РЕПУБЛИКА СРБИЈА
ВЛАДА
05 Број: 011-13435/2015
18. децембар 2015. године
Београд

НАРОДНОЈ СКУПШТИНИ

Б Е О Г Р А Д

Влада, на основу члана 123. тачка 4. Устава Републике Србије и члана 150. став 1. Пословника Народне скупштине („Службени гласник РС”, број 20/12 – пречишћен текст), подноси Народној скупштини Предлог закона о информационој безбедности, с предлогом да се узме у претрес.

За представника Владе у Народној скупштини одређен је др Расим Љајић, потпредседник Владе и министар трговине, туризма и телекомуникација, а за поверенике Сава Савић, помоћник министра трговине, туризма и телекомуникација, Небојша Васиљевић, виши саветник у Министарству трговине, туризма и телекомуникација и Наталија Радоја, шеф Одсека у Министарству трговине, туризма и телекомуникација.

ПРЕДСЕДНИК
Александар Вучић

4100315.004/76

ПРЕДЛОГ ЗАКОНА
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, 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 похрањују, 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;

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 аутономне покрајине, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, правно лице које оснива Република Србија, аутономна покрајна или јединица 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 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, 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.

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 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) електронска комуникација;

(6) издавање службеног гласила Републике Србије;

(7) управљање нуклеарним објектима;

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

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

(10) управљање отпадом;

(11) комуналне делатности;

(12) послови финансијских институција;

(13) здравствена заштита;

(14) услуге информационог друштва намењене другим пружаоцима услуга информационог друштва у циљу омогућавања пружања њихових услуга.

Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује 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 одговорности за њихову заштиту;

6) класификовање података тако да ниво њихове заштите одговара значају података у складу 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 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) 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) 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.

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 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. овог члана, финансијске институције обавештења упућују Народној банци Србије, телекомуникациони оператори регулаторном телу за електронске комуникације, а оператори ИКТ система за рад са тајним подацима поступају у складу са прописима којима се уређује област заштите тајних података.

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

Поступак достављања података, листу, врсте и значај инцидената и поступак обавештавања из става 1. овог члана уређује Влада.

Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 2. овог члана 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. овог члана 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. овог члана 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 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 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 у складу са потврђеним међународним уговорима.

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.

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 14.

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 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, 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,

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.

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, 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. овог члана доноси Надлежни орган.

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

Члан 18.

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 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 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, може обухватати:

1) израду интерних аката у области информационе безбедности;

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 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 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.

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

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

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

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

4) 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 правном лицу 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 правно лице ако о инцидентима у ИКТ систему не обавести Надлежни орган, односно орган надлежан за обезбеђење примене стандарда у области заштите тајних података, Народну банку Србије или регулаторно тело за електронске комуникације (члан 11. ст. 1. и 2.).

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

VII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рокови за доношење подзаконских аката

Члан 32.

Подзаконска акта предвиђена овим законом донеће се у року од 12 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".

О Б Р А З Л О Ж Е Њ Е

I. УСТАВНИ ОСНОВ ЗА ДОНОШЕЊЕ ЗАКОНА

Уставни основ за доношење овог закона садржан је у члану 97. тач. 4, 16. и 17. Устава Републике Србије, којима је, између осталог, прописано да Република Србија уређује и обезбеђује безбедност Републике Србије, организацију, надлежност и рад републичких органа, и да обезбеђује друге односе од интереса за Републику Србију.

II. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА

Стратегијом развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС", број 51/10), (у даљем тексту: Стратегија развоја ИД) је као једна од шест области приоритета одређена информациона безбедност. У Стратегији развоја ИД је истакнуто да је одговарајући степен информационе безбедности у свим облицима примене информационо-комуникационих технологија један од предуслова стварања одрживог информационог друштва. Као први приоритет у области информационе безбедности је одређено унапређење правног и институционалног оквира за информациону безбедност.

Постојећи законски оквир у овој области је Закон о тајности података („Службени гласник РС", број 104/09), Закон о заштити података о личности („Службени гласник РС", бр. 97/08 и 104/09 - други закон, 68/12 – УС и 107/12), Закон о електронском потпису („Службени гласник РС", број 135/04), Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала („Службени гласник РС", бр. 61/05 и 104/09), Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији („Службени гласник РС", бр. 88/09 55/12 – УС и 17/13) и Кривични законик („Службени гласник РС", бр. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13 и 108/14). У ширем контексту, правни оквир чине и Закон о електронским комуникацијама („Службени гласник РС", бр. 44/10 60/13 – УС и 62/14) и Закон о одбрани („Службени гласник РС", бр. 116/07, 88/09,104/09 116/07, 88/09 - др. закон, 104/09 – др. закон и 10/15). Усвајањем Закона о информационој безбедности и одговарајућих подзаконских аката успоставио би се целовит правни оквир у овој области.

Доношење Закона о информационој безбедности представља један од корака ка хармонизацији правног оквира Републике Србије са Европском унијом у области информационог друштва. У оквиру преговарачког поступка за придруживање Републике Србије Европској унији, материја информационе безбедности разматра се у оквиру Преговарачке групе 10 – Информационо друштво и медији. Националним програмом за усвајање правних тековина Европске уније (НПАА) од 2014-2018. године предвиђено је да ће Влада утврдити Предлог закона о информационој безбедности.

Европска унија донела је 2013. године Стратегију безбедности ИКТ система Европске уније, која утврђује основне смернице у овој области којима ЕУ и државе чланице треба да се руководе. Ради постизања отпорности на инциденте у ИКТ системима, неопходно је учешће бројних друштвених чинилаца, како у јавном, тако и у приватном сектору, с обзиром да појединачни напори често нису довољни да би се успоставио адекватан ниво безбедности и заштите ИКТ система. Путем очувања безбедности ИКТ система штите се основна људска права, лични подаци и приватност који су гарантовани међународним и националним правним актима. Стратегијом је одређено да је у области информационе безбедности потребно усвојити одговарајуће

правне акте (законе и подзаконска акта), одредити орган који ће у оквиру државе чланице бити надлежан за информациону безбедност и успоставити националне тимове за превенцију и реаговање на инциденте у ИКТ система – Национални ЦЕРТ (енг. Computer Emergency Response Team). У циљу ефикасније превенције и заштите, од велике је важности да надлежна тела држава чланица размењују податке о опасностима и инцидентима у ИКТ системима, као и да се одржавају посебне вежбе – симулације сајбер инцидената. Такође, истакнуто је да је, с обзиром да јавне институције, приватни сектор и грађани углавном нису довољно свесни ризика и опасности у сајбер простору, потребно ширити информације о претњама и тиме правовремено предузети мере заштите. Начела истакнута у овој стратегији одражавају се у Предлогу директиве о мрежној и информационој безбедности Европске уније (NIS Directive), која предвиђа регулисање наведених аспеката у државама чланицама, и чије се усвајање очекује у наредном периоду. Осим у неким случајевима, усаглашавање са Европском унијом оставља довољно широк простор да Република Србија пронађе оно решење које одговара њеним приликама, потребама и финансијским могућностима.

У смислу Предлога закона о информационој безбедности (у даљем тексту: Предлог закона) информациона безбедност представља скуп мера које омогућавају да ИКТ систем заштити тајност, интегритет, расположивост, аутентичност и непорецивост података којима се рукује путем тог система, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица. При томе се под информационо-комуникационим системом (у даљем тексту: ИКТ систем) подразумева електронска комуникациона мрежа у смислу закона који уређује електронске комуникације; уређаји или група међусобно повезаних уређаја, такав да се у оквиру тог уређаја, односно у оквиру барем једног из те групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма, потом подаци који се похрањују, обрађују, претражују или преносе помоћу средстава, а у сврху њиховог рада, употребе, заштите или одржавања, као и организациона структура путем које се управља ИКТ системом.

