Прегледни рад

005.334:351.759.6(497.11)
doi:10.5937/zrpfns59-62252

Ненад П. Радивојевић
Универзитет у Новом Саду
Правни факултет у Новом Саду
N.Radivojevic@pf.uns.ac.rs
ORCID ID: 0000-0002-0630-0632

Јана М. Марковић
Универзитет у Београду
Факултет безбедности
jana.markovic@fb.bg.ac.rs
ORCID ID: 0009-0003-0676-8213

ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ – АКТУЕЛНО СТАЊЕ И МОГУЋНОСТИ ДАЉЕГ РАЗВОЈА И УНАПРЕЂЕЊА*

***Сажетак**: Критична инфраструктура представља основ функционисања државе и друштва, те је један од кључних фактора безбедности и економског развоја, као и здравља и социјалног благостања грађана. Њена заштита добија посебан значај у ери глобализације и са све већом изложеношћу различитим ризицима – од природних катастрофа до терористичких и сајбер напада. Република Србија је, у складу са савременим безбедносним трендовима и процесом приближавања Европској унији, предузела низ конкретних нормативних и институционалних корака у циљу регулисања и унапређења система заштите критичне инфраструктуре. Један од тих корака је и усвајање првог системског закона који уређује ову област 2018. године – Закона о критичној инфраструктури.*

Циљ овог рада је да, кроз анализу стратешких докумената и позитивноправне регулативе у Републици Србији, прикаже актуелни модел зашти-

* Резултати рада су презентовани на 7. Међународној научној конференцији „Правна традиција и нови правни изазови“ у форми саопштења под називом „Critical Infrastructure Protection in the Republic of Serbia – Regulatory Framework and Implementation Challenges“. Конференција је одржана на Правном факултету у Новом Саду од 23. до 24. октобра 2025. године.

те критичне инфраструктуре. Посебан нагласак стављен је на анализу Закона о критичној инфраструктури, предузете остале активности у периоду од његовог доношења до данас, као и на идентификацију неких његових предности, недостатака и изазова у имплементацији. Рад указује на значај сарадње јавног и приватног сектора, као и на потребу усаглашавања релевантних прописа, јачања институционалних капацитета, координације различитих субјеката заштите и развоја отпорности критичне инфраструктуре. На основу спроведене анализе, аутори предлажу могуће правце даљег развоја и унапређења како нормативног оквира, тако и практичног деловања свих субјекта заштите критичне инфраструктуре у Републици Србији.

***Кључне речи**: критична инфраструктура, заштита критичне инфраструктуре, Закон о критичној инфраструктури, национална безбедност.*

1. УВОД

Критична инфраструктура (у даљем тексту: КИ) један је од стубова државе неопходних за њено свеукупно функционисање. Упркос непостојању универзалне дефиниције, под овим појмом подразумевају се објекти, системи, мреже и њихови делови који су од суштинског значаја за јавну добробит, те би њихово угрожавање потенцијално могло имати негативан утицај на здравље људи, њихову безбедност, економско и социјално благостање грађана, ефективно функционисање владе, одбрану и националну безбедност.[1] КИ чине материјална физичка средства (нпр. зграде, објекти, имања, животиње, производи и сл.), нематеријална физичка средства (нпр. информације), људски ресурси (запослени и екстерна релевантна физичка лица) и сајбер средства (хардвер, софтвер, подаци и мреже неопходне за функционисање).[2] У контексту индустријализације и глобализације, као и диверзификације ризика, КИ постаје све рањивија на различите облике угрожавања, нарочито у светлу могућих терористичких напада.[3]

У новије време, заштити КИ приступа се као питању од стратешког значаја, било да се посматра као заштита самих инфраструктурних система

[1] Јана Марковић, *Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије*, докторска дисертација, Факултет безбедности, Београд 2025, 136.

[2] US Army Training and Doctrine Command, DCSINT Handbook No. 1.02 Critical Infrastructure Threats and Terrorism, US Army Training and Doctrine Command, Fort Leavenworth 2006, I-1.

[3] Познати су случајеви терористичких напада у Њујорку и Вашингтону (2001), Мадриду (2004), Лондону (2005) и другим градовима.

или као физички и логички системи неопходни за подршку безбедности, сигурности и благостању заједнице.[4] Она обухвата „све активности[5] које имају за циљ да обезбеде функционалност, континуитет и интегритет КИ у циљу одвраћања, ублажавања и неутралисања претње, ризика или рањивости".[6] Томе треба додати и активности на јачању отпорности КИ, односно боље разумевање ризика и адекватније дефинисање улога и дужности релевантних субјеката одговорних за КИ.[7] При томе, треба имати у виду да се одговорност за заштиту не налази искључиво на државним органима и институцијама, већ и на приватном сектору, али и свим грађанима. Услед процеса приватизације и трансфера власништва над значајним деловима инфраструктуре на приватне субјекте, јавља се као неизоставни чинилац сарадња јавног и приватног сектора у обезбеђивању континуитета функционисања кључних система. Приватни сектор, укључујући и приватне субјекте безбедности, постаје један од кључних чинилаца у заштити КИ,[8] а тиме и у ширем контексту и националне безбедности.

Држава задржава централну улогу у креирању нормативног оквира заштите КИ, постављајући основу за њено спровођење кроз друге нивое менаџмента. Заштита КИ може се сагледати кроз систем који се састоји од управљачког и извршног дела.[9] Управљачки део чине државни органи овлашћени да планирају, регулишу, организују, координирају и врше надзор и контролу, док извршни део чине субјекти који су одговорни за предузимање конкретних мера и активности на заштити КИ (оператори КИ). Посматрано из другог угла, у складу са овлашћењима која су им дата, стратегијски ниво у Републици Србији чине Народна скупштина и Влада, координирајући ниво чине Министарство унутрашњих послова и Републички штаб за ванредне ситуације, док оперативни ниво чине министарства надлежна за секторе КИ.[10] Узимајући у обзир све нивое менаџмента, тактички ниво обухватао

---

[4] Robert S. Radvanovsky, and Allan McDougall, *Critical infrastructure: Homeland security and emergency preparedness*, CRC press, Boca Raton 2024, 8.

[5] Али и мере, процедуре и поступке.

[6] Council Directive, 2008/114/EC on the identification and design of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, L 345/75, art. 2.

[7] Council Directive, 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, L 333/164, Preambule.

[8] Ненад Радивојевић, Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним освртом на Републику Србију, докторска дисертација, Правни факултет у Новом Саду, Нови Сад 2019.

