Оригинални научни рад 351.74/.78:355(497.11)
doi:10.5937/zrpfns54-29401

Др Љубомир С. Стајић, редовни професор
Универзитет у Новом Саду
Правни факултет у Новом Саду
Lj.Stajic@pf.uns.ac.rs

Владан М. Мирковић, асистент
Универзитет у Новом Саду
Правни факултет у Новом Саду
V.Mirkovic@pf.uns.ac.rs

Др Ненад П. Радивојевић, доцент
Универзитет у Новом Саду
Правни факултет у Новом Саду
N.Radivojevic@pf.uns.ac.rs

БЕЗБЕДНОСНИ МЕНАЏМЕНТ У ОБЛАСТИ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ – СТАЊЕ И ПЕРСПЕКТИВЕ*

Сажетак: *Појам „критична инфраструктура“ постаје део безбедносног дискурса после Хладног рата када настају први правни и политички акти који садрже овај појам. Закон о критичној инфраструктури у Републици Србији усвојен је 2018. године, а као једно од важнијих питања које је уређено Законом јесте надлежност и одговорност субјеката у систему заштите критичне инфраструктуре. Предмет нашег истраживања био је безбедносни менаџмент у области заштите критичне инфраструктуре, а као резултати спроведеног истраживања у раду су: 1. Идентификовани нивои, врсте и надлежности безбедносног менаџмента у области заштите критичне инфраструктуре; 2. Утврђен њихов међусобни однос и 3. Дате препоруке мера и решења које је потребно предузети ради успостављања интегралног система заштите у овој области.*

* Рад је настао као резултат рада на научно-истраживачком пројекту „Правна традиција и нови правни изазови“ у 2020. години, а чији је носилац Правни факултет у Новом Саду.

Кључне речи: *безбедносни менаџмент, управљање ризиком, управљање кризом, критична инфраструктура, систем заштите, оператори критичне инфраструктуре.*

1. УВОД

Међународним документима на глобалном[1] и регионалном нивоу[2] утврђена је обавеза држава да предузму мере и активности на плану стварања стабилног и безбедног друштва у коме ће грађани бити заштићени од последица нежељених догађаја изазваних природним катастрофама, људским делатностима и техничким акцидентима. Ради испуњавања наведених обавеза потребно је изградити систем заштите који ће смањити ризик од наступања нежељеног догађаја односно који ће отклонити или умањити штетне последице уколико нежељени догађај наступи. У том смислу Народна скупштина донела је Националну стратегију заштите и спасавања у ванредним ситуацијама[3] чија је сврха „заштита живота, здравља и имовине грађана, животне средине и културног наслеђа Републике Србије“, док је Законом о смањењу ризика и управљању у ванредним ситуацијама (у даљем тексту: ЗоСРиУВС)[4] успостављен институционални оквир интегралног система заштите и спасавања у ванредним ситуацијама у Републици Србији. У ЗоСРиУВС утврђена су начела система заштите, одређени нивои на којима је потребно предузети мере и активности, одређени субјекти надлежни да предузимају мере и активности на сваком нивоу, уређен међусобни однос и конкретне обавезе обвезника овог закона.

---

[1] Вид. Миленијумску декларацију ОУН у којој се као један од приоритета помиње заштита рањивих категорија, пре свега деце, али и уопште грађана односно цивила у ванредним ситуацијама изазаваних ратом, природним катастрофама и сл. United Nations Millennum Declaration, A/55/L2, General Assembly, 18 September 2000. *https://undocs.org/A/RES/55/2,* 14.8. 2020. Такође вид. Оквир за смањење ризика од катастрофа из Сендаија за период 2015-2030 усвојен на Трећој светској конференцији Организација уједињених нација која је одржана 18. марта 2015. године у Сендаију, *http://ruczrs.org/wp-content/uploads/2019/09/Okvir-za-smanjenje-rizika-od-katastrofa-iz-Sendaija-za-period-2015.-2030..pdf*, 12.8.2020.

[2] Вид. Директиву 2007/779/ЕС којом се предвиђа успостављање Механизма за цивилну заштиту као механизма за сарадњу у државама чланицама ЕУ на плану спречавања односно смањења последица у случају већих катастрофа изазваних природним, технолошким или људским фактором. *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l28003*, приступљено 20.8.2020.

[3] Национална стратегија заштите и спасавања у ванредним ситуацијама, *Службени гласник РС*, бр. 86/11.

[4] Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама – ЗоСРиУВС, *Службени гласник РС*, бр. 87/18.

У исто време усвојен је и Закон о критичној инфраструктури[5] (у даљем тексту: ЗоКИ) којим је дефинисан систем заштите критичне инфраструктуре (у даљем тексту: систем заштите КИ). Систем заштите КИ као предмет заштите има само оне објекте, системе и мреже који су од егзистенцијалне важности за друштво у смислу да њиховим оштећењем, уништењем или нефункционисањем настају штетне последице по живот и здравље грађана, националну безбедност, јавно здравље или редовно функционисање државних органа. У том смислу систем заштите КИ и систем заштите и спасавања у ванредним ситуацијама комплементарни су системи који се заснивају на готово идентичним начелима. Због тога ЗоСРиУВС у општим питањима која нису регулисана ЗоКИ може имати супсидијарну примену и карактер општег закона (*lex generalis*), док директну примену има у ситуацијама када наступи нежељени догађај и када надлежност у управљању кризом прелази на Републички штаб за ванредне ситуације (у даљем тексту: РШВС).

