ПРЕДЛОГ

З А К О Н

О ИЗМЕНАМА И ДОПУНАМА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

Члан 1.

У Закону о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17), у члану 2. став 1. тачка 1) подтачка (3) реч: „похрањује” замењује се речима: „воде, чувају”.

После подтачке (4) додаје се подтачка (5), која гласи:

„(5) све типове системског и апликативног софтвера и софтверске развојне алате.”.

У тачки 2) речи: „орган јавне власти или организациона јединица органа јавне власти” замењују се речима: „орган власти или организациона јединица органа власти”.

Тачка 11) мења се и гласи:

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

После тачке 11) додаје се тачка 11а), која гласи:

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

Тачка 15) мења се и гласи:

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

Тачка 24) мења се и гласи:

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

После тачке 24) додају се тач. 25) и 26), које гласе:

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

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

Члан 2.

После члана 3. додаје се члан 3а, који гласи:

„Обрада података о личности

Члан 3а

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

Члан 3.

У члану 5. став 1. после речи: „Генералног секретаријата Владе” додају се речи: „Народне банке Србије”, а речи: „ЦЕРТ-а републичких органа и Националног ЦЕРТ-а” замењују се речима: „Центра за безбедност ИКТ система у органима власти и Националног центра за превенцију безбедносних ризика у ИКТ системима.”

У ставу 2. речи: „органа јавне власти” замењују се речима: „органа власти”.

Члан 4.

Члан 6. мења се и гласи:

„ИКТ системи од посебног значаја

Члан 6.

ИКТ системи од посебног значаја су системи који се користе:

1) у обављању послова у органима власти;

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

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

(1) енергетика:

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

(2) саобраћај:

- железнички, поштански, водни и ваздушни саобраћај;

(3) здравство:

- здравствена заштита;

(4) банкарство и финансијска тржишта:

- послови финансијских институција;
- послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама;

- послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;

(5) дигитална инфраструктура:

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

(6) добра од општег интереса:

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

(7) услуге информационог друштва:

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

(8) остале области:

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

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

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

Члан 5.

После члана 6. додају се чл. 6а и 6б, који гласе:

„Обавезе оператора ИКТ система од посебног значаја

Члан 6а

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

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

2) предузме мере заштите ИКТ система од посебног значаја;

3) донесе акт о безбедности ИКТ система;

4) врши проверу усклађености примењених мера заштите ИКТ система са актом о безбедности ИКТ система и то најмање једном годишње;

5) уреди однос са трећим лицима на начин који обезбеђује предузимање мера заштите тог ИКТ система у складу са законом, уколико

поверава активности у вези са ИКТ системом од посебног значаја трећим лицима;

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

7) достави статистичке податке о инцидентима у ИКТ систему.

Евиденција оператора ИКТ система од посебног значаја

Члан 6б

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

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

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

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

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

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

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

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

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

Члан 6.

У члану 7. став 2. реч: „минимизација” замењује се речју: „смањење”.

У ставу 3. тачка 11) реч: „односно” замењује се речју: „и”.

У тачки 23) речи: „питања информационе безбедности” замењују се речима: „испуњење захтева за информациону безбедност”.

Члан 7.

Члан 11. мења се и гласи:

„Обавештавање о инцидентима

Члан 11.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Члан 8.

После члана 11. додају се чл. 11а и 11б, који гласе:

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

Члан 11а

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

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

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

3) инциденте који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;

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

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

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

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

Достављање статистичких података о инцидентима

Члан 11б

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

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

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

Члан 9.

У члану 12. став 1. тачка 1) речи: „високи ризици” замењују се речју: „високоризични”.

Члан 10.

Изнад члана 13. додаје се назив члана, који гласи: „Самостални оператори ИКТ система”.

Члан 11.

После члана 13. додаје се члан 13а, који гласи:

„Сходна примена одредаба о самосталним операторима ИКТ система

Члан 13а

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

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

Члан 12.

У називу члана 14. и у ставу 1. речи: „Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ)” замењују се речима: „Национални ЦЕРТ”.

Члан 13.

Члан 15. мења се и гласи:

„Делокруг Националног ЦЕРТ-а

Члан 15.

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

1) прати стање о инцидентима на националном нивоу,

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

3) реагује по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и по пријавама физичких и правних лица, тако што пружа савете и препоруке на основу расположивих информација о инцидентима и предузима друге потребне мере из своје надлежности на основу добијених сазнања,

4) континуирано израђује анализе ризика и инцидената,

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

6) води евиденцију Посебних ЦЕРТ-ова,

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

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

Обрада података о лицу из става 1. тачка 3) овог члана обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

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

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

У циљу обезбеђивања континуитета рада, Национални ЦЕРТ треба да:

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

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

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

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

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

1) управљање и санирање ризика и инцидената;

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

Члан 14.

После члана 15. додаје се члан 15а, који гласи:

„Сарадња ЦЕРТ-ова у Републици Србији

Члан 15а

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

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

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

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

Члан 15.

Изнад члана 16. додаје се назив члана који гласи: „Надзор над радом Националног ЦЕРТ-а”.

Члан 16.

У члану 17. став 2. после речи: „правног лица” додају се речи: „са седиштем на територији Републике Србије”.

У ставу 4. после речи: „поште” додаје се запета и речи: „а у сврху ангажовања посебних ЦЕРТ-ова у случају безбедносних ризика и инцидената у ИКТ системима.”.

Став 5. мења се и гласи:

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

Члан 17.

Члан 18. мења се и гласи:

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

„Члан 18.

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

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

Послови ЦЕРТ-а органа власти обухватају:

1) заштиту Јединствене информационо-комуникационе мреже електронске управе;

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

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

Члан 18.

Изнад члана 19. додаје се назив члана који гласи: „ЦЕРТ самосталног оператора ИКТ система”.

У ставу 2. речи: „републичких органа” замењују се речима: „органа власти”.

Члан 19.

После члана 19. додаје се члан 19а, који гласи:

„Заштита деце при коришћењу информационо-комуникационих технологија

Члан 19а

Надлежни орган предузима превентивне мере за безбедност и заштиту деце на интернету, као активности од јавног интереса, путем едукације и информисања деце, родитеља и наставника о предностима, ризицима и начинима безбедног коришћења интернета, као и путем јединственог места за

пружање савета и пријем пријава у вези безбедности деце на интернету, и упућује пријаве надлежним органима ради даљег поступања.

Оператор електронских комуникација који пружа јавно доступне телефонске услуге дужан је да омогући свим претплатницима услугу бесплатног позива према јединственом месту за пружање савета и пријем пријава у вези безбедности деце на интернету.

У случају да наводи из пријаве упућују на постојање кривичног дела, на повреду права, здравственог статуса, добробити и/или општег интегритета детета, на ризик стварања зависности од коришћења интернета, пријава се прослеђује надлежном органу власти ради поступања у складу са утврђеним надлежностима.

Надлежни орган је овлашћен да врши обраду података о лицу које се обрати Надлежном органу у складу са законом који уређује заштиту података о личности и другим прописима.

Обрада података о лицу из става 4. овог члана обухвата име, презиме и број телефона и/или адресу електронске поште и врши се у сврху евидентирања поднетих пријава, информисања подносиоца пријаве о статусу предмета и, у случају потребе, упућивања пријаве надлежним органима ради даљег поступања, у складу са законом.

Подаци о личности из става 5. овог члана чувају се у роковима предвиђеним прописима који уређују канцеларијско пословање.

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

1) буде опремљен са одговарајућим системима за пријем пријава;

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

3) обезбеди инфраструктуру чији је континуитет осигуран.

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

Члан 20.

Члана 30. мења се и гласи:

„Члан 30.

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

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

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

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

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

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

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

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

Члан 21.

Члан 31. мења се и гласи:

„Члан 31.

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

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

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

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

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

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

Члан 22.

Подзаконски акти из чл. 4, 7. и 19. овог закона донеће се у року од шест месеци од дана ступања на снагу овог закона.

Подзаконски акти из чл. 5. и 8. овог закона донеће се у року од три месеца од дана ступања на снагу овог закона.

Члан 23.

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

Закон о информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17) донет је у јануару 2016. године и уредио је мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и надлежне органе за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите. Овај закон донет је у периоду пре усвајања Директиве ЕУ о мерама за висок ниво безбедности мрежних и информационих система у Европској унији број 2016/1148 (НИС директива), која је усвојена у јулу 2016. године. Иако је био донет пре усвајања ове директиве, Закон је у великој мери усклађен са овом директивом, будући да садржи решења која одговарају одредбама наведене директиве. Изради измена и допуна Закона о информационој безбедности приступило се првенствено из два разлога: први је преостало усклађивање са одредбама НИС директиве ради постизања потпуне усаглашености, а други је унапређење постојећих законодавних решења на бази потреба утврђених на основу досадашње примене закона.

Ради преосталих усклађивања са НИС директивом, у Предлогу закона извршене су следеће измене и допуне:

- допуна области у којима се користе ИКТ системи од посебног значаја, и то област дигиталне инфраструктуре и услуга информационог друштва (члан 6.);
- одређено је да се пре јавног објављивања обавештења о инциденту од стране надлежног органа изврше претходне консултације са оператором ИКТ система од посебног значаја који је доставио обавештење о инциденту (члан 11.);
- предвиђена је допуна одредаба о Националном ЦЕРТ-у које се односе на његову надлежност и потребне капацитете (члан 15.).

Током примене закона утврђена је потреба за изменом и допуном одређених норми, у циљу ефикаснијег спровођења закона у пракси. Сходно томе, Предлогом закона предвиђено је следеће:

- укључивање Народне банке Србије у рад Тела за координацију послова информационе безбедности (члан 5.);
- допуна области у којима се користе ИКТ системи од посебног значаја (производња и снабдевање хемикалијама, члан 6.);
- таксативно су набројане обавезе ИКТ система од посебног значаја (члан 6а);
- успостављање Евиденције оператора ИКТ система од посебног значаја (члан 6б);
- дефинисан је начин обавештавања о инцидентима који значајно угрожавају информациону безбедност преко портала Надлежног

органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима (члан 11.);
- обавеза Народне банке Србије и РАТЕЛ-а да добијена обавештења о инциденту проследе Надлежном органу (члан 11.);
- достављање обавештења о инциденту који је повезан са значајним нарушавањем информационе безбедности, које има или може имати за последицу угрожавање националне безбедности, Безбедносно-информативној агенцији (члан 11.);
- дефинисани су инциденти који треба да се пријаве, а који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11а);
- одређена је обавеза ИКТ система од посебног значаја да достављају статистичке податке о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11б);
- дефинисана је сарадња ЦЕРТ-ова у Републици Србији (члан 15а);
- додате су одредбе о заштити при коришћењу информационо-комуникационих технологија (члан 19а).

Наведене измене закона допринеће бољој повезаности свих релевантних актера у области информационе безбедности, будући да се Предлогом закона предвиђа успостављање евиденције ИКТ система од посебног значаја. На тај начин Надлежни орган и Национални ЦЕРТ имаће могућност интензивније сарадње са свим операторима ИКТ система од посебног значаја, нарочито у случају када се дешава инцидент, али у смислу пружања подршке, препоруке и савета за заштиту ИКТ система од посебног значаја.

Значајно унапређење лежи и у чињеници да је Надлежни орган успоставио Јединствени систем за пријем обавештења о инцидентима, тако да их ИКТ системи од посебног значаја обавештења могу прослеђивати преко портала Надлежног органа и Националног ЦЕРТ-а. Ово решење доприноси ефикасности пријављивања инцидената, као и потпуној информисаности свих релевантних учесника (Надлежни орган, Национални ЦЕРТ) који потом могу да учествују у отклањању инцидента.

Такође, Предлог закона предвиђа одредбе о Националном ЦЕРТ-у које се односе на јачање капацитета Националног ЦЕРТ-а, како би се успоставило благовремена и ефикасна подршка у случају инцидента, а за такву врсту подршке неопходно је стручно особље, одговарајућа инфраструктура у смислу опреме и просторија за рад, чије обезбеђивање је предвиђено Предлогом закона. Како Национални ЦЕРТ има и улогу превенције у области информационе безбедности, предвиђено је достављање статистичких података од стране ИКТ система од посебног значаја на бази којих ће Национални ЦЕРТ имати могућност израде адекватних анализа у области информационе безбедности и на основу чега ће припремати препоруке и савете за мере заштите у овој области.

С обзиром да је препозната потреба за континуираном сарадњом ЦЕРТ-ова у Републици Србији, предвиђене су одредбе којима се дефинише ова сарадња кроз организацију редовних заједничких састанака, а посебно у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Имајући у виду важност питања безбедности на интернету, Предлогом закона дефинисане су одредбе којима се предвиђају мере за безбедност и заштиту на интернету, као и генерално приликом коришћења информационо-комуникационих технологија.

III. ОБЈАШЊЕЊЕ ОСНОВНИХ ПРАВНИХ ИНСТИТУТА И ПОЈЕДИНАЧНИХ РЕШЕЊА

У члану 1. врше се измене и допуне појмова у Закону.

Чланом 2. додаје се нови члан 3а који се односи на обраду података о личности приликом вршења надлежности и испуњења обавеза из овог закона.

Чланом 3. допуњује се члан 5. Закона тако што се предвиђа укључење Народне банке Србије у рад Тела за координацију послова информационе безбедности.

У члану 4. мења се члан 6. Закона који се односи на одређивање ИКТ система од посебног значаја у Републици Србији.

Чланом 5. додају се нови чл. 6а и 6б који се односе на дефинисање обавеза ИКТ система од посебног значаја и на Евиденцију оператора ИКТ система од посебног значаја.

Чланом 6. врше се прецизирања појединих термина који се односе на мере заштите ИКТ система од посебног значаја.

У члану 7. мења се члан 11. Закона којим се уређује обавештавање о инцидентима који могу да имају значај на нарушавање информационе безбедности.

У члану 8. додају се нови чл. 11а и 11б, који уређују значајне инциденте које треба пријавити, као и достављање статистичких података о инцидентима Националном ЦЕРТ-у.

У члану 9. врши се језичко прилагођавање у члану 12. Закона.

Чланом 10. додаје се назив члана 13. који гласи: „Самостални оператори ИКТ система”.

Чланом 11. предвиђа се сходна примена одредаба о самосталним операторима ИКТ система на Народну банку Србије.

Чланом 12. се мења члан 14. из правнотехничких разлога, будући да се пун назив Националног центра за превенцију безбедносних ризика у ИКТ системима и скраћење његовог назива већ појављују у члану 6б Закона.

Чланом 13. мења се члан 15. који уређује надлежности Националног ЦЕРТ-а.

Чланом 14. додаје се члан 15а којим се уређује сарадња ЦЕРТ-ова у Републици Србији.

Чланом 15. се додаје се назив члана 16. „Надзор над радом Националног ЦЕРТ-а”.

Чланом 16. врши се промена члана 17. тако да одређује да Национални ЦЕРТ доноси Правилник о ближим условима за упис у Евиденцију Посебних центара за превенцију безбедносних ризика у ИКТ системима.

Чланом 17. врши се измена у члану 18. који се односи на промену назива досадашњег ЦЕРТ-а републичких органа.

Чланом 18. допуњује се члан 19. Закона тако што се додаје назив који гласи: „ЦЕРТ самосталног оператора ИКТ система”.

Чланом 19. додаје се нови члан 19а који регулише заштиту при коришћењу информационо-комуникационих технологија.

Чл. 20. и 21. мењају се и допуњују прекршајне одредбе Закона.

Чланом 22. утврђују се рокови за доношење подзаконских аката.

Чланом 23. утврђује се ступање на снагу овог закона.

IV. СРЕДСТВА ПОТРЕБНА ЗА СПРОВОЂЕЊЕ ЗАКОНА

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

V. ПРЕГЛЕД ОДРЕДАБА КОЈЕ СЕ МЕЊАЈУ, ОДНОСНО ДОПУЊУЈУ

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~~ ВОДЕ, ЧУВАЈУ, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања;

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

(5) СВЕ ТИПОВЕ СИСТЕМСКОГ И АПЛИКАТИВНОГ СОФТВЕРА И СОФТВЕРСКЕ РАЗВОЈНЕ АЛАТЕ.

