351.824.11(497.11)(061.1EU)
COBISS.SR-ID 112377865
DOI 10.5937/fb_godisnjak0-38489

НОРМАТИВНО-ПРАВНО УРЕЂЕЊЕ БЕЗБЕДНОСНИХ ПЛАНОВА ОПЕРАТОРА У ЗАШТИТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Миле Обреновић, демонстратор*
Универзитет у Београду, Факултет безбедности

* mileobrenovic1997@gmail.com

НОРМАТИВНО-ПРАВНО УРЕЂЕЊЕ БЕЗБЕДНОСНИХ ПЛАНОВА ОПЕРАТОРА У ЗАШТИТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Сажетак: *Сврха овог рада је да утврди на који начин је нормативно-правно регулисана основа за доношење безбедносних планова оператора у заштити критичне инфраструктуре на нивоу Републике Србије, са једне стране, и Европске уније, са друге. С обзиром на вишегодишње тенденције Републике Србије да приступи Европској унији, поставља се питање да ли је и у којој мери национална нормативно-правна уређеност безбедносних планова оператора у заштити критичне инфраструктуре у Републици Србији усклађена са истоветном нормативно-правном регулацијом на нивоу Европске уније. У раду настојимо да покажемо на који начин кровни документ у овој области у Републици Србији, Закон о критичној инфраструктури, уређује ову област и на који начин то чини кровни документ у Европској унији, Директива Савета Европске уније 2008/114, те и да утврдимо у којој мери је законско решење у Републици Србији усаглашено са европском нормативом. Упоредном анализом поменута два кровна документа евидентно је да постоји велики степен сагласја националне и регионалне нормативе у наведеној области, те уколико одређене разлике настају у пракси, оне су резултат различите имплементације ових легислативних основа, а не њихове различите уређености.*

Кључне речи: *заштита критичне инфраструктуре, оператори критичне инфраструктуре, безбедносни планови оператора*

Увод

Непосредно након терористичких напада на Сједињене Америчке Државе, 11. септембра 2001. године, критична инфраструктура добија свој потпуни значај, а њена заштита постаје један од приоритета сваке државе (Јаковљевић и Гачић, 2012). Различити приступи довели су до тога да је данас у оптицају више дефиниција критичне инфраструктуре и углавном се све односе на средства и имовину која је кључна за неометано функционисање економије и друштва.[1] Међутим, за раз-

1 Различите дефиниције критичне инфраструктуре у различитим земљама видету у: Gordon, K. and Dion, M. (2008). Protection of critical infrastructure and the role of investment policies relating to

лику од претходног периода, који је био фокусиран на адекватност инфраструктуре, сада је фокус све више усмерен на заштиту критичне инфраструктуре (Moteff and Parfomak, 2004). Да би се на адекватан начин заштитила критична инфраструктура било је неопходно првенствено успоставити адекватан нормативно-правни оквир који би прецизније уредио ову област и регулисао њену заштиту. Тако је Савет Европске уније (у даљем тексту: Савет ЕУ) 8. децембра 2008. године усвојио Директиву 2008/114 са циљем дефинисања и идентификације европске критичне инфраструктуре (у даљем тексту: ЕКИ), као и одређивања заједничког приступа за процену потреба како би се побољшала њена заштита (Anglmayer, 2021). Годину дана касније у Републици Србији је усвојен Закон о ванредним ситуацијама, а Уредбом о садржају и начину израде планова заштите и спасавања у ванредним ситуацијама, из 2011. године, први пут је у правни систем Републике Србије уведен појам критичне инфраструктуре. С обзиром на бројне празнине у овим документима, односно недостатак конкретизације елемената критичне инфраструктуре и уопште области инфраструктуре, као и субјеката одговорних за заштиту, било је неопходно усвојити нове правне акте којима ће се прецизније и адекватније регулисати ова област (Трбојевић, 2018). Тако, данас, у Републици Србији круцијални нормативно-правни акт који уређује ову област представља Закон о критичној инфраструктури (у даљем тексту: ЗоКИ) из 2018. године. Када је реч о идентификовању критичне инфраструктуре, национална нормативно-правна регулатива је у великој мери усклађена са европском, па тако, да би се одредила критична инфраструктура, користе се критеријуми усклађени са критеријумима ЕУ, који обухватају: људске губитке, економске губитке и утицај на јавност. Поред наведених критеријума, и сектори у којима се идентификује критична инфраструктура у Републици Србији су усклађени са европским секторима. Сходно томе, главни сектори националне критичне инфраструктуре обухватају: информације и комуникације, електричну енергију, транспорт, нафту и гас, банкарство и финансије, воду и службе за хитне случајеве, владу (Павић и Јокановић, 2021). Дефинисање и идентификовање критичне инфраструктуре је усклађено између ЗоКИ и Директиве 2008/114, међутим, имајући у виду да нормално фукнционисање друштва зависи од заштите

