П Р Е Д Л О Г

З А К О Н
О КРИТИЧНОЈ ИНФРАСТРУКТУРИ

I. ОСНОВНЕ ОДРЕДБЕ

Предмет закона

Члан 1.

Овим законом уређује се национална и европска критична инфраструктура, идентификација и одређивање критичне инфраструктуре Републике Србије (у даљем тексту: критична инфраструктура), заштита критичне инфраструктуре, надлежност и одговорност органа и организација у области критичне инфраструктуре (у даљем тексту: надлежни органи и организације) и информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области критичне инфраструктуре.

Значење израза

Члан 2.

Поједини изрази употребљени у овом закону имају следеће значење:

1) сектори критичне инфраструктуре су области одређене овим законом, у којима се врши поступак идентификације и одређивања критичне инфраструктуре;

2) идентификација критичне инфраструктуре је поступак утврђивања система, мрежа, објеката или њихових делова у одређеном сектору који се, у складу са утврђеним критеријумима, идентификују као критична инфраструктура;

3) одређивање критичне инфраструктуре подразумева поступак утврђивања система, мрежа, објеката, или њихових делова као критичне инфраструктуре у складу са овим законом;

4) заштита критичне инфраструктуре представља скуп активности и мера које имају за циљ осигурање функционисања критичне инфраструктуре у случају ометања или уништења, односно заштиту у случају претњи и спречавање настанка последице ометања или уништења;

5) оператори критичне инфраструктуре су државни органи, органи аутономне покрајине, органи јединице локалне самоуправе, јавна предузећа, привредна друштва или друга правна лица која управљају системима, мрежама, објектима или њиховим деловима који су одређени као критична инфраструктура;

6) Безбедносни план оператора за управљање ризиком је план који израђује оператор критичне инфраструктуре, којим се дефинишу безбедносни циљеви и мере оператора на основу анализе ризика коју план садржи;

7) официр за везу је лице запослено код оператора критичне инфраструктуре, а које је контакт између оператора критичне инфраструктуре и министарства надлежног за унутрашње послове (у даљем тексту: Министарство);

8) европска критична инфраструктура подразумева критичну инфраструктуру која се налази на територији земље чланице Европске уније, чије би ометање или уништење имало значајан утицај на најмање две земље чланице.

Начела деловања

Члан 3.

Надлежни органи и организације, грађани и други субјекти дужни су да се у предузимању мера и активности утврђених овим и другим законом, програмима, плановима и другим документима у области критичне инфраструктуре руководе следећим начелима:

1) начело интегрисаног приступа – у заштити критичне инфраструктуре пре, за време и после ометања или прекида у функционисању критичне инфраструктуре, учествују сви надлежни органи и организације, грађани и други субјекти узимајући у обзир различите врсте опасности које проистичу из анализе ризика, и узимајући у обзир међузависност сектора критичне инфраструктуре и њихову интеракцију;

2) начело одговорности – за функционисање критичне инфраструктуре директно су одговорни оператори критичне инфраструктуре, а за унапређење заштите критичне инфраструктуре, поред оператора, и сви надлежни органи и организације, грађани и други субјекти;

3) начело заштите од разних врста претњи – оператори, надлежни органи и организације, грађани и други субјекти у обезбеђивању континуираног рада критичне инфраструктуре дужни су да узму у обзир различите врсте ризика;

4) начело континуираног планирања заштите критичне инфраструктуре – заштита критичне инфраструктуре заснива се на сталном процесу анализе ризика по функционисање критичне инфраструктуре и процене адекватности мера заштите;

5) начело размене података и информација и заштите података – оператори, надлежни органи и организације, грађани и други субјекти дужни су да благовремено и континуирано размењују потребне податке и информације истовремено штитећи податке везане за критичну инфраструктуру, у складу са прописима којима се уређује заштита тајних података.

Критична инфраструктура

Члан 4.

Критична инфраструктура су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије.

Министарство уређује, планира, координира, контролише активности, комуницира и даје информације у вези са критичном инфраструктуром.

II. ИДЕНТИФИКАЦИЈА И ОДРЕЂИВАЊЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Идентификација критичне инфраструктуре

Члан 5.

Идентификација критичне инфраструктуре врши се секторски у складу са утврђеним критеријумима.

За спровођење поступка идентификације критичне инфраструктуре у одређеном сектору задужена су министарства надлежна за одређене области.

Критеријуме за идентификацију критичне инфраструктуре и начин извештавања, прописује Влада.

Сектори критичне инфраструктуре

Члан 6.

Сектори у којима се врши идентификација и одређивање критичне инфраструктуре јесу:

1) енерегетика;

2) саобраћај;

3) снабдевање водом и храном;

4) здравство;

5) финансије;

6) телекомуникационе и информационе технологије;

7) заштита животне средине;

8) функционисање државних органа.

Осим сектора из става 1. овог члана, критична инфраструктура може се одредити и у другим секторима, на предлог министарства надлежног за одређену област, у складу са овим законом.

Утврђивање сектора из става 2. овог члана и критеријуме за идентификацију критичне инфраструктуре у тим секторима, прописује Влада актом из члана 5. став 3. овог закона.

Одређивање критичне инфраструктуре

Члан 7.

Критичну инфраструктуру на предлог Министарства одређује Влада.

Министарства задужена за секторе критичне инфраструктуре дужна су да у року од шест месеци од доношења акта из члана 5. став 3. овог закона, а након завршеног поступка идентификације у складу са утврђеним критеријумима, Министарству доставе предлоге критичне инфраструктуре у свом сектору.

Министарства задужена за секторе критичне инфраструктуре дужна су да редовно, а најмање једном квартално извештавају Министарство о новонасталим променама у свом сектору.

Министарства задужена за секторе критичне инфраструктуре дужна су да након завршеног поступка идентификације Министарству сваке године, најкасније до 31. октобра, доставе предлоге измена и допуна критичне инфраструктуре у свом сектору.

Министарство може указати министарствима задуженим за секторе критичне инфраструктуре на потенцијалне критичне инфраструктуре.

Заштита, чување, коришћење, контрола и надзор критичне инфраструктуре у надлежности Министарства одбране и Војске Србије спроводи се у складу са Законом о одбрани и Законом о војсци Србије.

Акт о одређивању критичне инфраструктуре ажурира се сваке године, најкасније до 31. децембра.

III. ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Безбедносни план оператора за управљање ризиком

Члан 8.

Безбедносни план оператора за управљање ризиком је документ којим се утврђују мере смањења ризика, дефинишу одговорности и одређују дужности, те успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи дефинисаних у анализи ризика, која је саставни део плана.

