УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Марија Д. Мићовић

БЕЗБЕДНОСНИ АСПЕКТИ ФУНКЦИОНИСАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

ДОКТОРСКА ДИСЕРТАЦИЈА

Београд, 2016. год.

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Marija D. Mićović

SAFETY ASPECTS OF CRITICAL INFRASTRUCTURE FUNCTIONING IN EMERGENCIES

PhD DISSERTATION

Belgrade, 2016

Ментор:

1. др Владимир Јаковљевић, редовни професор
   Универзитет у Београду, Факултет безбедности

Чланови комисије:

2. др Зоран Кековић, редовни професор
   Универзитет у Београду, Факултет безбедности

3. др Милијана Ђорђевић, доцент
   Универзитет у Београду, Филолошки факултет

СЈЕНИМА МОЈИХ РОДИТЕЉА

ХВАЛА ВАМ

БЕЗБЕДНОСНИ АСПЕКТИ ФУНКЦИОНИСАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕУ ВАНРЕДНИМ СИТУАЦИЈАМА

Сажетак: Комплексност ванредних ситуација, посебно чињеница да се њиховом појавом угрожавају критични капацитети који су суштински у редовном процесу функционисања друштва, навеле су већину држава да развију акције које су имале за циљ да схвате елементе критичности рањивости различитих инфраструктура државе, дефинишу мере за смањење рањивости, осмисле и развију планове за ванредне ситуације и накнадни опоравак, подстакну развој сензибилитета код јавних и приватних оператера у погледу проблема заштите критичне инфраструктуре и подрже међународну сарадњу. У свету свакодневно расте број деструктивних активности, које се испољавају у облику вандализма, саботажа, терористичких активности, неодговорног понашања и сл.). Имајући у виду чињеницу да су објекти критичне инфраструктуре све више повезани и зависни, расте и њихова рањивост.

У овој докторској дисертацији је приказан поступак процене рањивости националних критичних инфраструктура, као и отпорност система критичне инфраструктуре у одговору на ванредну ситуацију у Републици Србији, са тежиштем на изабраним елементима критичне инфраструктуре: Нафтна индустрија Србије а.д., Јавно предузеће „Електропривреда Србије“, Јавно предузеће „Електромрежа Србије“, Јавно водопривредно предузеће „Србијаводе“, Јавно предузеће „Пошта Србије“, Јавно комунално предузеће „Београдски водовод и канализација“, Јавно предузеће „Путеви Србије“ и „Железнице Србије“ а.д. У емпиријским истраживањима спроведеним за потребе ове докторске дисертације анализирани су сви фактори који се односе на безбедносне аспекте функционисања критичне инфраструктуре у ванредним ситуацијама.

Резултати емпиријских истраживања јасно указују да је стање у погледу функционисања и заштите критичне инфраструктуре у Републици Србији незадовољавајуће. Област заштите критичних инфраструктура је још увек

законски неуређена, те је првенствено неопходно донети Закон о заштити критичне инфраструктуре чиме би се успоставио нормативни оквир за дефинисање, идентификацију, одређивање и заштиту националне критичне инфраструктуре. Након усвајања Закона о критичној инфраструктури биће потребно усвојити и подзаконска акта која ће обезбедити практична решења и критеријуме за идентификацију критичних инфраструктура и сектора критичне инфраструктуре.

Поред тога, израђен је модел процене угрожености критичне инфраструктуре у ванредним ситуацијама и дата је процена угрожености привредног друштва „Термоелектране Никола Тесла“. Основни разлог зашто је изабрана ова критична инфраструктура се огледа у чињеници да је то објекат од виталног значаја за нормално функционисање енергетског система Београда и околине.

