анализу безбедности ИКТ система у циљу процене ризика;

7) обуку запослених у области информационе безбедности.

Заштита деце при коришћењу информационо-комуникационих технологија

Члан 19а

Надлежни орган 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 власти ради поступања у складу са утврђеним надлежностима.

Надлежни орган је овлашћен да врши обраду података о лицу које се обрати Надлежном органу 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.

У циљу обезбеђивања континуитета рада јединственог места за пружање савета и пријем пријава у вези безбедности деце на интернету, Надлежни орган треба да:

1) буде опремљен са одговарајућим системима за пријем пријава;

2) има довољно запослених како би се осигурала доступност у раду;

3) обезбеди инфраструктуру чији је континуитет осигуран.

Влада ближе уређује начин спровођења мера за безбедност и заштиту деце на интернету из ст. 1. и 3. овог члана.

IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Надлежност

Члан 20.

Министарство надлежно за послове одбране је надлежно за послове информационе безбедности који се односе на одобравање криптографских производа, 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 21.

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.

Компромитујуће електромагнетно зрачење

Члан 22.

Мере заштите од КЕМЗ за руковање са тајним подацима у ИКТ системима 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.

Ближе услове за проверу КЕМЗ и начин процене ризика од отицања података путем КЕМЗ уређује Влада, на предлог министарства надлежног за послове одбране.

Мере криптозаштите

Члан 23.

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.

Влада, на предлог министарства надлежног за послове одбране уређује техничке услове 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.

Одобрење за криптографски производ

Члан 24.

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.

Влада, на предлог министарства надлежног за послове одбране, ближе уређује услове које морају да испуњавају криптографски производи из става 1. овог члана.

Издавање одобрења за криптографски производ

Члан 25.

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.

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

Опште одобрење за коришћење криптографских производа

Члан 26.

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 27.

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.

Влада, на предлог министарства надлежног за послове одбране, ближе уређује вођење регистара из става 1. овог члана.

V. ИНСПЕКЦИЈА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ

Послови инспекције за информациону безбедност

Члан 28.

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 надлежно за послове информационе безбедности 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 29.

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 остави рок;

2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок.

VI. КАЗНЕНЕ ОДРЕДБЕ

Члан 30.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се за прекршај оператор ИКТ система од посебног значаја ако:

1) не изврши упис у евиденцију у року из члана 6б став 4. овог закона;

2) не донесе Акт о безбедности ИКТ система из члана 8. став 1. овог закона;

3) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 8. став 2. овог закона;

4) не изврши проверу усклађености примењених мера из члана 8. став 4. овог закона;

5) не достави статистичке податке из члана 11б став 1. овог закона;

6) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 29. став 1. тачка 1. овог закона.

За прекршај из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Члан 31.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај оператор ИКТ система од посебног значаја ако:

1) о инцидентима у ИКТ систему не обавести органе из члана 11. ст. 1, 3. и 7. овог закона;

2) не доставља обавештења о битним догађајима у вези са инцидентом и активностима из члана 11. став 5. овог закона;

3) не достави завршни извештај у року из члана 11. став 6. овог закона.

За прекршаје из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара.

Изузетно од ст. 1. и 2. овог члана, ако финансијска институција не обавести Народну банку Србије о инцидентима у ИКТ систему од посебног значаја, Народна банка Србије изриче тој финансијској институцији мере и казне у складу са законом којим се уређује њено пословање.

VII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рокови за доношење подзаконских аката

Члан 32.

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

Члан 33.

Оператори ИКТ система од посебног значаја су дужни да донесу акт о безбедности ИКТ система од посебног значаја у року од 90 дана од дана ступања на снагу подзаконског акта из члана 10. овог закона.

Ступање на снагу

Члан 34.

Овај закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.