Оператори критичне инфраструктуре дужни су да израде Безбедносни план оператора за управљање ризиком и на исти прибаве сагласност Министарства одмах, а најкасније шест месеци по одређивању система, мрежа, објеката или њихових делова за критичну инфраструктуру.

Методологију, начин израде и садржај Безбедносног плана оператора за управљање ризиком прописује министар надлежан за унутрашње послове (у даљем тексту: министар).

Официр за везу

Члан 9.

Оператори критичне инфраструктуре морају имати официра за везу, односно лице које служи као контакт између оператора и Министарства, које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру, обавештава Министарство о евалуацији ризика, претњи и рањивости, координира Безбедносним планом оператора за управљање ризиком, врши тестирања кроз вежбе и друге активности предвиђене планом и обавља све друге послове везане за критичну инфраструктуру.

Официра за везу именује Министарство на предлог оператора критичне инфраструктуре из редова запослених.

Оператор критичне инфраструктуре Министарству доставља предлог за именовање официра за везу најкасније три месеца по одређивању система, мрежа, објеката или њихових делова за критичну инфраструктуру.

Предложено лице мора поседовати лиценцу за официра за везу.

Министарство издаје лиценцу из става 4. овог члана лицу које има:

1) високо образовање (мастер академске студије, специјалистичке академске или специјалистичке струковне студије, односно основне студије у трајању од најмање четири године по пропису који је уређивао високо образовање до 10. септембра 2005. године);

2) положен посебан стручни испит за официра за везу.

Полагање посебног стручног испита из тачке 2. овог члана организује и спроводи Министарство.

Начин и програм за полагање посебног стручног испита прописује министар.

Оператори критичне инфраструктуре обезбеђују континуитет вршења функције официра за везу у случају његовог одсуства обавештавањем Министарства о привременом обављању ових послова од стране другог лица, са свим потребним подацима.

Критична инфраструктура у планским документима

Члан 10.

Приликом израде планских докумената у области просторног и урбанистичког планирања, докумената из области националне безбедности и области смањења ризика и управљања ванредним ситуацијама, критична инфраструктура мора се третирати на посебан начин, нарочито у делу превентивних активности и активности везаних за одговор на ванредне ситуације у којима мора имати приоритет.

Републички штаб за ванредне ситуације

Члан 11.

У случају наступања околности угрожавања, ометања рада или уништења критичне инфраструктуре руковођење и координацију спровођења мера и задатака у наведеним околностима предузима Републички штаб за ванредне ситуације, у складу са законом.

Министарство пружа стручну подршку штабу из става 1. овог члана и доставља све неопходне податке и информације у циљу несметаног обављања активности на спровођењу утврђених задатака.

IV. ЕВРОПСКА КРИТИЧНА ИНФРАСТРУКТУРА

Појам

Члан 12.

Европска критична инфраструктура је критична инфраструктура од интереса за најмање две државе чланице Европске уније.

Одређивање европске критичне инфраструктуре

Члан 13.

Европска критична структура може се одредити у секторима које одређује Европска комисија.

Европску критичну инфраструктуру на територији Републике Србије, на предлог Министарства, одређује Влада, на захтев и у сагласности са заинтересованим државама чланицама Европске уније и обавештава заинтересоване државе чланице о одређивању европске критичне инфраструктуре на територији Републике Србије.

Ако се критична инфраструктура од значаја за Републику Србију налази на подручју друге државе чланице Европске уније, Влада предлаже надлежном телу те државе одређивање европске критичне инфраструктуре.

Заштита европске критичне инфраструктуре

Члан 14.

Европска критична инфраструктура на територији Републике Србије штити се на исти начин као и критична инфраструктура Републике Србије, осим када је то прописима Европске уније другачије уређено.

Извештавање о европској критичној инфраструктури

Члан 15.

Влада усваја годишњи извештај о броју европске критичне инфраструктуре по сектору и броју заинтересованих држава на које свака одређена критична инфраструктура има утицај, на предлог Министарства.

Извештај из става 1. овог члана доставља се Европској комисији и заинтересованим државама на које свака одређена критична инфраструктура има утицај.

Размена информација о европској критичној инфраструктури

Члан 16.

Контакт тачка за потребе размене информација и координацију активности у вези са европском критичном инфраструктуром са другим државама чланицама и телима Европске уније је Министарство.

V. ПОСТУПАЊЕ СА ТАЈНИМ ПОДАЦИМА

Одређивање и размена

Члан 17.

Одређени подаци у вези са критичном инфраструктуром могу се одредити као тајни подаци у складу са прописима којима се уређује тајност података.

Тајни подаци који се односе на Европску критичну инфраструктуру размењују се са страним државама и органима Европске уније у складу са законом којим је уређена тајност података и потписаним међународним споразумима о размени тајних података.

VI. НАДЗОР

Надлежност

Члан 18.

Надзор над применом овог закона и прописа донетих на основу њега врши Министарство.

Министарство врши инспекцијски надзор преко инспектора.

Овлашћења инспектора

Члан 19.

У вршењу инспекцијског надзора, инспектор има право да:

1) утврди стање извршавања обавеза предвиђених овим законом, упозори на уочене неправилности и одреди мере и рокове за њихово отклањање;

2) врши увид у документа која се односе на критичну инфраструктуру;

3) проверава спровођење издатих наредби и закључака и наложи мере за извршење;

4) наложи израду, доношење и ажурирање докумената предвиђених овим законом;

5) наложи обуставу мера и радњи које нису у складу са Безбедносним планом оператора за управљање ризиком;

6) наложи отклањање утврђених недостатака у спровођењу прописаних мера утврђених Безбедносним планом оператора за управљање ризиком;

7) поднесе предлог за покретање поступака за утврђивање прекршајне одговорности против правних и одговорних лица;

8) нареди предузимање хитних мера;

9) предузме и друге мере за које је овлашћен законом.

Против решења инспектора може се изјавити жалба у року од осам дана од дана достављања решења.

Жалба против решења инспектора донетог на основу става 1. тач. 5) и 8) овог члана не одлаже извршење решења.

VII. КАЗНЕНЕ ОДРЕДБЕ

Члан 20.

Новчаном казном у износу од 100.000 до 1.000.000 динара казниће се за прекршај јавно предузеће, привредно друштво или друго правно лице које управља системима, мрежама, објектима или њиховим деловима који су одређени као критична инфраструктура ако:

1) не прибави сагласност Министарства на Безбедносни план оператора за управљање ризиком (члан 8. став 2);

2) не достави Министарству предлог за именовање официра за везу (члан 9. став 3);

3) не поступи по налогу инспектора (члан 19. став 1).