national security. Paris: Organisation for Economic Co-operation and Development; Murray, T. A. and Grubešić, T. H. (2012). Critical Infrastructure protection: The vulnerability conundrum. *Telematics and informatics* 29(1): 56-65; Трбојевић, М. (2018). Заштита критичних инфраструктура – искуства транзиционих земаља. *Политичка ревија*, 56(2), 99–118.

критичне инфраструктуре, поставља се питање да ли су и у којој мери ови документи усклађени и на пољу безбедносних планова оператора, као једној од битних карика у заштити критичне инфраструктуре.

Оператори критичне инфраструктуре

Како би лакше утврдили положај оператора критичне инфраструктуре у сложеном систему заштите критичне инфраструктуре у Републици Србији, неопходно је да целокупну, сложену структуру система условно поделимо на управљачки и извршни део. Управљачки део чине субјекти који су овлашћени да планирају, руководе, организују, координирају, уређују и врше надзор и контролу над извршним делом система заштите критичне инфраструктуре. Ових субјеката са управљачком функцијом има више и они представљају безбедносни менаџмент у овој области. Народна скупштина је, и у овој области, надлежна да доноси законе и друга општа акта којима се ближе одређује ова област. Тако је Народна скупштина усвојила Закон о критичној инфраструктури и Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, којима су дефинисани правни и институционални оквири система заштите критичне инфраструктуре, а, такође, и Националну стратегију заштите и спасавања у ванредним ситуацијама, као стратешки и политички оквир за деловање на плану смањења ризика и управљања ванредним ситуацијама. Са друге стране, као што је раније и поменуто, Влада прописује критеријуме за идентификовање критичне инфраструктуре, одлучује о предлозима нових сектора критичне инфраструктуре који нису наведени ЗоКИ и одлуком одређује критичну инфраструктуру. Такође, унутар Владе, координирајући ниво менаџмента чини Министарство унутрашњих послова (у даљем тексту: МУП), које планира, координира, уређује и контролише активности, комуницира и даје информације у вези са критичном инфраструктуром и радом Републичког штаба за ванредне ситуације, који предузима мере на отклањању или смањењу последица нежељених догађаја. Оперативни део менаџмента чине министарства надлежна за секторе критичне инфраструктуре, која, по унапред прописаним критеријумима, спроводе поступак идентификације критичне инфраструктуре и достављају предлоге о изменама и допунама критичне инфраструктуре унутар сектора за које су надлежни, најкасније до 31. октобра сваке године (Стајић, Мирковић и Радивојевић, 2020).

Са друге стране, извршни део система заштите критичне инфраструктуре чине они субјекти који су дужни да предузимају конкретне, односно практичне мере и активности на плану смањења ризика, односно спречавања и/или отклањања негативних последица. Управо овај извршни део система заштите критичне инфраструктуре чине оператори критичне инфраструктуре, а безбедносни менаџмент тих оператора задужен је за израду Безбедносних планова у заштити критичне инфраструктуре (Стајић, Мирковић и Радивојевић, 2020). У легислативи Републике Србије одговор на питање ко су оператори критичне инфраструктуре се налази у ЗоКИ, где се истиче следеће: „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" (ЗоКИ, 2018, члан 2).