С обзиром на безбедоносне ризике у ИКТ системима, неопходно је да се Законом о информационој безбедности уреде мере заштите од безбедносних ризика у ИКТ системима, пропишу одговорности и обавезе правних лица приликом управљања и коришћења ИКТ система и одреде надлежни органи за спровођење мера заштите, односно надлежни орган државне управе за безбедност ИКТ система у Републици Србији, надлежни орган за одобравање криптографских производа, дистрибуцију криптоматеријала и заштиту од компромитујућег електромагнетног зрачења (у даљем тексту: КЕМЗ), образује Национални центар за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ), обезбеди координација између чинилаца заштите и праћење правилне примене прописаних мера заштите као и инспекцијски надзор у области информационе безбедности.

Предлогом закона се предвиђа да је министарство надлежно за послове информационе безбедности (у даљем тексту: Надлежни орган) орган државне управе надлежан за безбедност ИКТ система. Законом о министарствима („Службени гласник РС”, бр. 44/14, 14/15 и 54/15) предвиђено је да Министарство трговине, туризма и телекомуникација обавља послове државне управе у области информационог друштва који се односе на информациону безбедност.

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 овај Предлог закона предвиђа

да Влада образује Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе. Предложено је да ово тело сачињавају представници министарства надлежних за послове информационог друштва, 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.

Предлог закона уређује ИКТ системе од посебног значаја и предвиђа обавезе и одговорност оператора ИКТ система од посебног значаја за безбедност ИКТ система и предузимање мера заштите ИКТ система и у случају када су одређене активности у вези са тим ИКТ системом поверене трећим лицима, као и обавеза обавештавања надлежних органа о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности. ИКТ системи од посебног значаја су они ИКТ системи у којима је неопходно успоставити адекватан ниво информационе безбедности, имајући у виду њихове послове и делатности, као и ризик настанка штете по државу и грађане у случају инцидената у овим системима. Предлогом закона предвиђено је да Влада, на предлог министарства надлежног за послове информационе безбедности, ближе уређује листу послова и делатности код којих ће постојати обавеза примене адекватних мера у складу са законом.

Предлогом закона се уређује да 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, а послове Националног ЦЕРТ-а опредељује у надлежност Регулаторне агенције за електронске комуникације и поштанске услуге.

Предлог закона предвиђа да послове ЦЕРТ-а републичких органа обавља Управа за заједничке послове републичких органа, као Центар за безбедност ИКТ система у републичким органима (у даљем тексту: ЦЕРТ републичких органа), и то послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора.

Према дефиницији из члана 2. тачка 17) Предлога закона, самостални оператори ИКТ система су министарство надлежно за послове одбране, министарство надлежно за унутрашње послове, министарство надлежно за спољне послове и службе безбедности.

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

Предлог закона садржи посебну главу о криптобезбедности и заштити од компромитујућег електронског зрачења (КЕМЗ). Предлогом закона је предвиђено да је министарство надлежно за послове одбране 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. Предлогом закона се уређују послови и задаци министарства, обавеза примене метода криптозаштите, издавање одобрења за криптографски период и регистри у криптозаштити.

Ради ефикасне примене овог закона, потребно је обезбедити инспекцијски надзор над радом ИКТ система од посебног значаја и других ИКТ система стога је предвиђено у Предлогу закона да послове инспекције за информациону безбедност обавља министарство надлежно за послове информационе безбедности преко инспектора за информациону безбедност.

III. ОБЈАШЊЕЊЕ ОСНОВНИХ ПРАВНИХ ИНСТИТУТА И ПОЈЕДИНАЧНИХ РЕШЕЊА

У члану 1. Предлога закона се наводи предмет уређивања закона.

Чланом 2. се дефинишу термини који се користе у Предлогу закона.

Члан 3. садржи начела Предлога закона.

Чланом 4. се утврђује орган државне управе надлежан за безбедност ИКТ система.

У члану 5. прописује се да Влада образује Тело за координацију послова информационе безбедности), као координационо тело Владе 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.

У члану 6. су утврђени ИКТ системи од посебног значаја, а ставом 2. истог члана прописано је да Влада, на предлог министарства надлежног за послове информационе безбедности, ближе уређује листу послова и делатности из става 1. овог члана.

У члану 7. утврђују се дужност оператора ИКТ система од посебног значаја да предузимају одговарајуће мере заштите ИКТ система, којима 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. Овим чланом дефинишу се и мере заштите ИКТ система и утврђује да ближе услове за мере уређује Влада на предлог Надлежног органа, уважавајући међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

У члану 8. се уређује обавеза оператора ИКТ система од посебног значаја да донесе акт о безбедности ИКТ система, којим се одређују мере заштите ИКТ система, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система, као и да ближе услове за садржај акта о безбедности ИКТ система, начин провере ИКТ система и садржај извештаја о провери ИКТ система од посебног значаја који уређује Влада на предлог Надлежног органа.

Члан 9. регулише поверавање активности у вези са ИКТ системом од посебног значаја трећим лицима, у ком случају се прописује обавеза оператору да уреди однос са тим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом.

Чланом 10. прописан је изузетак од одредаба члана 9, уколико су активности у вези са ИКТ системом поверене прописом, да се тим прописом могу другачије уредити обавезе и одговорности оператора ИКТ система од посебног значаја у вези поверених активности.

Чланом 11. прописана је обавеза оператора ИКТ система од посебног значаја да обавештавају Надлежни орган о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

Чланом 12. се прописује дужност Надлежног органа да успостави и одржава међународну билатералну и мултилатералну сарадњу на пољу безбедности ИКТ система, а поготово да пружи рана упозорења о ризицима и инцидентима, а ако је инцидент у вези са извршењем кривичног дела, по добијању обавештења од Надлежног органа, министарство надлежно за унутрашње послове да у званичној процедури проследи пријаву надлежном телу у складу са потврђеним међународним споразумима.

Чланом 13. предвиђено је да ће самостални оператори ИКТ система одредити посебна лица, односно организационе јединице за интерну контролу сопствених ИКТ

система. А да ће лица за интерну контролу самосталних оператора ИКТ система извештај о извршеној интерној контроли подносити руководиоцу самосталног оператора ИКТ система.

Чланом 14. се уређује Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) који обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу и утврђује надлежност Регулаторне агенције за електронске комуникације и поштанске услуге за послове Националног ЦЕРТ-а.

Чланом 15. прописују се послови Националног ЦЕРТ-а да 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.

Чланом 16. прописује се надзор над радом Националног ЦЕРТ-а који врши Надлежни орган.

Чланом 17. прописује се оснивање посебног центра 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.

Чланом 18. прописује се надлежност Центра за безбедност ИКТ система у републичким органима (у даљем тексту: ЦЕРТ републичких органа) који обавља послове који се односе на заштиту од инцидената у ИКТ системима републичких органа, изузев ИКТ система самосталних оператора, у оквиру Управе за заједничке послове републичких органа.

Члан 19. прописује обавезу самосталних оператора ИКТ система да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима и дефинишу се послови из делокруга рада центра.

Чланом 20. прописано је да послове информационе безбедности који се односе на криптобезбедност и КЕМЗ обавља министарство надлежно за послове одбране.

Чланом 21. прописани су послови министарства надлежног за послове одбране у области криптобезбедности и КЕМЗ.

Чланом 22. уређује се заштита од компромитујућег електромагнетног зрачења.