Члан 21.

Новчаном казном од 50.000 до 100.000 динара казниће се за прекршај одговорно лице у надлежном државном органу, органу територијалне аутономије или органу јединице локалне самоуправе, ако:

1) не достави Министарству предлоге критичне инфраструктуре у свом сектору (члан 7. став 2);

2) не извештава Министарство о новонасталим променама у свом сектору (члан 7. став 3);

3) не достави Министарству предлоге измена и допуна критичне инфраструктуре у свом сектору (члан 7. став 4);

4) не поступи по налогу инспектора (члан 19. став 1).

VIII. ПРЕЛАЗНЕ И ЗАВРШНЕ ОДРЕДБЕ

Рок за доношење подзаконских аката

Члан 22.

Подзаконски акти за спровођење овог закона донеће се у року од шест месеци од дана ступања на снагу овог закона.

Рок за усаглашавање општег акта

Члан 23.

Измене акта о унутрашњем уређењу и систематизацији радних места у Министарству унутрашњих послова донеће министар у року од 30 дана од дана ступања на снагу овог закона.

Примена одредаба о европској критичној инфраструктури

Члан 24.

Одредбе овог закона које се односе на европску критичну инфраструктуру почињу да се примењују даном приступања Републике Србије Европској унији.

Ступање на снагу

Члан 25.

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

ОБРАЗЛОЖЕЊЕ

I. УСТАВНИ ОСНОВ ЗА ДОНОШЕЊЕ ЗАКОНА

Уставни основ за доношење овог закона садржан је у одредбама члана 97. став 1. тач. 4) и 17) Устава Републике Србије, којима је утврђено да Република Србија уређује и безбедност њених грађана и да уређује и друге односе од интереса за Републику Србију, у складу са Уставом.

II. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА

С обзиром да област критичне инфраструктуре није на јединствен начин уређена ни једним законом Републике Србије, а да је област критичне инфраструктуре преобимна, уочена је потреба да се ова област обједини и јасно уреди имајући у виду значај материје на коју се односи.

Будући да се ради о широкој недефинисаној теми, неопходно је критичну инфраструктуру уредити законом, којим би се дало усмерење за друге посебне законе, и како би се утврдиле стриктне надлежности и одговорности државе.

Појам „критичне инфраструктуре" помиње се у више различитих прописа и стратешких докумената:

Законом о ванредним ситуацијама („Службени гласник РС", бр. 111/09, 92/11 и 93/12), Република Србија определила се да Министарство унутрашњих послова буде надлежно за израду процене угрожености од елементарних непогода и других несрећа, коју доставља Влади на усвајање. Аутономне покрајине, јединице локалне самоуправе, министарства и други органи и организације израђују процену угрожености у делу који се односи на њихов делокруг и достављају је Министарству унутрашњих послова. Сам закон се не бави критичном инфраструктуром, већ тиме на који начин ове опасности посредством критичне инфраструктуре утичу на вредности које треба заштити. Овај закон прописује да се проценом угрожености идентификују извори могућег угрожавања, сагледавају могуће последице, потребе и могућности спровођења мера и задатака заштите и спасавања од елементарних непогода и других несрећа. Процена угрожености садржи нарочито: 1) карактеристике територије, критична постројења, критична места и просторе са гледишта угрожености од елементарних непогода и других несрећа, са евентуалним прекограничним ефектима удеса; 2) повредивост територије од елементарних непогода и других несрећа; 3) анализу могућих последица од елементарних и других несрећа; 4) потребе и могућности за заштиту људи, материјалних добара и животне средине од последица елементарних и других несрећа. Процена предвиђа свеобухватан приступ у заштити критичне инфраструктуре, мада оријентисан на идентификовање извора опасности и последица које поремећаји и прекид у функционисању критичне инфраструктуре има по економију и екологију.

На основу Закона о ванредним ситуацијама донета је ***Уредба о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама*** („Службени гласник РС", број 8/11). Овим прописом, поред већ наведених елемената процене угрожености, који су утврђени у Закону о ванредним ситуацијама, предвиђа се да ће део процене бити и процена критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа. У Републици Србији се овом уредбом први пут уводи појам критичне инфраструктуре, али и даље без јасног одређивања о којим је елементима или областима инфраструктуре реч. Такође, нису одређени субјекти који би сносили одговорност у заштити критичне инфраструктуре.

Поред наведеног, питање критичне инфраструктуре може се препознати и у другим нормативно-правним документима који су у претходном периоду донети у Републици Србији.

Један такав документ, у којем се помиње критична инфраструктура, је ***Стратегије развоја информационог друштва у Републици Србији до 2020. године***, у којој се у оквиру поглавља 6.2. помиње следеће: „Потребно је развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, што поред информационо-комуникационих система могу бити и други инфраструктурни системи којима се управља коришћењем информационо-комуникационих технологија, попут електро-енергетског система. У вези тога је потребно додатно уредити критеријуме за утврђивање критичне инфраструктуре са становишта информационе безбедности, критеријуме за карактеризацију напада применом информационих технологија на такву инфраструктуру у односу на класичне облике напада, као и услове заштите у овој области".

У оквиру ***Стратегије националне безбедности Републике Србије*** се не помиње директно појам „критична инфраструктура", али се наводе њени елементи у деловима који се односе на: проблеме економског развоја Републике Србије услед вишегодишњих економских санкција и уништења виталних објеката привредне и саобраћајне инфраструктуре, енергетску међузависност и осетљивост инфраструктуре за производњу и транспорт енергената и високотехнолошки криминал и угрожавање информационих и телекомуникационих система.

У ***Закону о информационој безбедности*** *(*„Службени гласник РС", број 6/16*)*, појам критичне информационе инфраструктуре се не помиње као такав, али закон предвиђа ИКТ (информационо-комуникациони систем) системе од посебног значаја који обављају делатности од општег интереса, међу којима многи представљају критичну инфраструктуру, као што су, рецимо, ИКТ системи који се користе у обављању делатности у областима енергетике, саобраћаја, производње и промета наоружања и војне опреме, комуналних делатности, ИКТ системи у здравству и финансијским институцијама. Ови субјекти ће имати обавезе да заштите своје ИКТ системе на одговарајуће начине и да пријављују инциденте надлежним телима, чиме се жели постићи подизање нивоа припремљености оператора (оператор ИКТ система је правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности;**)** и заштите ИКТ система у Републици Србији. На предлог ресорног министарства, Влада Републике Србије је у марту 2016. године образовала Тело за координацију послова информационе безбедности (у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Управе за заједничке послове републичких органа и Националног ЦЕРТ-а.)