Република Србија се определила да Министарство унутрашњих послова буде носилац свих активности на плану заштите људи и материјалних добара, па тако и критичне инфраструктуре, од елементарних и других несрећа. Тако су министарства надлежна за секторе у којима се врши одређивање и идентификација критичне инфраструктуре (енергетика, саобраћај, снабдевање водом и храном, здравство, финансије, телекомуникационе и информационе технологије, заштита животне средине, функционисање државних органа) дужна да, након спроведеног поступка идентификације, доставе предлоге критичних инфраструктура МУП-у (ЗоКИ, 2018, члан 6). На исти начин су и оператори критичне инфраструктуре дужни да на израђен Безбедносни план прибаве сагласност МУП-а одмах, а најкасније шест месеци након идентификовања одређеног система, мреже, објекта или њиховог дела као критичне инфраструктуре (ЗоКИ, 2018, члан 8). Такође, методологију, начин израде и садржај Безбедносног плана оператора у заштити критичне инфраструктуре прописује министар надлежан за унутрашње послове. С обзиром на повезаност између оператора и министарства, то јест потчињеност и одговорност оператора према МУП-у, оператори критичне инфраструктуре морају имати официра за везу, које служи као лице за „контакт између оператора и МУП-а". Између осталог, официр за везу је дужан да обезбеђује сталну контролу ризика и претњи; да обавештава МУП о евалуацији ризика, претњи и рањивости; да координира Безбедносним планом оператора; да обавештава о променама у односу на критичну инфра-

структуру и обавља све друге послове везане за критичну инфраструктуру. Оператор критичне инфрасруктуре је тај који доставља МУП-у предлог за именовање официра за везу најкасније три месеца након одређивања неког система, објекта, мреже или њихових делова за критичну инфраструктуру, а МУП након разматрања предлога именује официра за везу (ЗоКИ, 2018). Овим није уведена никаква новина јер се још у Закону о ванредним ситуацијама из 2009. године Република Србија определила да Министарство унутрашњих послова буде носилац свих активности на плану заштите људи и материјалних добара од елементарних непогода и других несрећа (Трбојевић, 2018). Такође, и сам надзор над применом овог закона и прописа донетих на основу њега врши МУП (Закон о ванредним ситуацијама, 2009). Сви остали актери, почевши од органа аутономних покрајина и локалних самоуправа, преко других министарстава и органа, до организација, израђују сопствене процене угрожености које достављају МУП-у, а који израђује целокупну процену угрожености и доставља је Влади на усвајање (Шкеро и Атељевић, 2015).

У најзначајнијем европском документу, односно Директиви Савета ЕУ 2008/114, такође се истиче значај оператора критичне инфраструктуре у целокупном систему заштите критичне инфраструктуре. У овом документу се истиче да првенствену и коначну одговорност у заштити европске критичне инфраструктуре имају како државе чланице тако и оператори, односно власници тих инфраструктура. У Директиви Савета ЕУ 2008/114 оператори, односно власници европске критичне инфраструктуре су дефинисани као: „субјекти одговорни за улагања у одређену имовину, систем или његов део који је на темељу ове Директиве означен као европска критична инфраструктура и/или за њихов свакодневни рад" (European Council, 2008, article 2). Ако упоредимо одређење оператора критичне инфраструктуре у ЗоКИ и Директиви 2008/114 видимо да они на причично сличан начин одређују ко су оператори; у првом случају то су они који „управљају", а у другом они који су „одговорни за улагања и свакодневни рад", имовине, система, мрежа, објеката или њихових појединих делова који су означени као критична инфраструктура. Дакле, у оба случаја оператори су субјекти који имају надлежност над критичном инфраструктуром и који су одговорни за њено нормално функционисање, или у виду адекватног управљања или у виду редовног улагања. Такође, у оба случаја је „штићени објекат" инфраструктура која је, у првом случају у складу са ЗоКИ, а у другом у складу са Директивом 2008/114, одређена као критична.