2) оператор ИКТ система је правно лице, ~~орган јавне власти или организациона јединица органа јавне власти~~ ОРГАН ВЛАСТИ ИЛИ ОРГАНИЗАЦИОНА ЈЕДИНИЦА ОРГАНА ВЛАСТИ који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;

3) информациона безбедност представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;

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

5) интегритет значи очуваност изворног садржаја и комплетности податка;

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

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

8) непорецивост представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;

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

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

11) ~~*инцидент* је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност~~

11) ИНЦИДЕНТ ЈЕ СВАКИ ДОГАЂАЈ КОЈИ ИМА СТВАРАН НЕГАТИВАН УТИЦАЈ НА БЕЗБЕДНОСТ МРЕЖНИХ И ИНФОРМАЦИОНИХ СИСТЕМА;

11а) ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА ЈЕ ИНФОРМАЦИОНИ СИСТЕМ У КОЈИ СЕ УНОСЕ ПОДАЦИ О ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ;

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

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

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

15) ~~*орган 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 покрајина или јединица локалне самоуправе, као и правно лице које се претежно, односно у целини финансира из буџета;~~

15) ОРГАН ВЛАСТИ ЈЕ ДРЖАВНИ ОРГАН, ОРГАН АУТОНОМНЕ ПОКРАЈИНЕ, ОРГАН ЈЕДИНИЦЕ ЛОКАЛНЕ САМОУПРАВЕ, ОРГАНИЗАЦИЈА И ДРУГО ПРАВНО ИЛИ ФИЗИЧКО ЛИЦЕ КОМЕ ЈЕ ПОВЕРЕНО ВРШЕЊЕ ЈАВНИХ ОВЛАШЋЕЊА;

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

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

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

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

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

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

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

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

24) ~~*информациона добра* обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично;~~

24) ИНФОРМАЦИОНА ДОБРА ОБУХВАТАЈУ ПОДАТКЕ У ДАТОТЕКАМА И БАЗАМА ПОДАТАКА, ПРОГРАМСКИ КÔД, КОНФИГУРАЦИЈУ ХАРДВЕРСКИХ КОМПОНЕНАТА, ТЕХНИЧКУ И КОРИСНИЧКУ ДОКУМЕНТАЦИЈУ, ЗАПИСЕ О КОРИШЋЕЊУ ХАРДВЕРСКИХ КОМПОНЕНТИ, ПОДАТАКА ИЗ ДАТОТЕКА И БАЗА ПОДАТАКА И СПРОВОЂЕЊУ ПРОЦЕДУРА АКО СЕ ИСТИ ВОДЕ, УНУТРАШЊЕ ОПШТЕ АКТЕ, ПРОЦЕДУРЕ И СЛИЧНО;

25) УСЛУГА ИНФОРМАЦИОНОГ ДРУШТВА ЈЕ УСЛУГА У СМИСЛУ ЗАКОНА КОЈИМ СЕ УРЕЂУЈЕ ЕЛЕКТРОНСКА ТРГОВИНА;

26) ПРУЖАЛАЦ УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА ЈЕ ПРАВО ЛИЦЕ КОЈЕ ЈЕ ПРУЖАЛАЦ УСЛУГЕ У СМИСЛУ ЗАКОНА КОЈИМ СЕ УРЕЂУЈЕ ЕЛЕКТРОНСКА ТРГОВИНА.

ОБРАДА ПОДАТАКА О ЛИЧНОСТИ

ЧЛАН 3А

У СЛУЧАЈУ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ ПРИЛИКОМ ВРШЕЊА НАДЛЕЖНОСТИ И ИСПУЊЕЊА ОБАВЕЗА ИЗ ОВОГ ЗАКОНА ПОСТУПА СЕ У СКЛАДУ СА ПРОПИСИМА КОЈИ УРЕЂУЈУ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ.

Тело за координацију послова информационе безбедности

Члан 5.

У циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада оснива Тело за координацију послова информационе безбедности (у даљем тексту: Тело за координацију), као координационо тело Владе, у чији састав улазе представници министарстава надлежних за послове информационе

безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, НАРОДНЕ БАНКЕ СРБИЈЕ, ~~ЦЕРТ-а републичких органа и Националног ЦЕРТ-~~а, ЦЕНТРА ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА У ОРГАНИМА ВЛАСТИ И НАЦИОНАЛНОГ ЦЕНТРА ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА.

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

Одлуком којом оснива Тело за координацију Влада одређује и његов састав, задатке, рок у коме оно подноси извештаје Влади и друга питања која су везана за његов рад.

II. БЕЗБЕДНОСТ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

~~ИКТ системи од посебног значаја~~

~~Члан 6~~

~~ИКТ системи од посебног значаја су системи који се користе:~~

~~1) у обављању послова у органима 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.~~

ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА

ЧЛАН 6.

ИКТ СИСТЕМИ ОД ПОСЕБНОГ ЗНАЧАЈА СУ СИСТЕМИ КОЈИ СЕ КОРИСТЕ:

1) У ОБАВЉАЊУ ПОСЛОВА У ОРГАНИМА ВЛАСТИ;

2) ЗА ОБРАДУ ПОСЕБНИХ ВРСТА ПОДАТАКА О ЛИЧНОСТИ, У СМИСЛУ ЗАКОНА КОЈИ УРЕЂУЈЕ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ;

3) У ОБАВЉАЊУ ДЕЛАТНОСТИ ОД ОПШТЕГ ИНТЕРЕСА И ДРУГИМ ДЕЛАТНОСТИМА И ТО У СЛЕДЕЋИМ ОБЛАСТИМА:

(1) ЕНЕРГЕТИКА:

- ПРОИЗВОДЊА, ПРЕНОС И ДИСТРИБУЦИЈА ЕЛЕКТРИЧНЕ ЕНЕРГИЈЕ;
- ПРОИЗВОДЊА И ПРЕРАДА УГЉА;
- ИСТРАЖИВАЊЕ, ПРОИЗВОДЊА, ПРЕРАДА, ТРАНСПОРТ И ДИСТРИБУЦИЈА НАФТЕ И ПРОМЕТ НАФТЕ И НАФТНИХ ДЕРИВАТА;
- ИСТРАЖИВАЊЕ, ПРОИЗВОДЊА, ПРЕРАДА, ТРАНСПОРТ И ДИСТРИБУЦИЈА ПРИРОДНОГ И ТЕЧНОГ ГАСА.

(2) САОБРАЋАЈ:

- ЖЕЛЕЗНИЧКИ, ПОШТАНСКИ, ВОДНИ И ВАЗДУШНИ САОБРАЋАЈ;

(3) ЗДРАВСТВО:

- ЗДРАВСТВЕНА ЗАШТИТА;

(4) БАНКАРСТВО И ФИНАНСИЈСКА ТРЖИШТА:

- ПОСЛОВИ ФИНАНСИЈСКИХ ИНСТИТУЦИЈА;

- ПОСЛОВИ ВОЂЕЊА РЕГИСТРА ПОДАТАКА О ОБАВЕЗАМА ФИЗИЧКИХ И ПРАВНИХ ЛИЦА ПРЕМА ФИНАНСИЈСКИМ ИНСТИТУЦИЈАМА;
- ПОСЛОВИ УПРАВЉАЊА, ОДНОСНО ОБАВЉАЊА ДЕЛАТНОСТИ У ВЕЗИ СА ФУНКЦИОНИСАЊЕМ РЕГУЛИСАНОГ ТРЖИШТА;

(5) ДИГИТАЛНА ИНФРАСТРУКТУРА:

- РАЗМЕНА ИНТЕРНЕТ САОБРАЋАЈА;
- УПРАВЉАЊЕ РЕГИСТРОМ НАЦИОНАЛНОГ ИНТЕРНЕТ ДОМЕНА И СИСТЕМОМ ЗА ИМЕНОВАЊЕ НА МРЕЖИ (ДНС СИСТЕМИ)

(6) ДОБРА ОД ОПШТЕГ ИНТЕРЕСА:

- КОРИШЋЕЊЕ, УПРАВЉАЊЕ, ЗАШТИТА И УНАПРЕЂИВАЊЕ ДОБАРА ОД ОПШТЕГ ИНТЕРЕСА (ВОДЕ, ПУТЕВИ, МИНЕРАЛНЕ СИРОВИНЕ, ШУМЕ, ПЛОВНЕ РЕКЕ, ЈЕЗЕРА, ОБАЛЕ, БАЊЕ, ДИВЉАЧ, ЗАШТИЋЕНА ПОДРУЧЈА);

(7) УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА:

- УСЛУГЕ ИНФОРМАЦИОНОГ ДРУШТВА У СМИСЛУ ЧЛАНА 2. ТАЧКА 25) ОВОГ ЗАКОНА;

(8) ОСТАЛЕ ОБЛАСТИ:

- ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ;
- ИЗДАВАЊЕ СЛУЖБЕНОГ ГЛАСИЛА РЕПУБЛИКЕ СРБИЈЕ;
- УПРАВЉАЊЕ НУКЛЕАРНИМ ОБЈЕКТИМА;
- ПРОИЗВОДЊА, ПРОМЕТ И ПРЕВОЗ НАОРУЖАЊА И ВОЈНЕ ОПРЕМЕ;
- УПРАВЉАЊЕ ОТПАДОМ;
- КОМУНАЛНЕ ДЕЛАТНОСТИ;
- ПРОИЗВОДЊА И СНАБДЕВАЊЕ ХЕМИКАЛИЈАМА;

4) У ПРАВНИМ ЛИЦИМА И УСТАНОВАМА КОЈЕ ОСНИВА РЕПУБЛИКА СРБИЈА, АУТОНОМНА ПОКРАЈИНА ИЛИ ЈЕДИНИЦА ЛОКАЛНЕ САМОУПРАВЕ ЗА ОБАВЉАЊЕ ДЕЛАТНОСТИ ИЗ ТАЧКЕ 3) ОВОГ СТАВА.

ВЛАДА, НА ПРЕДЛОГ МИНИСТАРСТВА НАДЛЕЖНОГ ЗА ПОСЛОВЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ, УТВРЂУЈЕ ЛИСТУ ДЕЛАТНОСТИ ИЗ СТАВА 1. ТАЧКА 3) ОВОГ ЧЛАНА.

ОБАВЕЗЕ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ЧЛАН 6А

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА У СКЛАДУ СА ОВИМ ЗАКОНОМ У ОБАВЕЗИ ЈЕ ДА:

1) УПИШЕ ИКТ СИСТЕМ ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИМ УПРАВЉА У ЕВИДЕНЦИЈУ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

2) ПРЕДУЗМЕ МЕРЕ ЗАШТИТЕ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

3) ДОНЕСЕ АКТ О БЕЗБЕДНОСТИ ИКТ СИСТЕМА;

4) ВРШИ ПРОВЕРУ УСКЛАЂЕНОСТИ ПРИМЕЊЕНИХ МЕРА ЗАШТИТЕ ИКТ СИСТЕМА СА АКТОМ О БЕЗБЕДНОСТИ ИКТ СИСТЕМА И ТО НАЈМАЊЕ ЈЕДНОМ ГОДИШЊЕ;

5) УРЕДИ ОДНОС СА ТРЕЋИМ ЛИЦИМА НА НАЧИН КОЈИ ОБЕЗБЕЂУЈЕ ПРЕДУЗИМАЊЕ МЕРА ЗАШТИТЕ ТОГ ИКТ СИСТЕМА У СКЛАДУ СА ЗАКОНОМ, УКОЛИКО ПОВЕРАВА АКТИВНОСТИ У ВЕЗИ СА ИКТ СИСТЕМОМ ОД ПОСЕБНОГ ЗНАЧАЈА ТРЕЋИМ ЛИЦИМА;

6) ДОСТАВЉА ОБАВЕШТЕЊА О ИНЦИДЕНТИМА КОЈИ ЗНАЧАЈНО УГРОЖАВАЈУ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ ИКТ СИСТЕМА;

7) ДОСТАВИ СТАТИСТИЧКЕ ПОДАТКЕ О ИНЦИДЕНТИМА У ИКТ СИСТЕМУ.

ЕВИДЕНЦИЈА ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

ЧЛАН 6Б

НАДЛЕЖНИ ОРГАН УСПОСТАВЉА И ВОДИ ЕВИДЕНЦИЈУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА (У ДАЉЕМ ТЕКСТУ: ЕВИДЕНЦИЈА) КОЈА САДРЖИ:

1) НАЗИВ И СЕДИШТЕ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

2) ИМЕ И ПРЕЗИМЕ, СЛУЖБЕНА АДРЕСА ЗА ПРИЈЕМ ЕЛЕКТРОНСКЕ ПОШТЕ И СЛУЖБЕНИ КОНТАКТ ТЕЛЕФОН АДМИНИСТРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

3) ИМЕ И ПРЕЗИМЕ, СЛУЖБЕНА АДРЕСА ЗА ПРИЈЕМ ЕЛЕКТРОНСКЕ ПОШТЕ И СЛУЖБЕНИ КОНТАКТ ТЕЛЕФОН ОДГОВОРНОГ ЛИЦА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА;

4) ПОДАТАК О ВРСТИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА, У СКЛАДУ СА ЧЛАНОМ 6. ОВОГ ЗАКОНА.

ПОРЕД ПОДАТАКА ИЗ СТАВА 1. ОВОГ ЧЛАНА, ЕВИДЕНЦИЈА МОЖЕ ДА САДРЖИ И ДРУГЕ ДОПУНСКЕ ПОДАТКЕ О ИКТ СИСТЕМУ ОД ПОСЕБНОГ ЗНАЧАЈА КОЈЕ ПРОПИСУЈЕ НАДЛЕЖНИ ОРГАН.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ИКТ СИСТЕМ ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИМ УПРАВЉА УПИШЕ У ЕВИДЕНЦИЈУ ИЗ СТАВА 1. ОВОГ ЧЛАНА.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА НАДЛЕЖНОМ ОРГАНУ ДОСТАВИ ПОДАТКЕ ИЗ СТАВА 1. ОВОГ ЧЛАНА НАЈКАСНИЈЕ 90 ДАНА ОД ДАНА УСВАЈАЊА ПРОПИСА ИЗ СТАВА 2. ОВОГ ЧЛАНА, ОДНОСНО 90 ДАНА ОД ДАНА УСПОСТАВЉАЊА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА.

НАДЛЕЖНИ ОРГАН СТАВЉА НА РАСПОЛАГАЊЕ НАЦИОНАЛНОМ ЦЕНТРУ ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (У

ДАЉЕМ ТЕКСТУ: НАЦИОНАЛНИ ЦЕРТ) АЖУРНУ ЕВИДЕНЦИЈУ ИЗ СТАВА 1. ОВОГ ЧЛАНА.

Мере заштите ИКТ система од посебног значаја

Члан 7.

Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и ~~минимизација~~ СМАЊЕЊЕ штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.

Мере заштите ИКТ система се односе на:

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

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

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

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

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

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

7) заштиту носача података;

8) ограничење приступа подацима и средствима за обраду података;

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

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

11) предвиђање одговарајуће употребе криптозаштите ради заштите тајности, аутентичности ~~односно~~ И интегритета података;

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

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

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

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

16) заштиту од губитка података;

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

18) обезбеђивање интегритета софтвера и оперативних система;

19) заштиту од злоупотребе техничких безбедносних слабости ИКТ система;

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

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

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

23) ~~питања информационе безбедности~~ ИСПУЊЕЊЕ ЗАХТЕВА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ у оквиру управљања свим фазама животног циклуса ИКТ система односно делова система;

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

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

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

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

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

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

~~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.~~

ОБАВЕШТАВАЊЕ О ИНЦИДЕНТИМА

ЧЛАН 11.

ОПЕРАТОРИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ОБАВЕШТАВАЊЕ О ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ ВРШЕ ПРЕКО ВЕБ СТРАНИЦЕ НАДЛЕЖНОГ ОРГАНА ИЛИ НАЦИОНАЛНОГ ЦЕРТ-А У ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА КОЈЕГ ОДРЖАВА НАДЛЕЖНИ ОРГАН.

УКОЛИКО ОРГАНИ ИЗ СТАВА 1. ОВОГ ЧЛАНА БУДУ ОБАВЕШТЕНИ О ИНЦИДЕНТУ НА ДРУГИ НАЧИН, ПОДАТКЕ О ИНЦИДЕНТУ УНОСЕ У СИСТЕМ ИЗ СТАВА 1. ОВОГ ЧЛАНА.

ИЗУЗЕТНО ОД СТАВА 1. ОВОГ ЧЛАНА, ОБАВЕШТЕЊЕ О ИНЦИДЕНТИМА СЕ УПУЋУЈЕ:

1) НАРОДНОЈ БАНЦИ СРБИЈЕ, У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (4) АЛИНЕЈЕ ПРВА И ДРУГА ОВОГ ЗАКОНА;

2) РЕГУЛАТОРНОМ ТЕЛУ ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА 8) АЛИНЕЈА ПРВА ОВОГ ЗАКОНА.

НАРОДНА БАНКА СРБИЈЕ И РЕГУЛАТОРНО ТЕЛО ЗА ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ ОБАВЕШТЕЊА ИЗ СТАВА 3. ОВОГ ЧЛАНА ДОСТАВЉАЈУ У ЈЕДИНСТВЕНИ СИСТЕМ ЗА ПРИЈЕМ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА НА НАЧИН ИЗ СТАВА 1. ОВОГ ЧЛАНА.