[9] Љубомир Стајић, Владан Мирковић, Ненад Радивојевић, „Безбедносни менаџмент у области заштите критичне инфраструктуре у Републици Србији – стање и перспективе", *Зборник радова Правног факултета у Новом Саду* 3/2020, 959.

[10] *Ibid*., 960.

би све непосредне извршиоце (субјекте), који поступају по налозима које задаје извршни део система заштите. У систему заштите КИ, значајно место заузима и приватни сектор, иако без интервенције влада он не може успешно да спроведе заштиту КИ.[11] У том погледу, Тед Левис (*Ted Lewis*) уочава негативан тренд када је у питању заштита КИ с обзиром на то да ни влади ни власницима из приватног сектора често нису јасне њихове улоге и одговорност у погледу ове заштите.[12]

Узимајући у обзир претходно наведено, предмет рада је анализа конкретног модела заштите КИ у Републици Србији. При томе, настојаћемо да кроз критичку анализу релевантних законских и подзаконских аката, као и стратешких докумената којима се директно и индиректно регулише област заштите КИ пружимо свеобухватан опис досадашњих најзначајних активности надлежних државних органа, као и кључних изазова који утичу на ниво заштите КИ у Републици Србији.

У вези са изнетим, аутори ће покушати да понуде одговоре на следећа питања: Да ли је Закон о критичној инфраструктури усаглашен са праксом заштите КИ, али и обратно? Које су предности, и који недостаци су уочени у периоду од 2018. године и доношења Закона о критичној инфраструктури до данас? Који су правци даљег деловања како у нормативноправном тако и у практичном аспекту заштите?

2. НА ПУТУ УСВАЈАЊА СИСТЕМСКОГ ЗАКОНА

Заштити КИ придаје се све већи значај и у нормативним активностима Европске уније (у даљем тексту: ЕУ). Наиме, још 2008. године усвојена је тзв. Директива о европској критичној инфраструктури, односно „Директива о утврђивању и означивању европске критичне инфраструктуре и процени потребе побољшања њене заштите“.[13] У питању је први обавезујући пропис ЕУ у тој области. У децембру 2020. године, Европска комисија је на основу неколико средњорочних извештаја и свеобухватног процеса јавног слушања заинтересованих страна, представила предлог за замену постојеће Директиве новом, познатом као „Директива о отпорности критичних субјеката“. Нова директива је коначно одобрена 2022. године, са применом од октобра

[11] Mark De Bruijne, and Michel van Eeten, „Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment“, *Journal of contingencies and crisis management* 1/2007, 23.

[12] Ted G. Lewis, *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley and Sons, New Jersey 2006, 29.

[13] Council Directive, 2008/114/EC on the identification and design of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, L 345/75.

2024.[14] Усвајањем ових директива развија се нова област европских интеграција, која постаје обавезујућа за све државе које теже чланству у ЕУ, па и за Републику Србију.

Кључна разлика у погледу ових директива тиче се измена које су извршене у погледу преласка са заштите КИ на њену отпорност, као и увођење новог термина „критични ентитет" као замена за термин КИ. У вези са отпорношћу, која је одређена као способност критичног ентитета да спречи, заштити се, одговори, одупре се, ублажи, апсорбује, прилагоди и опорави се од инцидента, нагласак је стављен на адаптивност и опоравак у погледу било које врсте угрожавања, односно поремећаја КИ.[15] „Критични ентитет" као новоуведен појам користи се као еквивалент оператору КИ, док у основи преноси „бригу" са сектора КИ на ниво конкретних објеката, односно оператора КИ. При томе, критични ентитет може бити и јавног или приватног карактера под условом да га је држава идентификовала у складу са одређеном процедуром. Опсег сектора који подлежу заштити, али и претњи које су препознате такође је проширен у новој Директиви ЕУ у односу на претходну.[16]

Као земља која тежи чланству у ЕУ, Република Србија има обавезу да нормативно уреди и регулише питања идентификације, одређења и заштите националне и европске КИ. Први корак на том путу је усвајање закона о КИ, а онда и пратећих подзаконских аката.[17] На путу европских интеграција, један од захтева који се нашао пред Републиком Србијом био је уређивање области заштите КИ и усаглашавање на том пољу са елементима Директиве о европској КИ из 2008. године. Акционим планом за Поглавље 24 у преговорима о приступању Србије ЕУ, Министарство унутрашњих послова (у даљем тексту: МУП) Републике Србије препознато је као орган надлежан да изради предлог законодавног оквира у овој области. У оквиру МУП-а, Сектор за ванредне ситуације одређен је као орган који координира активности на формирању међуресорне радне групе која ће дефинисати нацио-

---

[14] Council Directive, 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, L 333/164.

[15] О концепту отпорности и његовом значају у контексту заштите критичне инфраструктуре вид. Zoran Keković, Vladimir Ninković, „Towards a Conceptualization od Resilience in Security Studies", *Српска политичка мисао* 1/2020, 153-175 и Vladimir Ninković, „Critical Infrastructure Resilience – National Approches in the United States of America, the United Kingdom and Australia", *Зборник радова Правног факултета у Новом Саду* 4/2021, 1201-1255.

[16] Вид. Christer Pursiainen, Eero Kytömaa, „From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean?" *Sustainable and Resilient Infrastructure* 8/2022, 85-101; Francesco Trinchillo, „Critical infrastructures: European context and evolution of the law", *Journal of Defense Resources Management* 1/2025, 309-320.

[17] Зоран Кековић, Владимир Нинковић, *Заштита критичне инфраструктуре – системски приступ*, Центар за анализу ризика и управљање кризама, Београд 2025, 109.

налну политику заштите КИ или спроводити анализу недостатака на основу изабраног модела најбоље праксе у ЕУ.[18] Иако је Директива ЕУ из 2022. године обавезујућа само за државе чланице, несумњиво је да ће одређене обавезе настати и за Републику Србију у вези са преговарачким процесом. У првом реду, то би требало да обухвати и одређене измене и допуне постојећег нормативног оквира у вези са КИ.