За све именоване европске критичне инфраструктуре треба да постоје официри за везу који олакшавају сарадњу и комуникацију са одговарајућим државним телима надлежним за заштиту критичне инфраструктуре. Официр за везу делује као „контакт за сигурносна питања између оператора ЕКИ-ја и одговарајућег тела државе чланице" (European Council, 2008, article 6). Државе чланице су дужне да утврде да ли власници, односно оператори европске критичне инфраструктуре имају официра за везу или неко друго лице са једнако важним овлашћењима. Уколико се утврди да официр за везу не постоји, држава чланица је дужна да предузме све неопходне мере како би се успоставио официр за везу или лице са једнако важним овлашћењима (European Council, 2008). Свака држава чланица ће применити одговарајући механизам комуникације између одговарајућег тела државе чланице и официра за везу, или еквивалентног субјекта, са циљем размене релевантних информација у вези са идентификованим ризицима и претњама по ЕКИ. Овај комуникациони механизам не доводи у питање националне захтеве у погледу приступа осетљивим и поверљивим информацијама (Magdolen, 2019). Када је реч о официрима за везу, из наведеног се види да је национални нормативно-правни оквир и у овом погледу усаглашен са европским. Тако се и у ЗоКИ и у Директиви 2008/114 истиче да официр за везу служи као „контакт", са једне стране, између „оператора", а са друге, у Директиви 2008/114 „одговарајућег тела државе чланице", а у ЗоКИ, с обзиром на то да се Република Србија определила да МУП буде носилац свих активности на плану заштите критичне инфраструктуре, то тело је „МУП".

Безбедносни планови оператора у заштити критичне инфраструктуре

Разумевање ко су оператори у заштити критичне инфраструктуре је неопходно, зато што су управо они ти који доносе безбедносне планове. Безбедносни планови оператора у заштити критичне инфраструктуре су свакако обухваћени ЗоКИ, у његовом делу који се односи на заштиту критичне инфраструктуре. Безбедносни план оператора у заштити критичне инфраструктуре регулише члан 8. поменутог Закона, с тим да га означава као Безбедносни план оператора за управљање ризиком. Као што је и раније поменуто, у овом Закону се

наводи да су оператори ти који су дужни да израде Безбедносни план оператора за управљање ризиком и да на њега прибаве сагласност МУП-а одмах, а најкасније шест месеци након идентификовања критичне инфраструктуре. Оно што је наведено у претходном поглављу јесте повезаност између МУП-а и оператора, а та повезаност има још већи значај ако имамо у виду да се у члану 8. ЗоКИ истиче да је управо министар надлежан за унутрашње послове тај који прописује методологију, односно начин израде и садржај Безбедносног плана оператора за управљање ризиком (ЗоКИ, 2018). У ЗоКИ се Безбедносни план оператора за управљање ризиком дефинише као: „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" (ЗоКИ, 2018, члан 8).

Овде би требало обратити пажњу на то да процена ризика и Безбедносни план буду два одвојена акта и за то постоји више разлога. Прво, процена ризика је акт који идентификује потенцијалне облике угрожавања критичне инфраструктуре, слабе тачке система и где се могу јавити, вероватноћу њиховог наступања, опис њиховог садржаја, последице које би наступиле и томе слично. Сходно наведеном, јасно је да је процена ризика акт који претходи Безбедносном плану и на основу кога се безбедносне процедуре, које су саставни део безбедносног плана, израђују. Сагласност надлежног министарства, у овом случају МУП-а, на процену ризика представља елементарну основу за даљу израду адекватног Безбедносног плана. Друго, процена ризика има фундаментални значај не само за израду Безбедносног плана, него и за израду целокупног система заштите критичне инфраструктуре. Због тога је на стратегијском нивоу неопходно прописати методологију израде процене ризика која би била јединствена и заједничка за операторе у сваком сектору, што би омогућило успостављање јединствених критеријума за боље уочавање проблема, али и олакшало размену информација, како унутар извршног нивоа, односно између различитих оператора, тако и између извршног и управљачког дела система заштите критичне инфраструктуре (Стајић, Мирковић и Радивојевић, 2020). Тако се у Методологији израде и садржаја процене ризика од катастрофа и плана заштите и спасавања истиче да процена ризика од катастрофа Републике Србије, аутономне покрајине и јединице локалне самоуправе у општем делу садржи податке о: положају и карактеристикама територије и критичној инфраструктури.