Кључне речи: Безбедност, ванредне ситуације, критична инфраструктура, рањивост, заштита

Научна област: Науке безбедности

Ужа научна област: Студије Цивилне заштите и заштите животне средине

УДК број: 614.8:351.78(043.3)

SAFETY ASPECTS OF CRITICAL INFRASTRUCTURE FUNCTIONING IN EMERGENCIES

Abstract: The complexity of emergencies, particularly the fact that they endanger critical capacities that are essential for the normal functioning of society, have led most states to develop actions whose aim was to understand the elements of vulnerability of various critical infrastructures of a country, define measures to reduce vulnerability, design and develop emergency response and the subsequent recovery plans, encourage the development of sensitivity of both public and private operators in terms of the issue of protection of critical infrastructure and facilitate international cooperation. The number of destructive activities is constantly increasing in the world - in the form of vandalism, sabotages, terrorist activities, irresponsible behavior, etc. Bearing in mind the fact that the critical infrastructure facilities are increasingly interconnected and dependent, their vulnerability increases accordingly.

This doctoral thesis elaborates the procedure of assessment of vulnerability of national critical infrastructure, as well as the resistance of the critical infrastructure system in response to an emergency situation in the Republic of Serbia, with a focus on selected elements of critical infrastructure: "NIS a. d.", Public Enterprise "Electric Power Industry of Serbia", Public Enterprise "Elektromreža Srbije", Public Water Management Company "Srbijavode", Public Enterprise "Post of Serbia", Public Utility Company "Belgrade Waterworks and Sewage", Public Enterprise "Roads of Serbia" and "Serbian Railroads" JSC.

Empirical research carried out for the purpose of this doctoral thesis has analyzed all factors relating to safety aspects of critical infrastructure functioning in emergencies.

The results of empirical research clearly indicate that the situation regarding the functioning and protection of the critical infrastructure in the Republic of Serbia is unsatisfactory. The field of critical infrastructure protection is still legally unregulated, and therefore it is primarily necessary to passthe Law on Critical Infrastructure Protection, which would establish a regulatory framework for

defining, identifying, determining and protecting the national critical infrastructure. After the adoption of theLaw on Critical Infrastructure Protection, it will be necessary to adopt the bylaws as well, which will provide practical solutions and criteria to identify critical infrastructure and critical infrastructure sectors.

In addition, the risk assessment model of critical infrastructure in emergencies was developed, as well as the risk assessment of the Corporate Enterprise "Thermal Power Plants Nikola Tesla". The main reason why this critical infrastructure was selected is reflected in the fact that this facility is vital for the normal functioning of the energy system of Belgrade and its surroundings.

Keywords: Safety, emergencies, critical infrastructure, vulnerability, protection

Scientific Field: Security Sciencies

Scientific Area: Civil Protection and Environmental Protection Studies

UDK number: 614.8:351.78(043.3)

СПИСАК СКРАЋЕНИЦА

ADN	Европски споразум о међународном транспорту опасних материја унутрашњом пловидбом *(фр. Accord européen relatif au transport international des marchandises Dangereuses par voies de Navigation interieure)*
ADR	Европски споразум о међународном транспорту опасних материја у саобраћају на путевима *(фр. Accord européen relatif au transport international des marchandises Dangerousespar Route)*
AGSKI	Радна група за заштиту критичних инфраструктура *(нем. Arbeits Gruppe zum Schutz Kritischer Infrastrukturen)*
AMC	Аутоматска метеоролошка станица
AHD	Амерички речник термина *(енг. American Heritage Dictionary)*
БИА	Безбедносно-информативна агенција
ВС	Војска Србије
ВБА	Војнобезбедносна агенција
ВПЦ	Водопривредни центар
CIIP	Заштита критичних информационих инфраструктура *(енг. Critical Information Infrastructure Protection)*
CIKR	Критична инфраструктура и основни ресурси*(енг. Critical Infrastructure and Key Resources)*
CDRSC	*(енг. Committee on Disaster Research in the Social Sciences)*
CEMT	Европска комисија министара за транспорт *(fr. Conference Europeenne des Ministres des Transports)*
CECIS	Заједнички информациони систем *(енг. Common Emergency Communication and Information System)*
CEP	*(енг. Civil Emergency Planning)*
CERT/CC	*(енг. Computer Emergency Response Team/Coordination Centre)*
CIWIN	Информационе мреже критичне инфраструктуре *(енг. Critical Infrastructure Warning Information Network)*
COTIF	Конвенција о међународним превозима железницом *(fr. Convention Internationale pour le transport des Vozageurs)*
CSIRT	*(енг. Computer Security Incident Response Team)*
ДТД	Диверзантско-терористичка дејства
EAPCCPC	Одбор за цивилну заштиту Евроатланског већа *(енг. Euroatlantic Partnership Council, Civil Protection Committee)*
EADRU	Евроатлантска јединица за реаговање у случају катастрофа *(eng.*