Закон о приватном обезбеђењу („Службени гласник РС", бр. 104/13 и 42/15) дефинише појам „обавезно обезбеђених објеката" као „објеката од стратешког значаја за РС и њене грађане, као и објеката од посебног значаја чијим оштећењем или уништењем би могле наступити теже последице по живот или здравље људи или који су од интереса за одбрану земље." Под обавезно обезбеђеним објектима сматра се и простор на коме се налазе ти објекти и чине њихов саставни део, као и пратећи објекти који су у функцији тих објеката.

Поред наведених, постоји још читав низ секторских закона у областима одбране, тајности података, вода, безбедности хране, просторном планирању, заштити од пожара, заштити животне средине, јавно-приватном партнерству,

који не помињу конкретно термин „критична инфраструктура”, али који третирају поједине сегменте критичне инфраструктуре као полазну основу.

Такође, као један од важних задатака Републике Србије на путу европских интеграција јесте усвајање нормативног оквира везаног за критичну инфраструктуру који ће бити усклађен са елементима Директиве Европског савета 2008/114/ЕС. Директива Савета Европе 2008/114/ЕС из 2008. године дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре, заједнички приступ у процени потреба за побољшавање заштите. Она представља основу за наредне кораке у дефинисању критеријума за критичну инфраструктуру.

Имајући у виду најбољу европску праксу, израђена је анализа стања (гап анализа). Последњих година, Република Србија улаже значајне напоре у стварање интегрисаног система заштите и спасавања који би адекватно одговорио у условима угрожавања, пре свега људских живота, али и критичних националних ресурса.

У оквирима Европске уније, заштита критичне инфраструктуре првобитно је била посматрана из угла борбе против тероризма. Изазови са којима се данашње друштво суочава у сфери безбедносне политике су врло широки, од све учесталијих елементарних непогода до различито изазваних катастрофа, па је неопходно применити динамички, стратешки и, пре свега, мултидисциплинарни приступ када се ради о процесу планирања заштите критичне инфраструктуре. Различити су приступи у утврђивању критичне инфраструктуре у државама Европске уније.

Занимање ЕУ за критичну инфраструктуру земаља чланица проистиче из опасности да би разарање или поремећај извесне критичне инфраструктуре у једној земљи чланици могли непосредно дотицати друге земље чланице. У таквим случајевима заштитне мере су онолико снажне колико је то њихова најслабија карика.

Европска комисија идентификовала је одређене области критичне инфраструктуре. То су: енергија, информационе и комуникационе технологије, вода, храна, финансије, грађанске власти, јавни и правни поредак и сигурност, саобраћај, хемијска и нуклеарна постројења, космос и научно истраживање.

III. ОБЈАШЊЕЊЕ ОСНОВНИХ ПРАВНИХ ИНСТИТУТА И ПОЈЕДИНАЧНИХ РЕШЕЊА

Предлог закона о критичној инфраструктури састоји се од осам поглавља и 25 чланова.

Основним одредбама Предлога закона (чл. 1–4) одређени су предмет закона (члан 1), значење појединих израза употребљених у закону (члан 2), начела деловања (члан 3) и појам критичне инфраструктуре (члан 4). Дефиниције из члана 2. односе се на изразе који се користе у закону. Укупно је обухваћено осам израза, почев од сектора критичне инфраструктуре, па до европске критичне инфраструктуре. Код утврђивања дефиниција, углавном је коришћена прихваћена међународна терминологија, уз одговарајућа прилагођавања правилима и духу српског језика. Дефинисани су појмови и изрази чије значење није на обавезујући начин утврђено у неком другом пропису, а за потребе правилне примене и разумевања решења садржаних у овом закону неопходна је њихова прецизна дефиниција. Чланом 3. Предлога закона утврђено је укупно пет начела. Члан 4. одређује појам „критичне инфраструктуре”.

Друго поглавље носи наслов Идентификација и одређивање критичне инфраструктуре и обухвата чл. 5–7. Предлога закона. Наведеним одредбама

утврђена је идентификација критичне инфраструктуре, одређивање критичне инфраструктуре као и обавезни сектори у којима се критична инфраструктура идентификује и одређује, уз остављање могућности да иста буде одређена и у другим секторима.

Треће поглавље носи наслов Заштита критичне инфраструктуре и обухвата чл. 8–11. Предлога закона. Наведеним одредбама је дефинисан Безбедоносни план оператора за управљање ризиком, појам официра за везу и начин његовог именовања, као и критична инфраструктура у планским документима и начин њеног третирања у истим. Такође, прописано је да у случају угрожавања и оштећења критичне инфраструктуре, руковођење активностима у насталим околностима врши Републички штаб за ванредне ситуације, у складу са законом којим се уређује систем смањења ризика од катастрофа и управљање ванредним ситуацијама.

Четврто поглавље носи наслов Европска критична инфраструктура и обухвата чл. 12–16. Предлога закона којима се дефинише европска критична инфраструктура, начин одређивања европске инфраструктуре, заштита европске критичне инфраструктуре, као и начин извештавања о европској критичној инфраструктури и размени информација о европској критичној инфраструктури.

Пето поглавље носи наслов Поступање са тајним подацима и обухвата члан 17. Предлога закона којим се предвиђа да се одређени подаци у вези са критичном инфраструктуром могу одредити као тајни подаци у складу са законом који уређује тајност података.

Шесто поглавље носи наслов Надзор и обухвата чл. 18. и 19. Предлога закона којима је утврђено ко врши надзор над применом овог закона и прописа донетих на основу њега, као и овлашћења инспектора.

Седмо поглавље носи наслов Казнене одредбе и обухвата чл. 20. и 21. Предлога закона којима су прописане новчане казне за прекршаје јавних предузећа, привредних друштава и прекршаје другог правног лица, као и одговорног лица у надлежном државном органу.

Осмо поглавље носи наслов Прелазне и завршне одредбе и обухвата чл. 22–25. Предлога закона којима се предвиђају рокови за доношење подзаконских аката, рок у ком су министарства у обавези да доставе предлоге критичне инфраструктуре у свом сектору, одложену примену одредаба Закона које се односе на европску критичну инфраструктуру, као и да закон ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије”.

IV. ПРОЦЕНА ФИНАНСИЈСКИХ СРЕДСТВА ЗА СПРОВОЂЕЊЕ ОВОГ ЗАКОНА

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

Нове надлежности Министарства унутрашњих послова, у складу са овим законом, неће изискивати ново запошљавање, као ни додатна средства у буџетској 2018, 2019. и 2020. години.