Чланом 23. уређује се обавеза примене методе криптозаштите.

Чланом 24. прописано је да 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 (у даљем тексту: одобрење за криптографски производ) и да Влада, на предлог министарства надлежног за послове одбране, ближе уређује услове које морају да испуњавају криптографски производи из става 1. овог члана.

Чланом 25. уређује се издавање одобрења за криптографски производ.

Чланом 26. прописано је да опште одобрење за коришћење криптографских производа имају самостални оператори ИКТ система.

Чланом 27. прописано је да 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, а Регистар страних криптоматеријала води Канцеларија Савета за националну безбедност и заштиту тајних података, у складу са ратификованим међународним споразумима, као и да Влада, на предлог министарства надлежног за послове одбране, ближе уређује вођење регистара из овог члана.

У члану 28. прописани су послови инспекције за информациону безбедност која врши надзор над применом овог закона и радом оператора од посебног значаја, осим самосталних оператора ИКТ система и система за рад са тајним подацима.

У члану 29. прописана су овлашћења инспектора за информациону безбедност.

У чл. 30. и 31. прописане су казнене одредбе, предвиђене су новчане казне за одговорна лица која прекрше одредбе закона.

У члану 32. прописани су рокови за доношење подзаконских аката.

У члану 33. је дефинисан рок за доношење акта о безбедности ИКТ система од посебног значаја.

Члан 34. Предлога закона је завршна одредба о ступању закона на снагу.

IV СРЕДСТВА ПОТРЕБНА ЗА СПРОВОЂЕЊЕ ЗАКОНА

За спровођење овог закона није потребно обезбедити средства у буџету Републике Србије за 2015. годину.

Средства за реализацију закона у наредним годинама реализоваће се у складу са билансним могућностима буџета Републике Србије и предвиђеним лимитима.

За спровођење овог закона потребно је обезбедити средства у буџету Републике Србије за 2016. годину, 2017. годину и 2018. годину, у износу од 722.005.000 динара, односно 57.500.000, динара у 2016. години, 326.048.000 динара у 2017. години и 338.457.000 динара у 2018. години на разделима Министарства трговине, туризма и телекомуникација, Министарства одбране и Управе за заједничке послове републичких органа.

Предлогом закона о информационој безбедности предвиђено је да је надлежни орган државне управе за безбедност ИКТ система министарство надлежно за послове информационе безбедности, односно Министарство трговине, туризма и телекомуникација и да би на основу предложених законских решења то Министарство вршило следеће послове:

- припремало подзаконске акте Владе на основу закона;
- припремало и доносило подзаконске акте из своје надлежности;
- вршило инспекцијски надзор над операторима ИКТ система од посебног значаја (ИКТ система органа јавне власти, ИКТ система у којима се обрађују подаци који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности и ИКТ система који се користе у обављању делатности од општег интереса);
- примало обавештења о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности и налагало његово објављивање, ако је инцидент од интереса за јавност;
- успостављање и одржавање међународне билатералне и мултилатералне сарадње на пољу безбедности ИКТ система, а поготово пружање раних упозорења о ризицима и инцидентима;
- надзор над радом Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ).

Услед тога, како би се наведени послови могли извршавати у складу са законом, неопходно је повећати капацитете Министарства трговине, туризма и телекомуникација. Процењено је да би у Министарству у периоду од 2016. до 2018 години укупно требало

99.340.000 динара за реализацију закона, односно 25.500.000 динара у 2016. години, 38.420.000 динара у 2017. години и 38.420.000 динара у 2018. години.

Наиме, потребно је да се образује унутрашња организациона јединица за информациону безбедност и у њој запосли 11 државних службеника у 2017. години услед чега би укупни годишњи расходи за запослене износили 13.420.000 динара у 2017. години и 13.420.000 динара у 2018.години, а годишњи расходи за коришћење услуга и роба (службена путовања, обуке, услуге по уговору итд) 2.500.000 динара у 2016. години и 5.000.000 динара у 2017. години и 5.000.000 динара у 2018. години. У оквиру средстава за рад нове организационе јединице, поред основног канцеларијског опремања рачунарском опремом, биће потребна опрема за спровођење мера заштите тајних података, као и успостављање информационог система за пријем и обраду обавештења о инцидентима и инспекцијски надзор уз примену одговарајућих мера заштите ИКТ система, за шта се процењује да је у 2016. години потребно 20.000.000 динара, у 2017. години 20.000.000 динара и у 2018. години 20.000.000 динара.

Финансијска средства потребна Министарству одбране за спровођење закона би износила 428.665.000 динара, односно 194.628.000 динара у 2017. години и 234.037.000 динара у 2018. години.

Решења садржана у Предлогу закона о информационој безбедности која се тичу Министарстава одбране односе се на добијање националне надлежности за одговарајуће послове из области информационе безбедности – „одобравање криптографских производа“, „дистрибуција криптоматеријала“ и „заштиту од компромитујућег електромагнетског зрачења“ које би извршавала наменска установа у оквиру овог министарства.

Тренутно, наведена установа не располаже довољним ресурсима (људским, материјалним и стручним) за национални ниво, тако да не обезбеђује у потпуности извршавање свих послова и задатака који су предложени у Предлогу закона о информационој безбедности.

Да би наведена установа могла успешно да извршава послове и задатке из надлежности Министарства одбране које предвиђа Предлог закона о информационој безбедности, потребно је предузети мере за достизање недостајућих способности, а које се тичу обезбеђења додатних људских ресурса, опремања одговарајућом опремом за мерење компромитујућег електромагнетног зрачења (КЕМЗ) и специјалистичког оспособљавања персонала. Без наведеног, Министарство одбране не би било у могућности да успешно реализује надлежности предвиђене Предлогом закона.

У складу са наведеним, за потребе реализације закона потребна су Министарству одбране средства за расходе запослених у износу од 38.798.000 у 2017. години и 75.637.000 у 2018. години. Ради додатног опремања, пре свега за набавку опреме за детекцију и заштиту од КЕМЗ, која се може набавити само из иностранства и под одређеним условима неопходна новчана средства износе 142.847.000 динара у 2017. години и 140.000.000 динара 2018. години, док је за коришћење услуга и роба потребно 12.983.000 динара у 2017. години и 18.400.000 динара у 2018. години.

Финансијска средства потребна Управи за заједничке послове, у наредне три године за реализацију закона, износе укупно 194.000.000 динара, односно 35.000.000 динара у 2016. години, 93.000.000 динара у 2017. години и 66.000.000 у 2018. години.

Наиме, потребно је да се образује унутрашња организациона јединица за информациону безбедност и у њој запосли 12 државних службеника услед чега би укупни годишњи расходи за запослене износили у 2017. години и 23.000.000 динара и у 2018.

години 23.000.000 динара, док би годишњи расходи за коришћење услуга и роба износили 8.000.00 динара у 2016. години, 20.000.000 динара у 2017. години и 18.000.000 у 2018. години. У оквиру средстава за рад Управи је потребно у 2016. години 27.000.000 динара, у 2017. години 50.000.000 динара, а у 2018. години 25.000.000 динара.