	Euro-Atlantic Disaster Response Unit)
ECAC	Европска конференција цивилног ваздухопловства *(енг. European Civil Aviation Conference)*
ECHR	Евсопски суд за људска права*(енг. European Court of Human Rights)*
ECI	Европска критична инфраструктура *(енг. European Critical Infrastructure)*
ECHO	Европска комисија за хуманитарну помоћ и цивилну заштиту *(енг. European Comission Humanitarian Aid and Civil Protection)*
ENISA	Европска агенције за безбедност мрежа и информационих система *(енг. European Union Agency for Network and Information Security)*
ЕПОБ	Европска политика одбране и безбедности
EPCIP	Европски програм за заштиту критичне инфраструктуре *(енг. European Programme on Critical Infrastructure Protection)*
ETSI	Европски институт за телекомуникационе стандарде*(енг. European Telecommunications Standardards Institute)*
ГМО	Генетски модификовани организми
ЗиС	Заштита и спасавање
ЗКИ	Заштита критичне инфрастуктуре
ЗСПС	Заједничка спољна политика и сигурност
IAEA	Међународна агенција за атомску енергију *(eng. International Atomic Energy Agency)*
ICAO	Међународна организација цивилног ваздухопловста *(енг. International Civil Aviation Organization)*
IRT	*(енг. Incident Response Team)*
ISO	Међународна организација застандардизацију *(енг. International Standardisation Organization)*
ИКТ	Информационо-комуникационе технологије
ИТ	Информационе технологије
ИТС	Интелигентни транспортни системи
ITU	Међународна унија за телекомуникације *(енг. International Telecommunication Union)*
JAA	Заједничке ваздухопловне власти *(eng. Joint Aviation Authorities)*
ЈПЖС	Јавно предузеће „Железнице Србије“
КИ	Критична инфраструктура
MCEER	Мултидисциплинарни Центар за истраживање земљотреса *(енг. Multidisciplinary Center for Earthquake Engineering Research)*

МИС	Мрежна и информациона сигурност
МО	Министарство одбране
МУП	Министарство унутрашњих послова
NIAC	Национално саветодавно веће за инфраструктуру *(енг. National Infrastructure Advisory Council)*
NSSC	Национална стратегија обезбеђивања сајбер-простора*(енг. National Strategy to Secure Cyber space)*
НУС	Неексплодирана убојна средства
НЦКИ	Национални центар за критичне инфраструктуре
ОЕБС	Организација за европску развој и сарадњу *(енг. Organization for European Cooperation and Development)*
OPCW	Организација за забрану употребе хемијског оружја *(енг. Organization for the Prohibition of Chemical Weapons)*
PCCIP	*Председничка комисија за заштиту критичне инфраструктуре (енг. Presidential Commissionon Critical Infrastructure Protection)*
PDD	Председничка директива о заштити критичне инфраструктуре *(енг. President Decision Directives)*
ППВ	Погон за прераду воде
RID	Међународни прописи о транспорту опасних материја железницом *(фр. Reglement Internationall concernantle transport des marchandisces Dangereuses par le chemindefer)*
РХБ	Радиолошко-хемијско-биолошки
SBB	Швајцарска савезна железница *(нем. Schweizerische Bundesbahnen)*
SCADA	Систем за надзор, контролу и прикупљање података*(енг. Supervisory Control and Data Acquisition)*
SCEPC	Виши одбор за цивилно хитно планирање *(енг. Senior Civil Emergency Planning Committee)*
SERT	*(енг. Security Emergency Response Team)*
СМО	Светска метеоролошка организација
SN	Друштвене мреже *(енг. Social Networks)*
TEEN	Транс-европска енергетска мрежа *(енг. Trans European Energy Network)*
TETN	Транс-европска транспортна мрежа *(енг. Trans European Transport Network)*
TEU	Јединица еквивалента двадесет стопа *(eng. Twenty-footEquivalentUnit)*
UCIL	Хемијско постројење у Индији *(енг. Union Carbide India Limited)*
UNESCO	Организација за образовање, науку и културу Уједињених нација