Док посебан део ове Методологије обухвата: идентификацију опасности од катастрофа, смернице за израду сценарија и смернице за одређивање нивоа ризика (Упутство о методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, 2016). Методологија у области заштите од катастрофа може послужити као пример за методологију израде процене ризика и планова у области заштите критичне инфраструктуре. Треће, имајући у виду значај система заштите критичне инфраструктуре за целокупну државу, али и ниво одговорности оператора критичне инфраструктуре, требало би донети процену ризика за критичну инфраструктуру првенствено на националном нивоу, затим на секторском нивоу и тек на крају на нивоу сваког оператора критичне инфраструктуре понаособ. У том случају, процени ризика било би дато место које акт такве врсте има и у другим упоредним земљама (САД, Канада, Уједињено Краљевство) у систему заштите критичне инфраструктуре (Стајић, Мирковић и Радивојевић, 2020).

Идентификација и процена ризика је један од фундаменталних корака у стварању успешне стратегије унапређења безбедности и заштите критичне инфраструктуре. Када говоримо о ризицима који угрожавају критичну инфраструктуру, свакако, треба обухватити чиниоце који могу довести до угрожавања нормалног функционисања оператора и, уопште, безбедног функционисања критичне инфраструктуре (Мићовић, 2016). Тако би процена ризика на нивоу оператора критичне инфраструктуре требало да обухвати следеће: 1. анализу пословног, безбедносног, економског, социјалног и правног окружења у коме функционише оператор критичне инфраструктуре; 2. анализу секторске и међусекторске зависности са посебном анализом последица, те секторске и међусекторске зависности критичне инфраструктуре у секторима енергије, информационих технологија и саобраћајне инфраструктуре; 3. анализу потенцијалне секторске и међусекторске сарадње у управљању кризом и управљању ризиком; 4. анализу постојеће инфраструктуре са свим њеним идентификованим слабостима, као и могућим алтернативним решењима у случају наступања потпуног уништења или делимичног оштећења; 5. анализу извора и облика угрожавања са посебним нагласком на намерне и ненамерне акциденте, угрожавање у физичком и виртуелном простору, спољне или унутрашње облике угрожавања, појединачне или серијске нападе, облике угрожавања у једном сектору и оне који су део напада на друге секторе и томе слично (Стајић, Мирковић и Радивојевић, 2020).

Након спроведене процене на нивоу оператора критичне инфраструктуре потребно је израдити Безбедносни план, који треба да: садржи мере које треба предузети (организационе, правне, техничке, административне, санитарне и друге) ради смањења ризика, односно смањења последица уколико је штетни догађај већ наступио; дефинише одговорности оператора у систему заштите критичне инфраструктуре и утврди безбедносне процедуре као прописане стандарде поступања у свакој ситуацији која је у процени ризика идентификована као угрожавајућа. Иако ЗоКИ не предвиђа, Безбедносни план би могао да садржи и листу индикатора, односно показатеља да непосредна опасност по виталне и штићене системе предстоји, како би се благовремено предузеле све мере и активности на организовању и функционисању система заштите и како би се смањиле последице у случају да штетни догађај наступи (Стајић, Мирковић и Радивојевић, 2020).