Поред наведеног, један од главних разлога за доношење Закона о критичној инфраструктури (у даљем тексту: ЗоКИ) јесте непостојање јединственог законског акта из ове области, који ће на свеобухватан начин уредити основе система заштите КИ. До његовог усвајања, термин КИ се спомињао у више стратешких докумената, као и у законским и подзаконским актима. Између осталих, то су: Закон о ванредним ситуацијама,[19] Закон о информационој безбедности,[20] Закон о одбрани,[21] Закон о тајности података,[22] Закон о приватном обезбеђењу,[23] Уредба о садржају и методологији за израду планова заштите и спасавања у ванредним ситуацијама,[24] Упутство о методологији за процену ризика и планова заштите и спасавања у ванредним ситуацијама,[25] Методологија за израду процене угрожености од елементарних напогода и других несрећа и планова заштите и спасавања у ванредним ситуацијама.[26]

3. НОРМАТИВНИ ОКВИР ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

Идентификовање значаја КИ у оквиру највиших стратешких докумената Републике Србије представља полазну тачку у процесу њеног дефинисања и заштите. С тим у вези, анализу нормативног оквира заштите КИ почињемо са релевантним усвојеним (и важећим) стратегијама, на првом месту са Стратегијом националне безбедности Републике Србије.

Стратегија националне безбедности Републике Србије из 2019. године у одређеним деловима апострофира значај КИ и потребу њене заштите у контексту остваривања националне безбедности. Конкретно, реч је о: 1) потреби

---

[18] Action Plan for Chapter 24, 2015, 257-258, https://eupregovori.bos.rs/progovori-oprego-vorima/uploaded/Akcioni%20plan%20za%20poglavlje%2024%20od%2023.%20januara%20 2015_1.pdf, 04. октобар 2025.

[19] *Службени гласник РС*, бр. 111/2009, 92/2011 и 93/2012.

[20] *Службени гласник РС*, бр. 6/2016, 94/2017 и 77/2019.

[21] *Службени гласник РС*, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015 и 36/2018.

[22] *Службени гласник РС*, бр. 104/2009.

[23] *Службени гласник РС*, бр. 104/2013, 42/2015 и 87/2018.

[24] *Службени гласник РС*, бр. 8/2011.

[25] *Службени гласник РС*, бр. 96/2012.

[26] *Службени гласник РС*, бр. 18/2017.

за појачаном *заштитом критичне енергетске инфраструктуре* услед повећаног броја сукоба изазваних надметањем за обезбеђење енергената и других природних сировина, питке воде и хране која би чак укључила и употребу војних снага; 2) *опасности од напада на КИ* услед глобалног развоја информационих технологија и интензивирања активности у сајбер простору (део 1.); 3) *идентификовању и заштити објеката КИ* и спровођењу мера раног упозорења и превентивног реаговања у вези са очувањем унутрашње стабилности и безбедности Републике Србије и њених грађана (део 4.2.); 4) јачању регионалне стабилности, унапређењу развоја и повезивања кроз инфраструктуру (део 4.4.); 5) унапређењу појединих сегмената инфраструктуре (део 4.6.) и 6) субјектима значајним за националну безбедност, а надлежних за инфраструктуру (део 5.1.2.).[27] Из наведених одредби, уочава се да Стратегија уводи појам КИ, али без њеног свеобухватног дефинисања.

Опасност од сајбер напада на објекте КИ, као последица развоја информационих технологија, препозната је и у Стратегији одбране Републике Србије.[28] Ова стратегија посвећује већу пажњу заштити КИ у поређењу са Стратегијом националне безбедности, при чему је један од главних циљева осигурање безбедности ових објеката. То подразумева усклађивање са регулативом ЕУ у области идентификације, одређења и заштите КИ, као и посвећивање пажње потпуном спровођењу ових правних решења. Стратегија предвиђа стално предузимање превентивних мера заштите, посебно у погледу заштите од пожара, експлозија и терористичких напада, као и успостављање интегрисаног информационог система за безбедносни надзор ових објеката (део 4.2.).

Стратегија развоја информационог друштва и информационе безбедности Републике Србије за период од 2021. до 2026. године[29] препознаје критичну информациону инфраструктуру као ИКТ системе од посебног значаја. Овај документ наглашава важност одржавања несметаног функционисања ових система, јер њихово ометање или уништење може имати озбиљне последице, посебно у погледу јавне безбедности и великог броја корисника. Такође, ова Стратегија предвиђа и мере заштите, укључујући превенцију инцидената и смањење штете од њиховог наступања (део 3, посебни циљ 3, мера 3.2.).

Наведеним одредбама обухваћени су извесни аспекти заштите КИ. Ипак, иако су стратешки документи донети након усвајања ЗоКИ, не постоји јасна индикација да ови документи представљају основу за имплементацију одредби

[27] Стратегија националне безбедности Републике Србије, *Службени гласник РС*, бр. 94/2019.

[28] Стратегија одбране, *Службени гласник РС*, бр. 94/2019.

[29] Стратегија развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године, *Службени гласник РС*, бр. 86/2021.

ЗоКИ.[30] Овај недостатак експлицитне повезаности између стратешких докумената и законских норми, иако би по правилу требало да буде присутан с обзиром на обавезност стратешких аката, може указивати на извесне неусклађености у процесу планирања и регулације заштите КИ у земљи.

Поред стратешких докумената, потребно је указати и на повезаност ЗоКИ са другим релевантним законима који уређују заштиту КИ у различитим секторима или у различитим ситуацијама. Па тако, у случају угрожавања, ометања рада или уништења КИ, одредбе чл. 11, ст. 1 ЗоКИ упућују на директну примену Закона о смањењу ризика од катастрофа и управљању ванредним ситуацијама (у даљем тексту: ЗоСРиУВС).[31] Интересантно је да се у ЗоСРиУВС ни на једном месту не помиње критична инфраструктура или њена заштита.[32] Међутим, на основу ЗоСРиУВС[33] израђена је Методологија израде и садржај процене ризика од катастрофа и плана заштите и спасавања,[34] у којој постоје одредбе које се односе на КИ. У самој методологији, КИ се дефинише на начин на који је то учињено у ЗоКИ и даје се списак прецизно одређене КИ за одређених десет сектора.[35] Поред наведеног, ЗоСРиУВС уводи нову категорију субјеката – субјекти од посебног значаја за заштиту и спасавање, у вези са чиме је донета Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији.[36] Овом одлуком одређују се привредна друштва и друга правна лица, која су од значаја за спровођење мера заштите и спасавања, а који уједно припадају неким од сектора КИ одређених ЗоКИ.

На основу претходне анализе можемо рећи да је идентификацији КИ више пажње посвећено у ЗоСРиУВС и пратећим подзаконским актима него

---

[30] За Стратегију националне безбедности се каже да је „услов, основ, усмеравајући и корективни документ једне државе (друштва) настао као израз уважавања општеприхваћених стандарда безбедносног организовања савремених држава. То је уједно и документ пројекције развоја функционисања система безбедности у будућности, као и основа за све друге документе који се баве неким од безбедносних тема“. Љубомир Стајић, Ненад Радивојевић, Владан Мирковић, „Неки аспекти политике унутрашње безбедности као елемента Стратегије националне безбедности Републике Србије“, *Зборник радова Правног факултета у Новом Саду* 4/2017, 1327.

