АНАЛИЗА ЕФЕКАТА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

1. *Проблеми које акт треба да реши*

Закон о информационој безбедности 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. 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 одроварајући 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 Нацрта 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 инстиуција, 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 се класификација ИКТ система од посебног значаја врши на основу обима тог ИКТ система није усвојена, закон предизирао 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 Националеном и републичком ЦЕРТ-у додељена Нацртом закона адекватна и да је то модел који одговара потребана регулисања информационе безбедности у РС.

  Постављено је и питање где је и како дефинисано ко проприсује 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.
- Представаник „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“
- Представаник Националног конвента о Еврошској 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 безбености, како је и сугерисано.

- Исти представник истакао је да су одредбе о Националном ЦЕРТ-у адекватно написане.
- Представаник „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.
- Представаник 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.
- Представаник „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 инфорамционе безбеденост 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 раскоди 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 Нацрту 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 Нацрт 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 Нацртом 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 комуникацијеФинансијска 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 предивђа закон. Такође, Нацртом 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 Нацрта закона о информационој безбедности (у даљем тексту: Нацрт закона), предвиђено је да Влада донесе следеће акте:

- Одлука о образовању Тела за координацију послова информационе безбедности (на основу члана 5. Нацрта закона)
- Уредба о ближем уређењу Листе послова и делатности ИКТ система од посебног значаја (на основу члана 6. Нацрта закона)
- Уредба о ближим условима за мере заштите ИКТ система од посебног значаја(на основу члана 7. Нацрта 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. Нацрта закона)
- Уредба о начину рада Националног центра за превенцију безбедносних ризика у ИКТ системима (на основу члана 14. Нацрта закона)

- Уредба о ближим условима за проверу компромитујућег електромагнетног зрачења (КЕМЗ) и начина процене ризика од отицања података путем КЕМЗ (на основу члана 21. Нацрта 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 22. Нацрта 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 23. Нацрта 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 24. Нацрта 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 26. Нацрта закона).

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

- Правилник 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. Нацрта закона)
- Правилник о ближим условима за упис у евиденцију посебних центара за превенцију безбедносних ризика у ИКТ системима (на основу члана 16. Нацрта закона)

Нацртом закона предвиђено је да министарство надлежно за послове одбране доноси:

- Правилник о додатку на основну плату запосленима који обављају послове информационе безбедности, а који се односе на одобравање криптографских производа, дистрибуцију криптоматеријала и заштиту од КЕМЗ (на основу члана 27. Нацрта закона).

Према члану 35. Нацрта закона, подзаконска акта предвиђена овим законом донеће се у року од 12 месеци од дана ступања на снагу овог закона.