	(енг. United Nations Educational, Scientific and Cultural Organization)
UNOCHA	Канцеларија УН за координацију и хуманитарну помоћ *(енг. UN Office for the Coordination of Humanitarian Assistance)*
FEMA	Федерална агенција за хитно управљање *(енг. Federal Emergency Management Agency)*
ЦЗ	Цивилна заштита
WCED	Светска комисија за животну средину и развој *(енг. World Commision on Environment and Development)*
WHO	Светска здравствена организација *(енг. World Health Organization)*
WFP	Светски програм хране *(енг. World Food Programme)*

САДРЖАЈ

УВОД

Актуелне друштвене околности усложавају безбедносну проблематику, како разноврсношћу начина, тако и интензитетом угрожавања безбедности. Неуобичајеност облика угрожавања безбедности узрокује посебне безбедносне задатке, као одговор на истоврсне безбедносне проблеме. Данас смо сведоци све више природних, намерних, организованих инцидената са великим последицама за људе, имовину и животну средину. По обиму, последицама по људе, материјална добра и животну средину, поједине опасности веома често имају или могу имати карактер ванредних ситуација.

Ванредне ситуације представљају измењено стање друштвене заједнице изазвано догађајима великих размера, којима се паралише функционисање друштвеног система земље, или кад настану природне и техничко-технолошке катастрофе великог обима које угрожавају живот становништва и њихову имовину, материјална и културна добра. Пратећи трендове и штете изазване оваквим ванредним ситуацијама нужно се намеће императив за организованим решењем у погледу смањења ризика и управљања ванредним ситуацијама.

Без обзира на различит спектар ванредних ситуација, све оне имају заједничко својство - огромне људске жртве и материјална разарања, па стога и велику потенцијалну опасност по друштво у целини.

Функционисање модерног друштва, како у редовној, тако и у ванредној ситуацији, није могуће замислити без ефикасне заштите значајних инфраструктурних система и објеката, те се као један од примарних и најзначајнијих безбедносних изазова новог доба намеће проблем заштите критичних инфраструктура. Инфраструктуре као што су саобраћајне мреже, вода, храна, енергија, хемијска индустрија, нуклеарна индустрија и информационе и комуникационе технологије пружају основне услове за функционисање појединаца, па и друштва у целини.

Када је реч о односу ванредне ситуације и заштите критичних инфраструктура треба имати у виду да ће критична инфраструктура бити

погођена ванредном ситуацијом, али се исто од ње очекује да се што пре стабилизује и својом основном делатношћу узме учешће у активностима отклањања последица и стабилизације живота и рада на погођеном подручју.

Стога је успешна превенција и управљање ванредним ситуацијама у директној вези са ефикасним системом заштите критичних инфраструктура. Мере попут превенције, припремљености и адекватног одговора на ванредну ситуацију повећавају степен сигурности критичних инфраструктура.

Докторска дисертација је у методолошком смислу тако конципирана да садржи следећа поглавља:

У првом поглављу ове докторске дисертације приказан је методолошки оквир спроведених истраживања. У оквиру њега објашњен је проблем истраживања, предмет истраживања, циљеви истраживања, хипотетички оквир истраживања, начин истраживања, као и научна и друштвена оправданост истраживања.

У другом поглављу објашњени су теоријски аспекти дефинисања и схватања критичне инфраструктуре, појам критичне инфраструктуре и њена класификација. Обрађене су све карактеристике инфраструктурних система, а тежиште је дато на саобраћај, енергетику и обезбеђење водом јер оне представљају веома битне субјекте који се ангажују на отклањању последица ванредних ситуација и нормализацији живота и рада на погођеном подручју. Без функционисања наведених субјеката, немогуће је у потпуности остварити поуздан систем управљања ванредном ситуацијом у свим фазама њеног одвијања. Посебан значај је дат процесу управљања критичном инфраструктуром у свим стадијумима ванредне ситуације.