V. РАЗЛОЗИ ЗА ДОНОШЕЊЕ ЗАКОНА ПО ХИТНОМ ПОСТУПКУ

Услед све чешћих елементарних непогода, техничко-технолошких несрећа и акцидената изазваних људским фактором, потребно је системско реаговање у заштити оних система, мрежа и објеката који су препознати као критична инфраструктура а чијим би уништењем или оштећењем могло доћи до озбиљних последица по националну безбедност, здравље и животе људи,

имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије, тј. њених органа и организација. Сагласно наведеном, предлаже се доношење закона по хитном поступку како не би дошло до наступања штетних последица по живот и здравље људи, безбедност земље и рад органа и организација.

АНАЛИЗА ЕФЕКАТА

1. Који су проблеми које закон треба да реши?

Област критичне инфраструктуре није регулисана ни једним законом Републике Србије и постоји потреба да се ова област обједини и јасно дефинише.

Проблем који Закон о критичној инфраструктури треба да реши јесте стварање једног интегрисаног система заштите и спасавања који би адекватно одговорио у условима угрожавања, пре свега људских живота, али и критичних националних ресурса.

С обзиром да се ради о широкој, недефинисаној теми, неопходно је критичну инфраструктуру регулисати законом, којим би се дало усмерење за друге посебне законе. Наиме, Република Србија може бити рањива и постоји потреба да се овим законом дефинишу стриктне надлежности и одговорности државе.

Законом о ванредним ситуацијама („Службени гласник РС”, бр. 111/09, 92/11 и 93/12) Република Србија се определила да Министарство унутрашњих послова буде надлежно за израду процене угрожености од елементарних непогода и других несрећа, коју доставља Влади на усвајање. Аутономне покрајине, јединице локалне самоуправе, министарства и други органи и организације израђују процену угрожености у делу који се односи на њихов делокруг и достављају је Министарству унутрашњих послова. Сам закон се не бави критичном инфраструктуром, већ како ове опасности посредством критичне инфраструктуре утичу на вредности које треба заштити. Овај закон прописује да се проценом угрожености идентификују извори могућег угрожавања, сагледавају могуће последице, потребе и могућности спровођења мера и задатака заштите и спасавања од елементарних непогода и других несрећа. Процена угрожености садржи нарочито: 1) карактеристике територије, критична постројења, критична места и просторе са гледишта угрожености од елементарних непогода и других несрећа, са евентуалним прекограничним ефектима удеса; 2) повредивост територије од елементарних непогода и других несрећа; 3) анализу могућих последица од елементарних и других несрећа; 4) потребе и могућности за заштиту људи, материјалних добара и животне средине од последица елементарних и других несрећа. Процена предвиђа свеобухватан приступ у заштити критичне инфраструктуре, мада оријентисан на идентификовање извора опасности и последица које поремећаји и прекид у функционисању критичне инфраструктуре има по економију и екологију.

На основу Закона о ванредним ситуацијама донета је Уредба о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама („Службени гласник РС”, број 8/211). Овим документом, поред већ наведених елемената процене угрожености, који су дефинисани у Закону о ванредним ситуацијама, предвиђа се да ће део процене бити и процена критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа. У Србији се овом уредбом први пут уводи појам критичне инфраструктуре, али и даље без јасног дефинисања о којим је елементима или областима инфраструктуре реч. Такође, нису одређени субјекти који би сносили одговорност у заштити критичне инфраструктуре

Питање критичне инфраструктуре може се препознати и у другим нормативноправним документима у Републици Србији.

Један такав документ, у којем се помиње критична инфраструктура, је Стратегија развоја информационог друштва у Републици Србији до 2020, у којој се у оквиру поглавља 6.2. помиње следеће: „Потребно је развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, што поред информационо-комуникационих

система могу бити и други инфраструктурни системи којима се управља коришћењем информационо-комуникационих технологија, попут електро-енергетског система. У вези тога је потребно додатно уредити критеријуме за утврђивање критичне инфраструктуре са становишта информационе безбедности, критеријуме за карактеризацију напада применом информационих технологија на такву инфраструктуру у односу на класичне облике напада, као и услове заштите у овој области".

У оквиру Стратегије националне безбедности Републике Србије се не помиње директно појам „критична инфраструктура", али се наводе њени елементи у деловима који се односе на: проблеме економског развоја Републике Србије услед вишегодишњих економских санкција и уништења виталних објеката привредне и саобраћајне инфраструктуре, енергетску међузависност и осетљивост инфраструктуре за производњу и транспорт енергената и високотехнолошки криминал и угрожавање информационих и телекомуникационих система.

У Закону о информационој безбедности („Службени гласник РС", број 6/16), појам критичне информационе инфраструктуре се не помиње као такав, али закон предвиђа ИКТ (информационо-комуникациони систем) системе од посебног значаја који обављају делатности од општег интереса, међу којима многи представљају критичну инфраструктуру, као што су, рецимо, ИКТ системи који се користе у обављању делатности у областима енергетике, саобраћаја, производње и промета наоружања и војне опреме, комуналних делатности, ИКТ системи у здравству и финансијским институцијама. Ови субјекти ће имати обавезе да заштите своје ИКТ системе на одговарајуће начине и да пријављују инциденте надлежним телима, чиме се жели постићи подизање нивоа припремљености оператора (оператор ИКТ система је правно лице, орган јавне власти или организациона јединица органа јавне власти који користи ИКТ систем у оквиру обављања своје делатности, односно послова из своје надлежности) и заштите ИКТ система у Републици Србији. На предлог ресорног министарства, Влада Републике Србије је у марту 2016. године образовала Тело за координацију послова информационе безбедности (у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, Управе за заједничке послове републичких органа и Националног ЦЕРТ-а.)

Закон о приватном обезбеђењу („Службени гласник РС", бр. 104/13 и 42/15) дефинише појам „обавезно обезбеђених објеката" као „објеката од стратешког значаја за Републику Србију и њене грађане, као и објеката од посебног значаја чијим оштећењем или уништењем би могле наступити теже последице по живот или здравље људи или који су од интереса за одбрану земље." Под обавезно обезбеђеним објектима сматра се и простор на коме се налазе ти објекти и чине њихов саставни део, као и пратећи објекти који су у функцији тих објеката.

Поред наведених, постоји још читав низ секторских закона у областима одбране, тајности података, вода, безбедности хране, просторном планирању, заштити од пожара, заштити животне средине, јавно-приватном партнерству, који не помињу конкретно термин „критична инфраструктура", али који третирају поједине сегменте критичне инфраструктуре као полазну основу.