НАКОН ПРИЈАВЕ ИНЦИДЕНТА, УКОЛИКО ЈЕ ИНЦИДЕНТ И ДАЉЕ У ТОКУ, ОПЕРАТОРИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДОСТАВЉАЈУ ОБАВЕШТЕЊА О БИТНИМ ДОГАЂАЈИМА У ВЕЗИ СА ИНЦИДЕНТОМ И АКТИВНОСТИМА КОЈЕ ПРЕДУЗИМАЈУ ДО ПРЕСТАНКА ИНЦИДЕНТА ОРГАНУ КОМЕ СУ У СКЛАДУ СА ОВИМ ЗАКОНОМ ПРИЈАВИЛИ ИНЦИДЕНТ.

ОПЕРАТОРИ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДОСТАВЉАЈУ ЗАВРШНИ ИЗВЕШТАЈ О ИНЦИДЕНТУ ОРГАНУ КОГА СУ У СКЛАДУ СА ОВИМ ЗАКОНОМ ОБАВЕШТАВАЛИ О ИНЦИДЕНТУ У РОКУ ОД 15 ДАНА ОД ДАНА ПРЕСТАНКА ИНЦИДЕНТА, А КОЈИ ОБАВЕЗНО САДРЖИ ВРСТУ И ОПИС ИНЦИДЕНТА, ВРЕМЕ И ТРАЈАЊЕ ИНЦИДЕНТА, ПОСЛЕДИЦЕ КОЈЕ ЈЕ ИНЦИДЕНТ ИЗАЗВАО, ПРЕДУЗЕТЕ АКТИВНОСТИ РАДИ ОТКЛАЊАЊА ПОСЛЕДИЦА ИНЦИДЕНТА И, ПО ПОТРЕБИ, ДРУГЕ РЕЛЕВАНТНЕ ИНФОРМАЦИЈЕ.

У СЛУЧАЈУ ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА ОПЕРАТОРИ ТИХ ИКТ СИСТЕМА ПОСТУПАЈУ У СКЛАДУ СА ПРОПИСИМА КОЈИМА СЕ УРЕЂУЈЕ ОБЛАСТ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА.

ОДРЕДБЕ СТ. 1. И 7. ОВОГ ЧЛАНА НЕ ОДНОСЕ СЕ НА САМОСТАЛНЕ ОПЕРАТОРЕ ИКТ СИСТЕМА.

ВЛАДА, НА ПРЕДЛОГ НАДЛЕЖНОГ ОРГАНА, УРЕЂУЈЕ ПОСТУПАК ОБАВЕШТАВАЊА О ИНЦИДЕНТИМА, ЛИСТУ, ВРСТЕ И ЗНАЧАЈ ИНЦИДЕНАТА ПРЕМА НИВОУ ОПАСНОСТИ, ПОСТУПАЊЕ И РАЗМЕНУ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА ИЗМЕЂУ ОРГАНА ИЗ ЧЛАНА 5. ОВОГ ЗАКОНА.

АКО ЈЕ ИНЦИДЕНТ ОД ИНТЕРЕСА ЗА ЈАВНОСТ, НАДЛЕЖНИ ОРГАН, ОДНОСНО ОРГАН ИЗ СТАВА 3. ОВОГ ЧЛАНА КОМЕ СЕ УПУЋУЈУ ОБАВЕШТЕЊА О ИНЦИДЕНТИМА, МОЖЕ ОБЈАВИТИ ИНФОРМАЦИЈУ О ИНЦИДЕНТУ, НАКОН САВЕТОВАЊА СА ОПЕРАТОРОМ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА У КОМЕ СЕ ИНЦИДЕНТ ДОГОДИО.

АКО ЈЕ ИНЦИДЕНТ ВЕЗАН ЗА ИЗВРШЕЊЕ КРИВИЧНИХ ДЕЛА КОЈА СЕ ГОНЕ ПО СЛУЖБЕНОЈ ДУЖНОСТИ, ОРГАН КОМЕ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ О ИНЦИДЕНТУ, ОБАВЕШТАВА НАДЛЕЖНО ЈАВНО ТУЖИЛАШТВО, ОДНОСНО МИНИСТАРСТВО НАДЛЕЖНО ЗА УНУТРАШЊЕ ПОСЛОВЕ.

АКО ЈЕ ИНЦИДЕНТ ПОВЕЗАН СА ЗНАЧАЈНИМ НАРУШАВАЊЕМ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ, КОЈЕ ИМА ИЛИ МОЖЕ ИМАТИ ЗА ПОСЛЕДИЦУ УГРОЖАВАЊЕ ОДБРАНЕ РЕПУБЛИКЕ СРБИЈЕ, ОРГАН КОМЕ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ О ИНЦИДЕНТУ ОБАВЕШТАВА ВОЈНОБЕЗБЕДНОСНУ АГЕНЦИЈУ.

АКО ЈЕ ИНЦИДЕНТ ПОВЕЗАН СА ЗНАЧАЈНИМ НАРУШАВАЊЕМ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ, КОЈЕ ИМА ИЛИ МОЖЕ ИМАТИ ЗА ПОСЛЕДИЦУ УГРОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ, ОРГАН КОМЕ ЈЕ УПУЋЕНО ОБАВЕШТЕЊЕ О ИНЦИДЕНТУ ОБАВЕШТАВА БЕЗБЕДНОСНО-ИНФОРМАТИВНУ АГЕНЦИЈУ.

У СЛУЧАЈУ НАСТУПАЊА ОКОЛНОСТИ УГРОЖАВАЊА, ОМЕТАЊА РАДА ИЛИ УНИШТЕЊА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА РУКОВОЂЕЊЕ И КООРДИНАЦИЈУ СПРОВОЂЕЊА МЕРА И ЗАДАТАКА У НАВЕДЕНИМ ОКОЛНОСТИМА ПРЕДУЗИМА РЕПУБЛИЧКИ ШТАБ ЗА ВАНРЕДНЕ СИТУАЦИЈЕ, У СКЛАДУ СА ЗАКОНОМ.

ИНЦИДЕНТИ У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

ЧЛАН 11А

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ПРИЈАВИ СЛЕДЕЋЕ ИНЦИДЕНТЕ КОЈИ МОГУ ДА ИМАЈУ ЗНАЧАЈАН УТИЦАЈ НА НАРУШАВАЊЕ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ:

1) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА ВРШЕЊА ПОСЛОВА И ПРУЖАЊА УСЛУГА, ОДНОСНО ЗНАТНИХ ТЕШКОЋА У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊУ УСЛУГА;

2) ИНЦИДЕНТЕ КОЈИ УТИЧУ НА ВЕЛИКИ БРОЈ КОРИСНИКА УСЛУГА, ИЛИ ТРАЈУ ДУЖИ ВРЕМЕНСКИ ПЕРИОД;

3) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА, ОДНОСНО ТЕШКОЋА У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊА УСЛУГА, КОЈИ УТИЧУ НА ОБАВЉАЊЕ ПОСЛОВА И ВРШЕЊЕ УСЛУГА ДРУГИХ ОПЕРАТОРА ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ИЛИ УТИЧУ НА ЈАВНУ БЕЗБЕДНОСТ;

4) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО ПРЕКИДА КОНТИНУИТЕТА, ОДНОСНО ТЕШКОЋЕ У ВРШЕЊУ ПОСЛОВА И ПРУЖАЊУ УСЛУГА И ИМАЈУ УТИЦАЈ НА ВЕЋИ ДЕО ТЕРИТОРИЈЕ РЕПУБЛИКЕ СРБИЈЕ;

5) ИНЦИДЕНТЕ КОЈИ ДОВОДЕ ДО НЕОВЛАШЋЕНОГ ПРИСТУПА ЗАШТИЋЕНИМ ПОДАЦИМА ЧИЈЕ ОТКРИВАЊЕ МОЖЕ УГРОЗИТИ ПРАВА И ИНТЕРЕСЕ ОНИХ НА КОЈЕ СЕ ПОДАЦИ ОДНОСЕ;

6) ИНЦИДЕНТЕ КОЈИ СУ НАСТАЛИ КАО ПОСЛЕДИЦА ИНЦИДЕНТА У ИКТ СИСТЕМУ ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (7) ОВОГ ЗАКОНА, КАДА ИКТ СИСТЕМ ОД ПОСЕБНОГ ЗНАЧАЈА У СВОМ ПОСЛОВАЊУ

КОРИСТИ ИНФОРМАЦИОНЕ УСЛУГЕ ИКТ СИСТЕМА ИЗ ЧЛАНА 6. СТАВ 1. ТАЧКА 3) ПОДТАЧКА (7) ОВОГ ЗАКОНА.

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА ПРИЈАВИ И ИНЦИДЕНТЕ КОЈИ СУ ДОВЕЛИ ДО ЗНАЧАЈНОГ ПОВЕЋАЊА РИЗИКА ОД НАСТУПАЊА ПОСЛЕДИЦА ИЗ СТАВА 1. ОВОГ ЧЛАНА.

ДОСТАВЉАЊЕ СТАТИСТИЧКИХ ПОДАТАКА О ИНЦИДЕНТИМА

ЧЛАН 11Б

ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА ДУЖАН ЈЕ ДА, ПОРЕД ОБАВЕШТАВАЊА О ИНЦИДЕНТИМА ИЗ ЧЛАНА 11. ОВОГ ЗАКОНА, ДОСТАВИ НАЦИОНАЛНОМ ЦЕРТ-У СТАТИСТИЧКЕ ПОДАТКЕ О СВИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМУ У ПРЕТХОДНОЈ ГОДИНИ НАЈКАСНИЈЕ ДО 28. ФЕБРУАРА ТЕКУЋЕ ГОДИНЕ.

НАЦИОНАЛНИ ЦЕРТ ОБЈЕДИЊЕНЕ СТАТИСТИЧКЕ ПОДАТКЕ ИЗ СТАВА 1. ОВОГ ЧЛАНА ДОСТАВЉА НАДЛЕЖНОМ ОРГАНУ И ОБЈАВЉУЈЕ ИХ НА ВЕБ СТРАНИЦИ НАЦИОНАЛНОГ ЦЕРТ-А.

ВРСТУ, ФОРМУ И НАЧИН ДОСТАВЉАЊА СТАТИСТИЧКИХ ПОДАТАКА ИЗ СТАВА 1. ОВОГ ЧЛАНА УТВРЂУЈЕ НАЦИОНАЛНИ ЦЕРТ.

Међународна сарадња и рана упозорења о ризицима и инцидентима

Члан 12.

Надлежни орган остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

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

2) превазилазе или могу да превазиђу националне капацитете;

3) могу да имају негативан утицај на више од једне државе.

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

САМОСТАЛНИ ОПЕРАТОРИ ИКТ СИСТЕМА

Члан 13.

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

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

СХОДНА ПРИМЕНА ОДРЕДАБА О САМОСТАЛНИМ ОПЕРАТОРИМА ИКТ СИСТЕМА

ЧЛАН 13А

НА НАРОДНУ БАНКУ СРБИЈЕ КАО ОПЕРАТОРА ИКТ СИСТЕМА СХОДНО СЕ ПРИМЕЊУЈУ ОДРЕДБЕ ЧЛ. 13, 15, 15А, 19, 22, 26, 27. И 28. ОВОГ ЗАКОНА КОЈЕ СЕ ОДНОСЕ НА САМОСТАЛНЕ ОПЕРАТОРЕ ИКТ СИСТЕМА.

НА НАРОДНУ БАНКУ СРБИЈЕ КАО ОПЕРАТОРА ИКТ СИСТЕМА СХОДНО СЕ ПРИМЕЊУЈУ И ОДРЕДБЕ ЧЛ. 11. И 11А ОВОГ ЗАКОНА КОЈЕ СЕ ОДНОСЕ НА ОПЕРАТОРЕ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА.

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

~~НАЦИОНАЛНИ ЦЕНТАР ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (Национални ЦЕРТ)~~ НАЦИОНАЛИ ЦЕРТ

Члан 14.

~~НАЦИОНАЛНИ ЦЕНТАР ЗА ПРЕВЕНЦИЈУ БЕЗБЕДНОСНИХ РИЗИКА У ИКТ СИСТЕМИМА (У ДАЉЕМ ТЕКСТУ: Национални ЦЕРТ)~~ 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.~~

ДЕЛОКРУГ НАЦИОНАЛНОГ ЦЕРТ-А

ЧЛАН 15.

НАЦИОНАЛНИ ЦЕРТ ПРИКУПЉА И РАЗМЕЊУЈЕ ИНФОРМАЦИЈЕ О РИЗИЦИМА ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА, КАО И ДОГАЂАЈИМА КОЈИ УГРОЖАВАЈУ БЕЗБЕДНОСТ ИКТ СИСТЕМА И У ВЕЗИ ТОГА ОБАВЕШТАВА, ПРУЖА ПОДРШКУ, УПОЗОРАВА И САВЕТУЈЕ ЛИЦА КОЈА УПРАВЉАЈУ ИКТ СИСТЕМИМА У РЕПУБЛИЦИ СРБИЈИ, КАО И ЈАВНОСТ, А ПОСЕБНО:

1) ПРАТИ СТАЊЕ О ИНЦИДЕНТИМА НА НАЦИОНАЛНОМ НИВОУ,

2) ПРУЖА РАНА УПОЗОРЕЊА, УЗБУНЕ И НАЈАВЕ И ИНФОРМИШЕ РЕЛЕВАНТНА ЛИЦА О РИЗИЦИМА И ИНЦИДЕНТИМА,

3) РЕАГУЈЕ ПО ПРИЈАВЉЕНИМ ИЛИ НА ДРУГИ НАЧИН ОТКРИВЕНИМ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА, КАО И ПО ПРИЈАВАМА ФИЗИЧКИХ И ПРАВНИХ ЛИЦА, ТАКО ШТО ПРУЖА САВЕТЕ И ПРЕПОРУКЕ НА ОСНОВУ РАСПОЛОЖИВИХ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА И ПРЕДУЗИМА ДРУГЕ ПОТРЕБНЕ МЕРЕ ИЗ СВОЈЕ НАДЛЕЖНОСТИ НА ОСНОВУ ДОБИЈЕНИХ САЗНАЊА,

4) КОНТИНУИРАНО ИЗРАЂУЈЕ АНАЛИЗЕ РИЗИКА И ИНЦИДЕНАТА,

5) ПОДИЖЕ СВЕСТ КОД ГРАЂАНА, ПРИВРЕДНИХ СУБЈЕКАТА И ОРГАНА ВЛАСТИ О ЗНАЧАЈУ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ, О РИЗИЦИМА И МЕРАМА ЗАШТИТЕ, УКЉУЧУЈУЋИ СПРОВОЂЕЊЕ КАМПАЊА У ЦИЉУ ПОДИЗАЊА ТЕ СВЕСТИ,

6) ВОДИ ЕВИДЕНЦИЈУ ПОСЕБНИХ ЦЕРТ-ОВА,

7) ИЗВЕШТАВА НАДЛЕЖНИ ОРГАН НА КВАРТАЛНОМ НИВОУ О ПРЕДУЗЕТИМ АКТИВНОСТИМА.

НАЦИОНАЛНИ ЦЕРТ ЈЕ ОВЛАШЋЕН ДА ВРШИ ОБРАДУ ПОДАТАКА О ЛИЦУ КОЈЕ СЕ ОБРАТИ НАЦИОНАЛНОМ ЦЕРТ-У У СКЛАДУ СА ЗАКОНОМ КОЈИ УРЕЂУЈЕ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ И ДРУГИМ ПРОПИСИМА.

ОБРАДА ПОДАТАКА О ЛИЦУ ИЗ СТАВА 1. ТАЧКА 3) ОВОГ ЧЛАНА ОБУХВАТА ИМЕ, ПРЕЗИМЕ И БРОЈ ТЕЛЕФОНА И/ИЛИ АДРЕСУ ЕЛЕКТРОНСКЕ ПОШТЕ И ВРШИ СЕ У СВРХУ ЕВИДЕНТИРАЊА ПОДНЕТИХ ПРИЈАВА, ИНФОРМИСАЊА ПОДНОСИОЦА ПРИЈАВЕ О СТАТУСУ ПРЕДМЕТА И, У СЛУЧАЈУ ПОТРЕБЕ, УПУЋИВАЊА ПРИЈАВЕ НАДЛЕЖНИМ ОРГАНИМА РАДИ ДАЉЕГ ПОСТУПАЊА, У СКЛАДУ СА ЗАКОНОМ.

НАЦИОНАЛНИ ЦЕРТ ОБЕЗБЕЂУЈЕ НЕПРЕКИДНУ ДОСТУПНОСТ СВОЈИХ УСЛУГА ПУТЕМ РАЗЛИЧИТИХ СРЕДСТАВА КОМУНИКАЦИЈЕ.