У трећем поглављу„Угрожавање и улога критичне инфраструктуре у ванредним ситуацијама“, анализирани су ризици и претње по критичну инфраструктуру, улога критичне инфраструктуре у ванредним ситуацијама, као и сви расположиви ресурси. Посебан акценат је стављен на ресурсе критичне инфраструктуре, рањивост и улогу критичне инфраструктуре у ванредним ситуацијама. Тежиште је дато на анализу параметара за процену

рањивости критичне инфраструктуре, од којих су најважнији: изложеност, жилавост и истрајност, уз све манифестације димензија рањивости. Основа за наведену анализу представља Упутство о методологији за израду процене угрожености и планова заштите и спасавања у ванредним ситуацијама.[1]

У овом поглављу, приказан је садржај процене ризика по критичну инфраструктуру, процена угрожености привредног друштва и другог правног лица, процена критичне инфраструктуре са становишта угрожености од елементарних непогода и других несрећа, као и процена снага, средстава и превентивних мера за заштиту и спасавање.

У оквиру мера заштите критичне инфраструктуре обрађене су заштита критичне телекомуникационе инфраструктуре, преваре у електронским комуникацијама, надзор електронских комуникација за потребе државе, заштита критичне инфраструктуре у поштанском сектору, заштита критичне инфраструктуре у сектору енергетике и улога менаџмента у заштити критичне инфраструктуре. Имајући у виду значај сарадње са медијима у ванредним ситуацијама, приказани су облици интеракције са медијима у ванредној ситуацији, као и постојеће стратегије комуникације.

Четврто поглавље обухвата заштиту критичне инфраструктуре у Европској унији и другим државама. Приказана је идентификација и примена Европске критичне инфраструктуре која функционише у великом броју држава. Објашњене су обавезе које следе применом Европске критичне инфраструктуре и обавезе према власницима и операторима који примењују Европске критичне инфраструктуре. Анализирани су програми и механизми Европске уније у области заштите критичне инфраструктуре, са посебним освртом на информационе и комуникационе технологије, воду, храну, здравље, цивилну администрацију, финансије и транспорт. Такође, у овом поглављу је приказано стање и заштита критичне инфраструктуре у другим државама: САД, Руска Федерација и земље Европске уније.

У петом поглављу анализирана је заштита критичне инфраструктуре у

[1] *„Службени гласник РС“, бр. 96/2012.*

Републици Србији. Објашњен је Европски оквир и ситуација у Републици Србији и приказан нормативно-правни оквир функције и заштите критичне инфраструктуре у ванредним ситуацијама. Посебан значај је дат улози Сектора за ванредне ситуације у заштити критичне инфраструктуре, као и стању и могућности система критичне инфраструктуре у одговору на ванредну ситуацију у РС. Као критична инфраструктура идентификована су следећа предузећа: Нафтна индустрија Србије а.д., Јавно предузеће „Електропривреда Србије“, Јавно водопривредно предузеће „Србијаводе“, Јавно предузеће „Пошта Србије“ и Јавно комунално предузеће „Београдски водовод и канализација“. Анализиране су сви релевантни аспекти заштите критичне инфраструктуре у нашој држави.

Анализирани су природни облици угрожавања, техничко-технолошки облици угрожавања, спољни и унутрашњи облици угрожавања критичне инфраструктуре. Дат је приказ процеса оспособљавања лица ангажованих на пословима и задацима заштите система критичне инфраструктуре, особености процене ризика националних критичних инфраструктура и процедуре одлучивања у зависности од примењене концепције сложености.

У шестом поглављу које носи назив „Емпиријска истраживања“ приказани су резултати спроведених истраживања реализованих у овој докторској дисертацији чиме је у највећем делу обухваћена анализа свих фактора који се односе на безбедносне аспекте функционисања критичне инфраструктуре у ванредним ситуацијама. Ово истраживање је спроведено у форми анкетног упитника који је садржао 35 питања.