[31] Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, *Службени гласник РС*, бр. 87/2018.

[32] Спомињу се тзв. СЕВЕСО постројења, за која можемо претпоставити да ће чинити КИ у сектору енергетике и/или заштите животне средине.

[33] ЗоСРиУВС, чл. 17, ст. 10.

[34] Упутство о Методологији израде и садржај процене ризика од катастрофа и плана заштите и спасавања, *Службени гласник РС*, бр. 80/2019.

[35] Вид. Ј. Марковић, 2025, 184-185. Занимљиво је истаћи то да ЗоКИ идентификује осам сектора.

[36] На основу чл. 31. ст. 2 ЗоСРиУВС, донета је Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији, *Службени гласник РС*, бр. 69/2019.

у ЗоКИ, који треба на свеобухватан начин да уреди ову област и на тај начин послужи као основа другој, секторској регулативи у области заштите КИ.

Када је у питању Закон о приватном обезбеђењу (у даљем тексту: ЗоПО),[37] он се у контексту заштите КИ може сагледати са два аспекта. Први аспект се односи на „обавезно обезбеђене објекте", односно објекте који се овим актом одређују као објекти „од стратешког значаја за Републику Србију и њене грађане, као и објекте од посебног значаја чијим оштећењем или уништењем би могле наступити теже последице по живот и здравље људи или који су од интереса за одбрану земље, осим објеката чију заштиту обављају државни органи и објеката чија се заштита обавља сагласно прописима из области одбране."[38] Ова категорија објеката није ништа друго но КИ у добром делу.

Други аспект обухвата улогу коју приватно обезбеђење има у заштити КИ. У послове приватног обезбеђења, у складу са ЗоПО, спадају и следећи послови: „1) процена ризика у заштити лица, имовине и пословања; 2) заштита лица и имовине физичким и техничким средствима [...] 3) планирање, пројектовање и надзор над извођењем система техничке заштите, монтаже, пуштање у рад, одржавање система техничке заштите и обука корисника [...]."[39] Из наведеног следи да службеници обезбеђења израђују процене ризика, доносе планове обезбеђења (заштите), као и примењују мере заштите у складу са планом обезбеђења и процедурама рада. У случајевим настанка катастрофа и проглашења ванредне ситуације, приватно обезбеђење се јавља као субјекат који први на лицу места реагује те предузима мере складу са дефинисаним процедурама. Сагласни смо са ставом да приватно обезбеђење може имати значајну улогу у заштити КИ, а то су: израда безбедносних процена ризика и планова деловања; превенција и смањење ризика; рано упозоравање и мобилизација; садејство са другим органима на предузимању мера заштите КИ; отклањање штета; ширење безбедносне културе и обука шире популације на заштити КИ; заштита ширих зона непосредног ризика; учешће у штабовима за ванредне ситуације; уступање сопствених средстава и људства (мобилизација) државним органима у заштити КИ након проглашења ванредних ситуација; спровођење мера личне заштите, евакуације, збрињавања, спасавања, пружања прве медицинске помоћи; асанација терена и др.[40]

---

[37] Закон о приватном обезбеђењу, *Службени гласник РС*, бр. 104/2013, 42/2015 и 87/2018.

[38] ЗоПО, чл. 4, ст. 1. Треба напоменути и да је ступањем на снагу Уредбе о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије (*Службени гласник РС*, бр. 69/2022) укинута Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите (*Службени гласник РС*, бр. 98/2016), која је донета на основу ЗоПО.

[39] ЗоПО, чл. 6, ст. 1.

[40] Љубомир Стајић, „Заштита критичне инфраструктуре и приватно обезбеђење", *Хармонизација српског и мађарског права са правом Европске уније*, (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2018, 132.

Следећи закони на које треба указати јесу Закон о одбрани[41] и Закон о Војсци Србије.[42] Наиме, чл. 7, ст. 6 ЗоКИ је предвиђено да се „заштита, чување, коришћење, контрола и надзор КИ у надлежности Министарства одбране и Војске Србије спроводи у складу са Законом о одбрани и Законом о Војсци Србије". Законом о одбрани одређују се објекти од посебног значаја за одбрану земље, чиме се уједно и врши идентификација КИ. Наиме, анализом Закона о одбрани и одлука[43] као подзаконских аката добија се детаљнији попис КИ. У том контексту, закључује се да објекати од посебног значаја за одбрану и велики технички системи од стратешког значаја, истовремено јесу и да би као такви требало да буду одређени као КИ.[44]

На крају, у контексту заштите КИ треба анализирати и релевантне одредбе Закона о информационој безбедности.[45] Иако се у овом закону појам критичне (информационе) инфраструктуре не помиње као такав препознају се информационо-комуникациони (ИКТ) системи од посебног значаја који обављају различите делатности, међу којима су и оне од општег интереса.[46] Самим тим, недвосмислено се указује на то да одређени ИКТ системи од посебног значаја представљају КИ. Овај став поткрепљен је одредбама горе наведене Стратегије развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године.

Списак законских и подзаконских прописа којима се у извесној мери регулише област КИ се не завршава са овим који су наведени на овом месту. Бројни су секторски закони у областима попут тајности података, водних ресурса, безбедности хране, просторног планирања, заштите од пожара, заштите животне средине, јавно-приватног партнерства, који, иако децидно не помињу термин КИ, обухватају специфичне сегменте КИ и регулишу њену заштиту.

---

[41] Закон о одбрани, *Службени гласник РС*, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015 и 36/2018.

[42] Закон о Војсци Србије, *Службени гласник РС*, бр. 116/2007, 88/2009, 101/2010 – др. закон, 10/2015, 88/2015 – одлука УС, 36/2018, 94/2019 и 74/2021 – одлука УС.

[43] Одлука о објектима од посебног значаја за одбрану, *Службени гласник РС*, бр. 112/2008 и Одлука о одређивању великих техничких система од значаја за одбрану, *Службени гласник РС*, бр. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019, 67/2021, 62/2022 и 71/2023.

[44] Вид. Ј. Марковић, 2025, 185.

[45] Закон о информационој безбедности, *Службени гласник РС*, бр. 6/2016, 94/2017 и 77/2019.