Сходно наведеном укупни износ средстава за реализацију овог закона би у надлежним институцијама у наредне две године износио:

Средства	Година	МТТТ	МО	УЗЗРО	УКУПНО	
Расходи за запослене	2016	0	0	0	0	187.275.000
	2017	13.420.000	38.798.000	23.000.000	75.218.000	
	2018	13.420.000	75.637.000	23.000.000	112.057.000	
Коришћење услуга и роба	2016	2.500.000	0	8.000.000	10.500.000	89.883.000
	2017	5.000.000	12.983.000	20.000.000	37.983.000	
	2018	5.000.000	18.400.000	18.000.000	41.400.000	
Основна средства	2016	20.000.000	0	27.000.000	47.000.000	444.847.000
	2017	20.000.000	142.847.000	50.000.000	212.847.000	
	2018	20.000.000	140.000.000	25.000.000	185.000.000	
УКУПНО		**99.340.000**	**428.665.000**	**194.000.000**		**722.005.000**

Година	МТТТ	МО	УЗЗРО	УКУПНО
2016	22.500.000	0	35.000.000	57.500.000
2017	38.420.000	194.628.000	93.000.000	326.048.000
2018	38.420.000	234.037.000	66.000.000	338.457.000
УКУПНО	**99.340.000**	**428.665.000**	**194.000.000**	**722.005.000**

Финансијска средства потребна за успостављање капацитета за обављање послова Националног ЦЕРТ-а у оквиру РАТЕЛ-а процењују се да су слична средствима која су потребна Министарству трговине, туризма и телекомуникација за послове надлежног органа за информациону безбедност.

Указујемо да је доношење предметног закона предвиђено Националним програмом за усвајање правних тековина Европске уније (НПАА), као и да су приликом израде овог закона уважена стратешка решења ЕУ у овој области и правне тенденције. Стратегијом у овој области, Европска унија је декларисала одлучност да се област информационе безбедности уреди и да се њен ниво значајно подигне, у чему морају да учествују надлежни државни органи, који треба да имају адекватне људске и техничке капацитете.

АНАЛИЗА ЕФЕКАТА ЗАКОНА

1. Проблеми које акт треба да реши

Предметни закон представља оквир за уређење безбедности информационо-комуникационих система у Републици Србији. 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.

Употреба информационо-комуникационих технологија (ИКТ) од стране државе, привреде и грађана је у порасту, и све више послова и активности се заснива на њиховом коришћењу. Према подацима Републичког завода за статистику, објављеним у оквиру документа „Употреба информационо-комуникационих технологија у Републици Србији, 2015", утврђено је да 100% предузећа на територији Републике Србије користи рачунар у свом пословању, да 99,1% предузећа има интернет прикључак, а 98,0% има широкопојасну (broadband) интернет конекцију. Према истом извору, 94,5% предузећа користи електронске сервисе јавне управе. Са друге стране, 64,4% домаћинстава поседује рачунар, 63,8% домаћинстава поседује интернет прикључак, а 56% домаћинстава у Србији има широкопојасну (broadband) интернет конекцију. Такође, преко 1.500.000 лица користи електронске сервисе јавне управе, а преко 1.220.000 лица куповало је или поручивало робу/услуге путем интернета у последњих годину дана.

Развој нових технологија доноси несумњиве користи за друштво, јер се њиме омогућава значајно смањење трошкова, пословни процеси се аутоматизују, олакшавају и убрзавају, бројне информације постају доступне, а могућности комуникације се знатно проширују. Брзина развоја технологија је велика, и у кратким временским интервалима технологије напредују и садрже нове и напредније функционалности. Паралелно са развојем нових технологија, на глобалном нивоу расту и претње њиховој безбедности. Према наводима из Стратегије информационе безбедности Европске уније (*Cybersecurity Strategy of the European Union*), високотехнолошки криминал је врста криминала која је у највећем порасту, а милион људи свакодневно буде жртва напада. Према подацима Министарства унутрашњих послова, у 2013. години откривено је 855 кривичних дела у области високотехнолошког криминала, а у 2014. годину откривено је 780 кривичних дела. Преовлађујући облик овог криминала чине фалсификовање и злоупотреба платних картица. Извештаји институција који врше послове информационе безбедности у ИКТ системима републичких органа, односно научноистраживачкој и образовној заједници, говоре да су напади у Републици Србији у порасту, при чему се истиче да су напади на мрежу републичких органа свакодневни. Нарушавање информационе безбедности може да изазове велику штету по безбедност Републике Србије, имовину (јавну и приватну), личне податке грађана и друго.

Повезаност рачунара и система путем Интернета утиче да они буду рањивији и угроженији, као и на могућност напада са било које локације у свету. Превенција, и заштита ИКТ система, као и међусобна сарадња у овом пољу у Републици Србији постоје у одређеном броју државних и приватних субјеката, али се често врше на основу појединачних иницијатива. Неопходно је да се координација побољша, и то не само на националном нивоу, већ и међудржавном, имајући у виду да многи инциденти у ИКТ системима имају прекогранични карактер. Осим у појединим областима где постоје посебни прописи (у области заштите тајних података, електронских комуникација, у пословима финансијских институција), није регулисана обавеза за утврђивање мера које су неопходне да се предузму у циљу заштите ИКТ система. Органи јавне власти, лица која обрађују нарочито осетљиве податке о личности и правна лица која обављају делатности од општег интереса морају да повећају своју отпорност на угрожавање информационе безбедности, јер су послови који врше од великог значаја, а њихово неометано функционисање све више зависи од нових технологија. У појединим делатностима од општег интереса, употреба ИКТ система је неопходна за вршење тих делатности, те би угрожавање система могло да изазове велике сметње у обављању виталних функција и проузрокује значајну штету по државу и њене грађане. Поред тога, потребно је повећати ниво информисаности о инцидентима, на националном и глобалном нивоу, јер се тако ширење инцидената може зауставити, или смањити. Такође, сматра се да је, путем едукације, потребно повећати друштвену свест, односно свест грађана, о опасностима које могу да наруше информациону безбедност.

2. Циљеви који се актом постижу

Актом се информациона безбедност регулише на системски начин, уз намеру да се одреде надлежни органи у овој области и постигне да органи јавне власти, субјекти који обрађују нарочито осетљиве податке о личности и субјекти који обављају делатности од општег интереса (оператори ИКТ система од посебног значаја) предузму адекватне техничке и организационе мере заштите својих ИКТ система. Утврђује се надлежни орган за информациону безбедност у РС, који ће припремати подзаконске акте на основу овог закона, вршити међународну билатералну и мултилатералну сарадњу на пољу безбедности ИКТ система и вршити надзор над применом овог закона. Законом је предвиђено да ови субјекти морају да имају акт о безбедности ИКТ система, којим се одређују мере заштите ИКТ система, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности овог система, као и овлашћења и одговорности у вези са овом безбедношћу и ресурсима тог система. Тиме се постиже да се повећа безбедност ИКТ система и унапреди припремљеност за реаговање на инциденте у оним субјектима који врше послове чија природа и садржај захтевају одговарајући ниво заштите ИКТ система. Стратегијом информационе безбедности Европске уније истакнуто је да је, у циљу унапређења отпорности на нападе у ИКТ системима, неопходно да јавни сектор развије своје капацитете.

С обзиром на глобалну умреженост рачунара, већина инцидената у ИКТ системима има међународни карактер, а напади се могу вршити са територија различитих држава (као, на пример, путем ботнет мрежа, где нападнути и заражени рачунар постаје рачунар са кога се даље шире напади) и причињавати штету која није ограничена само на једну земљу. У случајевима оваквих напада, квалитетна комуникација између држава доприноси да се инциденти зауставе и умање, а починиоци открију и онеспособе. Предметни закон предвиђа да је надлежни орган за информациону безбедност у РС дужан да одржава међународну билатералну и мултилатералну сарадњу, а поготово да пружи рана упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова: 1) брзо расту или имају тенденцију да постају високи ризици, 2) превазилазе или могу да превазиђу националне капацитете, 3) могу да имају негативан утицај на више од једне државе.