Истраживањем су обухваћене све релевантне установе које су везане за домен критичне инфраструктуре:Сектор за ванредне ситуације МУП РС, Јавно комунално предузеће „Београдски водовод и канализација“, Јавно предузеће „Пошта Србије“, Јавно предузеће „Електропривреда Србије“, Нафтна индустрија Србије а.д., Јавно предузеће „Електромрежа Србије“, Јавно предузеће „Путеви Србије“, Железнице Србије а.д. и Јавно водопривредно предузеће „Србијаводе“. Добијени резултати су анализирани ради давања одговора везаних за циљеве ове докторске дисертације. Добијени резултати

су класификовани, статистички обрађени и анализирани ради давања потребних одговора везаних за циљеве ове докторске дисертације.

У седмом поглављу „Преглед критичних сектора у Републици Србији“ су наведени сви критични сектори у нашој земљи, анализирани постојећи проблеми и дат је предлог за модификацију изабраних модела. У вези са тим, у прилогу 2 је приказан један карактеристичан модел заштите критичне инфраструктуре у ванредним ситуацијама. Анализа је извршена у привредном друштву „Термоелектране Никола Тесла“ д.о.о. Обреновац. Детаљно је обрађена процена критичне инфраструктуре са становишта угрожености од елементарних непогода и других несрећа, идентификација опасности и процена ризика од елементарних непогода и других несрећа са предлогом мера.

Закључак докторске дисертације представља рекапитулацију теоријских и емпиријских истраживања са тежиштем на елаборацију уочених проблема у овој области и давање предлога мера чијом имплементацијом би се систем заштите критичних инфраструктура у Републици Србији подигао на ниво који би допринео њиховом поузданом функционисању у условима ванредних ситуација.

1. МЕТОДОЛОШКИ ОКВИР ИСТРАЖИВАЊА

1.1. ПРОБЛЕМ ИСТРАЖИВАЊА

Ванредне ситуације изазване природним и другим опасностима су више пута до сада показале бројне мањкавости у погледу реакције државе, њених органа, привредних субјеката и грађана у погледу превенције, одговора и отклањања изазваних последица. То се пре свега односи на нормативну неуређеност, недовољну функционалну и институционалну организованост и отежану координацију и управљање акцијама заштите и спасавања. Овакво стање много пута је допринело да здравствене, материјалне, социјалне и еколошке последице буду присутне у скоро свим испољеним опасностима које имају карактер ванредних ситуација. Поред свих наведених последица, материјалне последице су најочигледније и као такве захтевају од државе да чини додатне напоре на санацији истих уз велика финансијска улагања у дужем временском периоду. Оваква стања веома често могу зауставити тренд економског развоја државе или га чак вратити уназад за неколико година или деценија.

Приликом испољавања појединих опасности које имају карактер ванредних ситуација, бивају погођени сви сегменти друштва, државни органи и њихове институције, службе јавних делатности (здравство, социјална заштита, просвета, култура, информисање), привредни субјекти и сва друга правна и физичка лица. Такав обим угрожености захтева ангажовање свих субјеката државе, цивилног друштва, привредних субјеката и грађана да спровођењем мера на смањену ризика, ризике сведу на најмању могућу меру, а ако пак дође до њихове манифестације, буду спремни за одговор (акције помоћи и спасавања), ликвидацију и отклањање насталих последица. То подразумева да тоталност угрожавања захтева и тоталност у погледу превенције, одговору и управљању ванредним ситуацијама.

Веома важан сегмент управљања ванредним ситуацијама представља област функционисања критичне инфраструктуре у таквим условима, када се зна да и сама критична инфраструктура и њени поједини сегменти истовремено

бивају изложени деструктивним силама појединих опасности. Сам термин критична инфраструктура почео се експлоатисати у последњих двадесетак година и као такав је присутан у земљама Европске уније. Све израженије природне и друге катастрофе као и терористичке претње поставили су у први план питање безбедног функционисања критичне инфраструктуре са високим приоритетима државне регулативе. Решења и приступи појединих земаља у овом погледу су различита, што се огледа у различитости перцепције безбедносних претњи, искустава из прошлости, организације и политике државне структуре, степена приватног власништва у компанијама које управљају критичном инфраструктуром. Ова диференцијација приступа може се видети на европском нивоу, где је веома тешко доћи до координисане акције у области Европске заштите критичне инфраструктуре.