Имајући у виду најбољу европску праксу, израђена је анализа стања (гап анализа). Последњих година, Република Србија улаже значајне напоре у стварању интегрисаног система заштите и спасавања који би адекватно одговорио у условима угрожавања, пре свега људских живота, али и критичних националних ресурса.

Занимање ЕУ за критичну инфраструктуру земаља чланица проистиче из опасности да би разарање или поремећај извесне критичне инфраструктуре у једној земљи чланици могли непосредно дотицати друге земље чланице. У таквим случајевима заштитне мере су онолико снажне колико је то њихова најслабија карика.

Европска комисија идентификовала је одређене области критичне инфраструктуре. То су: енергија, информационе и комуникационе технологије, вода, храна, финансије, грађанске власти, јавни и правни поредак и сигурност, саобраћај, хемијска и нуклеарна постројења, космос и научно истраживање.

2. Циљеви који се доношењем Закона постижу

Циљ Закона о критичној инфраструктури јесте идентификација и одређивање критичне инфраструктуре Републике Србије и идентификација и одређивање европске критичне инфраструктуре. Одређивање критичне инфраструктуре подразумева процес одређивања система, мрежа и објеката као и њихових делова, као критичне инфраструктуре у складу са овим законом.

Означавање критичне инфраструктуре има за циљ да се смањи ризик од поремећаја елемената критичне инфраструктуре, који могу утицати на живот становништва.

С обзиром да инфраструктура, идентификована као критична, има велики значај за друштво, постоји обавеза на стварање довољно добрих сигурносних мера које ће служити за умањење ризика од прекида рада. Циљ европске политике у овом подручју представља осигуравање прикладног и једнаког степена заштите за постројења одабране критичне инфраструктуре, што је изводљиво једино на основу заједничког европског оквира за заштиту критичне инфраструктуре.

Новим Законом о критичној инфраструктури уређује се :

- идентификација и одређивање критичне инфраструктуре Републике Србије,
- принципи и планирање заштите критичне инфраструктуре,
- надлежност и одговорност органа и организација у области критичне инфраструктуре,
- информације, извештавање, пружање подршке одлучивању, заштита података, управљање и надзор у области критичне инфраструктуре.

3. Друге могућности за решавање проблема

Изради Закона о критичној инфраструктури приступило се након што се дошло до закључка да би једино доношење новог закона на свеобухватан и ефикасан начин могло да регулише широку област критичне инфраструктуре.

4. Зашто је доношење акта најбољи начин решавања проблема

Ни једним законом ни подзаконским актом област критичне инфраструктуре у Републици Србији није у целини регулисана, због чега је неопходно да се ова важна област прецизно дефинише и обједини једним законом, с обзиром да се ради о озбиљној материји која је од значаја за Републику Србију и све њене грађане.

Последњих година, Република Србија улаже значајне напоре у стварање интегрисаног система заштите и спасавања који би адекватно одговорио у условима угрожавања, пре свега људских живота, али и критичних националних ресурса.

Такође, један од важних задатака Републике Србије на путу европских интеграција јесте усвајање нормативног оквира везаног за критичну инфраструктуру који ће бити усклађен са елементима Директиве Европског

савета 2008/114/ЕС. Директива Европског савета 2008/114/ЕС из 2008. године дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре, заједнички приступ у процени потреба за побољшавање заштите.

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

Влада на предлог Министарства унутрашњих послова одређује критичну инфраструктуру.

Министарства задужена за секторе критичне инфраструктуре имају обавезу да у року дефинисаним Законом, након завршеног поступка идентификације у складу са дефинисаним критеријумима, Министарству које је задужено за имплеметацију и спровођење овог закона, доставе предлоге критичне инфраструктуре у свом сектору.

Оператори критичне инфраструктуре су дужни да израде Безбедносни план оператора за управљање ризиком и на исти прибаве сагласност Министарства, при чему су оператори критичне инфраструктуре: министарства, јавна предузећа, привредна друштва или друга правна лица која управљају објектима, мрежама или системима, или њиховим деловима који су одређени као критична инфраструктура.

Такође министар надлежан за унутрашње послове доноси ближе прописе о методологији, начину израде и садржају Безбедносног плана оператора за управљање ризиком

6. Какве трошкове ће примена Закона изазвати грађанима и привреди, нарочито малим и средњим предузећима

Примена Закона неће изазвати трошкове грађанима и привреди, а посебно не малим и средњим предузећима.

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

За спровођење Закона о критичној инфраструктури није потребно обезбедити додатна средства из буџета Републике Србије, а ефекат предложених решења оправдава доношење Закона.

8. Да ли се Законом подржава стварање нових привредних субјеката и тржишна конкуренција

Закон о критичној инфраструктури нема утицаја на стварање нових привредних субјеката и на тржишну конкуренцију.

9. Да ли су заинтересоване стране имале прилике да се изјасне о Закону

На изради Нацрта закона радила је многочлана интерресорна радна група која је поред представника надлежних органа државне управе у свој рад укључила и друге субјекте као што су Стална конференција градова и општина, Привредна комора Србије, Факултет безбедности, Српска асоцијација менаџера корпоративне безбедности и др. У том смислу. није било потребе за одржавањем јавне расправе будући да су сви релевантни субјекти већ били укључени у израду Нацрту закона.

Текст нацрт закона о критичној инфраструктури достављен је на мишљење, поред осталих, и надлежним министарствима и субјектима чији су представници узели учешће у раду горе наведене радне групе.

10. Које ће се мере током примене закона предузети да би се постигло оно што се законом предвиђа?

Министарство унутрашњих послова врши надзор над применом Закона о критичној инфраструктури и прописа донетих на основу њега, као и инспекцијски надзор преко инспектора.

Министарство ће спроводити полагање испита и издавати лиценце официрима за везу, у складу са овим законом.

Влада ће донети прописе о критеријумима за дефинисање критичне инфраструктуре и начину извештавања, а министар унутрашњих послова донеће пропис о методологији, начину израде и садржају Безбедносног план оператора за управљање ризиком.

На крају, Предлог закона о критичној инфраструктури прописује прекршајне санкције за правна лица, као и за одговорна лица у државним органима, уколико не поштују одредбе овог закона или поступају супротно њима.

