НАЦРТ

ЗАКОН О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

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, такавих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програмома;

(3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из подтачака (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

(4) организациону структуру путем које се управља ИКТ системом;

2) *оператор ИКТ система* је правно лице, орган јавне власти или организациона јединица органа јавне 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 унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;

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 јавне власти* је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, правно лице које оснива државни орган, орган територијалне аутономије или локалне самоуправе, као и правно лице које се претежно, односно у целини финансира из буџета;

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, унутрашње опште акте, процедуре и слично.

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.

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 образује Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарства 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, Управе за заједничке послове републичких органа и Националног ЦЕРТ-а.

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

Актом Владе ближе се уређује организација и начин рада Тела за координацију и образују се стручне радне групе за потребе Тела за координацију.

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 јавне власти;

2) за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности;

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

(1) производња, пренос и дистрибуција електричне енергије;

(2) производња и прерада угља;

(3) истраживање, производња, прерада, транспорт и дистрибуција нафте и природног и течног гаса;

(4) промет нафте и нафтних деривата; железничког, поштанског и ваздушног саобраћаја;

(5) електронске комуникација;

(6) издавање службеног гласила Републике Србије;

(7) издавање уџбеника;

(8) управљање нуклеарним објектима;

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

(10) производња, промет и превоз наоружања и војне опреме,

(11) управљање отпадом;

(12) комуналне делатности;

(13) послови финансијских институција;

(14) здравствена заштита;

(15) пружање услуга информационог друштва уколико се тим услугама омогућавају друге услуге информационог друштва.

Влада, на предлог министарства надлежног за послове информационе безбедности, ближе уређује листу послова и делатности из става 1. тачка 3) 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 минимизација 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 оговорности за њихову заштиту;

6) класификовање података тако да ниво њихове заштите одговара значају података;

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 односно 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) заштита 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) заштита података и средства за обраду података од злонамерног софтвера;

16) заштита од губитка података;

17) записивање догађаја који могу бити од значаја за безбедност ИКТ система;

18) обезбеђивање интегритета софтвера и оперативних система;

19) заштита од злоупотребе техничких безбедносних слабости ИКТ система;

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

21) заштита 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) питања информационе безбедности 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.

Ближе услове за мере заштите ИКТ система уређује Влада на предлог Надлежног органа, уважавајући начела из члана 3. овог закона, 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 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, 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 Надлежног органа о инцидентима

Члан 11.

Оператори ИКТ система од посебног значаја обавезни су да обавесте Надлежни орган о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

Изузетно од става 1, оператори ИКТ система за рад са тајним подацима обавештења из става 1. упућују органу надлежном за обезбеђење примене стандарда и прописа у области заштите тајних података, финансијске институције обавештења упућују Народној банци Србије, а телекомуникациони оператори регулаторном телу за електронске комуникације.

Одредбе ст. 1 и 2. овог члана не односе се на самосталне операторе ИКТ система.

Листу инцидената и начин обавештавања из става 1. ближе уређује Надлежни орган.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима, може наложити његово објављивање.

Ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима, обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове.

Ако је инцидент повезан са нарушавањем права на заштиту података о личности, Надлежни орган, односно орган из става 2. коме се упућују обавештења о инцидентима и самостални оператор ИКТ система, о томе обавештавају и Повереника за информације од јавног значаја и заштиту података о личности.

Међународна сарадња и рана упозорења о ризицима и инцидентима

Члан 12.

Надлежни орган је дужан да успостави и одржава међународну билатералну и мултилатералну сарадњу на пољу безбедности ИКТ система, а поготово да пружи рана упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

1) брзо расту или имају тенденцију да постану високи ризици;

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 надлежном телу у складу са потврђеним међународним споразумима.

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

Национални центар за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ)

Члан 13.

Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: 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.

Члан 14.

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, 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, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања,

4) континуирано израђује анализе ризика и инцидената, које чини јавно доступним,

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

6) води евиденцију Посебних ЦЕРТ-ова.

Евиденција из става 1. тачка 6) овог члана 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.

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 републичких органа.

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

1) управљање и санирање ризика и инцидената;

2) класификацију информација о ризицима и инцидентима;

3) класификацију озбиљности инцидената и ризика;

4) дефиницију формата и модела података за размену информација о ризицима и инцидентима и дефиницију правила по којима ће се именовати значајни системи.