Имајући у виду да је област заштите критичне инфраструктуре заузела значајно место у скоро свим савременим системима заштите и спасавања, те да је ова област у нормативном, функционалном и институционалном погледу уређена или је сам поступак у току, онда покретање овог истраживања са аспекта сагледавања стања у овој области у Републици Србији има пуног оправдања. Истраживањем се жели доћи до сазнања како се штити и функционише критична инфраструктура у Европској унији и другим државама, какво је стање у овом погледу у Републици Србији. То је веома значајно ако се има у виду поступак преговора приступања РС у чланство Европске уније, где ће се и ово питање отворити у неком од преговарачких поглавља. Тренутно стање по овом питању у Републици Србији је такво да ова област представља новину у реторичком смислу па је самим тим и веома мали број теоријских радова из ове области, мала је заступљеност ове проблематике у законским решењима која третирају области заштите и спасавања у ванредним ситуацијама и нема ни посебног закона који би ову област у потпуности уредио као што је то случај у другим земљама. Међутим, били би смо неискрени ако би смо рекли да се у Републици Србији до сада ништа није чинило на овом плану, те да се налазимо на самим почецима, ако се зна да су у свим системима (велики

технички системи) које данас називамо критичном инфраструктуром организовани послови одбране, безбедности и заштите у чијем делокругу се налазе и питања процене ризика, смањења ризика и функционисања тих инфраструктурних система у ванредним ситуацијама.

Дакле реч је о новој терминологији, новој реторици, а послови одбране, безбедности и заштите су у овим системима већ одавно успостављени, функционишу у складу са позитивно правним прописима. Да је то тако показују бројни примери успешног функционисања појединих критичних инфраструктура у условима НАТО бомбардовања Савезне Републике Југославије где су они били приоритетна мета напада. Такође, ту су и примери који говоре о угрожавању и виталности ових система и њиховом функционисању у условима ванредних ситуација изазваних поплавама, земљотресима и другим већим природним непогодама. Наведене чињенице јасно указују да су погрешне тврдње којима се веома често констатује да Република Србија нема искуства у области заштите кључних објеката, институција и процеса који су данас терминолошки дефинисани као критичне инфраструктуре.

Изградња адекватног система заштите критичне инфраструктуре данас представља изузетно сложен задатак за скоро све земље а посебно земље у транзицији којима припада и Република Србија. Имајући у виду да је основна мисија критичне инфраструктуре да обезбеди нормално и ефикасно функционисање свих сегмената друштва, државе и њених органа и грађана, као и сложеност безбедносног окружења и претњи, онда се справом може констатовати да је пред државом и њеним органима и самим операторима изузетно изазован задатак у погледу обезбеђења неопходних услова за безбедно функционисање критичне инфраструктуре у свим условима, у миру, ванредним ситуацијама и рату. Међутим, у претходном периоду, у многим земљама, па и у Републици Србији, веома често се због ограничености финансијских, људских и организационих ресурса, питање заштите критичних инфраструктура у оквиру дефинисаних приоритета стратешког менаџмента појединих организација или компанија налазило

при самом дну лествице. Присуство различитих ставова и схватања значаја критичне инфраструктуре, парцијалних интереса појединих компанија и државних институција (министарстава) су само неке од тензија које прате неадекватно управљање и функционисање система заштите критичне инфраструктуре. Овакво стање може да доведе до значајних кашњења у развоју система заштите критичне инфраструктуре у нашој земљи.