[46] Термин „ИКТ системи од посебног значаја" задржан је и у новом Предлогу Закона о информационој безбедности који је усвојила Влада средином 2025. године. При томе, прави се само разлика између „приоритетних" и „важних" ИКТ система. Вид. чл. 5 и 6 Predloga Zakona o informacionoj bezbednosti – Tekst propisa, https://www.paragraf.rs/dnevne-vesti/040325/040325-vest12.html, 10. октобар 2025.

3.1. Закон о критичној инфраструктури

Први закон у Србији којим је регулисан систем заштите КИ јесте ЗоКИ. Ступио је на снагу 21. новембра 2018. године. Овим законом успостављен је правни оквир за дефинисање, идентификацију, одређивање и заштиту како националне, тако и европске КИ.[47] У складу са ЗоКИ, 2022. године донета је Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије (у даљем тексту: Уредба).[48]

ЗоКИ критична инфраструктура одређена је као скуп „система, мрежа, објеката или њихових делова, 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.“[49] Из наведене дефиниције разликују се два елемента „инфраструктура“ и „критично“. Први елемент обухвата системе, мреже, објекте и њихове делове, односно физичку инфраструктуру, али и робе и услуге које су од значаја за функционисање државе. Други елемент односи се на кључну, виталну и суштинску инфраструктуру која омогућава остваривање националне безбедности, здравља и живота људи, заштиту имовине, животне средине, безбедност грађана, економску стабилност, односно функционисање државе.[50]

Заштита КИ обухвата „скуп активности и мера које имају за циљ осигурање функционисања КИ у случају ометања или уништења, односно заштиту у случају претњи и спречавање настанка последице ометања или уништења.“[51] Поред МУП-а, активности од значаја за заштиту КИ спроводе и министарства задужена за секторе КИ, оператори КИ, као и Републички штаб за ванредне ситуације.

Како је предуслов заштите КИ идентификација и одређивање њених елемената, намеће се као незаобилазно давање одговора на питање шта је то што се штити, односно шта је то што чини КИ. Уредбом су прописани критеријуми идентификације и то у односу на процену последица које могу

---

[47] Одредбе ЗоКИ које се односе на европску КИ почињу да се примењују даном приступања Републике Србије ЕУ. ЗоКИ, чл. 24.

[48] Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије, *Службени гласник РС*, бр. 69/2022.

[49] ЗоКИ, чл. 4, ст. 1.

[50] Љубомир Стајић, Владан Мирковић, Ненад Радивојевић, „Безбедносни менаџмент у области заштите критичне инфраструктуре у Републици Србији – стање и перспективе“, *Зборник радова Правног факултета у Новом Саду* 3/2020, 956 и Ј. Марковић, 2025, 180.

[51] ЗоКИ, чл. 2, ст. 1, тач. 4.

да наступе услед ометања или уништења КИ, као и на основу последица које могу да наступе у случају претњи по КИ.[52] Уз то, критеријуми, односно последице одређене су за сваки сектор КИ, а уважавајући специфичности појединачних сектора. Реч је о секторима енергетике, саобраћаја, снабдевања водом и храном, здравства, финансија, телекомуникационих и информационих технологија, заштите животне средине и функционисања државних органа.[53] Сектори КИ у Србији у великој мери се поклапају са онима у земљама региона. Анализа доступних правних аката земаља у региону показује да све државе препознају седам кључних сектора: енергетику, транспорт, водоснабдевање, снабдевање храном, здравство, финансије и информационо-комуникационе технологије.[54]

Министарства надлежна за поједине секторе КИ имају обавезу да предложе објекте КИ у свом домену, док коначну одлуку о одређивању КИ доноси Влада. Према ЗоКИ, министарства су у року од шест месеци од доношења Уредбе била дужна да МУП-у доставе предлоге, редовно извештавају о променама, те доставе предлоге измена и допуна КИ, док је Влада дужна да ажурира акте о одређивању сваке године, најкасније до 31. децембра.[55] Иако је требало акте донети још почетком 2023. године, није познато да ли је то заиста и учињено, нити да ли су у министарствима одређена лица одговорна за ова питања. Такође, недостају подаци о томе и да ли су правна лица идентификовала и пријавила објекте КИ под својом управом.

Према ЗоКИ, МУП је надлежан за уређивање, планирање, координацију, контролу и комуникацију у области КИ.[56] Изузетак су, као што смо раније навели, објекти од посебног значаја за одбрану, који су под ингеренцијом Министарства одбране и Војске Србије, у складу са Законом о одбрани и Законом о Војсци Србије. ЗоКИ је предвидео да се у року од 30 дана од његовог ступања на снагу измени акт о унутрашњој организацији МУП-а[57], али информације о томе да ли је то учињено нису доступне јавности. Отвара се и питање да ли МУП тренутно располаже капацитетима за ефикасно спровођење надлежности у овој области. Нејасно је и да ли ће бити формирана посебна организациона јединица за КИ, или ће те послове преузети постојећи Сектор за ванредне ситуације. Ово је нарочито значајно ако се узме у обзир да је МУП надлежан да врши надзор над применом ЗоКИ, као и прописа донетих на основу њега.[58]

---

[52] Уредба, чл. 2, ст. 1.

[53] Уредба, чл. 4, ст. 2.

[54] Јана Марковић, „Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије“, *Безбедност* 2/2023, 197-214.

[55] ЗоКИ, чл. 7, ст. 2-4, ст. 7.

[56] ЗоКИ, чл. 4, ст. 2.

[57] ЗоКИ, чл. 23.

[58] ЗоКИ, чл. 18, ст. 1.

У складу са садашњом регулативом, МУП делује као субјекат задужен за координацију у систему заштите КИ на оперативном нивоу. На нижим, оперативно-извршним нивоима, заштитом се баве други субјекти националне безбедности, надлежне агенције и друга тела формирана за конкретне секторе КИ. Непосредну заштиту спроводе полиција, штабови за ванредне ситуације (у случајевима проглашења ванредних ситуација), здравствене установе, ватрогасно-спасилачке јединице, као и службе физичког и техничког обезбеђења, односно приватни сектор безбедности са сопственим капацитетима.[59]

У контексту улоге МУП-а у заштити КИ осврнућемо се и на одредбе Нацрта Закона о критичној инфраструктури (у даљем тексту: Нацрт)[60] из 2018. године. Највећа новина и значајан предлог, који је из неког разлога изостављен у коначној верзији закона који је усвојен нешто касније, у новембру исте године, било је формирање Центра за координацију и заштиту КИ, као посебне организационе јединице у МУП-у. Центар је требало да регулише, планира, координира, контролише, комуницира и даје информације у вези са КИ,[61] што је било позитивно решење узимајући у обзир значај КИ. Међутим, све одредбе Нацрта које су Центру давале извесне обавезе и овлашћења у усвојеној верзији ЗоКИ су изостале, тако да је улога са Центра пребачена на сам МУП.

