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”, бр. 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 чиниоца, 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 Нацрта закона о информационој безбедности (у даљем тексту: Нацрт 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 у складу са рачунарским програмом и рачунарски подаци који се похрањују, обрађују, претражују или преносе помоћу средстава, а у сврху њиховог рада, употребе, заштите или одржавања.

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.

Нацртом закона се предвиђа да министарство надлежно за послове информационог друштва (у даљем тексту: Надлежни орган) је орган државне управе надлежан за безбедност ИКТ система. Законом о министарствима („Службени гласник РС”, број 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 Нацрт 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.

Нацрт закона уређује ИКТ системе од посебног значаја и предвиђа обавезе руковаоца ИКТ система од посебног значаја и одговорност руковаоца ИКТ 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 надлежног 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. Нацртом закона предвиђено је да Влада, на предлог министарства надлежног за послове информационог друштва, ближе уређује листу послова и делатности код којих ће постојати обавеза примене адекватних мера у складу са законом.

Нацртом закона 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, а послове Националног ЦЕРТ-а опредељује у надлежност Регулаторне агенција за електронске комуникације и поштанске услуге.

Нацрт 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 руковаоца.

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

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

Нацрт закона садржи посебну главу о криптобезбедности и заштити од компромитујућег електронског зрачења (КЕМЗ). Законом 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. Законом 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 Нацрту закона да послове инспекције за информациону безбедност обавља министарство надлежно за послове информационог друштва преко инспектора за информациону безбедност.

III. ОБЈАШЊЕЊЕ ОСНОВНИХ ПРАВНИХ ИНСТИТУТА И ПОЈЕДИНАЧНИХ РЕШЕЊА

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

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

Члан 3. садржи начела Нацрта 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.

Чланом 6. се прописује одговорност руковаоца свих ИКТ система у Републици Србији за предузимање одговарајућих мера 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. Ставом 2. овог члана прописано је да ближе услове за мере из става 1. овог члана уређује Влада на предлог Надлежног органа, уважавајући међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

Чланом 7. је прописана обавеза руковаоца ИКТ система да на захтев безбедносних служби и министарства надлежног за унутрашње послове, стави на располагање податке из области информационе безбедности, који су службама безбедности и министарству надлежном за унутрашње послове потребни при обављању послова из њихове надлежности у складу са законом.

У члану 8. су утврђени ИКТ системи од посебног значаја, а ставом 2. истог члана прописано је да Влада, на предлог министарства надлежног за послове информационог друштва, ближе уређује листу послова и делатности из става 1. овог члана.

У члану 9. утврђују се дужност руковаоца 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 и да ближе услове за мере из става 1. овог члана уређује Влада на предлог Надлежног органа, уважавајући међународне стандарде и стандарде који се примењују у одговарајућим областима рада.

У члану 10. се уређује обавеза руковалаца 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 интерне провере ИКТ система и садржај извештаја о интерној провери ИКТ система уређује Влада на предлог Надлежног органа.

Члан 11. регулише поверавање активности у вези са ИКТ системом од посебног значаја трећим лицима, у ком случају се прописује обавеза руковаоцу да уреди однос са тим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом.

Чланом 12. прописан је изузетак од одредаба члана 11, уколико су активности у вези са ИКТ системом поверене прописом, да се тим прописом могу другачије уредити обавезе и одговорности руковаоца ИКТ система од посебног значаја у вези поверених активности.

Чланом 13. прописана је обавеза руковаоца 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 14. се прописује овлашћење Надлежног органа да испита да ли руковаоци ИКТ система од посебног значаја доследно спроводе обавезе прописане од чл. 8. до чл. 13. овог закона, као и право да захтева да доставе све неопходне информације о свом ИКТ систему, интерне акте о безбедности ИКТ система и извештаје о интерној провери ИКТ система, а ставом 3. овог члана је прописано да се ове одредбе не примењују на ИКТ системе самосталних руковаоца и ИКТ системе за рад са тајним подацима.

Чланом 15. 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 Европске полицијске канцеларије (ЕУРОПОЛ).

Чланом 16. 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 агенција за електронске комуникације и поштанске услуге за послове Националног ЦЕРТ-а.

Чланом 17. 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 18. прописује се надзор над радом Националног ЦЕРТ-а који врши Надлежни орган.

Чланом 19. 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 20. 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 руковаоца, у оквиру Управе за заједничке послове републичких органа.

Чланом 21. прописује обавезу самосталних руковаоца ИКТ система да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима.

Чланом 22. прописано је да послове информационе безбедности који се односе на криптобезбедност и КЕМЗ обавља министарство надлежно за послове одбране.

Чланом 23. прописани су послови Министарства надлежног за послове одбране у области криптобезбедности и КЕМЗ.

Чланом 24. уређује се заштита од компромитујућег електромагнетног зрачења.

Чланом 25. уређује се обавеза примене методе криптозаштите.

Чланом 26. 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 27. уређује се издавање одобрења за криптографски производ.

Чланом 28. прописано је да опште одобрење за коришћење криптографских производа имају самостални руковаоци ИКТ система.

Чланом 29. прописано је да самостални руковаоци 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 ст. 1. овог члана.

У члану 30. се уређују услови за унутрашњу организацију и прописује оббавеза руковаоца ИКТ система за рад са тајним подацима и самостални руковаоци ИКТ система да формирају организационе јединице за информациону безбедност.

У члану 31. прописани су послови инспекције за информациону безбедност која врши надзор над применом овог закона и радом руковаоца од посебног значаја, осим самосталних руковаоца ИКТ система и система за рад са тајним подацима.

У члану 32. прописан је инспекцијски надзор самосталних руковаоца ИКТ система.

У члану 33. прописана су овлашћења инспектора за информациону безбедност.

У члану 34. прописане су казнене одредбе, предвиђене су новчане казне за одговорна лица која прекрше одредбе закона.

У члану 35. прописани су рокови за доношење подзаконских аката.

Члан 36. Нацрта 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.