У најважнијем регионалном документу који уређује ову област, Директиви Савета ЕУ 2008/114, наглашавају се три специфична захтева који оператори ЕКИ морају да испуне: да именују официра за везу, што је раније објашњено, затим да спроведу анализу ризика на основу сценарија претњи и да осмисле Безбедносни план оператора. У Директиви Савета ЕУ 2008/114 област Безбедносних планова оператора регулисана је у члану 5. овог документа. Прво се наводи да се у поступку Безбедносног плана оператора утврђује имовина критичне инфраструктуре која има обележја ЕКИ, а потом и безбедносна решења која се утврђују, а касније и имплементирају ради заштите ЕКИ. Минимални садржај који се обрађује поступком Безбедносних планова оператора дефинисан је у прилогу (анексу) 2. У поменутом прилогу се истиче да ће Безбедносни планови оператора утврдити имовину критичне инфраструктуре и сигурносна решења која постоје или се примењују ради њихове заштите (European Council, 2008). У складу са поменутом директивом, од држава чланица се захтева да процене да ли постоје безбедносни планови оператора за сву ЕКИ која је идентификована на њиховој територији или друге одређене еквивалентне мере (Шкеро и Атељевић, 2015). Када држава чланица утврди да Безбедносни план оператора или једнаковредне мере постоје и да се редовно и на адекватан начин ажурирају, спровођење даљих радњи више није неопходно. Уколико, у другом случају, држава чланица утврди да такав Безбедносни план оператора или једнаковредне мере не постоје, неопходно је да тада држава чланица предузме све мере

које сматра неопходним како би обезбедила припрему Безбедносних планова оператора или једнаковредних мера. Сам поступак Безбедносних планова оператора обухвата најмање: „1. утврђивање важне имовине; 2. спровођење анализе ризика на темељу сценарија главних претњи, слабости сваке имовине и могућега учинка; 3. утврђивање, одабир и одређивање приоритета за противмере и поступке" (European Council, 2008: 178). Поменути поступак је шири и обухватнији у односу на поступак у Републици Србији, јер је: 1) утврђивање важне имовине у надлежности министарстава задужених за утврђене секторе критичне инфраструктуре; 2) спровођење анализе ризика на нивоу Републике Србије регулисано је проценом ризика, актом који је одвојен од безбедносног плана и који му претходи; 3) противмере су и на националном нивоу потпуно обухваћене Безбедносним плановима оператора у заштити критичне инфраструктуре. Тако, ЗоКИ регулише питање Безбедносних планова оператора за управљање ризиком усмеравајући се искључиво на мере заштите и, сходно томе, усклађен је са Директивом 2008/114 у оном делу који се односи на противмере и сигурносна решења Безбедносних планова оператора.

Закључак

Доношењем Закона о критичној инфраструктури 2018. године учињен је најбитнији корак у регулисању заштите критичне инфраструктуре, између осталог и у успостављању основе за израду Безбедносних планова оператора. Нарочито, имајући у виду да се у некадашњем Закону о ванредним ситуацијама из 2009. године није ни помињала критична инфраструктура, те је овај закон 2018. године замењен Законом о смањењу ризика од катастрофа и управљању ванредним ситуацијама. Тако је 2018. година постала најзначајнија година у српској легислативи на пољу заштите критичне инфраструктуре, и у оквиру тога и у области безбедносних планова оператора у заштити критичне инфраструктуре. С обзиром на то да је ЕУ ово подручје нешто раније, 2008. године, нормативно-правно регулисала, доношењем Директиве Савета Европске уније 2008/114, Република Србија је имала одређени основ за прецизније уређење ове области. Из наведеног рада и упоредном анализом ЗоКИ и Директиве 2008/114 јасно је да је Република Србија у одређењу оператора и њихових безбедносних планова своју националну правну регулисаност ускладила са

европском и резултат тога је велика усаглашеност ЗоКИ и Директиве 2008/114 у овој области.