Поред тога, овим законом се у оквиру РАТЕЛ-а успоставља Национални центар за превенцију и заштиту од безбедносних ризика у ИКТ системима у Републици Србији (Национални ЦЕРТ), који прати стање о инцидентима о националном нивоу, обавештава релевантна лица о ризицима и инцидентима, реагује по пријављеним инцидентима, израђује анализе ризика и инцидената и подиже свест друштва о значају информационе безбедности. Једна од важних функција Националног ЦЕРТ-а је и сарадња са истим институцијама из других земаља. Имајући у виду да инциденти у ИКТ системима најчешће имају прекогранични карактер, односно да се дешавају на територији више земаља, међусобна сарадња ЦЕРТ-ова је од изузетног значаја, како би се међусобном разменом информација успешно одговорило на инциденте. Република Србија је једна од малобројних европских држава која нема Национални ЦЕРТ, што знатно отежава прикупљање информација о инцидентима и реаговање на њих. Формирање ове институције предвиђено је Стратегијом развоја информационог друштва у Републици Србији.

Законом се регулише и област криптозаштите и заштите од компромитујућег електромагнетног зрачења (КЕМЗ). Мере криптозаштите примењују се ради заштите интегритета, аутентичности и непорецивости података. Криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни, морају да буду верификовани и одобрени за коришћење, имајући у виду својства података који се преносе и чувају, те се законом регулише издавање одобрења за криптографски производ.

3. Разматране могућности да се проблем реши и без доношења акта

Имајући у виду садржину Закона, који одређује надлежности органа, обавезе у погледу заштите ИКТ система, надзор над применом закона и друге одредбе, било је неопходно да се ова област уреди законом. Стратегијом развоја информационог друштва у Републици Србији до 2020. године („Службени гласник РС" број 51/10) у поглављу III. Области и приоритети стратегије предвиђени су приоритети у шест области информационог друштва. У оквиру области информационе безбедности предвиђена су четири приоритета: Унапређење правног и институционалног оквира за информациону

безбедност, заштита критичне инфраструктуре, борба против високотехнолошког криминала, научно-истраживачки и развојни рад у области информационе безбедности. Конкретни циљеви предвиђени приоритетом 6.1. Унапређење правног и институционалног оквира за информациону безбедност подразумевају да је потребно донети прописе из информационе безбедности, којима ће се додатно уредити стандарди информационе безбедности, подручја информационе безбедности, као и надлежности и задаци појединих институција у овој области.

4. Зашто је доношење акта најбољи начин за решавање проблема

Законом се обавезују оператори ИКТ система од посебног значаја да предузму мере заштите у својим ИКТ системима, што је веома важно како би се обезбедило да ти системи буду превентивно заштићени и спремни за реакцију у случају инцидената. Утврђује се надлежни орган за информациону безбедност у РС, који ће припремати подзаконске акте на основу овог закона, вршити међународну билатералну и мултилатералну сарадњу на пољу безбедности ИКТ система и вршити надзор над применом овог закона. Успостављањем Националног ЦЕРТ-а допринеће се унапређењу реакције на инциденте, подизању степена обавештености и свести о инцидентима у ИКТ системима и вршити едукација. Такође, Законом се утврђује надлежност органа у области криптобезбедности и заштите од КЕМЗ-а.

5. На кога ће и како ће највероватније утицати решења у закону

Будући да информациона безбедност значи заштиту система, података и инфраструктуре у циљу очувања поверљивости, интегритета и расположивости информација, примена закона ће имати утицај на све грађане, органе јавне власти и привредне субјекте који користе информационо-комуникационе технологије. Наиме, законским решењима постиже се поверење корисника у безбедно функционисање ИКТ система, поверење грађана у заштићеност података о личности у ИКТ системима, ширење свести о неопходности спровођења мера информационе безбедности, заштита података, заштита ИКТ система, безбедност електронских трансакција, ефикасни механизми заштите и остваривање права у процесима електронског пословања и електронске размене података.

Закон одређује ИКТ системе од посебног значаја у Републици Србији. То су ИКТ системи који се користе у обављању послова у органима јавне власти, ИКТ системи за обраду података који се, у складу са законом који уређује заштиту података о личности, сматрају нарочито осетљивим подацима о личности и ИКТ система у обављању делатности од општег интереса. Решења у закону ће утицати на ова правна лица, односно органе (операторе ИКТ система од посебног значаја) тако што ће они бити дужни да предузму адекватне техничке и организационе мере заштите својих ИКТ система и да донесу акт о безбедности ИКТ система, којим се наведене мере заштите одређују. 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, чиме се обезбеђује адекватна заштита субјеката регулације у домену

информационе безбедности. Оператори ИКТ система од посебног значаја моћи ће да повере активности у вези са својим ИКТ системом трећим лицима, при чему ће морати да уреде однос са тим лицима тако да се обезбеди предузимање мера заштите ИКТ система у складу са законом. Оператори ИКТ система од посебног значаја биће дужни да обавештавају Надлежни орган (министарство надлежно за послове информационог друштва) о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

У глави закона која се односи на криптобезбедност и заштиту од компромитујућег електромагнетног зрачења (КЕМЗ) одређено је да се, уколико је у оквиру ИКТ система предвиђено руковање подацима који су одређени као тајни, у складу са законом, у ИКТ систему, ради спречавања нарушавања информационе безбедности, примењују мере заштите од КЕМЗ-а. Такође, 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.

6. Какве трошкове ће примена закона створити грађанима и привреди (нарочито малим и средњим предузећима)

Примена Закона неће створити трошкове грађанима. Привредним субјектима који су оператори ИКТ система од посебног значаја се намећу одређене обавезе овим законом. За привредне субјекте који су успоставили систем управљања информационом безбедношћу у складу са међународним стандардима и добром праксом у овој области, не очекује се да примена закона изазове значајне трошкове.

Привредни субјекти који представљају операторе ИКТ система од посебног значаја, а који до сада нису успоставили одговарајући систем управљања информационом безбедношћу имаће одређене трошкове за испуњење законских обавеза који се огледају у евентуалном додатном технолошком опремању, обуци запослених, ангажовању нових стручњака и слично. Прецизни износи додатних трошкова за наведене субјекте варирају у великом распону, будући да исти зависе од више фактора који могу да буду веома различити у различитим привредним субјектима. Наиме, колико ће финансијских средстава за примену закона издвојити ови привредни субјекти зависи од њихове величине, односно броја запослених, технолошке опремљености (поседовање рачунарске опреме, информационог система), обучености запослених за коришћење информационих технологија у домену информационе безбедности, и других фактора од којих функционисање информационе безбедности зависи у једном привредном субјекту. Сходно наведеном, није могуће дати ни тачне, ни оквирне износе по привредном субјекту.

У образложењу Предлога закона, одељку IV Финансијска средства, приказани су трошкови за реализацију закона у наредне две године, који ће се финансирати из Буџета Републике Србије.

7. *Да ли су позитивне последице доношења закона такве да оправдавају трошкове које ће он створити*

Неспорно је да ће доношење Закона о информационој безбедности довести до позитивних последица, уређења, развоја и унапређења информационе безбедности у Републици Србији, и да су трошкови које ће примена закона створити у потпуности оправдани.

Законом се успоставља институционални оквир у Републици Србији, којим се обезбеђује очување безбедности ИКТ система, тако што се одређују надлежне институције и дефинише делокруг њиховог рада у области информационе безбедности (надлежни орган за ИБ, Национални ЦЕРТ, ЦЕРТ републичких органа, министарство надлежно за послове одбране).