ИЗЈАВА О УСКЛАЂЕНОСТИ ПРОПИСА СА ПРОПИСИМА ЕВРОПСКЕ УНИЈЕ

1. Овлашћени предлагач прописа: Влада
Обрађивач:Министарство унутрашњих послова

2. Назив прописа
Предлог закона о критичној инфраструктури
Draft Law on critical infrastructure

3. Усклађеност прописа са 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 саржину прописа
/

б) Прелазни рок за усклађивање законодавства према одредбама Споразума

в) Оцена испуњености обавезе које произлазе из наведене одредбе Споразума
/

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 – трећа ревизија, од фебруара 2018. године - у оквиру тачке 3.24.7. Борба против тероризма, наслов Планови за усклађивање са правним тековинама Европске уније предвиђено је: „Извршиће се додатно усклађивање са Директивом 2008/114/ЕС по питању идентификације и обележавања Европске критичне инфраструктуре. С тим у вези, предлог законодавног оквира у овој области ће бити сачињен током 2018. године".

4. Усклађеност прописа са прописима Европске уније

а) Навођење одредби примарних извора права ЕУ и усклађеност са њима
/

б) Навођење секундарних извора права ЕУ и оцена усклађености са њима
Директива Европског савета 2008/114/ЕС од 8.12.2008. године о утврђивању и означавању европске критичне инфраструктуре и процени потребе побољшања њене заштите

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)

в) Навођење осталих извора права ЕУ и усклађенст 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 супретходно наведени извори права Европске уније преведени на српски језик?
Не

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

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

1. Назив прописа Европске уније : Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance) Директива Европског савета 2008/114/ЕС од 8.12.2008. године о утврђивању и означавању европске критичне инфраструктуре и процени потребе побољшања њене заштите	2. „CELEX" ознака ЕУ прописа 32008L0114
3. Овлашћени предлагач прописа: Влада	4. Датум израде табеле:
Обрађивач: МИНИСТАРСТВО УНУТРАШЊИХ ПОСЛОВА	19.06.2018.
5. Назив (нацрта, предлога) прописа чије одредбе су предмет анализе усклађености са прописом Европске уније: ПРЕДЛОГ ЗАКОНА О КРИТИЧНОЈ ИНФРАСТРУКТУРИ Draft Law on critical infrastructure	6. Бројчане ознаке (шифре) планираних прописа из базе НПАА: Пропис није унет у базу НПАА
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
Article 1	Subject matter	Нема одговарајуће одредбе				
Article 2 2.1.a	Definitions For the purpose of this Directive: (a) 'critical infrastructure' means an	Član 2. 2.1.1	**Значење израза** Поједини изрази употребљени у овом закону имају следеће значење:	ПУ		

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

а)	а1)	б)	б1)	в)	г)	д)
	asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;		1) *критична инфраструктура* представља имовину и услуге, систем или његов део који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на функционисање државе; 3) *сектори критичне инфраструктуре* су области одређене од стране Владе у којима се врши процес идентификације и одређивања критичне инфраструктуре; 4) *идентификација критичне инфраструктуре* је процес утврђивања система, мрежа, објеката и имовине у одређеном сектору у складу са дефинисаним критеријумима; 5) *одређивање критичне инфраструктуре* подразумева процес одређивања система, мрежа и објеката као критичне инфраструктуре у складу са овим законом;			

а)	а1)	б)	б1)	в)	г)	д)
	(b) ‘European critical infrastructure’ or ‘ECI’ means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;	2.1.10	10) *европска критична инфраструктура* подразумева критичну инфраструктуру лоцирану на територији земље чланице, чије би ометање или уништење имало значајан утицај на најмање две земље чланице.	ПУ		
	(c) ‘risk analysis’ means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;	2.1.8	8) *безбедоносно-оперативни план за управљање ризиком* је план који израђује оператор критичне инфраструктуре, а којим се дефинишу обим и безбедоносни циљеви и мере оператора на основу процене ризика;	ПУ		
	(d) ‘sensitive critical infrastructure protection related information’ means facts about a critical infrastructure,	17.1	Подаци у вези са критичном инфраструктуром представљају тајне	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;	17.2	податке у складу са законом којим се уређује тајност података и прописима донетим на основу овог закона. Тајни подаци који се односе на Европску критичну инфраструктуру размењују се са страним државама и органима Европске уније у складу са законом којим је уређена тајност података и потписаним међународним споразумима о размени тајних података.			
	(e) ‘protection’ means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;	2.1.6.	6) *заштита критичне инфраструктуре* представља скуп активности и мера које имају за циљ осигурање функционалности, непрекидног рада и испоруке услуга и робе објеката и система критичне инфраструктуре;	ПУ		
	(f) ‘owners/operators of ECIs’ means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.	2.1.7.	7) *оператори критичне инфраструктуре* су министарства, јавна предузећа, привредна друштва или друга правна лица која управљају објектима, мрежама или системима који су одређени као критична инфраструктура;	ПУ		
3.1.	1. Pursuant to the procedure provided in Annex III, each Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria	6.1	Идентификација критичне инфраструктуре врши се секторски у	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	and meet the definitions set out in Article 2(a) and (b). 23.12.2008 Official Journal of the European Union L 345/77 EN (1) OJ L 145, 31.5.2001, p. 43. The Commission may assist Member States at their request to identify potential ECIs. The Commission may draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI. Each Member State and the Commission shall continue on an		складу са дефинисаним критеријума.			
		6.2.	За спровођење процеса идентификације критичне инфраструктуре у одређеном сектору задужена су министарства надлежна за одређене секторе.			
		6.3.	Ближе прописе о дефинисању сектора, надлежних министарстава и критеријумима за идентификацију критичне инфраструктуре одређује Влада.			
		13.3.	Ако се критична инфраструктура од значаја за Републику Србију налази на подручју друге државе чланице, Влада предлаже надлежном телу те државе одређивање европске критичне инфраструктуре.			
		13.1.	Европска критична структура се може одредити у секторима које одређује Европска комисија.			
		13.2	Европску критичну инфраструктуру на територији Републике Србије, на предлог Центра, одређује Влада, на захтев и у сагласности са заинтересованим државама чланицама Европске уније			