Систем заштите КИ у Републици Србији представља сложен систем кога чине субјекти различитог нивоа, статуса, функције и овлашћења, а који предузимају низ мера и активности у циљу заштите критичне инфраструктуре (у даљем тексту: КИ) чиме се остварују претпоставке за нормално и редовно функционисање друштва и државе. Имајући у виду велики број различитих актера који предузимају мере и спроводе активности на плану заштите КИ у Републици Србији, улога безбедносног менаџмента у систему заштите намеће се као питање од изузетне важности. Из тог разлога, предмет нашег истраживања је безбедносни менаџмент у области заштите КИ у Републици Србији.

2. КРИТИЧНА ИНФРАСТРУКТУРА И СИСТЕМ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Концепт КИ представља релативно нов концепт. Међутим, новина у овом концепту није свест о томе да је потребно заштити најважнију инфраструктуру која је *condicio sine qua non* опстанка друштва и државе. Још је у Првом додатном протоколу Женевске конвенције из 1949. године (Протокол 1)[6] била предвиђена заштита инфраструктуре која је неопходна да цивилно становништво преживи. У истом акту у делу који се односи на заштиту цивила као предмет заштите наведени су и животна средина и инсталације

[5] Закон о критичној инфраструктури – ЗоКИ, *Службени гласник РС,* бр. 87/18.

[6] Вид. чл. 53 – 56, Првог додатног протокола Женевске конвенције из 1949. године. У: Извори међународног хуманитарног права, (ур. *Весна Кнежевић-Предић, Саша Аврам и Жељко Лежаја*), Београд, 2007. *http://www.mfa.gov.rs/sr/images/stories/komisija/MKCK%20-%20Izvori%20MHP.pdf*, 14.8.2020.

које садрже опасне силе (бране, насипи, нуклеарни објекти и сл.), а чијим би оштећењем или уништењем били проузроковани велики цивилни губици. У том смислу новина у концепту КИ јесте свест о потреби за јединственим приступом у заштити целокупне КИ која се остварује деловањем интегрисаног система заштите. Терористички напади у Њујорку (2001), Вашингтону (2001), Мадриду (2004), Лондону (2005) и другим европским и светским градовима само су учврстили идеју о стварању интегрисаног система заштите због чега је и појам КИ постао заступљенији у јавном дискурсу.

Први корак у успостављању јединственог система заштите КИ представља дефинисање појма КИ. Значење именице „инфраструктура“[7] указује да је реч о материјалној основни која је претпоставка обављања функција државе или организације, а придев „критична“ ближе одређује материјалну основу као виталну, суштинску односно од егзистенцијалне важности за обављање најважнијих функција државе односно организације. Анализа политичких[8], правних[9], стручних[10] и теоријских[11] одређења КИ потврдила

---

[7] Вид. Речник српског језика, Матица српска, Нови Сад, 2011, стр. 462 или Longman Dictionary of Contemporary English 5th Edition.

[8] Вид. на пример: Austrian Cyber Security Strategy, Federal Chancellery of the Republic of Austria, Vienna, 2013, p. 20.; *https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf*, 12.8.2020. An Emergency Management Framework for Canada – Third Edition, Emergency Management Policy and Outreach Directorate, May 2017, p. 21.; *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx*, 12.8.2020. Presidential Police Directive – Critical Infrastructures Security and Resilience, The White House, February 12 2013. *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil,* 12.8.2020.; National Strategy for Critical Infrastructure Protestion (CIP Strategy), Federal Ministry of the Interior, Berlin, 17th June 2009, p. 4. *https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile*, 12.8.2020.

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

[10] Вид. Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018, p. 19. *https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf*, 12.8.2020. или Protection of Critical Infrastructures – Baseline Protection Concept, Federal Ministry of the Interior, *www.bmi.bund.de,* 12.8.2020.; Nicolas Castellon and Erik Frinking, Securing Critical Infrastructures in the Netherlands – Towards a National Testbed, The Hague Security Delta, 2015. https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf, 12.8.2020.

[11] Вид. Давор Милошевић, „Противтерористичка заштита енергетских постројења”, *Војно дело* 6/2018, 363-382; Danijela Protić, “Critical Infrastructures: Threats, Vulnerabilities and Protection”, *Military Technical Courier*, 2016., Vol 64, No 3, 812-837; Мирко Шкеро, Владимир Атељевић, „Заштита критичне инфраструктуре и основни елементи усклађивања са Директивом Савета Европе 2008/114/ES”, *Војно дело* 3/2015, 192-207; Марија Мићовић, Безбедносни

је да су основни елементи за дефинисање критичне инфраструктуре управо материјална основа (путеви, железнице, постројења, техничко – технолошки системи и средства и сл.) и инструментални карактер такве основе у смислу да се њеним постојањем или нормалним функционисањем доприноси задовољењу потреба друштва, државе и појединца. Решење прихваћено у ЗоКИ у складу је са резултатима наведене анализе и према њему критичну инфраструктуру чине „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“[12].

Следећи корак у успостављању јединственог система заштите јесте одређивање сектора у којима постоји инфраструктура која има критични значај. Одређивање критичних сектора увек је повезано са функцијама које неко друштво сматра условом опстанка и нормалног живота. Историјско – компаративним методом утврђено је да се временом ширио број кључних функција[13], па се према томе ширио и круг сектора[14]. Овом ширењу функција допринели су политички процеси који су вредности појединца и његове потребе истакли у први план државних приоритета, али и развој технологије која је данас претпоставка редовног функционисања свих појединачних сектора, због чега се говори о критичној информационој инфраструктури[15], као посебном сегменту заштите у систему заштите целокупне КИ.