ПРОСТОРИЈЕ И ИНФОРМАЦИОНИ СИСТЕМИ НАЦИОНАЛНОГ ЦЕРТ-А МОРАЈУ ДА СЕ НАЛАЗЕ НА БЕЗБЕДНИМ ЛОКАЦИЈАМА.

У ЦИЉУ ОБЕЗБЕЂИВАЊА КОНТИНУИТЕТА РАДА, НАЦИОНАЛНИ ЦЕРТ ТРЕБА ДА:

1) БУДЕ ОПРЕМЉЕН СА ОДГОВАРАЈУЋИМ СИСТЕМИМА ЗА ОБАВЉАЊЕ ПОСЛОВА ИЗ СВОГ ДЕЛОКРУГА;

2) ИМА ДОВОЉНО ЗАПОСЛЕНИХ КАКО БИ СЕ ОСИГУРАЛА ДОСТУПНОСТ У СВАКО ДОБА;

3) ОБЕЗБЕДИ ИНФРАСТРУКТУРУ ЧИЈИ ЈЕ КОНТИНУИТЕТ ОСИГУРАН, ОДНОСНО ДА ОБЕЗБЕДИ РЕДУНДАНТНЕ СИСТЕМЕ И РЕЗЕРВНИ РАДНИ ПРОСТОР.

НАЦИОНАЛНИ ЦЕРТ НЕПОСРЕДНО САРАЂУЈЕ СА НАДЛЕЖНИМ ОРГАНОМ, ПОСЕБНИМ ЦЕРТ-ОВИМА У РЕПУБЛИЦИ СРБИЈИ, СЛИЧНИМ ОРГАНИЗАЦИЈАМА У ДРУГИМ ЗЕМЉАМА, СА ЈАВНИМ И ПРИВРЕДНИМ СУБЈЕКТИМА, ЦЕРТ-ОВИМА САМОСТАЛНИХ ОПЕРАТОРА ИКТ СИСТЕМА, КАО И СА ЦЕРТ-ОМ ОРГАНА ВЛАСТИ.

НАЦИОНАЛНИ ЦЕРТ ПРОМОВИШЕ УСВАЈАЊЕ И КОРИШЋЕЊЕ ПРОПИСАНИХ И СТАНДАРДИЗОВАНИХ ПРОЦЕДУРА ЗА:

1) УПРАВЉАЊЕ И САНИРАЊЕ РИЗИКА И ИНЦИДЕНАТА;

2) КЛАСИФИКАЦИЈУ ИНФОРМАЦИЈА О РИЗИЦИМА И ИНЦИДЕНТИМА, ОДНОСНО КЛАСИФИКАЦИЈУ ПРЕМА НИВОУ ИНЦИДЕНАТА И РИЗИКА.

САРАДЊА ЦЕРТ-ОВА У РЕПУБЛИЦИ СРБИЈИ

ЧЛАН 15А

НАЦИОНАЛНИ ЦЕРТ, ЦЕРТ ОРГАНА ВЛАСТИ И ЦЕРТ-ОВИ САМОСТАЛНИХ ОПЕРАТОРА ИКТ СИСТЕМА ОДРЖАВАЈУ КОНТИНУИРАНУ САРАДЊУ.

ЦЕРТ-ОВИ ИЗ СТАВА 1. ОВОГ ЧЛАНА ОДРЖАВАЈУ МЕЂУСОБНЕ САСТАНКЕ У ОРГАНИЗАЦИЈИ НАЦИОНАЛНОГ ЦЕРТ-А НАЈМАЊЕ ТРИ ПУТА

ГОДИШЊЕ, КАО И ПО ПОТРЕБИ У СЛУЧАЈУ ИНЦИДЕНАТА КОЈИ ЗНАЧАЈНО УГРОЖАВАЈУ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ У РЕПУБЛИЦИ СРБИЈИ.

САСТАНЦИМА ЦЕРТ-ОВА ИЗ СТАВА 1. ОВОГ ЧЛАНА ПРИСУСТВУЈУ И ПРЕДСТАВНИЦИ НАДЛЕЖНОГ ОРГАНА.

САСТАНЦИМА ЦЕРТ-ОВА ИЗ СТАВА 1. ОВОГ ЧЛАНА МОГУ, ПО ПОЗИВУ, ДА ПРИСУСТВУЈУ И ПРЕДСТАВНИЦИ ПОСЕБНИХ ЦЕРТ-ОВА, КАО И ДРУГА ЛИЦА.

НАДЗОР НАД РАДОМ НАЦИОНАЛНОГ ЦЕРТ-А

Члан 16.

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

Посебни центри за превенцију безбедносних ризика у ИКТ системима

Члан 17.

Посебан центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Посебан ЦЕРТ) обавља послове превенције и заштите од безбедносних ризика у ИКТ системима у оквиру одређеног правног лица, групе правних лица, области пословања и слично.

Посебан ЦЕРТ је правно лице или организациона јединица у оквиру правног лица СА СЕДИШТЕМ НА ТЕРИТОРИЈИ РЕПУБЛИКЕ СРБИЈЕ, које је уписано у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ.

Упис у евиденцију посебних ЦЕРТ-ова врши се на основу пријаве правног лица у оквиру кога се налази посебан ЦЕРТ.

Евиденција посебних ЦЕРТ-ова од података о личности садржи податке о одговорним лицима, и то: име, презиме, функцију и контакт податке као што су адреса, број телефона и адреса електронске поште, А У СВРХУ АНГАЖОВАЊА ПОСЕБНИХ ЦЕРТ-ОВА У СЛУЧАЈУ БЕЗБЕДНОСНИХ РИЗИКА И ИНЦИДЕНАТА У ИКТ СИСТЕМИМА.

~~Ближе услове за упис у евиденцију из става 3. овог члана доноси надлежни орган.~~

НАЦИОНАЛНИ ЦЕРТ ПРОПИСУЈЕ САДРЖАЈ, НАЧИН УПИСА И ВОЂЕЊА ЕВИДЕНЦИЈЕ ИЗ СТАВА 3. ОВОГ ЧЛАНА.

~~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 орган надлежан за пројектовање, развој, изградњу, одржавање и унапређење рачунарске мреже 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.~~

ЦЕНТАР ЗА БЕЗБЕДНОСТ ИКТ СИСТЕМА У ОРГАНИМА ВЛАСТИ (ЦЕРТ ОРГАНА ВЛАСТИ)

„ЧЛАН 18.

ЦЕРТ ОРГАНА ВЛАСТИ ОБАВЉА ПОСЛОВЕ КОЈИ СЕ ОДНОСЕ НА ЗАШТИТУ ОД ИНЦИДЕНАТА У ИКТ СИСТЕМИМА ОРГАНА ВЛАСТИ, ИЗУЗЕВ ИКТ СИСТЕМА САМОСТАЛНИХ ОПЕРАТОРА.

ПОСЛОВЕ ЦЕРТ-А ОРГАНА ВЛАСТИ ОБАВЉА ОРГАН НАДЛЕЖАН ЗА ПРОЈЕКТОВАЊЕ, РАЗВОЈ, ИЗГРАДЊУ, ОДРЖАВАЊЕ И УНАПРЕЂЕЊЕ РАЧУНАРСКЕ МРЕЖЕ РЕПУБЛИЧКИХ ОРГАНА.

ПОСЛОВИ ЦЕРТ-А ОРГАНА ВЛАСТИ ОБУХВАТАЈУ:

1) ЗАШТИТУ ЈЕДИНСТВЕНЕ ИНФОРМАЦИОНО-КОМУНИКАЦИОНЕ МРЕЖЕ ЕЛЕКТРОНСКЕ УПРАВЕ;

2) КООРДИНАЦИЈУ И САРАДЊУ СА ОПЕРАТОРИМА ИКТ СИСТЕМА КОЈЕ ПОВЕЗУЈЕ ЈЕДИНСТВЕНА МРЕЖА ИЗ ТАЧКЕ 1) ОВОГ СТАВА У ПРЕВЕНЦИЈИ ИНЦИДЕНАТА, ОТКРИВАЊУ ИНЦИДЕНАТА, ПРИКУПЉАЊУ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА И ОТКЛАЊАЊУ ПОСЛЕДИЦА ИНЦИДЕНАТА;

3) ИЗДАВАЊЕ СТРУЧНИХ ПРЕПОРУКА ЗА ЗАШТИТУ ИКТ СИСТЕМА ОРГАНА ВЛАСТИ, ОСИМ ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА.

ЦЕРТ САМОСТАЛНОГ ОПЕРАТОРА ИКТ СИСТЕМА

Члан 19.

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

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

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

1) израду интерних аката у области информационе безбедности;

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

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

4) надзор имплементације и примене безбедносних процедура;

5) управљање и коришћење криптографских производа;

6) анализу безбедности ИКТ система у циљу процене ризика;

7) обуку запослених у области информационе безбедности.

ЗАШТИТА ДЕЦЕ ПРИ КОРИШЋЕЊУ ИНФОРМАЦИОНО-КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

ЧЛАН 19А

НАДЛЕЖНИ ОРГАН ПРЕДУЗИМА ПРЕВЕНТИВНЕ МЕРЕ ЗА БЕЗБЕДНОСТ И ЗАШТИТУ ДЕЦЕ НА ИНТЕРНЕТУ, КАО АКТИВНОСТИ ОД ЈАВНОГ ИНТЕРЕСА, ПУТЕМ ЕДУКАЦИЈЕ И ИНФОРМИСАЊА ДЕЦЕ, РОДИТЕЉА И НАСТАВНИКА О ПРЕДНОСТИМА, РИЗИЦИМА И НАЧИНИМА БЕЗБЕДНОГ КОРИШЋЕЊА ИНТЕРНЕТА, КАО И ПУТЕМ ЈЕДИНСТВЕНОГ МЕСТА ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ, И УПУЋУЈЕ ПРИЈАВЕ НАДЛЕЖНИМ ОРГАНИМА РАДИ ДАЉЕГ ПОСТУПАЊА.

ОПЕРАТОР ЕЛЕКТРОНСКИХ КОМУНИКАЦИЈА КОЈИ ПРУЖА ЈАВНО ДОСТУПНЕ ТЕЛЕФОНСКЕ УСЛУГЕ ДУЖАН ЈЕ ДА ОМОГУЋИ СВИМ ПРЕТПЛАТНИЦИМА УСЛУГУ БЕСПЛАТНОГ ПОЗИВА ПРЕМА ЈЕДИНСТВЕНОМ МЕСТУ ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ.

У СЛУЧАЈУ ДА НАВОДИ ИЗ ПРИЈАВЕ УПУЋУЈУ НА ПОСТОЈАЊЕ КРИВИЧНОГ ДЕЛА, НА ПОВРЕДУ ПРАВА, ЗДРАВСТВЕНОГ СТАТУСА, ДОБРОБИТИ И/ИЛИ ОПШТЕГ ИНТЕГРИТЕТА ДЕТЕТА, НА РИЗИК СТВАРАЊА ЗАВИСНОСТИ ОД КОРИШЋЕЊА ИНТЕРНЕТА, ПРИЈАВА СЕ ПРОСЛЕЂУЈЕ НАДЛЕЖНОМ ОРГАНУ ВЛАСТИ РАДИ ПОСТУПАЊА У СКЛАДУ СА УТВРЂЕНИМ НАДЛЕЖНОСТИМА.

НАДЛЕЖНИ ОРГАН ЈЕ ОВЛАШЋЕН ДА ВРШИ ОБРАДУ ПОДАТАКА О ЛИЦУ КОЈЕ СЕ ОБРАТИ НАДЛЕЖНОМ ОРГАНУ У СКЛАДУ СА ЗАКОНОМ

КОЈИ УРЕЂУЈЕ ЗАШТИТУ ПОДАТАКА О ЛИЧНОСТИ И ДРУГИМ ПРОПИСИМА.

ОБРАДА ПОДАТАКА О ЛИЦУ ИЗ СТАВА 4. ОВОГ ЧЛАНА ОБУХВАТА ИМЕ, ПРЕЗИМЕ И БРОЈ ТЕЛЕФОНА И/ИЛИ АДРЕСУ ЕЛЕКТРОНСКЕ ПОШТЕ И ВРШИ СЕ У СВРХУ ЕВИДЕНТИРАЊА ПОДНЕТИХ ПРИЈАВА, ИНФОРМИСАЊА ПОДНОСИОЦА ПРИЈАВЕ О СТАТУСУ ПРЕДМЕТА И, У СЛУЧАЈУ ПОТРЕБЕ, УПУЋИВАЊА ПРИЈАВЕ НАДЛЕЖНИМ ОРГАНИМА РАДИ ДАЉЕГ ПОСТУПАЊА, У СКЛАДУ СА ЗАКОНОМ.

ПОДАЦИ О ЛИЧНОСТИ ИЗ СТАВА 5. ОВОГ ЧЛАНА ЧУВАЈУ СЕ У РОКОВИМА ПРЕДВИЂЕНИМ ПРОПИСИМА КОЈИ УРЕЂУЈУ КАНЦЕЛАРИЈСКО ПОСЛОВАЊЕ.

У ЦИЉУ ОБЕЗБЕЂИВАЊА КОНТИНУИТЕТА РАДА ЈЕДИНСТВЕНОГ МЕСТА ЗА ПРУЖАЊЕ САВЕТА И ПРИЈЕМ ПРИЈАВА У ВЕЗИ БЕЗБЕДНОСТИ ДЕЦЕ НА ИНТЕРНЕТУ, НАДЛЕЖНИ ОРГАН ТРЕБА ДА:

1) БУДЕ ОПРЕМЉЕН СА ОДГОВАРАЈУЋИМ СИСТЕМИМА ЗА ПРИЈЕМ ПРИЈАВА;

2) ИМА ДОВОЉНО ЗАПОСЛЕНИХ КАКО БИ СЕ ОСИГУРАЛА ДОСТУПНОСТ У РАДУ;

3) ОБЕЗБЕДИ ИНФРАСТРУКТУРУ ЧИЈИ ЈЕ КОНТИНУИТЕТ ОСИГУРАН.

ВЛАДА БЛИЖЕ УРЕЂУЈЕ НАЧИН СПРОВОЂЕЊА МЕРА ЗА БЕЗБЕДНОСТ И ЗАШТИТУ ДЕЦЕ НА ИНТЕРНЕТУ ИЗ СТ. 1. И 3. ОВОГ ЧЛАНА.

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 30.

НОВЧАНОМ КАЗНОМ У ИЗНОСУ ОД 50.000,00 ДО 2.000.000,00 ДИНАРА КАЗНИЋЕ СЕ ЗА ПРЕКРШАЈ ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА АКО:

1) НЕ ИЗВРШИ УПИС У ЕВИДЕНЦИЈУ У РОКУ ИЗ ЧЛАНА 6Б СТАВ 4. ОВОГ ЗАКОНА;

2) НЕ ДОНЕСЕ АКТ О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ИЗ ЧЛАНА 8. СТАВ 1. ОВОГ ЗАКОНА;

3) НЕ ПРИМЕНИ МЕРЕ ЗАШТИТЕ ОДРЕЂЕНЕ АКТОМ О БЕЗБЕДНОСТИ ИКТ СИСТЕМА ИЗ ЧЛАНА 8. СТАВ 2. ОВОГ ЗАКОНА;

4) НЕ ИЗВРШИ ПРОВЕРУ УСКЛАЂЕНОСТИ ПРИМЕЊЕНИХ МЕРА ИЗ ЧЛАНА 8. СТАВ 4. ОВОГ ЗАКОНА;

5) НЕ ДОСТАВИ СТАТИСТИЧКЕ ПОДАТКЕ ИЗ ЧЛАНА 11Б СТАВ 1. ОВОГ ЗАКОНА;

6) НЕ ПОСТУПИ ПО НАЛОГУ ИНСПЕКТОРА ЗА ИНФОРМАЦИОНУ БЕЗБЕДНОСТ У ОСТАВЉЕНОМ РОКУ ИЗ ЧЛАНА 29. СТАВ 1. ТАЧКА 1. ОВОГ ЗАКОНА.

ЗА ПРЕКРШАЈ ИЗ СТАВА 1. ОВОГ ЧЛАНА КАЗНИЋЕ СЕ И ОДГОВОРНО ЛИЦЕ У ОПЕРАТОРУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА НОВЧАНОМ КАЗНОМ У ИЗНОСУ ОД 5.000,00 ДО 50.000,00 ДИНАРА.

~~Члан 31~~

~~Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај 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.~~

ЧЛАН 31.