а)	а1)	б)	б1)	в)	г)	д)
			и обавештава заинтересоване државе чланице о одређивању европске критичне инфраструктуре на територији Републике Србије.			
4.1 4.2.	Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI. 2. Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI. The Commission may participate in these discussions but shall not have access to detailed information which would allow for the unequivocal identification of a particular infrastructure. A Member State that has reason to believe that it may be significantly affected by the potential ECI, but has not been identified as such by the Member State on whose territory the potential ECI is located, may inform the Commission about its wish to be engaged in bilateral and/or multilateral discussions on this	13.2. 13.3.	Европску критичну инфраструктуру на територији Републике Србије, на предлог Центра, одређује Влада, на захтев и у сагласности са заинтересованим државама чланицама Европске уније и обавештава заинтересоване државе чланице о одређивању европске критичне инфраструктуре на територији Републике Србије. Ако се критична инфраструктура од значаја за Републику Србију налази на подручју друге државе чланице, Влада предлаже надлежном телу те државе одређивање европске критичне инфраструктуре.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
4.3	issue. The Commission shall without delay communicate this wish to the Member State on whose territory the potential ECI is located and endeavour to facilitate agreement between the parties. 3. The Member State on whose territory a potential ECI is located shall designate it as an ECI following an agreement between that Member State and those Member States that may be significantly affected. The acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be require					
4.4.	4. The Member State on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated	15.1.	Влада усваја годишњи извештај о броју европске критичне инфраструктуре по сектору и броју заинтересованих држава на које свака одређена критична инфраструктура	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
4.5.	ECI. Only those Member States that may be significantly affected by an ECI shall know its identity. 5. The Member States on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.	15.2. 17.1. 17.2.	има утицај, а на предлог Центра. Извештај из члана 1. овог члана доставља се Европској комисији и заинтересованим државама на које свака одређена критична инфраструктура има утицај. Подаци у вези са критичном инфраструктуром представљају тајне податке у складу са законом којим се уређује тајност података и прописима донетим на основу овог закона. Тајни подаци који се односе на Европску критичну инфраструктуру размењују се са страним државама и органима Европске уније у складу са законом којим је уређена тајност података и потписаним међународним споразумима о размени тајних података.			
5.1. 5.2.	The operator security plan (‘OSP’) procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Annex II. 2. Each Member State shall assess	9.1.	Безбедносно-оперативни план за управљање ризиком је документ којим се утврђују мере смањења и ризика, дефинишу одговорности и одређују дужности, те успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
5.3.	whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures addressing the issues identified in Annex II. If a Member State finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary. 3. If a Member State finds that such an OSP or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the OSP or equivalent is prepared addressing the issues identified in Annex II. Each Member State shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI. This period may be extended in exceptional circumstances, by agreement with the Member State authority and with a notification to the Commission.	14. 19.	дефинисаних у анализи ризика. Европска критична инфраструктура на територији Републике Србије штити се на исти начин као и критична инфраструктура Републике Србије, осим када је то прописима Европске уније другачије уређено. У вршењу инспекцијског надзора, инспектор Центра има право да: 1)утврди стање извршавања обавеза предвиђених овим законом, упозори на уочене неправилности и одреди мере и рокове за њихово отклањање; 2) врши увид у документа која се односе на критичну инфраструктуру; 3) проверава спровођење издатих наредби и закључака и наложи мере за извршење; 4) наложи израду, доношење и ажурирање докумената предвиђених овим законом;			

а)	а1)	б)	б1)	в)	г)	д)
			5)наложи обуставу мера и радњи које нису у складу са Безбедоносно-оперативним планом; 6) наложи отклањање утврђених недостатака у спровођењу прописаних мера утврђених Безбедоносно-оперативним планом;			
6.1. 6.2. 6.4.	1. The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority. 2. Each Member State shall assess whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent. If a Member State finds that such a Security Liaison Officer is in place or an equivalent exists, no further implementation action shall be necessary. 4. Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security	16.	Оператори критичне инфраструктуре морају имати Официра за везу, односно лице које служи као контакт између оператора и Центра, које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру, обавештава Центар о евалуацији ризика, претњи и рањивости, координира безбедоносно-оперативним планом, врши тестирања кроз вежбе и друге активности предвиђене планом и обавља све друге послове везане за критичну инфраструктуру. Контакт тачка за потребе размене информација и координацију активности у вези са европском критичном инфраструктуром са	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned. This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.		другим државама чланицама и телима Европске уније је Центар.			
	1. Each Member State shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.	8.2. 8.3.	Министарства задужена за секторе критичне инфраструктуре су дужна да редовно, а најмање једном квартално извештавају Центар о новонасталим променама у свом сектору. Министарства задужена за секторе критичне инфраструктуре су дужна да након завршеног поступка идентификације у складу са дефинисаним критеријумима Центру сваке године, најкасније до 31. октобра доставе предлоге измена и допуна критичне инфраструктуре у свом сектору.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	2. Each Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated pursuant to Article 4 and is located on its territory. A common template for these reports may be developed by the Commission in cooperation with the Member States. Each report shall be classified at an appropriate level as deemed necessary by the originating Member State. 23.12.2008 Official Journal of the European Union L 345/79 EN 3. Based on the reports referred to in paragraph 2, the Commission and the Member States shall assess on a sectoral basis whether further protection measures at Community level should be considered for ECIs. This process shall be undertaken in conjunction with the review of this Directive as laid down in Article 11. 4. Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the Member States. The use of such guidelines shall be optional for the Member States.			НП НП	Односи се само на земље чланице	
9.1.	1. Any person handling classified information pursuant to this Directive on behalf of a Member State or the					

а)	а1)	б)	б1)	в)	г)	д)
9.2.	Commission shall have an appropriate level of security vetting. Member States, the Commission and relevant supervisory bodies shall ensure that sensitive European critical infrastructure protection-related information submitted to the Member States or to the Commission is not used for any purpose other than the protection of critical infrastructures. 2. This Article shall also apply to non-written information exchanged during meetings at which sensitive subjects are discussed.	17.1. 17.2.	Подаци у вези са критичном инфраструктуром представљају тајне податке у складу са законом којим се уређује тајност података и прописима донетим на основу овог закона. Тајни подаци који се односе на Европску критичну инфраструктуру размењују се са страним државама и органима Европске уније у складу са законом којим је уређена тајност података и потписаним међународним споразумима о размени тајних података.	ПУ		
10.1. 10.2.	1. Each Member State shall appoint a European critical infrastructure protection contact point (‘ECIP contact point’). 2. ECIP contact points shall coordinate European critical infrastructure protection issues within the Member State, with other Member States and	17.	Контакт тачка за потребе размене информација и координацију активности у вези са европском критичном инфраструктуром са другим државама чланицама и телима Европске уније је Центар.	ПУ		

а)	а1)	б)	б1)	в)	г)	д)
	with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a Member State from being involved in European critical infrastructure protection issues.					
11.	Review	Нема одговарајуће одредбе		НП		
12.	Implementation	Нема одговарајуће одредбе		НП		
13.	Entry into force	Нема одговарајуће одредбе		НП		
14.	Addressees	Нема одговарајуће одредбе		НП		