аспекти функционисања критичне инфраструктуре у ванредним ситуацијама – докторска дисертација, Факултет безбедности, Београд 2016, 31.

[12] ЗоКИ, чл. 4. ст. 1.

[13] У САД је председничка директива из 1996. године третирала критичну инфраструктуру кроз призму утицаја на економску и одбрамбену моћ, да би након терористичких напада 2001. године критичну инфраструктуру чинили објекти, системи и мреже које доприносе националној безбедности, економској безбедности, јавном здрављу и безбедности. Упор. Critical Infrastructures: What Makes Infrastructure Critical? Report for Congress, Congressional Research Service, The Library of Congress, updated January 29, 2003. и National Infrastructures Protection Plan, Department for Homeland Security, 2019, *https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf*, 14.8.2020.

[14] Првобитно америчко решење садржало је 8 сектора, да би касније било 13 и на крају 16 сектора критичне инфраструктуре. Види претходни извор. У теоријским радовима у Републици Србији у којој до 2018. године није било закона у овој области као сектори критичне инфраструктуре идентификовани су енергетски сектор, телекомуникације, банкарство, транспорт, водоснабдевање, хитне службе и сл. Вид. Давор Милошевић, „Противтерористичка заштита енергетских постројења”, *Војно дело* 6/2018, 365-366. или рад у коме је идентификовано 6 сектора критичне инфраструктуре Danijela Protić, “Critical Infrastructures: Threats, Vulnerabilities and Protection”, *Military Technical Courier*, 3/2016.

[15] Идентификовање посебне важности информационих технологија као критичне информационе инфраструктуре као основе за целокупну критичну инфраструктуру присутно је у Стратегији развоја информационе безбедности у Републици Србији за период од 2017.

„Анализом сектора у којима се врши идентификација КИ у Републици Србији, можемо видети да је одређивање КИ код нас у значајној мери хармонизовано са решењима других држава. Међутим, оно што до сада није размотрено јесте степеновање елемената КИ јер, објективно гледано, нису сви елементи истог значаја. То би значило да би заштита појединих елемената морала да се одвија према степену њиховог значаја (1, 2, 3 степен). Даље то значи да треба одредити и критеријуме за степеновање елемената КИ што ни у једном документу (правном, безбедносном или другом) није учињено.“[16] У Холандији[17] постоји подела на А и Б категорије сектора КИ, при чему је на пример категорија А дистрибуција електричне енергије на националном нивоу, производња нафте и гаса, складиштење нуклеарних материја и сл., а категорија Б дистрибуција електричне енергије на регионалном нивоу, финансијски сектор, државни органи који рад заснивају на доступности и поузданости информационих система. Формално истицање значаја одређених сектора, али без категоризације на више и ниже секторе, присутно је и у Директиви 2008/114 Европског савета која је донета ради предузимања мера и активности у енергетском сектору и у области саобраћаја на нивоу ЕУ, док је председничком директивом у САД[18], којом је формулисана политика у области заштите КИ у САД, истакнут значај истих сектора (енергетика и саобраћај).

Трећи корак у успостављању јединственог система заштите јесте одређивање места, улоге, обавеза и међусобног односа свих субјеката који чине система заштите КИ и прописивање планова и процедура по којима поступају. Одговорност за уређивање, организовање, координацију, надзор и контролу система заштите КИ има неколико субјеката са управљачким овлашћењима који чине безбедносни менаџмент у овој области. Четврти корак подразумева поступак идентификације и одређивања конкретних система,

---

до 2020. године (*Службени ӣласник РС,* бр. 53/17) и у Закону о информационој безбедности (*Службени ӣласник РС*, бр. 6/2016, 94/2017 77/2019). У другим државама такође је истакнут значај информационих технологија у овој области. Види: Austrian Cyber Security Strategy, Federal Chancellery of the Republic of Austria, Vienna, 2013, 20.; Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018; An Emergency Management Framework for Canada – Third Edition, Emergency Management Policy and Outreach Directorate, May 2017, 21.

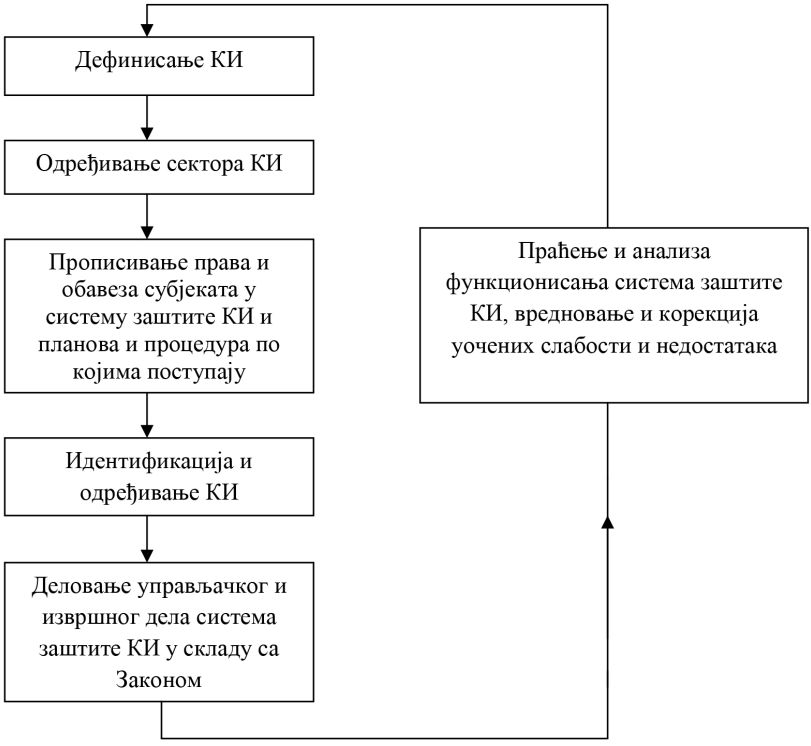
[16] Љубомир Стајић, „Заштита критичне инфраструктуре и приватно обезбеђење”, У *Хармонизација срӣској и мађарској ӣрава са ӣравом Европске уније*, (ур. Љубомир Стајић), Правни факултет у Новом Саду, Нови Сад, 2018, 124-125.