Улога надлежних институција која се дефинише овим законом састоји се у превенцији, заштити, очувању и несметаном функционисању ИКТ система на територији Републике Србије.

Трошкови који настају доношењем закона су неопходни за јачање улоге државних институција у овој области и примену закона у потпуном обиму, како би се њихови послови обављали на начин који ће омогућити одржавање адекватног нивоа информационе безбедности у Републици Србији.

Такође, законска решења која се тичу ИКТ система од посебног значаја предвиђају обавезе ових система да предузму мере заштите ИКТ система, којим 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, односно донесу Акт о безбедности ИКТ система којим се одређују 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.

Примена закона којим се операторима ИКТ системима од посебног значаја прописују наведене обавезе су од посебне важности, будући да се ови ИКТ системи користе у обављању послова у органима јавне власти, за обраду нарочито осетљивих података о личности и у обављању делатности од општег интереса.

Законска решења која утврђују улогу надлежних институција у домену информационе безбедности, као и увођење обавеза операторима ИКТ система од посебног значаја, ствара користи које се огледају у очувању безбедности ИКТ система, националне безбедности, заштити основних људских права, личних података и приватности који су гарантовани међународним и националним правним актима.

Трошкови који ће се створити применом овог закона су нужни и неопходни, имајући у виду да нарушавање информационе безбедности може да изазове велику штету по националну безбедност, функционисање органа јавне власти и привредних субјеката, личне податке, имовину и друга добра, као и пораст високотехнолошког криминала, неопходно је предузети превентивне мере у циљу заштите од инцидената, и, у случају

инцидента, реаговати на брз и ефикасан начин. Да би се то постигло, важно је обезбедити да ИКТ систем заштити тајност, интегритет, расположивост, аутентичност и непорецивост података којима се рукује путем тог система, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица. С обзиром на значај информационе безбедности, трошкови који ће настати ради примена мере заштите су нужни и оправдани, јер је неспорно да ИКТ системи морају да буду заштићени и да трошкови који настану представљају улагање које треба да донесе општу корист. Евентуалне штете које би се десиле нарушавањем информационе безбедности у многим случајевима би могле да далеко премаше висину улагања у безбедност ИКТ система.

8. *Да ли се законом подржава стварање нових привредних субјеката на тржишту и тржишна конкуренција*

Као што је наведено, Законом је планирано да се уреде мере заштите од безбедносних ризика у ИКТ системима у Републици Србији. Очекује се да ће се због тога јавити потреба за набављањем производа, односно услуга које ће, поред осталих функција, служити и за заштиту ових система. Услед тога, процењује се да ће примена овог закона утицати на развој тржишта ИКТ производа и услуга у области информационе безбедности, што ће довести и до присуства већег броја учесника на тржишту односно веће тржишне конкуренције у тој области.

9. *Да ли су све заинтересоване стране имале прилику да се изјасне о закону*

Министарство трговине, туризма и телекомуникација спровело је јавну расправу о Нацрту закона о информационој безбедности у периоду од 3. до 23. јула 2015. године, на основу закључка Одбора за привреду и финансије Владе 05 Број: 011-7073/2015-1 од 2. јула 2015. године. Нацрт закона је објављен на сајту Министарства трговине, туризма и телекомуникација www.mtt.gov.rs и порталу еУправа www.euprava.gov.rs. У оквиру јавне расправе, одржан је округли сто у Привредној комори Србије 10. јула 2015. године, који је био веома успешан и посећен. У јавној расправи учествовали су представници државних органа, привредног сектора, академске заједнице, невладиних организација и еминентни стручњаци у овој области. Министарство је, током јавне расправе, путем Канцеларије за европске интеграције упутило Нацрт закона Европској комисији, ради прибављања експертизе.

Током јавне расправе упућени су следећи коментари и сугестије на текст Нацрта закона:

- Представник „Друштва за информатику Србије" истакао је да је потребно утврдити у закону одговорности руковаоца (оператора) ИКТ система као и да се Телу за координацију послова информационе безбедности дају јача, извршена овлашћења. У вези са наведеном примедбом, констатовано је да су Нацртом закона утврђене обавезе оператора ИКТ система од посебног значаја и њихова одговорност, посебно у случају поступања супротно закону.
  У вези примедбе да се Телу за координацију послова дају јача овлашћења, констатовано је да то Тело није нова институција, већ скуп представника органа

који су релевантни у тој области чија ће непосредна сарадња и комуникација обезбедити да се послови информационе безбедности врше ефикасно.

- Томислав Ункашевић је изнео сугестију да није јасна улога Тела за координацију послова информационе безбедности и предложио да се класификација ИКТ система од посебног значаја врши на основу обима тог ИКТ система. У вези примедбе на улогу Тела за координацију послова информационе безбедности разјашњена је улога коју исто има и значај учешћа сарадње и комуникације у функционисању истог. Примедба се класификација ИКТ система од посебног значаја врши на основу обима тог ИКТ система није усвојена, закон прецизирао који су то системи који спадају у ИКТ система од посебног значаја, при томе не улазећи у питање обима тог ИКТ система.

  Такође, именовани је истакао да Национални ЦЕРТ треба да има оперативнију улогу, и да ЦЕРТ републичких органа треба да буде на хијерархијски вишем нивоу у односу на предложено решење из Нацрта закона. Став представника радне групе, био је да се улога која је Националном и републичком ЦЕРТ-у додељена Нацртом закона адекватна и да је то модел који одговара потребама регулисања информационе безбедности у РС.

  Постављено је и питање где је и како дефинисано ко прописује критеријуме које крипотографски производ треба да испуни како би се решавало о њиховом одобравању, након чега је указано од стране представника Министарства одбране, да дефинисање процедуре и критеријума за евалуацију криптографских безбедносних решења врши Министарство одбране.

- Представник „Share фондације" предложио је да се у Тело за координацију послова информационе безбедности укључе и друга тела из привредног сектора и академске заједнице, НВО и других, што је прихваћено, те је законским решењем предложена да представници овог сектора могу да буду у саставу стручних радних група Тела за координацију.

  Од стране истог представника предложено је да се допуне и казнене одредбе што је прихваћено и извршена је допуна чланова који регулишу казнене одредбе.

  Предложено је такође да се у члану 7. дефинише достављање података безбедносним службама и министарству надлежном за послове унутрашње политике само по налогу суда, међутим овај члан закона је брисан, имајући у виду да је предметна материја већ уређена Закоником о кривичном поступку и другим прописима, тако да примедба није од утицаја.

  Сугестија, истог представника, да се подаци о инцидентима од стране оператора ИКТ система од посебног значаја не достављају само Надлежном органу, већ и Националном ЦЕРТ-у, као и да се оснажи улога ЦЕРТ није прихваћена будући да је став радне групе био да се ЦЕРТ-у не дају већа овлашћења и одговорности од оне која је предвиђена Нацртом закона.

- Дат је предлог да се термин „руковалац ИКТ система" промени, што је и прихваћена, те је термин замењен термином „оператор ИКТ система"

- Представник Националног конвента о Европској унији сматрао је да је закон уопштено написан, а нарочито код уређења ИКТ система под посебног значаја.

Поводом тога извршене су измене и допуњене су одредбе које се тичу ИКТ система од посебног значаја, тако што су дефинисане мере заштите ИКТ система којима се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности. Приликом дефинисања мера узети су у обзир међународни стандарди у области информационе безбедности, како је и сугерисано.