Једна од кључних активности на плану заштите КИ јесте израда безбедносних процена и планова заштите. ЗоКИ предвиђа да сваки оператор изради Безбедносни план за управљање ризиком,[62] документ којим се утврђују мере смањења ризика, дефинишу одговорности и одређују дужности, као и успоставља оквир за поступање у циљу отклањања или смањења последица безбедносних претњи идентификованих у анализи ризика, која је саставни део плана.[63] Међутим, нису прописане конкретне мере смањења ризика нити је дат оквир за њихово дефинисање, па се препушта сваком оператору да их самостално утврди на основу идентификованих ризика. Овакво законско

[59] Ј. Марковић, 2025, 182.

[60] Nacrt Zakona o kritičnoj infrastrukturi – Tekst propisa, https://www.paragraf.rs/dnevne-vesti/270418/270418-vest18.html.

[61] Nacrt Zakona o kritičnoj infrastrukturi – Tekst propisa, чл. 4.

[62] Занимљиво је напоменути да је Нацртом ЗоКИ било предвиђено да оператори израђују „безбедносно-оперативни план“, да би у усвојеној верзији ЗоКИ био прихваћен назив „безбедносни план“. Иако је наведена промена терминолошка, поставља се питање оправданости јер планови могу бити (према хијерархији) стратегијски, оперативни и тактички. Међутим, како оператори заузимају оперативни ниво деловања заједно са надлежним министарствима, онда је дефинисање плана као безбедносног оправдано, јер с обзиром на то да се спроводи од стране оперативних субјеката онда би било и сувишно одређивати га као безбедносно-оперативни.

[63] ЗоКИ, чл. 8, ст. 1.

решење доводи до тога да су начини заштите у потпуности препуштени различитим тумачењима и праксама самих оператора.

Такође, иако је било предвиђено да министар унутрашњих послова донесе методологију за израду и садржај Безбедносног плана,[64] седам година након ступања ЗоКИ на снагу, та методологија још увек није усвојена. Теоријски посматрано, анализа и процена ризика су фазе које претходе усвајању плана, а које законодавац није препознао.[65] Постоје теоријска становишта, према којима се предлаже раздвајање процене ризика[66] и Безбедносног плана у два одвојена акта. Поједини аутори наводе три разлога за то: 1. Процена ризика, која садржи идентификоване ризике, њихову вероватноћу и последице, треба да добије сагласност пре израде самог плана; 2. Израда процене ризика захтева посебну методологију која би била јединствена и заједничка за оператере у сваком сектору, сличну оној која се користи у области смањења ризика од катастрофа; и 3. Процена ризика треба да се врши хијерархијски – прво на националном, затим секторском, па тек на нивоу појединачног оператора – што додатно указује да она треба да буде засебан документ.[67] У досадашњој пракси су уочени одређени недостаци и недоумице који могу представљати изазов за ефикасност система заштите КИ, пре свега у вези са израдом релевантних докумената. Они су се у основи сводили на неусаглашеност процена, планова и мера заштите, недостатак контроле њиховог доношења и примене. Лица која исте одређују немају исто образовање нити су едуковани за ову врсту посла, немају иста и довољно функционална средства нити су сви финансијски опскрбљени за тај посао.[68]

---

[64] *Ibid*, чл. 8, ст. 3.

[65] Љубомир Стајић, „Безбедносни и правни аспекти заштите критичне енергетске инфраструктуре у Републици Србији“, *Хармонизација српског и мађарског права са правом Европске уније,* (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2022, 51.

[66] Процена ризика се може схватити двојако, као процес који обухата анализу, оцену и третман ризика, или као акт који се израђује попут безбедносних планова и процедура и који им претходи. Тренутно, у области заштите КИ, израђују се две процене ризика, и то: „процена ризика у заштити лица, имовине и пословања“ према ЗоПО и „процена ризика од катастрофа“ према ЗоСРиУВС. Исти закони предвиђају и израду „плана обезбеђења“ и „план заштите и спасавања“ Вид. Nenad Radivojević, „Uloga privatnog obezbeđenja u upravljanju rizicima od katastrofa”, *Pravni i bezbednosni aspekti upravljanja rizicima od prirodnih i antropogenih katastrofa*, (ур. Владимир М. Цветковић), Beograd 2022, 117-118. Тим поводом, можемо поставити два питања: Зашто је у ЗоКИ изостала било каква процена ризика на основу које би следила израда и доношење безбедносног плана? Зашто се, бар када је реч о КИ, због њене специфичности, није покренуло питање постојања једне процене ризика која ће испунити све захтеве који проистичу како из ЗоПО, тако и из ЗоСРиУВС, а опет и уважити специфичности и захтеве заштите КИ? Поставља се и питање да ли постојеће решење намеће операторима КИ обавезу израде појединих дуплих аката (планова заштите и спасавања у складу са ЗоСРиУВС и безбедносног плана у складу са ЗоКИ)? Наведено решење би додатно оптеретило како операторе КИ приликом њихове израде тако и МУП који треба да их одобри.

[67] Љ. Стајић, В. Мирковић, Н. Радивојевић, 2020, 961.

[68] Љ. Стајић, 2018, 127.

Наведени проблеми би требало да буду отклоњени применом ЗоКИ у делу који уређује издавање лиценци официрима за везу. Наиме, у складу са прописима ЕУ, ЗоКИ предвиђа увођење улоге официра за везу – лица које делује као посредник између оператора КИ и МУП-а, што је позитивна новина. Његов задатак је да врши сталну контролу ризика и претњи, обавештава о променама и евалуацијама ризика, координира Безбедносним планом, спроводи тестирања кроз вежбе и друге активности у вези са КИ,[69] што његову улогу чини и реактивном и превентивном. Лиценца за официра за везу издаје се лицу које има високо образовање и положен посебан стручни испит.[70] Полагање посебног стручног испита организује и спроводи МУП, а начин и програм полагања посебног стручног испита прописује министар унутрашњих послова.[71] Међутим, предметни правилник још увек није донет.