[17] Вид. Nicolas Castellon and Erik Frinking, Securing Critical Infrastructures in the Netherlands – Towards a National Testbed, The Hague Security Delta, 2015, 9.

[18] Вид. Presidential Police Directive – Critical Infrastructures Security and Resilience, The White House, February 12, 2013. *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*, 12.8.2020.

објеката и мрежа као КИ из чега следе обавезе за операторе тако одређених система, мрежа и објеката. Пети корак подразумева предузимање конкретних мера и активности на плану смањења ризика односно отклањања штетних последица у складу са претходно дефинисаним улогама у систему заштите. На крају, последњи корак подразумева континуирано праћење и анализу функционисања система заштите КИ, вредновање резултата и евентуално отклањање уочених недостатака.

Шема 1. Поступак организовања и функционисања система заштите КИ



3. БЕЗБЕДНОСНИ МЕНАЏМЕНТ У ОБЛАСТИ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

3.1. Управљачки део система заштите КИ

У сложеном систему заштите КИ разликује се управљачки и извршни део система. Управљачки део чине они субјекти који су овлашћени да планирају, уређују, организују, координирају и врше надзор и контролу над

извршним делом система заштите КИ, док извршни део чине они субјекти који су дужни да предузимају мере и активности на плану смањења ризика односно спречавања и/или отклањања штетних последица. Субјеката са управљачким функцијама има више и они представљају безбедносни менаџмент у овој области. Стратегијски ниво менаџмента чине Народна скупштина и Влада. Народна скупштина донела је Националну стратегију заштите и спасавања у ванредним ситуацијама као политички и стратешки оквир за деловање на плану смањења ризика и управљања у ванредним ситуацијама, као и ЗоКИ и ЗоСРиУВС којима су дефинисани правни и институционални оквири система заштите КИ и система заштите и спасавања у ванредним ситуацијама.

ЗоКИ дефинише КИ (чл. 4), прописује поступак идентификације и одређивања КИ (чл. 5 – 7), субјекте који учествују у наведеним поступцима и њихова овлашћења и дужности, идентификује основне принципе организовања и функционисања система заштите КИ (чл. 3) и др. ЗоСРиУВС је комплементаран правни акт у области заштите КИ, због чега решења из ЗоСРиУВС могу бити модел приликом предузимања мера у области заштите КИ. Поред тога, ЗоСРиУВС има директну примену у области заштите КИ у оном делу[19] који уређује питање надлежности РШВС чија надлежност се успоставља у случају наступања угрожавања, ометања рада или уништења КИ. Влада прописује критеријуме за идентификовање КИ, одлучује о предлозима нових сектора КИ који нису предвиђени ЗоКИ и одлуком одређује КИ.

Координирајући ниво менаџмента чини МУП који уређује, планира, координира, контролише активности, комуницира и даје информације у вези са КИ[20] и РШВС који предузима мере на отклањању или смањивању штетних последица нежељеног догађаја. Министарства надлежна за секторе КИ чине оперативни део менаџмента који, по унапред прописаним критеријумима, спроводе поступак идентификације КИ и достављају предлоге измена и допуна КИ у својим секторима најкасније до 31. октобра сваке године.

3.2. Безбедносни менаџмент оператора КИ

Извршни део система заштите КИ чине оператори КИ чији безбедносни менаџмент је дужан да изради Безбедносни план за управљање ризиком[21] (у даљем тексту: Безбедносни план) и да га поднесе на сагласност МУП-у. Безбедносни план садржи мере смањења ризика, дефинише одговорност и

[19] ЗоКИ, чл. 11.
[20] ЗоКИ, чл. 4, ст. 2.
[21] ЗоКИ, чл. 8.

одређује дужности, те успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи дефинисаних у анализи ризика, која је саставни део плана. Овде би требало размислити о томе да процена ризика и Безбедносни план буду два одвојена аката и за то постоји више разлога. Прво, процена ризика је акт који садржи потенцијалне облике угрожавања КИ, опис њиховог садржаја, вероватноћу наступања, последице које би настале, где се могу јавити и које су слабе тачке система, индикаторе и сл. У том смислу процена ризика је акт који претходи Безбедносном плану и на основу кога се безбедносне процедуре које су саставни део плана израђују. Сагласност МУП-а на процену ризика била би основа за израду адекватног и квалитетног Безбедносног плана.