- Исти представник истакао је да су одредбе о Националном ЦЕРТ-у адекватно написане.
- Представник „Друштва за информациону безбедност" напоменуо је да је питању крипотозаштите и заштите од КЕМЗ-а дато превише простора у Нацрту закона, као и да би лица која обављају послове у ИКТ системима морала бити сертификована. У вези са тим, указујемо да су Нацртом закона предвиђене мере заштите које оператори ИКТ система морају предузети у односу на запослена лица.
- Представник Регистра националног Интернет домена Србије поновио је да би одредбе о достављању података безбедносним службама и МУП-у морале да се допуне у смислу да се ти подаци могу достављати уз налог суда, с тим да је члан 7. које то питање регулише брисан, из разлога који су горе наведени, па је самим тим примедба без утицаја.
- Представник „Дипло фондације" истакао је да је превише обавеза дато министарству надлежном за информационо друштво и да је потребно оснажити Национални ЦЕРТ.

  Такође је сугерисано да Тело за координацију послова информационе безбедности треба да садржи и чланове из других структура, што је и прихваћено и те је законским решењем предложено да представници овог сектора буду у саставу стручних радних група Тела за координацију.
- Представник компаније „SBB" сматрао је да Нацрт закона садржи много подзаконских аката, што је прихваћено и смањен је број подзаконских аката, тако што су уместо доношења подзаконског акта одређене ставке регулисане у самом Закону.

У складу са наведеним коментари на текст Нацрта закона, изнети током јавне расправе, најчешће се односе на неколико питања које Нацрт закона обухвата. Истакнуто је да је доношење овог закона веома значајно и да га је неопходно што пре донети, с обзиром на потребу да се информационо-комуникациони (ИКТ) системи у Републици Србији заштите на начин који ће омогућити потребан ниво информационе безбедности. Исказани су предлози за измену и прецизирање дефиниција појмова датих у Закону.

Више учесника је упућивало питање о томе на које ће се субјекте овај закон односити, да ли само на државне органе, или и на привредне субјекте. Представници Министарства су на округлом столу указали да су чланом 8. Нацрта закона о информационој безбедности обухваћени ИКТ системи које користе државни органи, али и субјекти у приватном сектору.

Коментарисано је оснивање Тела за координацију послова информационе безбедности, које се оснива у складу са чланом 62. Закона о државној управи („Службени гласник РС"

број 79/05, 101/07, 95/10 и 99/14) у циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, и наведено је да је потребно овом телу дати извршна овлашћења, као и да би, поред државних органа, у његов рад требало укључити представнике привреде, невладиних организација и других субјеката, што је прихваћено и те је законским решењем предложено да представници овог сектора буду у саставу стручних радних група овог Тела.

У вези са чланом 6, којим се прописује да су руковаоци свих ИКТ система одговорни за предузимање одговарајућих мера информационе безбедности, напоменуто је да је одредба сувише уопштена и да није регулисана одговорност за њено кршење, те је та одредба закона брисана.

У погледу члана 7, којим се предвиђа обавеза достављања података од значаја за информациону безбедност, који су службама безбедности и министарству надлежном за унутрашње послове потребни при обављању послова из њихове надлежности у складу са законом, сугерисано је да је неопходно извршити прецизирање тог члана, односно да се конкретно дефинише који се подаци достављају, као и да се предвиди да подаци могу да се траже на основу одлуке суда. Међутим, члан 7. је брисан јер је обавеза достављања података безбедоносним службама и министарству задуженом за унутрашње послове већ регулисана Закоником о кривичном поступку и Законом о електронским комуникацијама.

Такође, наведено је да се члан 11, којим се дефинише поверавање ИКТ система трећим лицима треба детаљније уредити, пре свега по питања регулисања односа између оператора ИКТ система од јавног значаја и трећих лица у погледу евентуалне одговорности за штету. Указујемо да је питање накнаде штете уређено општим прописима који се сходно примењују.

У погледу одредаба закона о Националном центру за превенцију безбедносних ризика у ИКТ системима (Националном ЦЕРТ-у), више учесника је сугерисало да би Национални ЦЕРТ требао да има снажнија овлашћења, у смислу да му је потребно дати оперативне надлежности. Међутим како се Национални ЦЕРТ први пут оснива овим законом идеја је да његова улога буде са тзв. меким овлашћењима, те ће се у пракси потом утврдити да ли је потребно његову улогу учинити јачом или не.

Учесници сматрају да је предвиђено мало казнених одредби у Закону и да би требало прописати више прекршајних казни, што је прихваћено и извршене су измене казнених одредби у Нацрту закона.

Истакнуте су примедбе на бројност подзаконских аката који треба да се донесу на основу закона, као и на, како се сматра, предуге рокове за доношење подзаконских аката, који износе 12 месеци од дана на ступања на снагу овог закона. Прихваћена је сугестија о смањењу броју подзаконских аката, те је број истих смањен тако што су уместо доношења подзаконског акта одређене ставке регулисане у самом закону, међутим рок од 12 месеци за доношење подзаконских аката није мењан, будући да је услед комплексности материје која се регулише подзаконским актима процењено да је потребан рок од 12 месеци за доношење истих.

10. Које ће се мере током примене закона предузети да би се остварило оно што се доношењем закона намерава

Институционалне мере потребно је предузети у следећим органима:

- Надлежни орган (министарство надлежно за послове информационе безбедности, односно Министарство трговине, туризма и телекомуникација)

  У оквиру Надлежног органа, односно Министарства трговине, туризма и телекомуникација потребно је да се образује унутрашња организациона јединица за информациону безбедност и у њој запосли 11 државних службеника услед чега би укупни годишњи расходи за запослене износили 13.420.000 динара, а годишњи расходи за коришћење услуга и роба (службена путовања, обуке, услуге по уговору итд) 5.000.000 динара. У оквиру средстава за рад нове организационе јединице, поред основног канцеларијског опремања рачунарском опремом, биће потребна опрема за спровођење мера заштите тајних података, као и успостављање информационог система за пријем и обраду обавештења о инцидентима и инспекцијски надзор уз примену одговарајућих мера заштите ИКТ система, за шта се процењује да је у 2016. години потребно 40.000.000 динара, а у 2017. години 20.000.000 динара.

  На предлог министарства надлежног за послове информационе безбедности формира се и Тело за координацију послова информационе безбедности. Наведено Тело образује Влада 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, као координационо тело Владе. Образовање Тела за координацију информационе безбедности не изискује додатне трошкове.

- Министарство надлежно за послове одбране (Министарство одбране)

  Решења садржана у Предлогу закона о информационој безбедности која се тичу Министарстава одбране односе се на добијање националне надлежности за одговарајуће послове из области информационе безбедности – „одобравање криптографских производа“, „дистрибуција криптоматеријала“ и „заштиту од компромитујућег електромагнетског зрачења“ које би извршавала наменска установа у оквиру овог министарства.

  Да би наведена установа могла успешно да извршава послове и задатке из надлежности Министарства одбране које предвиђа Предлог закона о информационој безбедности, потребно је предузети мере за достизање недостајућих способности, а које се тичу обезбеђења додатних људских ресурса, опремања одговарајућом опремом за мерење компромитујућег електромагнетног зрачења (КЕМЗ) и специјалистичког оспособљавања персонала. Без наведеног, Министарство одбране не би било у могућности да успешно реализује надлежности предвиђене Предлогом закона.

У складу са наведеним, за потребе реализације закона потребна су Министарству одбране средства за расходе запослених у износу од 60.580.000 динара у 2016. години и 71.360.000 у 2017. години. Ради додатног опремања, пре свега за набавку опреме за детекцију и заштиту од КЕМЗ, која се може набавити само из иностранства и под одређеним условима неопходна новчана средства износе 142.847.000 динара у 2016. години и 140.000.000 динара 2017. години, док је за коришћење услуга и роба потребно у наредне две године по 18.919.000 динара.