Оно што можемо видети из претходно наведеног јесте да опис послова официра за везу одговара опису послова приватног обезбеђења, па је за очекивати да ће овај посао обављати неко са знањем и образовањем у области безбедности и права.[72] Оно што је позитивно у ЗоКИ јесте то да се истиче значај интеграције КИ у просторне, безбедносне и планове за ванредне ситуације, с нагласком на превентивне мере и приоритетно деловање у кризама,[73] чиме се подстиче проактиван приступ заштити.

4. ЗАКЉУЧАК

Упркос усвајању ЗоКИ, као и напорима да се унапреди систем заштите КИ, рекло би се да можемо да потврдимо став да усвојени позитивноправни оквир не даје довољно основа ни упутстава за организовање и функционисање интегрисаног „система (јавне и приватне) безбедности који би омогућио ефикасну и ефективну заштиту КИ.“[74] Иако је усвојен системски закон, КИ се и даље одређује на бројним местима кроз друге законске и подзаконске акте. Анализом је утврђено да је управо у тим документима идентификована КИ. Остаје нада да ће министарства надлежна за одређене области приликом

---

[69] ЗоКИ, чл. 9 ст. 1.

[70] Узимајући у обзир значај КИ као и улогу официра за везу, требало би размислити о прописивању додатног услова за стицање лиценце, а то је непостојање безбедносних сметњи и обавезне безбедносно-оперативне провере.

[71] ЗоКИ, чл. 9, ст. 4-7.

[72] Љ. Стајић, 2022, 51.

[73] ЗоКИ, чл. 10.

[74] Љубомир Стајић, „Јавно-приватно партнерство у систему безбедности у Стратегији националне безбедности Републике Србије“, *Хармонизација српског и мађарског права са правом Европске уније: тематски зборник* (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2020, 70.

спровођења поступка идентификације КИ имати у виду претходно идентификоване објекте, системе и мреже одређене секторским прописима. То ће нужно захтевати висок степен сарадње и размене информација између истих.

Како је већ наведено, Влада је тек јуна 2022. године усвојила Уредбу о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије. Овај документ је једини подзаконски акт усвојен као испуњење обавеза које проистичу из ЗоКИ до данас. МУП, односно надлежни министар, још увек није донео два предметна правилника којима се уређују методологија, начин израде и садржај безбедносног плана оператора за управљање ризиком, као и начин и програм за полагање посебног стручног испита за добијање лиценце за официра за везу. То имплицира да за седам година од усвајања ЗоКИ, није урађено пуно. Нису извршени идентификација и одређивање КИ по секторима (па самим тим нису одређени ни оператори КИ), нису одређени официр за везу у сваком оператору (пошто нико још није ни добио лиценцу), нису усвојени безбедносни планови оператора за управљање ризиком, а није јасно ни како се врши надзор над применом ЗоКИ када све претходно наведено није реализовано. На овај начин стиче се утисак да је ЗоКИ донет из чисто формалних разлога у виду испуњавања услова на плану придруживања ЕУ, а не ради свеобухватног и системског регулисања заштите КИ.

Републици Србији недостаје стратегија из области заштите КИ, као и ЗоКИ уређена процена ризика која ће да обухвати утврђивање и анализу потенцијалних релевантних претњи, рањивости и опасности које би могле довести до инцидента, те процену могућег губитка или поремећаја изазваних тим инцидентом. Најадекватније решење било би доношење јединствене процене која ће поред специфичности појединих КИ обухватити и све сегменте процене ризика у заштити лица, имовине и пословања према ЗоПО и процене ризика од катастрофа према ЗоСРиУВС. Поред одређења објеката који испуњавају критеријуме КИ, корисно би било и на националном нивоу утврдити субјекате/ентитете који су зависни од КИ, те донети мере за јачање њихове отпорности. Посебно издвајамо неопходност формирања организационе јединице у оквиру МУП-а, регулисање њеног делокруга рада и надлежности, као и њено кадровско и материјално оснаживање у циљу ефикасног спровођења додељене улоге у систему заштите КИ, а посебно надзорне. Издваја се и разматрање могућности уређења питања непостојања безбедносних сметњи и безбедносно-оперативне провере као услова за стицање лиценци официра за везу. На тај начин, проактивно се предузимају мере заштите од угрожавања КИ изнутра. С обзиром на новине које проистичу из Директиве 2022/2557, као и то да Република Србија тежи европским интеграцијама, за очекивати је да ће бити и предузете активности на усаглашавању са истом. Након тога требало би приступити измени и допуни или

усвајању новог ЗоКИ, као и усаглашавању одредаба ЗоКИ са осталим релевантним законима, тако да процес измена и допуна буде транспарентан, уз јавну расправу, као и уважавање изнетих критика од стране научне и стручне јавности. Након тога требало би приступити и усвајању пратећих подзаконских аката у законским роковима.

ЛИСТА РЕФЕРЕНЦИ

Vladimir Ninković, „Critical Infrastructure Resilience – National Approches in the United States of America, the United Kingdom and Australia“, *Зборник радова Правног факултета у Новом Саду* 4/2021.

Zoran Keković, Vladimir Ninković, „Towards a Conceptualization od Resilience in Security Studies“, *Српска политичка мисао* 1/2020.

Зоран Кековић, Владимир Нинковић, *Заштита критичне инфраструктуре – системски приступ*, Центар за анализу ризика и управљање кризама, Београд 2025.

Јана Марковић, „Улога корпоративне безбедности у заштити критичне инфраструктуре Републике Србије“, *Безбедност* 2/2023.

Јана Марковић, *Корпоративна безбедност као елемент система националне безбедности у заштити критичне инфраструктуре Републике Србије* – докторска дисертација, Факултет безбедности, Београд 2025.

Љубомир Стајић, Ненад Радивојевић, Владан Мирковић, „Неки аспекти политике унутрашње безбедности као елемента Стратегије националне безбедности Републике Србије“, *Зборник радова Правног факултета у Новом Саду* 4/2017.

Љубомир Стајић, „Заштита критичне инфраструктуре и приватно обезбеђење“ *Хармонизација српског и мађарског права са правом Европске уније,* (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2018.

Љубомир Стајић, „Јавно-приватно партнерство у систему безбедности у Стратегији националне безбедности Републике Србије“, (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2020.

Љубомир Стајић, Владан Мирковић, Ненад Радивојевић, „Безбедносни менаџмент у области заштите критичне инфраструктуре у Републици Србији – стање и перспективе“, *Зборник радова Правног факултета у Новом Саду* 3/2020.