Друго, процена ризика има фундаментални значај за израду адекватног система заштите КИ, па је због тога на стратегијском нивоу потребно прописати методологију израде процене ризика која би била јединствена и заједничка за операторе у сваком сектору, што би омогућило боље уочавање проблема и размену информација између оператора и оператора и управљачког дела система заштите КИ. Методологија у области заштите од катастрофа може послужити као основа и пример за методологију израде процене ризика и планова у области заштите критичне инфраструктуре. Треће, имајући у виду значај система заштите КИ и ниво одговорности оператора КИ требало би донети процену ризика за КИ на националном нивоу, затим на секторском нивоу и тек на крају на нивоу појединачног оператора КИ. У том смислу процени ризика било би дато место које акт такве врсте има у систему заштите КИ у упоредним решењима[22], у нашем систему смањења ризика и управљања у ванредним ситуацијама и у нашим решењима поводом неких других питања као што је борба против прања новца и финансирања тероризма[23].

Процена ризика на нивоу оператора КИ требало би да обухвати:

1. Анализу пословног, безбедносног, правног, економског и социјалног окружења у коме функционише оператер КИ;
2. Анализу секторске и међусекторске зависности са посебним освртом на последице секторске и међусекторску зависност КИ у сектору енергије, информационих технологија и саобраћајне инфраструктуре;
3. Анализу могуће секторске и међусекторске сарадње у управљању ризиком и управљању кризом;

---

[22] Вид. примере Уједињеног Краљевства, Канаде, САД и др. у Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018.

[23] Вид. Закон о спречавању прања новца и финансирања тероризма, *Службени ɪласник РС,* бр. 113/17.

4. Анализу постојеће инфраструктуре са идентификованим слабостима и могућим алтернативним решењима у случају наступања уништења или оштећења (на пример мостова или саобраћајница и сл.);
5. Анализу извора и облика угрожавања са посебним освртом на намерне и ненамерне акциденте; угрожавање у физичком и виртуелном простору; појединачне или серијске нападе; спољне или унутрашње облике угрожавања; облике угрожавања у једном сектору и оне који су део напада на друге секторе и др.

На основу извршене процене на нивоу оператора КИ потребно је израдити Безбедносни план који треба да садржи мере које треба предузети (административне, организационе, правне, техничке, санитарне и сл.) ради смањења ризика односно смањења последица уколико штетни догађај наступи, дефинисати одговорност у систему заштите оператора КИ и израдити безбедносне процедуре као прописане стандарде поступања у свакој ситуацији која је у процени ризика идентификована као угрожавајућа. Иако Закон то не предвиђа, Безбедносни план могао би да садржи и листу индикатора односно показатеља да непосредна опасност по штићени систем предстоји, како би активности на организовању и функционисању система заштите биле благовремене и отклониле угрожавање односно смањиле последице у случају да штетни догађај наступи.

Законом је прописано да оператор одређује официра за везу[24] као лице које је одговорно за координацију и комуникацију оператора са МУП. Официра за везу бира МУП на предлог оператора. Официр за везу је лице које служи као контакт између оператора и МУП-а, које обезбеђује сталну контролу ризика и претњи, обавештава о променама у односу на критичну инфраструктуру, обавештава МУП о евалуацији ризика, претњи и рањивости, координира Безбедносним планом, врши тестирања кроз вежбе и друге активности предвиђене планом и обавља све друге послове везане за критичну инфраструктуру.

3.3. Неки проблеми безбедносног менаџмента у систему заштите КИ

Идентификација КИ је поступак у коме министарства надлежна за секторе КИ идентификују инфраструктуру која испуњава одређене услове као критичну инфраструктуру. Да би надлежно министарство спровело поступак идентификације КИ потребно је претходно утврдити шта је инфраструктура у сваком сектору и утврдити критеријуме на основу којих надлежно министарство врши тзв. процену критичности односно идентификује одре-

[24] ЗоКИ, чл. 9.

ћену инфраструктуру као критичну. У Методологији израде и садржаја процене ризика од катастрофа и плана заштите и спасавања (у даљем тексту: Методологија) која се налази у прилогу Упутства о методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања наведено је шта обухвата инфраструктура у сваком сектору[25] КИ и то може бити полазна основа при идентификацији КИ.

Влада треба да утврди опште, секторске и међусекторске критеријуме[26] према којима би се наведена инфраструктура идентификовала и одредила као КИ. Упоредна решења не дају јединствен одговор у вези начина идентификације критеријума[27], али постоје адекватни предлози који могу послужити као основа за српско решење. Као полазна основна може послужити Директива 2008/114[28] у којој се као критеријуми наводе: број жртава (који се процењује спрам могућег броја мртвих и рањених); последице по привреду (економска вредност, последице по животну средину, степен смањења квалитета услуге или производа) и утицај на јавност (утицај на редовно задовољавање потреба, телесне патње, поверење у функционисање јавних служби). У заједничкој студији Комитета за борбу против тероризма ОУН и Интерпола[29] као критеријуми се помињу: обим територије на којој оштећење, уништење односно поремећај у обављању функција производи последице; трајање последица; озбиљност последица с обзиром на то које и колике су економске последице, број мртвих и повређених, утицај на животну средину и поверење према власти.