НОВЧАНОМ КАЗНОМ У ИЗНОСУ ОД 50.000,00 ДО 500.000,00 ДИНАРА КАЗНИЋЕ СЕ ЗА ПРЕКРШАЈ ОПЕРАТОР ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА АКО:

1) О ИНЦИДЕНТИМА У ИКТ СИСТЕМУ НЕ ОБАВЕСТИ ОРГАНЕ ИЗ ЧЛАНА 11. СТ. 1, 3. И 7. ОВОГ ЗАКОНА;

2) НЕ ДОСТАВЉА ОБАВЕШТЕЊА О БИТНИМ ДОГАЂАЈИМА У ВЕЗИ СА ИНЦИДЕНТОМ И АКТИВНОСТИМА ИЗ ЧЛАНА 11. СТАВ 5. ОВОГ ЗАКОНА;

3) НЕ ДОСТАВИ ЗАВРШНИ ИЗВЕШТАЈ У РОКУ ИЗ ЧЛАНА 11. СТАВ 6. ОВОГ ЗАКОНА.

ЗА ПРЕКРШАЈЕ ИЗ СТАВА 1. ОВОГ ЧЛАНА КАЗНИЋЕ СЕ И ОДГОВОРНО ЛИЦЕ У ОПЕРАТОРУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА НОВЧАНОМ КАЗНОМ У ИЗНОСУ ОД 5.000,00 ДО 50.000,00 ДИНАРА.

ИЗУЗЕТНО ОД СТ. 1. И 2. ОВОГ ЧЛАНА, АКО ФИНАНСИЈСКА ИНСТИТУЦИЈА НЕ ОБАВЕСТИ НАРОДНУ БАНКУ СРБИЈЕ О ИНЦИДЕНТИМА У ИКТ СИСТЕМУ ОД ПОСЕБНОГ ЗНАЧАЈА, НАРОДНА БАНКА СРБИЈЕ ИЗРИЧЕ ТОЈ ФИНАНСИЈСКОЈ ИНСТИТУЦИЈИ МЕРЕ И КАЗНЕ У СКЛАДУ СА ЗАКОНОМ КОЈИМ СЕ УРЕЂУЈЕ ЊЕНО ПОСЛОВАЊЕ.

VI. АНАЛИЗА ЕФЕКАТА ЗАКОНА О ИЗМЕНАМА И ДОПУНАМА ЗАКОНА О ИНФОРМАЦИОНОЈ БЕЗБЕДНОСТИ

1) Који показатељи се прате у области, који су разлози због којих се ови показатељи прате и које су њихове вредности?

У области информационе безбедности показатељи који се прате односе се на:

- примену мера од безбедносних ризика у информационо-комуникационим системима и
- инциденте који значајно угрожавају информациону безбедност, а којима су изложени ИКТ системе под посебног значаја.

Наиме, Законом и информационој безбедности („Службени гласник РС”, бр. 6/16 и 94/17) (у даљем тексту: Закон) дефинисани су оператори ИКТ система од посебног значаја, као и мере заштите, односно техничке и организационе мере које су оператори ИКТ системи од посебног значаја у обавези да примењују, а у циљу одржавања адекватног нивоа безбедности система.

Сходно томе, оператори ИКТ система од посебног значаја дужни су да донесу акт о безбедности ИКТ система и дефинишу мере заштите, а нарочито принципе, 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.

Инспекцијским надзором над радом оператора ИКТ система од посебног значаја утврђује се да ли су оператори донели акт о безбедности и применили мере заштите, односно да ли је успостављен адекватан ниво безбедности система. Инспекцијски надзор до сада није вршен, будући да је први инспектор у новоформираној инспекцији за информациону безбедност запослен у другој половини 2018. године и, сходно томе, инспекцијски надзор се спроводи од 2019. године.

Оператори ИКТ система од посебног значаја у складу са Законом обавезни су да обавесте Надлежни орган, односно Министарство трговине, туризма и телекомуникација о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности.

На основу пријављених инцидената Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) 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. Национални ЦЕРТ на основу пријављених инцидената прати трендове у овој области и континуирано израђује анализе ризика и инцидената. Према извештајима Националног ЦЕРТ-а у 2017. години пријављено је 17 инцидената који значајно угрожавају информациону безбедност, а у 2018. години укупно 31 инцидент.

2) Да ли се у предметној области спроводи или се спроводио документ јавне политике или пропис? Представити резултате спровођења тог документа јавне политике или прописа и образложити због чега добијени резултати нису у складу са планираним вредностима.

У предметној области на снази је Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године

(„Службени гласник РС”, број 53/17), као и акциони план за 2018. и 2019. годину којим се ближе дефинишу активности предвиђене овом стратегијом. У складу са наведеним документима, у претходном периоду спроведене су следеће активности у оквиру стратешких приоритета:

1) Безбедност информационо-комуникационих система, што се односи на ризике нарушавања функционисања органа власти, привреде и организација као последица инцидената у информационо-комуникационим системима:

- успостављено је Владино Тело за координацију послова информационе безбедности у Републици Србији, које чине представници органа чији су послови од значаја за информациону безбедност;
- успостављен је Национални ЦЕРТ у оквиру РАТЕЛ-а;
- успостављен је ЦЕРТ републичких органа, као и ЦЕРТ-ови самосталних оператора ИКТ система;
- регистровано је 6 посебних ЦЕРТ-ова;
- успостављен је јединствени систем за пријем обавештења о инцидентима у ИКТ системима од посебног значаја;
- формирана је инспекција за информациону безбедност у Министарству трговине, туризма и телекомуникација;
- Национални ЦЕРТ и ЦЕРТ МУП акредитовани су на „Trusted Introducer” листи.

2) информациона безбедност грађана, што се односи на ризике нарушавања безбедности грађана злоупотребом информационо-комуникационих технологија:

- У фебруару 2017. године Министарство трговине, туризма и телекомуникација је основало Национални контакт центар за безбедност деце на интернету. Путем Националног контакт центра за безбедност деце на интернету, поред саветовања, омогућава се и пријем пријава штетног, непримереног и нелегалног садржаја и понашања на интернету, односно угрожености интереса и права деце, телефонским путем и путем електронског обрасца на веб сајту. Почев од оснивања, укупна комуникација регистрована у Националном контакт центру за безбедност деце на интернету остварена путем телефонских позива, мејлова, пријава путем сајта и друштвених мрежа од оснивања износи 7.965.
- Ради унапређења сарадње и размене идеја, оператери/едукатори Националног контакт центра за безбедност деце на интернету одржали су до данас презентације на тему безбедности деце на интернету и то:
    - За 150 запослених у домовима здравља (директорима, педијатрима школских диспанзера и психолозима) и
    - За 12.405 деце и 4.335 родитеља у 112 основних школа
- Од 2016. године Министарство трговине, туризма и телекомуникација сваке године спроводи „ИТ караван”, едукативну кампању за промоцију корисне, креативне и безбедне употребе информационих технологија. и укључује едукацију о

безбедности деце на интернету (представе за децу, интерактивни разговори са децом кроз илустративне примере, такмичарски квиз и сл.). ИТ караван, одржана је четврту годину за редом у 2019. години. До сада је овом кампањом обухваћено укупно 58 основних школа, више од 11.000 ђака, а директан пренос презентације, који је претходне године организован из Ниша и Новог Пазара, пратило је путем интернета још око 800 школа.

3) борба против високотехнолошког криминала, што се односи на превенцију и санкционисање кривичних дела која се заснивају на злоупотреби информационо-комуникационих технологија;

- Република Србија је потписница Конвенције о високотехнолошком криминалу, Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених преко рачунарских система, као и Конвенција Савета Европе о заштити деце од сексуалног искоришћавања и сексуалног злостављања.
- Република Србија је учествовала у пројекту „Сарадња у борби против криминала у сајбер простору: циљање имовине стечене криминалом на интернету у Југоисточној Европи и Турској"; научно-истраживачком пројекту „Advanced Tools for fighting online illegal trafficking – АНИТА (787061)" у склопу Horizon 2020; пројекту Европске уније и Савета Европе iPROCEEDS@IPA који има за циљ оспособљавање и јачање капацитета државних органа надлежних за борбу против високотехнолошког криминала у Републици Србији и земљама у региону у поступцима одузимања имовине у предметима високотехнолошког криминала.
- Према подацима Посебног одељења за борбу против високотехнолошког криминала у протеклих пет година на територији Републике Србије (период 2013–2017. година) стопа криминала је у порасту.

4) информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система;

- Од 2016. године у Републици Србији организују се на годишњем нивоу сајбер вежбе „Сајбер Тесла" у сарадњи Војске Србије и Националне гарде Охаја.
- У циљу подизања капацитета запослених у ЦЕРТ-овима у Републици Србији, укључујући и ЦЕРТ-ове самосталних оператора, у оквиру пројекта „Унапређење информационе безбедности" на Западном Балкану организоване су тренинзи и обуке.

5) међународна сарадња, што подразумева сарадњу са страним државним органима, међународним организацијама и другим партнерима у области информационе безбедности.

- Република Србија постала члан Глобалног форума за сајбер експертизу у 2018. години;
- Република Србија активно учествује у раду неформалне радне групе ОЕБС за дефинисање мера поверења у сајбер простору;
- Република Србија учествовала у раду Групе УН за информациону безбедност у 2017. години.

3) Да ли су уочени проблеми у области и на кога се они односе? Представити узроке и последице проблема.

Чланом 6. Закона дефинисани су ИКТ системи од посебног значаја и подељени су у три групе и то:

1) ИКТ системи који се користе у обављању послова у органима јавне власти;

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

3) ИКТ системи који се користе у обављању делатности од општег интереса.

Међутим, током имплементације Закона утврђено је да наведеном дефиницијом обухваћен велики број органа јавне власти, чији системи по свом значају не спадају у ИКТ системе од посебног значаја. Будући да примена мера заштите подразумева примену техничких и организационих мера, за чију примену су потребна финансијска улагања, ови системи су били у обавези да своје системе унапреде, односно примене мере заштите, међутим, предложеном изменом Закона, предвиђено је смањење броја ИКТ системе који се користе у органима јавне власти, јер је утврђено да ти системи нису од посебног значаја за информациону безбедност у Републици Србији.

Током имплементације Закона утврђено је да ИКТ системи од посебног значаја не достављају информације о инцидентима који значајно угрожавају информациону безбедност, иако су обавезни да то чине. Услед тога Национални ЦЕРТ није у могућности да прати трендове у овој области, нити да израђује анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањања потенцијалних инцидената.

У складу са Законом предвиђено је оснивање Националног ЦЕРТ, међутим, иако је Национални ЦЕРТ основан, потребно је и даље улагати у његове капацитете у смислу техничких, организационих и људских капацитета. Наиме, како би Национални ЦЕРТ био у могућности да пружа адекватну подршку ИКТ системима од посебног значаја у случају инцидената који значајно угрожавају информациону безбедност постојећи ресурси нису довољни, јер поред опреме, неопходно је да се Национални ЦЕРТ оснажи и запосли стручњаке у овој области. У супротном, може се наставити тренд непријављивања инцидената у ИКТ системима од посебног значаја, услед чега није могуће пратити кретања у овој области, нити предлагати мере за њено унапређење.

Како је у складу са Законом предвиђен рад како Националног ЦЕРТ, тако и ЦЕРТа републичких органа и ЦЕРТова самосталних оператора ИКТ система, у претходном периоду је констатовано да не постоји законски основ за њихову системску сарадњу која би омогућавала размену информација и међусобно пружање подршке у случају инцидената који значајно угрожавају информациону безбедност.

4) Која промена се предлаже и да ли је промена заиста неопходна и у ком обиму?

Измене Закона су инициране из разлога што је Закон ступио на снагу пре усвајања Директиве ЕУ о мерама за висок ниво безбедности мрежних и информационих система у Европској унији број 2016/1148 (у даљем тексту: НИС директива), која је усвојена у јулу 2016. године. Иако је био донет пре усвајања НИС директиве, Закон је у великој мери усклађен са овом директивом, будући да садржи решења која одговарају одредбама наведене директиве.

Међутим, изради Предлога закона о изменама и допунама Закона о информационој безбедности (у даљем тексту: Предлог закона) приступило се првенствено из два разлога: први је преостало усклађивање са одредбама НИС директиве ради постизања потпуне усаглашености Закона, а други је унапређење постојећих законодавних решења на бази потреба утврђених на основу досадашње примене.

Ради преосталих усклађивања са НИС директивом, у Предлогу закона извршене су следеће измене и допуне:

- допуна области у којима се користе ИКТ системи од посебног значаја, и то област дигиталне инфраструктуре и услуга информационог друштва (члан 6.);
- одређено је да се пре јавног објављивања обавештења о инциденту од стране надлежног органа изврше претходне консултације са оператором ИКТ система од посебног значаја који је доставио обавештење о инциденту (члан 11.);
- предвиђена је допуна одредаба о Националном ЦЕРТ-у које се односе на његову надлежност и потребне капацитете (члан 15.).

Током примене закона утврђена је потреба за изменом и допуном одређених норми, у циљу ефикаснијег спровођења закона у пракси. Сходно томе, Предлогом закона предвиђено је следеће:

- укључивање Народне банке Србије у рад Тела за координацију послова информационе безбедности (члан 5.);
- допуна области у којима се користе ИКТ системи од посебног значаја (производња и снабдевање хемикалијама, члан 6.);
- таксативно су набројане обавезе ИКТ система од посебног значаја (члан 6а);
- успостављање Евиденције оператора ИКТ система од посебног значаја (члан 6б);
- дефинисан је начин обавештавања о инцидентима који значајно угрожавају информациону безбедност преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима (члан 11.);
- обавеза Народне банке Србије и РАТЕЛ-а да добијена обавештења о инциденту проследе Надлежном органу (члан 11.);
- достављање обавештења о инциденту који је повезан са значајним нарушавањем информационе безбедности, које има или може имати

за последицу угрожавање националне безбедности, Безбедносно-информативној агенцији (члан 11.);

- дефинисани су инциденти који треба да се пријаве, а који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11а);
- одређена је обавеза ИКТ система од посебног значаја да достављају статистичке податке о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности (члан 11б);
- дефинисана је сарадња ЦЕРТ-ова у Републици Србији (члан 15а);
- додате су одредбе о заштити при коришћењу информационо-комуникационих технологија (члан 19а).

Наведене измене закона допринеће бољој повезаности свих релевантних актера у области информационе безбедности, будући да се Предлогом закона предвиђа успостављање евиденције ИКТ система од посебног значаја. На тај начин Надлежни орган и Национални ЦЕРТ имаће могућност интензивније сарадње са свим операторима ИКТ система од посебног значаја, нарочито у случају када се дешава инцидент, али у смислу пружања подршке, препоруке и савета за заштиту ИКТ система од посебног значаја.

Значајно унапређење лежи и у чињеници да је Надлежни орган успоставио Јединствени систем за пријем обавештења о инцидентима, тако да их ИКТ системи од посебног значаја обавештења могу прослеђивати преко портала Надлежног органа и Националног ЦЕРТ-а. Ово решење доприноси ефикасности пријављивања инцидената, као и потпуној информисаности свих релевантних учесника (Надлежни орган, Национални ЦЕРТ) који потом могу да учествују у отклањању инцидента.

Такође, Предлог закона предвиђа одредбе о Националном ЦЕРТ-у које се односе на јачање капацитета Националног ЦЕРТ-а, како би се успоставило благовремена и ефикасна подршка у случају инцидента, а за такву врсту подршке неопходно је стручно особље, одговарајућа инфраструктура у смислу опреме и просторија за рад, чије обезбеђивање је предвиђено Предлогом закона. Како Национални ЦЕРТ има и улогу превенције у области информационе безбедности, предвиђено је достављање статистичких података од стране ИКТ система од посебног значаја на бази којих ће Национални ЦЕРТ имати могућност израде адекватних анализа у области информационе безбедности и на основу чега ће припремати препоруке и савете за мере заштите у овој области.

С обзиром да је препозната потреба за континуираном сарадњом ЦЕРТ-ова у Републици Србији, предвиђене су одредбе којима се дефинише ова сарадња кроз организацију редовних заједничких састанака, а посебно у случају инцидената који значајно угрожавају информациону безбедност у Републици Србији.

Имајући у виду важност питања безбедности на интернету, Предлогом закона дефинисане су одредбе којима се предвиђају мере за безбедност и заштиту на интернету, као и генерално приликом коришћења информационо-комуникационих технологија.

5) На које циљне групе ће утицати предложена промена? Утврдити и представити циљне групе на које ће промена имати непосредан односно посредан утицај.

Измене и допуне Закона имаће непосредан утицај на:

- ИКТ системе од посебног значаја;
- Национални ЦЕРТ;
- нове ИКТ системе од посебног значаја у област дигиталне инфраструктуре и услуга информационог друштва
- ЦЕРТове самосталних оператора ИКТ система.

6) Због чега је неопходно постићи жељену промену на нивоу друштва? (одговором на ово питање дефинише се општи циљ).