- Управа за заједничке послове републичких органа

  Финансијска средства потребна Управи за заједничке послове, у наредне две године за реализацију закона, односно за основна средства износе укупно 132.138.000 динара, односно 82.138.000 динара у 2016. години и 50.000.000 динара у 2017. години. Будући да овај орган располаже људским капацитетима, средстава за те намене нису предвиђена.

- Регулаторна агенција за електронске комуникације
  Финансијска средства потребна за успостављање капацитета за обављање послова Националног ЦЕРТ-а у оквиру РАТЕЛ-а процењују се да су слична средствима која су потребна Министарству трговине, туризма и телекомуникација за послове надлежног органа за информациону безбедност и да износе око 100 милиона динара за период од наредне две године.

- Нерегулаторне мере

  Након усвајања Закона, министарство надлежно за послове информационе безбедности планира упознавање јавности са законом, како у оквиру својих редовних информативних кампања, тако и путем наменских округлих столова и других видова информисања којима ће се грађанима Републике Србије пружити неопходне информације о решењима која предвиђа закон. Такође, Предлогом закона је предвиђено да је једна од надлежности Национални ЦЕРТ-а да 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.

Ради извршавања Предлога закона о информационој безбедности (у даљем тексту: Предлог закона), предвиђено је да Влада донесе следеће акте:

- Одлука о образовању Тела за координацију послова информационе безбедности (на основу члана 5. Предлога закона)
- Уредба о ближем уређењу Листе послова и делатности ИКТ система од посебног значаја (на основу члана 6. Предлога закона)
- Уредба о ближим условима за мере заштите ИКТ система од посебног значаја (на основу члана 7. Предлога закона)
- Уредба о ближем садржају акта о безбедности ИКТ система, начину интерне провере ИКТ система и садржају извештаја о провери ИКТ система (на основу члана 8. Предлога закона)

- Уредба о усвајању Листе инцидената и начину обавештавања о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности (на основу члана 11. Предлога закона)
- Уредба о ближим условима за проверу компромитујућег електромагнетног зрачења (КЕМЗ) и начина процене ризика од отицања података путем КЕМЗ (на основу члана 22. Предлога закона)
- Уредба о техничким условима 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 (на основу члана 23. Предлога закона)
- Уредба о ближим условима које морају да испуњавају криптографски производи који се користе за заштиту преноса и чувања података који су одређени као тајни (на основу члана 24. Предлога закона)
- Уредба о садржају захтева за издавање одобрења за криптографски производ, условима за издавање одобрења за криптографски производ, начину издавања одобрења, накнади за издавање одобрења и садржају регистра издатих одобрења за криптографски производ (на основу члана 25. Предлога закона)
- Уредба о ближим условима за вођење регистара криптографских производа, криптоматеријала, правила и прописа и кадра криптозаштите које воде самостални руковаоци ИКТ система (на основу члана 27. Предлога закона).

Предлогом закона предвиђено је да министарство надлежно за послове информационог друштва доноси следеће подзаконске акте:

- Правилник о ближим условима за упис у евиденцију посебних центара за превенцију безбедносних ризика у ИКТ системима (на основу члана 17. Предлога закона)

Према члану 32. Предлога закона, подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона.

ИЗЈАВА О УСКЛАЂЕНОСТИ ПРОПИСА СА ПРОПИСИМА ЕВРОПСКЕ УНИЈЕ

1. Овлашћени предлагач прописа: Влада

Обрађивач: Министарство трговине, туризма и телекомуникација

2. Назив прописа

Предлог закона о информационој безбедности
Draft Law on Information Security

3. Усклађеност прописа с одредбама Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране („Службени гласник РС", број 83/08) (у даљем тексту: Споразум), односно с одредбама Прелазног споразума о трговини и трговинским питањима између Европске заједнице, са једне стране, и Републике Србије, са друге стране („Службени гласник РС", број 83/08) (у даљем тексту: Прелазни споразум):

а) Одредба Споразума и Прелазног споразума која се односе на нормативну садржину прописа

Наслов VII „Политике сарадње", члан 105. Информационо друштво - Споразум о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије са друге стране.

б) Прелазни рок за усклађивање законодавства према одредбама Споразума и Прелазног споразума

Три године.

в) Оцена испуњености обавезе које произлазе из наведене одредбе Споразума и Прелазног споразума

Испуњава у потпуности.

г) Разлози за делимично испуњавање, односно неиспуњавање обавеза које произлазе из наведене одредбе Споразума и Прелазног споразума

/

д) Веза са Националним програмом за усвајање правних тековина Европске уније

Национални програм за усвајање правних тековина Европске уније (2014-2018), Прилог А – План усклађивања законодавства Републике Србије са правним тековинама Европске уније, 3.10. Информационо друштво и медији, 3.10.2. Информационо друштво, Редни број 28, Шифра план. прописа: 2014-345. План законодавног поступка: 2015/VI

4. Усклађеност прописа са прописима Европске уније:
а) Навођење одредби примарних извора права Европске уније и оцене усклађености са њима

Наслов V, Поглавље I, члан 67. и 73. Уговора о функционисању Европске уније. Предлог закона о информационој безбедности је потпуно усклађен са наведеним члановима.

б) Навођење секундарних извора права Европске уније и оцене усклађености са њима

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / JOIN/2013/01 final */* - ПОТПУНО УСКЛАЂЕНО

в) Навођење осталих извора права Европске уније и усклађеност са њима

/

г) Разлози за делимичну усклађеност, односно неусклађеност

/

д) Рок у којем је предвиђено постизање потпуне усклађености прописа са прописима Европске уније

/

5. Уколико не постоје одговарајуће надлежности Европске уније у материји коју регулише пропис, и/или не постоје одговарајући секундарни извори права Европске уније са којима је потребно обезбедити усклађеност, потребно је образложити ту чињеницу. У овом случају, није потребно попуњавати Табелу усклађености прописа. Табелу усклађености није потребно попуњавати и уколико се домаћим прописом не врши пренос одредби секундарног извора права Европске уније већ се искључиво врши примена или спровођење неког захтева који произилази из одредбе секундарног извора права (нпр. Предлогом одлуке о изради стратешке процене утицаја биће спроведена обавеза из члана 4. Директиве 2001/42/ЕЗ, али се не врши и пренос те одредбе директиве).
У области коју закон уређује није донет пропис (директива) Европске уније, услед чега није било могуће сачињавање табеле усклађености. Приликом израде Предлог закона о информационој безбедности, уважена су решења из Предлога директиве о мрежној и информационој безбедности (*Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013/0027 (COD))*. Такође, поштована су начела из Стратегије информационе безбедности Европске уније (*JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace /* JOIN/2013/01 final */,)*.
С обзиром да је предлог горе наведене директиве још увек у фази припреме и усаглашавања на нивоу ЕУ, и да није важећи акт, табела усклађености није израђена.

6. Да ли су претходно наведени извори права Европске уније преведени на српски језик?

/

7. Да ли је пропис преведен на неки службени језик Европске уније?
/

8. Учешће консултаната у изради прописа и њихово мишљење о усклађености

Текст Нацрта закона о информационој безбедности послат је Европској комисији, путем Канцеларије за европске интеграције, ради давања експертизе. Имајући у виду да пропис Европске уније из ове области још увек није донет, представници Европске комисије обавестили су Канцеларију за европске интеграције да анализа усклађености Нацрта закона о информационој безбедности пре доношења директиве није целисходна.