---

[25] Тако на пример, енергетску инфраструктуру чине: термо и хидроелектране, термоелектране – топлане и други објекти за производњу електричне енергије, као и електроенергетски водови, далеководи и трансформаторске станице; објекти за производњу електричне енергије из обновљивих извора; високе бране и акумулације напуњене водом; објекти за производњу и прераду нафте и гаса, производњу биогорива и биотечности. Саобраћајну инфраструктуру чине: друмски, железнички, ваздушни саобраћај (ауто-пут, државни путеви I и II реда; категорисани и некатегорисани путеви, мостови, тунели, надвожњаци и аутобуске станице; железничка мрежа, железничке станице; аеродроми), речни пловни путеви, луке и гранични прелази итд. Види Упутство о методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, *Службени ɪласник РС*, бр. 80/19.

[26] Упркос законском року од 6 месеци, Влада до тренутка предавања текста рада у часопис Зборник радова Правног факултета у Новом Саду није донела подзаконски акт који регулише ово питање.

[27] Вид. Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018, 44.

[28] Вид. чл. 2 Директиве Европског савета, Council Directive, 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L 345/75.

[29] Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018, 44.

У Републици Хрватској као критеријуми[30] се наводе: живот и здравље људи; трајање штетне последице односно поремећаја у раду; обим поремећаја односно колико ће производи односно услуге бити погођене; законски, регулаторни и уговорни значај; привредна односно финансијска штета. Анализом претходних решења утврђено је да општи критеријуми за одређивање КИ могу бити квантитативни, квалитативни и временски. Ове врсте критеријума Александер Фекете[31] дефинисао је и детаљније разрадио као: критичну размеру (квантитативно исказивање последица у апсолутним или релативним износима – величина територије, број жртава, износ материјалне штете и сл.), критично време (време трајања нефункционисања КИ, време потребно да се последице отклоне и сл.) и критични квалитет (одређени ниво квалитета пружене услуге, произведеног добра или поверење грађана у пружаоца услуга односно државне органе, постојање одрживих алтернативних решења и др.).

Опште критеријуме потом је потребно даље разрадити у смислу утврђивање специфичних квантитативних, квалитативних и временских критеријума за сваки сектор. Сваки критеријум има својствене показатеље, па тако квантитативни критеријуми могу бити изражени кроз број људских жртава, број објеката или елемената који су уништени, износ материјалне штете, површину територије и сл.; временски критеријуми могу се изразити у сатима, данима, недељама, месецима или годинама, док се квалитативни критеријуми могу изразити описно (на пример: висок, умерен, низак ниво или степен оштећења и сл.). Утврђивање специфичних критеријума за идентификацију КИ даље захтева њихово укрштање унутар сектора, а затим утврђивање секторске међузависности (која је нарочито присутна код енергетског сектора, саобраћаја и информационих система) и на крају њихово вредновање.

Ради лакшег и егзактнијег одређивања прага критичности, по узору на један модел бодовања поводом одређивање критичне информационе инфраструктуре[32], све показатеље у оквиру свих врста критеријума могуће је изразити одређеним бројем бодова. У табели испод дата је оријентациона дистрибуција бодова по критеријумима од 0 до 100, при чему укупан износ бодова указује на обим поремећаја у пружању услуга, задовољавању потреба и сл. уколико дође до оштећења или уништења КИ. Што је збир бодова свих

---

[30] Pravilnik o metodologiji za izradu analize rizika i poslovanja kritičnih infrastruktura, *Narodne novine* 47/2016, čl. 5.

[31] Александар Фекете запослен је у Савезној канцеларији за цивилну заштиту и помоћи при катастрофама у Немачкој. Вид. Alexander Fekete, Common Criteria for the Assessment of Critical Infrastructures, *International Journal of Disaster Risk Science,* 2011, 2 (1): 18-19.

[32] Soontai Park, Wans Yi, The Evaluation Criteria for Designation of Critical Information Infrastructure, *8th WSEAS International Conference on E-Activities and information security and privacy*, December 2009, *https://www.researchgate.net/publication/262257062*, 16.8.2020.

показатеља ближи максималном износу (100 бодова), то је значај такве инфраструктуре критичнији. На крају, потребно је одредити границу преко које инфраструктура постаје КИ. Бодовање може допринети утврђивању оптималног решења за КИ у Републици Србији јер би се инфраструктура у зависности од исказаног броја бодова могла разврстати према степену њеног значаја.

Табела 1. Дистрибуција бодова према критеријумима за одређивање КИ

Врста критеријума	**Бодови (max)**
Квантитативни критеријуми	25
Квалитативни критеријуми	25
Временски критеријуми	10
Секторска међузависност	10
Међусекторска зависност	30
Укупно:	100

По спроведеном поступку идентификовања „обједињен и дефинисан предлог система, мрежа, објеката и њихових делова идентификованих у наведеним секторима МУП подноси Влади која одређује КИ.“[33] Законом је прописано да се акт о одређивању критичне инфраструктуре ажурира сваке године, а најкасније до 31. децембра, због чега су министарства надлежна за секторе КИ дужна да редовно, а најмање једном квартално извештавају МУП о новонасталим променама у свом сектору. Одлуком о одређивању КИ одређује се шта је конкретно КИ у Републици Србији чиме настају обавезе за конкретне субјекте који се у смислу овог Закона називају оператори КИ.

Следећи важан проблем који је идентификован у току истраживања јесте неадекватност положаја, функције и састава организационе јединице МУП-а односно РШВС у систему заштите КИ. У редовним околностима организациона јединица МУП-а која по Закону треба да се организује ради вршења послова на уређивању, планирању, координацији, контроли активности, комуникацији и размени информација у вези са КИ, има кључну координирајућу улогу у систему заштите КИ. Међутим, у случају наступања угрожавања односно у случају ометања рада или уништења КИ руковођење и координација мера и послова је у надлежности РШВС у складу са ЗоСРиУВС.