ЛИТЕРАТУРА

Anglmayer, I. (2021). European critical infrastructure Revision of Directive 2008/114/EC. Brussels: European Parliamentary Research Service. Retrieved March 13, 2022; from https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662604/EPRS_BRI(2021)662604_EN.pdf

European Council (2008). Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Aberdeen: Official Journal of the European Union. Retrieved March 10, 2022; from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114

Gordon, K. and Dion, M. (2008). Protection of critical infrastructure and the role of investment policies relating to national security. Paris: Organisation for Economic Co-operation and Development. Retrieved March 13, 2022; from https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

Magdolen, M. (2019). Critical infrastructure protection in European legislation. Žilina: Faculty of Security Engineering. Retrieved March 20, 2022; from http://www.kforce.gradjevinans.net/images/Fajlovi/Teaching_mobility/UT/5/Lecture.pdf

Moteff, J. and Parfomak, P. (2004). Critical infrastructure and key assets: definition and identification. Washington DC: Congressional Research Service. Retrieved March 20, 2022; from https://apps.dtic.mil/sti/pdfs/ADA454016.pdf

Murray, T. A. and Grubešić, T. H. (2012). Critical Infrastructure protection: The vulnerability conundrum. *Telematics and informatics*, 29(1): 56–65.

Закон о ванредним ситуацијама, „Сл. гласник РС", бр.111/2009.

Закон о критичној инфраструктури, „Сл. гласник РС", бр. 87/18.

Јаковљевић, В. и Гачић, Ј. (2012). Заштита критичне инфраструктуре у кризним ситуацијама. У М. Богавац (Ур.) (2012). *Међународна научна конференција – МЕНАЏМЕНТ* (стр. 280–286). Младеновац: Факултет за индустријски менаџмент.

Мићовић, М. (2016). Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама. Докторски рад. Београд: Факултет безбедности.

Упутство о методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, „Сл. гласник РС", бр. 80/19.

Национална стратегија заштите и спасавања у ванредним ситуацијама, „Сл. гласник РС", бр. 86/11.

Павић, М. и Јокановић, И. (2021). Законодавство о критичној инфраструктури у Републици Србији, региону и Европској унији. У М. Бешевић и Љ. Козарић (Урс.) (2021). *Зборник радова Грађевинског факултета*, 39(17–28). Суботица: Грађевински факултет.

Стајић, Љ., Мирковић, В. и Радивојевић, Н. (2020). Безбедносни менаџмент у области заштите критичне инфраструктуре у Републици Србији – стање и перспективе. У С. Орловић (Ур.) (2020). *Правна традиција и нови правни изазови* (стр. 953–970). Нови Сад: Правни факултет.

Трбојевић, М. (2018). Заштита критичних инфраструктура – искуства транзиционих земаља. *Политичка ревија*, 56(2), 99–118.

Шкеро, М. и Атељевић, В. (2015). Заштита критичне инфраструктуре и основни елементи усклађивања са Директивом Савета Европе 2008/114/ЕС. *Војно дело*, 67(3), 192–207.

NORMATIVE-LEGAL REGULATION OF OPERATOR SECURITY PLANS IN THE PROTECTION OF CRITICAL INFRASTRUCTURE

Mile Obrenović, Student-Assistant
University of Belgrade, Faculty of Security Studies

Summary

The aim of this paper is to determine the manner in which the normative-legal basis is constituited for the adoption of security plans of operators in the protection of critical infrastructure in the Republic of Serbia on the one hand, and in the European Union on the other. Long-standing tendencies of the Republic of Serbia to join the European Union arises questions as whether and to what extent the national normative-legal regulation of security plans of operators in critical infrastructure protection in the Republic of Serbia is harmonized with the same normative-legal regulation at the European Union level. In this paper we try to show how the most important document in this area in the Republic of Serbia, the Law on Critical Infrastructure, regulates this area and how it is done under the umbrella document in the European Union, Council Directive (EU) 2008/114, and to determine in which extent the legal solution of the Republic of Serbia is harmonized with the European norm. A comparative analysis of these two umbrella documents shows that there is a high degree of agreement between national and regional norms in this area, and if certain differences arise in practice, they are the result of different implementation of these legislative bases and not their different regulation.

Keywords: *critical infrastructure protection, operators of critical infrastructure, operator security plans.*