Начин рада Националног ЦЕРТ-а ближе прописује Влада, на предлог Надлежног органа.

Члан 15.

Надзор над радом Националног ЦЕРТ-а врши Надлежни орган, који периодично, а најмање једном годишње, проверава да ли Национални ЦЕРТ располаже одговарајућим ресурсима, врши послове у складу са чланом 14. овог закона и контролише учинак успостављених процеса за управљање сигурносним инцидентима.

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 16.

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, 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.

Ближе услове за упис у евиденцију из става 3. доноси Надлежни орган.

Центар за безбедност ИКТ система у републичким органима (ЦЕРТ републичких органа)

Члан 17.

Центар за безбедност ИКТ система у републичким органима (у даљем тексту: ЦЕРТ републичких органа) обавља послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора.

Послове ЦЕРТ-а републичких органа обавља Управа за заједничке послове републичких органа.

Послови ЦЕРТ-а републичких органа обухватају:

1) заштиту ИКТ система Рачунарске мреже републичких органа (у даљем тексту: РМРО);

2) координацију и сарадњу са операторима ИКТ система које повезује РМРО у превенцији инцидената, откривању инцидената, прикупљању информација о инцидентима и отклањању последица инцидената;

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

Члан 18.

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 републичких органа, 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, обухвата:

1) израду потребне безбедносне документације;

2) избор, тестирање и имплементација 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.

IV. КРИПТОБЕЗБЕДНОСТ И ЗАШТИТА ОД КОМПРОМИТУЈУЋЕГ ЕЛЕКТРОМАГНЕТНОГ ЗРАЧЕЊА

Надлежност

Члан 19.

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 20.

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, 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 изадатих 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.

Компромитујуће електромагнетно зрачење

Члан 21.

Уколико је у оквиру ИКТ система предвиђено руковање подацима који су одређени као тајни, у складу са законом, у ИКТ систему се, ради спречавања нарушавања информационе безбедности, примењују мере заштите од компромитујућег електромагнетног зрачења.

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 за отицање тајних података 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.

Обавеза примене метода криптозаштите

Члан 22.

Мере криптозаштите примењују се када се тајни подаци преносе средствима електронске комуникације изван безбедносне зоне која је утврђена за чување и поступање са одговарајућим подацима.

Мере криштозаштите се могу применити и као мере заштите тајних података који се чувају, као и за заштиту интегритета, аутентичности и непорецивости 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 23.

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 24.

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 60 дана од дана подношења уредног захтева, који се може продужити у случају посебне сложености провере највише за још 90 дана.

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

Регистар из става 5. 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. 3. и 4. 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, накнаду за издавање одобрења и садржај регистра издатих одобрења за криптографски производ.

Опште одобрење за коришћење криптографских производа

Члан 25.

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 26.

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

Регистар кадра 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 страних криптоматеријала 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 ст. 1. овог члана.

Члан 27.

Због посебних услова рада, сложености и природе посла, запосленима у министарству надлежном за послове одбране који обављају послове информационе безбедности, а који се односе на одобравање криптографских производа, дистрибуцију криптоматеријала и заштиту од КЕМЗ и послове и задатке у складу са овим законом и прописима донетим на основу овог закона, може се одредити додатак на основну плату у висини до 30%, а у складу са прописом који доноси министар надлежан за послове одбране.

VI. 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.

Члан 29.

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.

Овлашћења инспектора за информациону безбедност

Члан 30.

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

1) наложи отклањањање утврђених неправилности и за то остави рок;

2) забрани коришћење неодговарајућих поступака и техничких средстава и за то остави рок.

VII. ОСТАЛЕ ОДРЕДБЕ

Казнене одредбе

Члан 31.

Новчаном казном у износу од 50.000,00 до 2.000.000,00 динара казниће се правно лице за прекршај ако:

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

2) не изврши проверу из члана 8. став 4. овог закона;

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

4) не поступи у остављеном року по налогу инспектора за информациону безбедност из члана 33. став овог закона.

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

Члан 32.

Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се правно лице за прекршај ако:

1) не поступи у складу са чланом 11. ст. 1, 2. и 7. овог закона;

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

VIII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рокови за доношење подзаконских аката

Члан 33.

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

Члан 34.

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

Ступање на снагу

Члан 35.

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