Релевантна упоредна решења[34] прописују посебно тело или постојећи орган као координирајући ниво менаџмента у овој области који би требало

[33] Љ. Стајић, 124. И у том смислу види члан 5. ЗоКИ којим је прописан поступак идентификације.

[34] Вид. решење у САД, Немачкој, Француској и Уједињеном Краљевству. Поред тога преглед неких решења у Protection of Critical Infrastructures against Terrorist Attacks:

да обезбеди јединствен и интегрисан одговор на угрожавање КИ. У Аустралији постоји Поуздана мрежа за размену информација, у САД постоје координациона тела на нивоу сектора и на међусекторском нивоу, у Уједињеном Краљевству постоји Секретаријат за цивилне послове, у Канади координацију врши Национални међусекторски форум, у Шпанији постоји Национални сектор за заштиту критичне инфраструктуре и тд. Заједничка карактеристика ових тела јесте партиципација представника управљачког и извршног дела система заштите КИ у циљу бољег разумевања, размене информација, уједначавања праксе у секторима и међу секторима и сл.

Овде је реч о вишем координирајућем нивоу безбедносног менаџмента. Такву улогу према Законом о смањењу ризика и управљању у ванредним ситуацијама може да има РШВС који, као национална платформа у области смањења ризика и управљања ванредним ситуацијама, може да окупи стручњаке, научне раднике и сл. Међутим, надлежност РШВС успоставља се само изузетно, а комуникација са МУП-ом врши се поводом конкретних догађаја. Отуда би Влада требало да оснује сталну координациону групу (по узору на ону из области спречавања прања новца и финансирања тероризма[35]) која би окупила све релевантне субјекте управљачког и извршног дела система заштите, али и друга лица која могу да допринесу успешном раду, ради сталне комуникације, координације, размене искустава и проблема и сл., а која би била виши координациони ниво и у односу на МУП у редовним околностима и у односу на РШВС у ванредним ситуацијама. Тако би се обезбедила континуирана сарадња и комуникација на нивоу који може да обезбеди интеграцију јавног и приватног сектора. Такво тело, аналогно решењу у области спречавања прања новца и финансирања тероризма, могло би оснивати стручне тимове, ангажовати експерте, али и успоставити и водити регистар КИ и регистар ризика.

4. ЗАКЉУЧАК

Интегрисан и функционалан систем заштите КИ представља императив сваке државе. У том смислу у раду је извршена анализа постојећег политичког и правног оквира система заштите КИ у Републици Србији, извршена

Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018, 51-55.

[35] Вид. Одлуку о образовању Координационог тела за спречавање прања новца и финансирање тероризма, *Службени ɪласник РС*, бр. 54/18 и Одлуку о образовању Сталне координационе групе за надзор над спровођењем Националне стратегије за борбу против прања новца и финансирања тероризма, *Службени ɪласник РС*, бр. 37/15 и 90/17.

упоредна анализа неких кључних питања у вези улоге безбедносног менаџмента у овој области и утврђени предлози који би требало да допринесу успостављању интегралног и ефикасног система заштите КИ.

У Републици Србији не постоји посебна стратегија у области заштите критичне инфраструктуре која је у студији ОУН и Интерпола наведена као пример добре праксе у овој области. Међутим, постојећа Стратегија у области спасавања и управљања у ванредним ситуацијама може представљати добру основу за организовање и деловање система заштите КИ, док се не усвоји посебна стратегија или усвоји стратегија која обухвата све аспекте смањења ризика и управљања кризама. На организационом плану Влада би требало да утврди критеријуме за идентификацију КИ, образује сталну координациону групу која би била централно место координације и комуникација свих субјеката система заштите КИ, изради методологију за процену ризика и израду безбедносних планова, усвоји националну процену ризика и др.

Као важна мера на плану успостављања интегрисаног система заштите било би оснивање сталне координационе групе која би као виши координирајући ниво била задужена за: координацију послова свих субјеката у систему заштите КИ; утврђивање методологије за израду процене ризика; израду предлога националне процене ризика коју би усвајала Влада; давање препорука у вези критеријума на основу којих се врши идентификација КИ; комуникацију и размену информација између свих обвезника ЗоКИ поводом питања која се односе на заштиту КИ; утврђивање смерница за комуникацију и сарадњу МУП-а и РШВС у редовним и ванредним ситуацијама; организовање округлих столова, семинара и конференција на којима би се разговарало о позитивним решењима, слабостима и утврђивале препоруке у циљу отклањања слабости у систему заштите КИ; развијање безбедносне културе и подстицање свести о потреби интегрисаног институционалног одговора на угрожавање КИ и др.

На нижем координирајућем нивоу МУП и РШВС задржали би своје надлежности на плану координације и комуникације са обвезницима Закона ради смањења ризика односно отклањања штетних последица. На оперативном нивоу министарства надлежна за секторе КИ, поред поступка идентификације требало би да израде секторску процену ризика и прате стање у својим областима. Безбедносни менаџмент оператера КИ остао би одговоран за израду аката (одговарајућих правних аката, процене ризика, безбедносног плана и листе индикатора), одређивање официра за везу и спровођење конкретних мера и активности којима се оператор КИ штити од свих облика и носилаца угрожавања.