Љубомир Стајић, „Безбедносни и правни аспекти заштите критичне енергетске инфраструктуре у Републици Србији“, (ур. Т. Бугарски, С. Орловић, Г. Дракић, Б. Тубић), Нови Сад 2022, 37-56.

Mark De Bruijne, and Michelvan Eeten, „Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment“, *Journal of contingencies and crisis management* 1/2007.

Ненад Радивојевић, *Јавно-приватно партнерство у области јавне безбедности у развијеним земљама са посебним освртом на Републику Србију*, докторска дисертација, Правни факултет у Новом Саду, Нови Сад 2019.

Nenad Radivojević, „Uloga privatnog obezbeđenja u upravljanju rizicima od katastrofa", *Pravni i bezbednosni aspekti upravljanja rizicima od prirodnih i antropogenih katastrofa*, (ур. Владимир М. Цветковић), Beograd 2022.
Robert S. Radvanovsky, and Allan McDougall, *Critical infrastructure: Homeland security and emergency preparedness*, CRC press, Boca Raton 2024.
Ted G. Lewis, *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley and Sons, New Jersey 2006.
US Army Training and Doctrine Command, *DCSINT Handbook No. 1.02 Critical Infrastructure Threats and Terrorism*, US Army Training and Doctrine Command, Fort Leavenworth 2006.
Francesco Trinchillo, „Critical infrastructures: European context and evolution of the law", *Journal of Defense Resources Management* 1/2025.
Christer, Pursiainen, Eero Kytömaa, „From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean?", *Sustainable and Resilient Infrastructure* 8/2022.

ПРАВНИ И ДРУГИ ИЗВОРИ

Council Directive, 2008/114/EC on the identification and design of European critical infrastructures and the assessment of the need to improve their protection, *Official Journal of the European Union*, L 345/75.
Council Directive, 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, L 333/164.
Закон о ванредним ситуацијама, *Службени гласник РС*, бр. 111/2009, 92/2011 и 93/2012.
Закон о тајности података, *Службени гласник РС*, бр. 104/2009.
Закон о информационој безбедности, *Службени гласник РС*, бр. 6/2016, 94/2017 и 77/2019.
Закон о одбрани, *Службени гласник РС*, бр. 116/2007, 88/2009, 88/2009, 104/2009, 10/2015 и 36/2018.
Закон о приватном обезбеђењу, *Службени гласник РС*, бр. 104/2013, 42/2015 и 87/2018.
Закон о критичној инфраструктури, *Службени гласник РС*, бр. 87/18.
Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, *Службени гласник РС*, бр. 87/18.
Predlog Zakona o informacionoj bezbednosti – Tekst propisa, https://www.paragraf.rs/dnevne-vesti/040325/040325-vest12.html.
Nacrt Zakona o kritičnoj infrastrukturi – Tekst propisa, https://www.paragraf.rs/dnevne-vesti/270418/270418-vest18.html.
Уредба о садржају и методологији за израду планова заштите и спасавања у ванредним ситуацијама, *Службени гласник РС*, бр. 8/2011.
Уредба о ближим критеријумима за одређивање обавезно обезбеђених објеката и начину вршења послова њихове заштите, *Службени гласник РС*, бр. 98/2016.

Уредба о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије, *Службени гласник* РС, бр. 69/2022;
Одлука о објектима од посебног значаја за одбрану, *Службени гласник РС*, бр. 112/2008.
Одлука о одређивању великих техничких система од значаја за одбрану, *Службени гласник РС*, бр. 41/2014, 35/2015, 86/2016, 53/2017, 26/2019, 94/2019, 67/2021, 62/2022 и 71/2023.
Одлука о одређивању субјеката од посебног значаја за заштиту и спасавање у Републици Србији, *Службени гласник РС*, бр. 69/2019.
Упутство о методологији за процену ризика и планова заштите и спасавања у ванредним ситуацијама, *Службени гласник РС*, бр. 96/2012.
Упутство о Методологији израде и садржај процене ризика од катастрофа и плана заштите и спасавања, *Службени гласник РС*, бр. 80/2019.
Методологија за израду процене угрожености од елементарних напогода и других несрећа и планова заштите и спасавања у ванредним ситуацијама, *Службени гласник РС*, бр. 18/2017.
Стратегија националне безбедности Републике Србије, *Службени гласник РС*, бр. 94/2019.
Стратегија одбране, *Службени гласник РС*, бр. 94/2019.
Стратегија развоја информационог друштва и информационе безбедности у Републици Србији од 2021. до 2026. године, *Службени гласник РС*, бр. 86/2021.
Action Plan for Chapter 24, 2015, https://eupregovori.bos.rs/progovori-pregovorima/uploaded/Akcioni%20plan%20za%20poglavlje%2024%20od%2023.%20januara%202015_1.pdf.

Nenad P. Radivojević
University o f Novi Sad
Faculty o f Law Novi Sad
N.Radivojevic@pf.uns.ac.rs
ORCID ID: 0000-0002-0630-0632

Jana M. Marković
University of Belgrade
Faculty of Security Studies
jana.markovic@fb.bg.ac.rs
ORCID ID: 0009-0003-0676-8213

Critical Infrastructure Protection in the Republic of Serbia – Current Status and Opportunities for further Development and Improvement

***Abstract**: Critical infrastructure is considered the basis of the functioning of the state and society, and is one of the key factors of security and economic development, as well as the health and social well-being of citizens. Its protection is gaining particular importance in the era of globalization and with increasing exposure to various risks – from natural disasters to terrorist and cyber attacks. The Republic of Serbia, in accordance with modern security trends and the process of rapprochement with the European Union, has taken a number of specific normative and institutional steps to regulate and improve the critical infrastructure protection system. One of these steps is the adoption of the first systemic law regulating this area in 2018 – the Law on Critical Infrastructure.*

The aim of this paper is to present the current model of critical infrastructure protection through an analysis of the strategic and legal framework of the Republic of Serbia. Special emphasis is placed on the analysis of the Law on Critical Infrastructure, its implementation in the seven-year period since its adoption, as well as the identification of advantages, shortcomings and challenges in its implementation. The paper points to the importance of cooperation between the public and private sectors, as well as the need to strengthen institutional capacities, coordination and resilience of the critical infrastructure system. Based on the analysis conducted, the authors propose possible directions for further development and improvement of both the regulatory and practical framework for the protection of critical infrastructure in the Republic of Serbia.

***Keywords**: critical infrastructure, critical infrastructure protection, Law on Critical Infrastructure, national security.*

Датум пријема рада: 18. 10. 2025.
Датум прихватања рада: 12. 11. 2025.