Измене и допуне Закона су неопходне првенствено ради потпуног усклађивања са НИС директивом, а потом ради боље повезаности свих релевантних актера у области информационе безбедности, чиме се доприноси адекватнијем нивоу безбедности информационих система од посебног значаја у Републици Србији.

7) Шта се предметном променом жели постићи? (одговором на ово питање дефинишу се посебни циљеви, чије постизање треба да доводе до остварења општег циља. У односу на посебне циљеве, формулишу се мере за њихово постизање).

Изменама и допунама Закона постиже се успостављање евиденције о ИКТ системима од посебног значаја, што ће допринети бољој комуникацији између Министарства и Националног ЦЕРТа са једне стране и ИКТ система од посебног значаја са друге стране.

Наведена евиденција биће успостављена у Министарству као надлежном органу за информациону безбедност које поседује капацитете за вођење ове евиденције, будући да Министарство већ води различите врсте регистара из области електронског пословања.

Такође се предвиђа јачање капацитета Националног ЦЕРТа и то технолошких, људских и организационих капацитета, што ће Националном ЦЕРТу омогућити прелазак са информативне и саветодавне улоге на оперативнију улогу. Пружајући адекватнију помоћ ИКТ системима од посебног значаја у случају пријављених инцидената, поспешиће се међусобна сарадња и створити поверење што ће последично довести до тога да ИКТ системи од посебног значаја пријављују инциденте у складу са Законом.

Обавезивањем ИКТ система од посебног значаја да достављају статистичке податке о свим инцидентима који се дешавају у њиховим системима, Национални ЦЕРТ ће бити у могућности да прати трендове у овој области и припрема анализе ризика и инцидената на основу којих би се пружали савети и предлагале мере за отклањање потенцијалних инцидената.

Предвиђена сарадња између ЦЕРТова у Републици Србији омогућиће размену информација и међусобно пружање подршке у случају инцидената који значајно угрожавају информациону безбедност.

8) Да ли су општи и посебни циљеви усклађени са важећим документима јавних политика и постојећим правним оквиром, а пре свега са приоритетним циљевима Владе?

Стратегијом развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године неки од предвиђених приоритетних области

информационе безбедности у складу су са општим и посебним циљевима који се постижу изменама и допунама Закона, и то:

- безбедност информационо-комуникационих система, што се односи на ризике нарушавања функционисања органа власти, привреде и организација као последица инцидената у информационо-комуникационим системима и
- информациона безбедност Републике Србије, што се односи на ризике нарушавања националне безбедности путем информационо-комуникационих система.

9) На основу којих показатеља учинка ће бити могуће утврдити да ли је дошло до остваривања општих односно посебних циљева?

Основни показатељи учинка измена и допуна Закона огледају се у следећем:

- успостављена евиденција ИКТ система од посебног значаја
- успостављен систем доставе статистичких података од стране ИКТ система од посебног значаја
- успостављена сарадња између ЦЕРТова у Републици Србији.

На основу горе наведених показатеља, успоставиће се Евиденција ИКТ система од посебног значаја, што ће омогућити координацију са ИКТ системима од посебног значаја и дати могућност за преиспитивање обухвата ИКТ система од посебног значаја и на бази тога формирање додатних критеријума за њихово утврђивање.

На основу достављених статистичких података, биће омогућено испуњавање законских одредби који се тичу праћења стања у области информационе безбедности и израда неопходних анализа у овој области, а циљу унапређења стања у ИКТ системима од посебног значаја.

Увођењем механизма сарадње између ЦЕРТ-ова у Републици Србији доприноси се већем степену заштите ИКТ система у свим областима у Републици Србији и бољој координацији у случају инцидената који могу да угрозе информациону безбедност, али и националну безбедност Републике Србије.

10) Да ли је финансијске ресурсе за спровођење изабране опције потребно обезбедити у буџету, или из других извора финансирања и којих?

Средства потребна за реализацију обавеза из Предлога закона није потребно обезбедити у буџету, будући да ће иста бити обезбеђена из средстава РАТЕЛа, за потребе подизања капацитета Националног ЦЕРТа.

11) Колики су процењени трошкови увођења промена који проистичу из спровођења изабране опције (оснивање нових институција, реструктурирање постојећих институција и обука државних службеника) исказани у категоријама капиталних трошкова, текућих трошкова и зарада и да ли је могуће финансирати расходе изабране опције кроз редистрибуцију постојећих средстава?

Будући да је НИС директивом предвиђено повећавање капацитета Националног ЦЕРТа у наредном периоду предвиђа се повећавање броја запослених као и куповина неопходне опреме. У том смислу трошкови повећања капацитета Националног ЦЕРТа би били следећи:

- 150.000 евра за набавку платформе за увежбавање сајбер напада ради промовисања информационе безбедности;
- 10.000 евра у периоду од три године за набавку форензичке лабораторије;
- 20.000 евра у периоду од три године за набавку софтвер за сајбер безбедност и пратеће лиценце;
- 15.000 евра у периоду од три године за набавку хардвера;
- 144.000 евра у периоду од три године дана износ зараде за 5 новозапослених (5 х запослених х 800 евра х 3 године);
- 90.000 евра у периоду од три године за обуке за запослене (10 запослених х 3.000 евра х 3 године)

12) Које трошкове и користи (материјалне и нематеријалне) ће изабрана опција проузроковати привреди, појединој грани, односно одређеној категорији привредних субјеката?

Нови ИКТ системи од посебног значаја у области дигиталне инфраструктуре и услуга информационог друштва који су предвиђени изменама и допунама Закона су у обавези да примене мере заштите, односно техничке и организационе мере у циљу успостављања адекватног нивоа безбедности система.

Уколико су ти привредни субјекти већ 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. Међутим, привредни субјекти који представљају операторе ИКТ система од посебног значаја у складу са изменама Закона, 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.

13) Да ли је за спровођење изабране опције обезбеђена подршка свих кључних заинтересованих страна и циљних група? Да ли је спровођење изабране опције приоритет за доносиоце одлука у наредном периоду (Народну скупштину, Владу, државне органе и слично)?

Министарство трговине, туризма и телекомуникација је у 2018. години формирало радну групу за израду Нацрта закона о изменама и допунама

Закона о информационој безбедности кога су чинили представници релевантних министарстава и институција.

Министарство трговине, туризма и телекомуникација спровело је јавну расправу о Нацрту закона о изменама и допунама Закона о информационој безбедности у периоду од 04. до 25. фебруара 2019. године, на основу закључука Одбора за привреду и финансије Владе 05 Број: 011-882/2019 од 31. јануара 2019. 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 20. фебруара 2019. 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 по окончању јавне расправе путем Министарства за европске интеграције упутило Нацрт закона Европској комисији, ради давања мишљења.

Доношење овог закона је приоритет имајући у виду чињеницу да се истим врши усклађивање са европском регулативом, односно НИС директивом.

14) Које додатне мере треба спровести и колико времена ће бити потребно да се спроведе изабрана опција и обезбеди њено касније доследно спровођење, односно њена одрживост?

Ради реализације Предлога закона, предвиђено је доношење следећих подзаконских аката:

- Уредба о утврђивању Листе делатности у којима се користе ИКТ системи од посебног значаја;
- Уредба о поступку обавештавања о инцидентима, листи, врстама и значају инцидената према нивоу опасности, поступање и размени информација о инцидентима
- Правилник о евиденцији ИКТ система од посебног значаја;
- Правилник о статистичким подацима о инцидентима у ИКТ системима од посебног значаја
- Уредба о начину спровођења мера за безбедност и заштиту деце на интернету.

15) Да ли су обезбеђена финансијска средства за спровођење изабране опције? Да ли је за спровођење изабране опције обезбеђено довољно времена за спровођење поступка јавне набавке уколико је она потребна?

Средства за реализацију законских обавеза обезбеђује РАТЕЛ, као организација у чијем се саставу налази Национални ЦЕРТ. Очекује се да ће у буџету наведене институције почев од 2020. године бити обезбеђена средства потребна за додатно запошљавање као и за куповину неопходне опреме.

ОБРАЗАЦ ИЗЈАВЕ О УСКЛАЂЕНОСТИ ПРОПИСА СА ПРОПИСИМА ЕВРОПСКЕ УНИЈЕ

1. Орган државне управе, односно други овлашћени предлагач прописа: Влада
   Обрађивач: Министарство трговине, туризма и телекомуникација

2. Назив прописа

Предлог закона о изменама и допунама Закона о информационој безбедности
Draft Law on Amendments to the 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):

а) Одредба Споразума која се односе на нормативну садржину прописа

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

Три године.

в) Оцена испуњености обавезе које произлазе из наведене одредбе Споразума

Испуњава у потпуности.

г) Разлози за делимично испуњавање, односно неиспуњавање обавеза које произлазе из наведене одредбе Споразума
/
д) Веза са Националним програмом за усвајање правних тековина Европске уније

Национални програм за усвајање правних тековина Европске уније, 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 1, Шифра план. прописа: 2017-510

4. Усклађеност прописа са прописима Европске уније:

а) Навођење одредби примарних извора права Европске уније и оцене усклађености са њима
/
б) Навођење секундарних извора права Европске уније и оцене усклађености са њима

Директива ЕУ о мерама за висок ниво безбедности мрежних и информационих система у Европској унији број 2016/1148 (НИС директива) која је усвојена у јулу 2016. године.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

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).
/

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?

Предлог закона о изменама и допунама Закона о информационој безбедности преведен је на енглески језик.

8. Сарадња са Европском унијом и учешће консултаната у изради прописа и њихово мишљење о усклађености

Предлог закона о изменама и допунама Закона о информационој безбедности послат је на мишљење Европској комисији.

1. Назив прописа Европске уније : Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	2. „CELEX" ознака ЕУ прописа 32016L1148
3. Орган државне управе, односно други овлашћени предлагач прописа: Влада	4. Датум израде табеле:
Обрађивач: Министарство трговине, туризма и телекомуникација	25.3.2019.
5. Назив (нацрта, предлога) прописа чије одредбе су предмет анализе усклађености са прописом Европске уније: Предлог закона о изменама и допунама Закона о информационој безбедности	6. Бројчане ознаке (шифре) планираних прописа из базе НПАА: 2017-510
7. Усклађеност одредби прописа са одредбама прописа ЕУ:	

а)	а1)	б)	б1)	в)	г)	д)
Одредба прописа ЕУ	Садржина одредбе	Одредбе прописа Р. Србије	Садржина одредбе	Усклађеност[1]	Разлози за делимичну усклађеност, неусклађеност или непреносивост	Напомена о усклађености
1.1.	This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.			НП	Одредба је непреносива, с обзиром да се њоме одређује предмет ЕУ директиве.	
1.2.	To that end, this Directive: (a) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems;			НП	Одредба је непреносива, с обзиром да се њоме одређује предмет ЕУ директиве.	

[1] Потпуно усклађено - ПУ, делимично усклађено - ДУ, неусклађено - НУ, непреносиво – НП

а)	а1)	б)	б1)	в)	г)	д)
	(b) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; (c) creates a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; (d) establishes security and notification requirements for operators of essential services and for digital service providers; (e) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.					
1.3.	The security and notification requirements provided for in this Directive shall not apply to undertakings which are subject to the requirements of Articles 13a and 13b of Directive 2002/21/EC, or to trust service providers which are subject to the requirements of Article 19 of Regulation (EU) No 910/2014.			НП	Одредба је непреносива, с обзиром да се њом одређује примена ЕУ директиве.	
1.4.	This Directive applies without prejudice to Council Directive 2008/114/EC (14) and Directives 2011/93/EU (15) and 2013/40/EU (16) of the European Parliament and of the Council.			НП	Одредба је непреносива, с обзиром да се њом одређује примена ЕУ директиве.	
1.5.	Without prejudice to Article 346 TFEU, information that is confidential pursuant to Union			НП	Одредба је непреносива, с обзиром да регулише размену поверљивих	

а)	а1)	б)	б1)	в)	г)	д)
	and national rules, such as rules on business confidentiality, shall be exchanged with the Commission and other relevant authorities only where such exchange is necessary for the application of this Directive. The information exchanged shall be limited to that which is relevant and proportionate to the purpose of such exchange. Such exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of operators of essential services and digital service providers.				информација држава чланица ЕУ са Европском комисијом и другим телима ЕУ.	
1.6.	This Directive is without prejudice to the actions taken by Member States to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Member States consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.			НП	Одредба је непреносива, с обзиром да регулише размену поверљивих информација држава чланица ЕУ са Европском комисијом и другим телима ЕУ.	
1.7.	Where a sector-specific Union legal act requires operators of essential services or digital service providers either to ensure the security of their network and information systems or to notify incidents, provided that such requirements are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.			НП	Одредба је непреносива, јер се њоме одређује да други акти ЕУ који прописују мере заштите ИКТ система и обавештавање о инцидентима у ИКТ системима за поједине области треба да пропишу одредбе које захтевају најмање једнак ниво обавеза као НИС директива.	
2.1.	Processing of personal data pursuant to this Directive shall be carried out in accordance with Directive 95/46/EC.	3а	У случају обраде података о личности приликом вршења надлежности и испуњења обавеза из овог закона поступа се	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			у складу са прописима који уређују заштиту података о личности.			
2.2.	Processing of personal data by Union institutions and bodies pursuant to this Directive shall be carried out in accordance with Regulation (EC) No 45/2001.			НП	Одредба прописује обраду личних податке од стране институција и тела ЕУ.	
3.	Without prejudice to Article 16(10) and to their obligations under Union law, Member States may adopt or maintain provisions with a view to achieving a higher level of security of network and information systems.			НП	Одредба се односи на давање могућности државама чланицама ЕУ да својим прописима одреде виши ниво безбедности ИКТ система.	
4.1.	'For the purposes of this Directive, the following definitions apply: network and information system' means:	2.1.1.	Поједини термини у смислу овог закона имају следеће значење: информационо -комуникациони систем (ИКТ систем) је технолошко -организациона целина која обухвата:	ПУ		
4.1.a)	an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC;	2.1.1.1.	електронске комуникационе мреже у смислу закона који уређује електронске комуникације	ПУ		
4.1.b)	any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or	2.1.1.2.	уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			уређаја, врши аутоматска обрада података коришћењем рачунарског програма;			
4.1.c)	digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;	2.1.1.3.	податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава из подтач. (1) и (2) ове тачке, а у сврху њиховог рада, употребе, заштите или одржавања.	ПУ		
4.2.	‘security of network and information systems’ means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;	2.1.3.	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;	ПУ		
4.3.	‘national strategy on the security of network and information systems’ means a framework providing strategic objectives and priorities on the security of			НП	Одредба није преносива у Закон о информационој безбедности, будући да су другим прописима РС утврђени појам и предмет стратегија	

а)	а1)	б)	б1)	в)	г)	д)
	network and information systems at national level;				Владе.	
4.4.	‘operator of essential services’ means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);	2.1.2.	оператор ИКТ система је правно лице, орган власти или организациона јединица органа власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности	ПУ		
4.5.	‘digital service’ means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council (17) which is of a type listed in Annex III;	2.1.25.	25) услуга информационог друштва је услуга у смислу закона којим се уређује електронска трговина	ПУ		
4.6.	‘digital service provider’ means any legal person that provides a digital service;	2.1.26.	26) пружалац услуге информационог друштва је правно лице које је пружалац услуге у смислу закона којим се уређује електронска трговина	ПУ		
4.7.	‘incident’ means any event having an actual adverse effect on the security of network and information systems;	2.1.11.	инцидент је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;	ПУ		
4.8.	‘incident handling’ means all procedures supporting the detection, analysis and containment of an incident and the response thereto;	7.3.27.	Мере заштите ИКТ система се односе на: 27) превенцију и	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама			
4.9.	‘risk’ means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;	2.1.9.	ризик значи могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;	ПУ		
4.10.	‘representative’ means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;			НП	Одредба је непреносива, с обзиром да се односи на појам представника (заступника) са пребивалиштем или седиштем у Европској унији. Закон о информационој безбедности се односи на ИКТ системе у Републици Србији.	
4.11.	‘standard’ means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;	7.4.	Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			уважавајући начела из члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.			
4.12.	‘specification’ means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;	7.4.	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.	ПУ		
4.13.	‘internet exchange point (IXP)’ means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;	6.1.3.5.1.	ИКТ системи од посебног значаја су системи који се користе: (5) дигитална инфраструктура: - размена интернет саобраћаја;	ПУ		
4.14.	‘domain name system (DNS)’ means a hierarchical distributed naming system in a network which refers queries for domain names;	6.1.3.5.2.	ИКТ системи од посебног значаја су системи који се користе: (5) дигитална инфраструктура:	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			- управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)			
4.15.	‘DNS service provider’ means an entity which provides DNS services on the internet;	6.1.3.5.2.	ИКТ системи од посебног значаја су системи који се користе: (5) дигитална инфраструктура: - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)	ПУ		
4.16.	top-level domain name registry’ means an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD);	6.1.3.5.2.	ИКТ системи од посебног значаја су системи који се користе: 5) дигитална инфраструктура: - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)	ПУ		
4.17.	‘online marketplace’ means a digital service that allows consumers and/or traders as respectively defined in point (a) and in point (b) of Article 4(1) of Directive 2013/11/EU of the European Parliament and of the Council (18) to conclude online sales or service contracts with traders either on the online marketplace's website or	6.1.3.7.	ИКТ системи од посебног значаја су системи који се користе: (7)услуге информационог друштва:	ДУ	Ова врста ИКТ система од посебног значаја биће дефинисана подзаконским актом.	