ЛИТЕРАТУРА И ИЗВОРИ

Alexander Fekete, Common Criteria for the Assessment of Critical Infrastructures, *International Journal of Disaster Risk Science,* 2011, 2 (1): 15–24;

Austrian Cyber Security Strategy, Federal Chancellery of the Republic of Austria, Vienna, 2013;

An Emergency Management Framework for Canada – Third Edition, Emergency Management Policy and Outreach Directorate, May 2017;

Compendium of Good Practices, Compiled by Counter – Terrorism Committee Executive Directorate (CTED) and United Nations Office of Counter – Terrorism (UNOCT) in 2018;

Critical Infrastructures: What Makes Infrastructure Critical? Report for Congress, Congressional Research Service, The Library of Congress, updated January 29, 2003;

National Infrastructures Protection Plan, Department for Homeland Security, 2019;

Давор Милошевић, Противтерористичка заштита енергетских постројења, *Војно дело* 6/2018;

Danijela Protić, Critical Infrastructures: Threats, Vulnerabilities and Protection, *Military Technical Courier*, 2016., Vol 64, No 3;

Љубомир Стајић, Заштита критичне инфраструктуре и приватно обезбеђење, У Хармонизација српског и мађарског права са правом Европске уније, (ур. *Љубомир Стајић*), Правни факултет у Новом Саду, Нови Сад, 2018.

Мирко Шкеро, Владимир Атељевић, Заштита критичне инфраструктуре и основни елементи усклађивања са Директивом Савета Европе 2008/114/ES, *Војно дело* 3/2015;

Марија Мићовић, Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама – докторска дисертација, Факултет безбедности, Београд, 2016;

Nicolas Castellon and Erik Frinking, Securing Critical Infrastructures in the Netherlands – Towards a National Testbed, The Hague Security Delta, 2015;

Soontai Park, Wans Yi, The Evaluation Criteria for Designation of Critical Information Infrastructure, *8th WSEAS International Conference on E-Activities and information security and privacy*, December 2009;

United Nations Millennum Declaration, A/55/L2, General Assembly, 18 September 2000;

Оквир за смањење ризика од катастрофа из Сендаија за период 2015-2030 усвојен на Трећој светској конференцији Организација Уједињених нација која је одржана 18. марта 2015. године у Сендаију;

National Strategy for Critical Infrastructures Protestion (CIP Strategy), Federal Ministry of the Interior, Berlin, 17th June 2009;

Presidential Police Directive – Critical Infrastructures Security and Resilience, The White House, February 12, 2013;

Protection of Critical Infrastructures – Baseline Protection Concept, Federal Ministry of the Interior;

Council Directive, 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L 345/75;
Први додатни протокол Женевске конвенције из 1949. године. У: Извори међународног хуманитарног права, (ур. *Весна Кнежевић-Предић, Саша Аврам и Жељко Лежаја*), Београд, 2007;
Национална стратегија заштите и спасавања у ванредним ситуацијама, *Службени ɪласник РС*, бр. 86/11;
Закон о критичној инфраструктури, *Службени ɪласник РС*, бр. 87/18;
Закон о смањењу ризика од катастрофа и управљању ванредним ситуацијама, *Службени ɪласник РС*, број 87/18;
Закон о спречавању прања новца и финансирања тероризма, *Службени ɪласник РС*, бр. 113/17;
Одлука о образовању Координационог тела за спречавање прања новца и финансирање тероризма (Одлука), *Службени ɪласник РС*, бр. 54/18;
Одлука о образовању Сталне координационе групе за надзор над спровођењем Националне стратегије за борбу против прања новца и финансирања тероризма, *Службени ɪласник РС*, бр. 37/15 и 90/17;
Упутству о методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања, *Службени ɪласник РС*, бр. 80/19;
Pravilnik o metodologiji za izradu analize rizika i poslovanja kritičnih infrastruktura, *Narodne novine* br. 47/2016;
Речник српског језика, Матица српска, Нови Сад, 2011, стр. 462 или Longman Dictionary of Contemporary English 5th Edition.

Ljubomir S. Stajić, Ph.D., Full Professor
University of Novi Sad
Faculty of Law Novi Sad
Lj.Stajic@pf.uns.ac.rs

Vladan M. Mirković, Assistant
University of Novi Sad
Faculty of Law Novi Sad
V.Mirkovic@pf.uns.ac.rs

Nenad P. Radivojević, Ph.D., Assistant Professor
University of Novi Sad
Faculty of Law Novi Sad
N.Radivojevic@pf.uns.ac.rs

Security Management in the Field of Critical Infrastructure Protection in the Republic of Serbia – State and Perspectives

Abstract: *Term „critical infrastructure" became part of the post-Cold War security discourse when the first legal and political acts, containing this term, emerged. The Law on Critical Infrastructure in the Republic of Serbia was adopted in 2018, and some of the most important issues regulated by the Law are the competences and responsibilities of entities in the critical infrastructure protection system. The subject of our research was security management in the field of critical infrastructure protection. As a result of the research in the paper: 1. Levels, types and competencies of security management in the field of critical infrastructure protection have been identified; 2. Their mutual relationship has been determined and 3. Recommendations of measures and solutions that need to be taken in order to establish an integrated protection system in this area have been given.*

Keywords: *security management, risk management, crisis management, critical infrastructure, protection system, critical infrastructure operators.*

Датум пријема рада: 16.11.2020.