а)	а1)	б)	б1)	в)	г)	д)
	on a trader's website that uses computing services provided by the online marketplace;		- услуге информационог друштва у смислу члана 2. тачка 25) овог закона			
4.18.	‘online search engine’ means a digital service that allows users to perform searches of, in principle, all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;	6.1.3.7.	ИКТ системи од посебног значаја су системи који се користе: (7)услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона	ДУ	Ова врста ИКТ система од посебног значаја биће дефинисана подзаконским актом.	
4.19.	‘cloud computing service’ means a digital service that enables access to a scalable and elastic pool of shareable computing resources.	6.1.3.7.	ИКТ системи од посебног значаја су системи који се користе: (7)услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона	ДУ	Ова врста ИКТ система од посебног значаја биће дефинисана подзаконским актом.	
5.1.	By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory.			НП	Одредба је непреносива у Закон о изменама и допунама Закона о информационој безбедности, с обзиром да прописује обавезу држава чланица да у датом року утврде листу оператора кључних услуга на својој територији.	

а)	а1)	б)	б1)	в)	г)	д)
5.2.	The criteria for the identification of the operators of essential services, as referred to in point (4) of Article 4, shall be as follows:	6.1.				
5.2.а)	an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;	6.1.	ИКТ системи од посебног значаја су системи који се користе: 1) у обављању послова у органима власти; 2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности; 3) у обављању делатности од општег интереса и другим делатностима и то у следећим областима: (1) енергетика: - производња, пренос и дистрибуција електричне енергије; - производња и прерада угља; - истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата; - истраживање, производња, прерада, транспорт и дистрибуција природног и течног	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			гаса. (2) саобраћај: - железнички, поштански, водени и ваздушни саобраћај; (3) здравство: - здравствена заштита; (4) банкарство и финансијска тржишта: - послови финансијских институција; - послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама; - послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта; (5) дигитална инфраструктура: - размена интернет саобраћаја; - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи) (6) добра од општег интереса: - коришћење, управљање, заштита и унапређивање добара			

а)	а1)	б)	б1)	в)	г)	д)
			од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја); (7) услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона; (8) остале области: - електронске комуникације; - издавање службеног гласила Републике Србије; - управљање нуклеарним објектима; - производња, промет и превоз наоружања и војне опреме; - управљање отпадом; - комуналне делатности; - производња и снабдевање хемикалијама. 4) у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне			

а)	а1)	б)	б1)	в)	г)	д)
			самоуправе за обављање делатности из тачке 3) овог става.			
5.2b)	the provision of that service depends on network and information systems; and	6.1.	ИКТ системи од посебног значаја су системи који се користе: 1) у обављању послова у органима власти; 2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности; 3) у обављању делатности од општег интереса и другим делатностима и то у следећим областима: (1) енергетика: - производња, пренос и дистрибуција електричне енергије; - производња и прерада угља; - истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата; - истраживање, производња, прерада, транспорт и дистрибуција природног и течног	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			гаса. (2) саобраћај: - железнички, поштански, водени и ваздушни саобраћај; (3) здравство: - здравствена заштита; (4) банкарство и финансијска тржишта: - послови финансијских институција; - послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама; - послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта; (5) дигитална инфраструктура: - размена интернет саобраћаја; - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи) (6) добра од општег интереса: - коришћење, управљање, заштита и унапређивање добара			

а)	а1)	б)	б1)	в)	г)	д)
			од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја); (7) услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона; (8) остале области: - електронске комуникације; - издавање службеног гласила Републике Србије; - управљање нуклеарним објектима; - производња, промет и превоз наоружања и војне опреме; - управљање отпадом; - комуналне делатности; - производња и снабдевање хемикалијама. 4) у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне			

а)	а1)	б)	б1)	в)	г)	д)
			самоуправе за обављање делатности из тачке 3) овог става.			
5.2.c)	an incident would have significant disruptive effects on the provision of that service.	6.1.	ИКТ системи од посебног значаја су системи који се користе: 1) у обављању послова у органима власти; 2) за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности; 3) у обављању делатности од општег интереса и другим делатностима и то у следећим областима: (1) енергетика: - производња, пренос и дистрибуција електричне енергије; - производња и прерада угља; - истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата; - истраживање, производња, прерада, транспорт и дистрибуција природног и течног	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			гаса. (2) саобраћај: - железнички, поштански, водени и ваздушни саобраћај; (3) здравство: - здравствена заштита; (4) банкарство и финансијска тржишта: - послови финансијских институција; - послови вођења регистра података о обавезама физичких и правних лица према финансијским институцијама; - послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта; (5) дигитална инфраструктура: - размена интернет саобраћаја; - управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи) (6) добра од општег интереса: - коришћење, управљање, заштита и унапређивање добара			

а)	а1)	б)	б1)	в)	г)	д)
			од општег интереса (воде, путеви, минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја); (7) услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона; (8) остале области: - електронске комуникације; - издавање службеног гласила Републике Србије; - управљање нуклеарним објектима; - производња, промет и превоз наоружања и војне опреме; - управљање отпадом; - комуналне делатности; - производња и снабдевање хемикалијама. 4) у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне			

а)	а1)	б)	б1)	в)	г)	д)
			самоуправе за обављање делатности из тачке 3) овог става. Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу делатности из става 1. тачка 3) овог члана.”			
5.3.	For the purposes of paragraph 1, each Member State shall establish a list of the services referred to in point (a) of paragraph 2.	6.2.	Влада, на предлог министарства надлежног за послове информационе безбедности, утврђује листу делатности из става 1. тачка 3) овог члана.”	ПУ		
5.4.	For the purposes of paragraph 1, where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other. That consultation shall take place before a decision on identification is taken.			НП	Одредба се односи на сарадњу две или више држава чланица ЕУ у случају да оператор ИКТ система пружа услуге у две или више држава чланица.	
5.5.	Member States shall, on a regular basis, and at least every two years after 9 May 2018, review and, where appropriate, update the list of identified operators of essential services.			НП	Одредба се односи на обавезу држава чланица ЕУ да на сваке две године размотре листе оператора кључних услуга и по потреби их мењају.	
5.6.	The role of the Cooperation Group shall be, in accordance with the tasks referred to in Article 11, to support Member States in taking a consistent approach in the process of identification of operators of essential services.			НП	Норма се односи на задатаак Групе за сарадњу коју, на основу члана 11. предметне директиве образују представници држава чланица ЕУ, Европске комисије и ЕНИСА.	

а)	а1)	б)	б1)	в)	г)	д)
5.7. 5.8.	For the purpose of the review referred to in Article 23 and by 9 November 2018, and every two years thereafter, Member States shall submit to the Commission the information necessary to enable the Commission to assess the implementation of this Directive, in particular the consistency of Member States' approaches to the identification of operators of essential services. That information shall include at least: a) national measures allowing for the identification of operators of essential services; b) the list of services referred to in paragraph 3; c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector; d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1). In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph.			НП	Одредбе су непреносиве, с обзиром да се односи на обавезу држава чланица ЕУ да подносе Европској комисији извештаје о примени директиве, као и да се односи на садржај извештаја.	
6.1.	When determining the significance of a disruptive			НП	Одредба је непреносива, с обзиром	

а)	а1)	б)	б1)	в)	г)	д)
	effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors: a)the number of users relying on the service provided by the entity concerned; b)the dependency of other sectors referred to in Annex II on the service provided by that entity; c)he impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; d)the market share of that entity; e)the geographic spread with regard to the area that could be affected by an incident; f)the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.				да су њоме предвиђене смернице за одређивање оператора кључних услуга приликом израде одговарајућих прописа.	
6.2.	In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors.			НП	Одредба је непреносива, с обзиром да је њоме предвиђена смерница за одређивање оператора кључних услуга приликом израде одговарајућих прописа.	
7.1.	Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at			ПУ	Република Србија је усвојила Стратегију развоја информационе безбедности у Републици Србњи за период од 2017.до 2020. године («Службени гласник РС» 53/17), у складу са обавезом из НИС	

а)	а1)	б)	б1)	в)	г)	д)
	least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues: a)the objectives and priorities of the national strategy on the security of network and information systems; b)a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors; c)the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors; d)an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems; e)an indication of the research and development plans relating to the national strategy on the security of network and information systems; f)a risk assessment plan to identify risks; g)a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.				директиве.	
7.2.	Member States may request the assistance of ENISA in developing national strategies on the security of network and information systems.			НП	Одредба је непреносива, јер се односи на могућност држава чланица ЕУ да приликом израде националних стратегија замоле за помоћ ЕНИСА.	

а)	а1)	б)	б1)	в)	г)	д)
7.3.	Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. In so doing, Member States may exclude elements of the strategy which relate to national security.			НП	Одредба је непреносива, јер се односи на обавезу држава чланица ЕУ да доставе Европској комисији своје националне стратегије у року од три месеца од дана усвајања.	
8.1.	Each Member State shall designate one or more national competent authorities on the security of network and information systems (‘competent authority’), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities.	4.	Орган државне управе надлежан за безбедност ИКТ система је министарство надлежно за послове информационе безбедности (у даљем тексту: Надлежни орган).	ПУ		
8.2.	The competent authorities shall monitor the application of this Directive at national level.	16. 28.	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. Инспекција за	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			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.			
8.3.	Each Member State shall designate a national single point of contact on the security of network and	12.1.	Надлежни орган остварује	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	information systems (‘single point of contact’). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.		међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова: 1) брзо расту или имају тенденцију да постану високоризични; 2) превазилазе или могу да превазиђу националне капацитете; 3) могу да имају негативан утицај на више од једне државе.			
8.4.	The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12.	12.1.	Надлежни орган остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова: 1) брзо расту или имају тенденцију да постану високоризични; 2) превазилазе или могу да превазиђу националне капацитете; 3) могу да имају негативан утицај на	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			више од једне државе.			
8.5.	Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the Cooperation Group.			НП	Одредба је непреносива, с обзиром да се односи на обавезу држава чланица ЕУ да обезбеде адекватне ресурсе за примену ове директиве.	
8.6.	The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.			НП	Према законодавству Републике Србије, државни органи су у обавези да међусобно сарађују, те сматрамо да није неопходно да се ова одредба пренесе у овај закон.	
8.7.	Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts.			НП	Одредба је непреносива, с обзиром да се односи на обавезу држава чланица ЕУ да обавесте Европску комисију о надлежним органима и тачкама за контакт.	
9.1.	Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority.	14.	Национални центар за превенцију безбедносних ризика у ИКТ системима обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.			
9.2.	Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I. Member States shall ensure the effective, efficient and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12.			НП	Одредба је непреносива, с обзиром да се односи на обавезу чланица ЕУ да обезбеде адекватне ресурсе за функционисање ЦЕРТ-ова, као и на обавезу сарадње са националним ЦЕРТ-овима држава чланица ЕУ.	
9.3.	Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level.	15.4.	У циљу обезбеђивања континуитета рада, Национални ЦЕРТ треба да: 1) буде опремљен са одговарајућим системима за управљање инцидентима; 2) има довољно запослених како би се осигурала доступност у свако доба; 3) обезбеди инфраструктуру чији је континуитет осигуран, односно да обезбеди редундантне системе и резервни радни простор.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
9.4.	Member States shall inform the Commission about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.		.	НП	Одредба је непреносива, јер се односи на обавезу обавештавања Европске комисије од стране држава чланица о раду Националног ЦЕРТ-а.	
9.5.	Member States may request the assistance of ENISA in developing national CSIRTs.			НП	Одредба је непреносива, с обзиром да се односи на право чланица ЕУ да затраже помоћ ЕНИСА у развоју националних ЦЕРТ-ова.	
10.1.	Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive.	15.6.	Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом органа власти.	ПУ		
10.2.	Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6).	11.1.	Оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			за пријем обавештења који одржава Надлежни орган.			
10.3.	Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive. By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6).			НП	Одредба је непреносива, с обзиром да се односи на обавезу подношења извештаја ЕУ Групи за координацију о инцидентима.	
11.1.	1. In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems in the Union, a Cooperation Group is hereby established. 2. The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3. 11.2. The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA. Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work.			НП	Одредбе су непреносиве, с обзиром да се односи на успостављање, састав, послове и обавезе тела Европске уније (Групе за координацију).	

а)	а1)	б)	б1)	в)	г)	д)
	The Commission shall provide the secretariat. 3. The Cooperation Group shall have the following tasks: a) providing strategic guidance for the activities of the CSIRTs network established under Article 12; b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6); c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems; d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice; e) exchanging information and best practice on awareness-raising and training; f) exchanging information and best practice on research and development relating to the security of network and information systems; g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies; h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations; i) collecting best practice information on risks and incidents;					

а)	а1)	б)	б1)	в)	г)	д)
	j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3); k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA; l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents; m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16. By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive. 4. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article. 5. The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).					

а)	а1)	б)	б1)	в)	г)	д)
	For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017.					
12.	In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established. 2. The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs. 3.The CSIRTs network shall have the following tasks: a) exchanging information on CSIRTs' services, operations and cooperation capabilities; b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident; c) exchanging and making available on a voluntary basis non-confidential information concerning			НП	Одредбе су непреносиве, с обзиром да се односи на успостављање, састав, послове и обавезе тела Европске уније (мреже ЦЕРТ-ова ЕУ).	

а)	а1)	б)	б1)	в)	г)	д)
	individual incidents; d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State; e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance; f) discussing, exploring and identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents; g)informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard; h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA; i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; .j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation. 4. For the purpose of the review referred to in					

а)	а1)	б)	б1)	в)	г)	д)
	Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under this Article. That report shall also be submitted to the Cooperation Group. 5. The CSIRTs network shall lay down its own rules of procedure.					
13.	The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data.			НП	Одредба је непреносива, јер се односи на закључење међународних уговора Европске уније са трећим државама о придруживању појединим активностима Групе за координацију.	
14.1.	Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.	7.2.	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.	ПУ		
14.2	Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and	7.2.	Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.		од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.			
14.3.	Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.	11.1.	Оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима који одржава Надлежни орган.	ПУ		
14.4.a)	In order to determine the significance of the impact of an incident, the following parameters in particular shall be taken into account: the number of users affected by the disruption of the essential service;	11а.1.2.	Оператор ИКТ система од посебног значаја дужан је да пријави следеће инциденте: 2) инциденти који утичу на велики број корисника услуга, или трају дужи временски период.	ПУ		
14.4.b)	the duration of the incident;	11а.1.1.	1) инциденти који доводе до прекида континуитета вршења	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
		11а.1.2.	послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга; 2) инциденти који утичу на велики број корисника услуга, или трају дужи временски период.			
14.4.c)	the geographical spread with regard to the area affected by the incident.	11а.1.4.	4) инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;	ПУ		
14.5.1.	On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification.	12.1.1.	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;	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			3) могу да имају негативан утицај на више од једне државе.			
14.5.2.	Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling.	15.1.3.	Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно: 3) реагује по пријављеним или на други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и другим ИКТ системима у Републици Србији, тако што пружа савете и препоруке на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			основу добијених сазнања			
14.5.3.	At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States.	12.1.	Надлежни орган остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова: 1) брзо расту или имају тенденцију да постану високоризични; 2) превазилазе или могу да превазиђу националне капацитете; 3) могу да имају негативан утицај на више од једне државе.	ПУ		
14.6.	After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident.	11.10..	Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 3. овог члана коме се упућују обавештења о инцидентима, може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио..	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
14.7.	Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4.			НП	Одредба је непреносива, с обзиром да се односи на рад тела ЕУ (Групе за координацију).	
15.1.	Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems.	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	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			безбедност утврђује да ли су испуњени услови прописани овим законом и прописима донетим на основу овог закона.			
15.2.a)	Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide: the information necessary to assess the security of their network and information systems, including documented security policies;	29.1.	Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом: 1) наложи отклањање утврђених неправилности и за то остави рок; 2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок.	ПУ		
15.2.b)	evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.	29.1.	Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required.		вршења инспекцијског надзора утврђених законом: 1) наложи отклањање утврђених неправилности и за то остави рок; 2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок.			
15.3.	Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified.	29.1.	Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом: 1) наложи отклањање утврђених неправилности и за то остави рок; 2) забрани коришћење поступака и техничких средстава којима се угрожава или нарушава информациона безбедност и за то остави рок.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
15.4.	The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches.			НП		Обавеза пријављивања нарушавања права на заштиту података о личности, као и сарадње руковаоца података о личности са Повереником већ је утврђена Законом о заштити података о личности.
16.1.а)	Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: the security of systems and facilities;	6.1.3.7. 7.2.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (7) услуге информационог друштва. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
16.1.b)	incident handling;	7.3.27.	Мере заштите ИКТ система се односе на: 27) превенцију и реаговање на безбедносне инциденте, што подразумева адекватну размену информација о безбедносним слабостима ИКТ система, инцидентима и претњама;	ПУ		
16.1.c)	business continuity management;	7.3.28.	28) мере које обезбеђују континуитет обављања посла у ванредним околностима.	ПУ		
16.1.d)	monitoring, auditing and testing;	8.4.	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.	ПУ		
16.1.e)	compliance with international standards.	7.4.	Влада, на предлог Надлежног органа, ближе уређује мере заштите ИКТ система уважавајући начела из	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			члана 3. овог закона, националне и међународне стандарде и стандарде који се примењују у одговарајућим областима рада.			
16.2.	Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.	7.3.28.	28) мере које обезбеђују континуитет обављања посла у ванредним околностима.	ПУ		
16.3.	Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.	11.1.	Оператори ИКТ система од посебног значаја обавештавање о инцидентима у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности врше преко портала Надлежног органа или Националног ЦЕРТ-а у јединствени систем за пријем обавештења о инцидентима који одржава Надлежни орган.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
16.4.a)	In order to determine whether the impact of an incident is substantial, the following parameters in particular shall be taken into account: the number of users affected by the incident, in particular users relying on the service for the provision of their own services;	11a.1.2.	Оператор ИКТ система од посебног значаја дужан је да пријави следеће инциденте: 2) инциденте који утичу на велики број корисника услуга, или трају дужи временски период;	ПУ		
16.4.b)	the duration of the incident;	11a.1.1. 11a.1.2.	1) инциденти који доводе до прекида континуитета вршења послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга; 2) инциденти који утичу на велики број корисника услуга, или трају дужи временски период.	ПУ		
16.4.c)	the geographical spread with regard to the area affected by the incident;	11a.1.4.	4) инциденти који доводе до прекида континуитета, односно тешкоће у вршењу послова и пружању услуга и имају утицај на већи део територије Републике Србије;	ПУ		
16.4.d)	the extent of the disruption of the functioning of the service;	11a.1.1.	1) инциденти који доводе до прекида континуитета вршења	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			послова и пружања услуга, односно знатних тешкоћа у вршењу послова и пружању услуга;			
16.4.e)	the extent of the impact on economic and societal activities. The obligation to notify an incident shall only apply where the digital service provider has access to the information needed to assess the impact of an incident against the parameters referred to in the first subparagraph.	11а.1.3.	3) инциденти који доводе до прекида континуитета, односно тешкоћа у вршењу послова и пружања услуга, који утичу на обављање послова и вршење услуга других оператора ИКТ система од посебног значаја или утичу на јавну безбедност;	ПУ		
16.5	Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator.	11а.1.6.	6) инциденте који су настали као последица инцидента у ИКТ систему из члана 6. став 1. тачка 3) подтачка (7) овог закона, када ИКТ систем од посебног значаја у свом пословању користи информационе услуге ИКТ система из члана 6. став 1. тачка 3) подтачка (7) овог закона.	ПУ		
16.6.	Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected	12.1.	Надлежни орган остварује међународну сарадњу у области безбедности ИКТ система, а	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided.	11.10.	нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова: 1) брзо расту или имају тенденцију да постану високоризични; 2) превазилазе или могу да превазиђу националне капацитете; 3) могу да имају негативан утицај на више од једне државе. Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 3. овог члана коме се упућују обавештења о инцидентима, може објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио..			
16.7.	After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where	11.10.	Ако је инцидент од интереса за јавност, Надлежни орган, односно орган из става 3. овог члана коме се упућују обавештења о инцидентима, може	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.		објавити информацију о инциденту, након саветовања са оператором ИКТ система од посебног значаја у коме се инцидент догодио..			
16.8.	The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017.			НП	Одредба је непреносива, јер се њоме одређује овлашћење Европској комисији да ближе уреди одредбе ове директиве.	
16.9.	The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2).			НП	Одредба је непреносива, јер се њоме одређује овлашћење Европској комисији да ближе уреди одредбе ове директиве.	
16.10.	Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers.			НП	Одредба је непреносива, јер се односи на обавезу држава чланица ЕУ да у свом законодавству не предвиде додатне захтеве за пружаоце дигиталних услуга.	
16.11.	Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (19).			НУ	Одредба није усклађена, јер и оваква предузећа могу да обављају делатности које су од посебног значаја.	
17.1.	Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such	28.1.	Инспекција за информациону безбедност врши инспекцијски надзор над применом овог закона и радом оператора ИКТ	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	evidence may be submitted by a competent authority of another Member State where the service is provided.		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.			
17.2.a)	For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to: provide the information necessary to assess the security of their network and information systems, including documented security policies;	28.3.	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.	ПУ		
17.2.b)	remedy any failure to meet the requirements laid down in Article 16.	29.1.1.	Инспектор за информациону безбедност је овлашћен да у поступку спровођења надзора, поред налагања мера за које је овлашћен инспектор у поступку вршења инспекцијског надзора утврђених законом: 1) наложи отклањање утврђених неправилности и за то остави рок;	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
17.3.	If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2.			НП	Одредба је непреносива, јер се односи на сарадњу држава чланица ЕУ у случају да пружалац дигиталних услуга има своје ИКТ системе у једној или више држава.	
18.1.	For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State.			НП	Одредба је непреносива, јер се односи на одређивање јурисдикције држава чланица ЕУ.	
18.2.	A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established.			НП	Одредба је непреносива, јер се односи на одређивање јурисдикције држава чланица ЕУ.	
18.3.	The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself.			НП	Одредба је непреносива, јер се односи на одређивање јурисдикције држава чланица ЕУ.	

а)	а1)	б)	б1)	в)	г)	д)
19.1.	In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.	7.3.	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.	ПУ		
19.2.	ENISA, in collaboration with Member States, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered.			НП	Одредба је непреносива, јер се односи на давање овлашћења ЕНИСА да изради смернице који се односе на стандарде заштите ИКТ система.	
20.1.	Without prejudice to Article 3, entities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.	15.1.3.	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: 3) реагује по пријављеним или на	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			други начин откривеним инцидентима у ИКТ системима од посебног значаја, као и другим ИКТ системима у Републици Србији, 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,			
20.2.	When processing notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned. Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification.			НП	Одредба је непреносива, с обзиром да се њоме даје могућност (не и обавеза) држава чланица да предвиде могућност добровољног обавештавања о инциденту у ИКТ систему. Напомињемо да се обавезе које проистичу из Предлога закона односе само на оне ИКТ системе од посебног значаја који имају обавезу пријављивања инцидената.	
21.	Member States shall lay down the rules on penalties applicable to infringements of national provisions	30.	Новчаном казном у износу од 50.000,00 до	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them.		2.000.000,00 динара казниће се за прекршај оператор ИКТ система од посебног значаја ако: 1) не изврши упис у евиденцију у року из члана 6б овог закона; 2) не донесе Акт о безбедности ИКТ система из члана 8. став 1. овог закона; 3) не примени мере заштите одређене Актом о безбедности ИКТ система из члана 8. став 2. овог закона; 4) не изврши проверу усклађености примењених мера из члана 8. став 4. овог закона; 5) не достави статистичке податке из члана 11б овог закона; 6) не поступи по налогу инспектора за информациону безбедност у остављеном року из члана 29. став 1. тачка 1. овог закона. За прекршај из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00			

а)	а1)	б)	б1)	в)	г)	д)
			динара. 31. Новчаном казном у износу од 50.000,00 до 500.000,00 динара казниће се за прекршај оператор ИКТ система од посебног значаја ако: 1) о инцидентима у ИКТ систему не обавести органе из члана 11. ст. 1, 3. и 7. овог закона; 2) не доставља обавештења о битним догађајима у вези са инцидентом и активностима из члана 11 став 5. овог закона; 3) не достави завршни извештај из члана 11. став 6. овог закона. За прекршаје из става 1. овог члана казниће се и одговорно лице у оператору ИКТ система од посебног значаја новчаном казном у износу од 5.000,00 до 50.000,00 динара. Изузетно од ст.1. и 2. овог члана, ако финансијска институција не обавести Народну банку Србије о инцидентима у ИКТ систему од посебног значаја, Народна			

а)	а1)	б)	б1)	в)	г)	д)
			банка Србије изриче тој финансијској институцији мере и казне у складу са законом којим се уређује пословање финансијских институција.			
22.1.	The Commission shall be assisted by the Network and Information Systems Security Committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.			НП	Одредба је непреносива, јер се односи на успостављање комитета Европске комисије.	
22.2.	Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.			НП	Одредба је непреносива, јер се односи на успостављање комитета Европске комисије.	
23.1.	By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services.			НП	Одредба је непреносива, с обзиром да се односи на подношење извештаја од стране Европске комисије.	
23.2.	The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021.			НП	Одредба је непреносива, јер се односи на разматрање примене ове директиве од стране Европске комисије.	

а)	а1)	б)	б1)	в)	г)	д)
24.1.	Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017.			НП	Одредба је непреносива, јер се односи на почетак рада тела ЕУ (Групе за координацију и мреже ЦЕРТ-ова ЕУ).	
24.2.	For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6.			НП	Одредба је непреносива, јер се односи на рад тела ЕУ (Групе за координацију).	
24.3.	By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network.			НП	Одредба је непреносива, јер се односи на рад тела ЕУ (Групе за координацију).	
25.1.	Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof.			НП	Одредба је непреносива, с обзиром да се односи на рок у коме државе чланице ЕУ морају да имплементирају ову директиву.	

а)	а1)	б)	б1)	в)	г)	д)
	They shall apply those measures from 10 May 2018. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.					
25.2.	Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.			НП	Одредба је непреносива, јер се односи на обавезу извештавања Европске комисије од страна држава чланица ЕУ.	
26.	This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.			НП	Одредба је непреносива, јер се односи на ступање на снагу ове директиве.	
27.	This Directive is addressed to the Member States.			НП	Одредба је непреносива, јер прописује да се ова директива односи на државе чланице ЕУ.	
A.I.1.a)	REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs) The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following: CSIRTs shall ensure a high level of availability of their communications services by avoiding single	15.2.	Национални ЦЕРТ обезбеђује доступност својих услуга путем различитих средстава комуникације, која су непрекидно доступна.	ПУ	Први параграф А 1.1.а) тачке представља инструктивну одредбу НИС директиве која је реализована одређивањем захтева за ЦЕРТ и његових надлежности у складу са датом инструкцијом. Други параграф А 1.1. а) пренет је одредбом члана 15. став 2) закона тако што је предвиђено да ЦЕРТ обезбеђује доступност својих услуга	

а)	а1)	б)	б1)	в)	г)	д)
	points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.				путем различитих средстава комуникације (чиме се избегава да постоји само једно средство у случају чије недоступности би била онемогућена комуникација са ЦЕРТ-ом, односно обезбеђује се да ЦЕРТ има више средстава комуникације).	
A.I.1.b)	CSIRTs' premises and the supporting information systems shall be located in secure sites.	15.3.	Просторије и информациони системи Националног ЦЕРТ-а морају да се налазе на безбедним локацијама.	ПУ		
A.I.1.c)	Business continuity: CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers. CSIRTs shall be adequately staffed to ensure availability at all times. CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.	15.4.	У циљу обезбеђивања континуитета рада, Национални ЦЕРТ треба да: 1) буде опремљен са одговарајућим системима за управљање инцидентима; 2) има довољно запослених како би се осигурала доступност у свако доба; 3) обезбеди инфраструктуру чији је континуитет осигуран, односно да обезбеди редундантне системе и резервни радни простор.	ПУ		
A.I.1.d)	CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.	15.5.	Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом органа јавне власти.			
A.I.2.a)	CSIRTs' tasks: CSIRTs' tasks shall include at least the following: (i) monitoring incidents at a national level; (ii) providing early warning, alerts, announcement and dissemination of information to relevar stakeholders about risks and incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis ar situational awareness; (v) participating in the CSIRTs network.	15.1.	Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, пружа подршку, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно: 1) прати стање о инцидентима на националном нивоу, 2) пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима, 3) реагује по пријављеним или на други начин	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			откривеним инцидентима у ИКТ системима од посебног значаја, као и другим ИКТ системима у Републици Србији, тако што пружа савете и препоруке 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 власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести, 6) води евиденцију Посебних ЦЕРТ-ова; 7) извештава Надлежни орган на кварталном нивоу о предузетим активностима.			
A.I.2.b)	CSIRTs shall establish cooperation relationships with the private sector.	15.5.	Национални ЦЕРТ непосредно сарађује	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом органа власти.			
A.I.2.c)	To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for: (i) incident and risk-handling procedures; (ii)incident, risk and information classification schemes.	15.7.	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.	ПУ		
A.II.						
A.II.1.						
A.II.1.a)	TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4 Energy Electricity	6.1.3.1.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима:	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	–Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council (1), which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive –Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC –Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC		(1) енергетика: - производња, пренос и дистрибуција електричне енергије;			
A.II.1.b)	Oil — Operators of oil transmission pipelines –Operators of oil production, refining and treatment facilities, storage and transmission	6.1.3.1.3.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (1) енергетика: -истраживање, производња, прерада, транспорт и дистрибуција нафте и промет нафте и нафтних деривата;	ПУ		
A.II.1.c)	Gas –Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council (2) –Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC –Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC –Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC	6.1.3.1.4.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (1) енергетика: -истраживање, производња, прерада, транспорт и дистрибуција	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	–LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC –Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC —Operators of natural gas refining and treatment facilities		природног и течног гаса;			
A.II.2.a)	Air transport –Air carriers as defined in point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council (3) –Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council (4), airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council (5), and entities operating ancillary installations contained within airports –Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council (6)	6.1.3.2.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (2) саобраћај: -железнички, поштански, водени и ваздушни саобраћај;	ПУ		
A.II.2.b)	Rail transport –Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council (7) –Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point	6.1.3.2.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (2) саобраћај:	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	(12) of Article 3 of Directive 2012/34/EU		-железнички, поштански, водени и ваздушни саобраћај;			
A.II.2.c)	Water transport –Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council (8), not including the individual vessels operated by those companies –Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council (9), including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports –Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council (10)	6.1.3.2.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (2) саобраћај: -железнички, поштански, водени и ваздушни саобраћај;	ПУ		
A.II.2.d)	Road transport –Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 (11) responsible for traffic management control –Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council (12)	6.1.2.6.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (6) добра од општег интереса: - коришћење, управљање, заштита и унапређивање добара од општег интереса (воде, путеви,	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
			минералне сировине, шуме, пловне реке, језера, обале, бање, дивљач, заштићена подручја);			
А.II.3.	Banking Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council (13)A	6.1.3.4.1.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (4) банкарство и финансијска тржишта: - послови финансијских институција;	ПУ		
А.II.4.	Financial market infrastructures –Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council (14) –Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council (15)	6.1.3.4.3.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (4) банкарство и финансијска тржишта: - послови управљања, односно обављања делатности у вези са функционисањем регулисаног тржишта;	ПУ		
А.II.5.	Health sector Health care settings (including hospitals and private clinics)	6.1.3.3.1.	ИКТ системи од посебног значаја су системи који се	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council (16)		користе: 3) у обављању делатности од општег интереса и то у областима: (3) здравство: -здравствена заштита.			
А.II.6.	Drinking water supply and distribution Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC (17) but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services	6.1.3.8.5.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (8) остале области: - комуналне делатности;	ПУ		Напомена: Снабдевање водом за пиће је комунална делатност у складу са Законом о комуналним делатностима.
А.II.7.	Digital Infrastructure — IXPs — DNS service providers — TLD name registries	6.1.3.5.	ИКТ системи од посебног значаја су системи који се користе: 3) у обављању делатности од општег интереса и то у областима: (5)дигитална инфраструктура -размена интернет саобраћаја; -управљање регистром националног интернет домена и системом за именовање на мрежи (ДНС системи)	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
А.III.	TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF POINT (5) OF ARTICLE 4 Online marketplace. Online search engine Cloud computing service.	6.1.3.7. .	ИКТ системи од посебног значаја су системи који се користе: (7)услуге информационог друштва: - услуге информационог друштва у смислу члана 2. тачка 25) овог закона	ДУ		ИКТ системи у којима се врше ове услуге биће дефинисани као ИКТ системи од посебног значаја подзаконским актом.