Република Србија као земља у транзицији неминовно мора приступити спровођењу системских мера у области регулисања заштите критичне инфраструктуре. У овом прелазном периоду, због промена друштвено-политичких односа у правцу тржишне економије, у обиму актера који су важни за ефикасно функционисање система критичне инфраструктуре, појаве приватног капитала који кроз власништво у компанијама које управљају критичном инфраструктуром су кључни фактори и нови моменти који пресудно утиче на перцепцију промена које су наступиле у овој области у односу на систем пре транзиције. Због наведеног, процеси и ефикасни модели јавно-приватног партнерства представљају основу успешног система заштите критичне инфраструктуре. Систем заштите критичне инфраструктуре у Републици Србији у периоду који је пред нама, може бити ефикасан само под претпоставком да све заинтересоване стране (држава на првом месту, компаније и други учесници) разумеју позитивне ефекте регулације система заштите критичне инфраструктуре и да уложе неопходне напоре и ресурсе у његову изградњу на новим основама. Држава представља централну тачку у изградњи и осигурању ефикасног система критичне инфраструктуре, и и том смислу, највећи интерес државе је да критична инфраструктура без обзира на власничку структуру компанија, непрекидно функционише чиме се остварује и функционисање заједнице у свим условима па и у условима ванредних ситуација. Стога држава својим регулаторним мерама, мерама контроле и сталног надзора мора утицати на менаџмент компанија које њима управљају, да се процес изградње система заштите критичне инфраструктуре доведе до захтеваног нивоа.

Имајући у виду наведене чињенице, у даљем образложењу проблема

истраживања, неопходно је идентификовати кључне факторе који ће утицати на динамику изградње ефикасног и међународно упоредивог система критичне инфраструктуре у Републици Србији. Тежиште у наредном периоду мора се усмерити на решавање следећих питања: подизање свести о важности критичне инфраструктуре у кључним групама које формирају јавно-приватно партнерство; успостављање адекватног правног оквира за функционисање критичне инфраструктуре; успостављање адекватног система јавно-приватног партнерства и поверења између свих актера у области заштите критичне инфраструктуре; изградња одговарајућих критеријума за одређивање и класификовање критичне инфраструктуре у Републици Србији; успостављање одговарајућег система јасног дефинисања власти и одговорности у области заштите критичне инфраструктуре; имплементација релевантне европске регулативе у процесу приближавања Републике Србије ЕУ; обезбеђење неопходних финансијских средстава; обезбеђење квалитетних људских ресурса и система образовања будућих стручњака у области заштите критичне инфраструктуре.

Сва наведена питања могу бити предмет посебних истраживања а оно што се може уочити као проблем овог истраживања, односи се на организацију мера заштите и спремност ових система за функционисање у условима ванредних ситуација. У том смислу неопходно је теоријски образложити сам појам критичне инфраструктуре, нормативну уређеност, међународна искуства, дати преглед најчешћих ризика којима је изложена критична инфраструктура и сагледати њену улогу у ванредним ситуацијама. Емпиријски део проблема истраживања обухвата идентификацију и анализу ризика којима је критична инфраструктура у РС изложена, стање и квалитет ресурса, као и стање организације и спровођења мера безбедности и заштите критичне инфраструктуре у Републици Србији.

Досадашња истраживања на плану организовања државе и друштва за спречавање и отклањање последица ванредних ситуација указују да се овом питању прилазило са више аспеката (стратешког, нормативног, институционалног, техничког, образовног и сл.), или су истраживања

тежишно била усмерена на функционисање појединих елемената система заштите и спасавања у ванредним ситуацијама (цивилне заштите, службе осматрања и обавештавања...), али је веома мали број истраживања који су третирали проблематику функционисања критичне инфраструктуре у ванредним ситуацијама. Наведене чињенице су јасно указале на празнину која постоји у овој области и дале су простор за истраживањем којим би се употпунила слика о значају, улози, могућностима и начину функционисања критичне инфраструктуре у ванаредним ситуацијама.

Сагледавајући сву ширину проблемског захвата, сам проблем истраживања се може дефинисати на следећи начин: Да ли су критичне инфраструктуре Републике Србије, које су оптерећене свим променама који носи процес транзиције, спремне да ефикасно функционишу у условима ванредних ситуација?

Овако дефинисан проблем истраживања произилази из чињенице што се критична инфраструктура и њено функционисање у ванредним ситуацијама схвата као:

- објекат на коме се догађа ванредна ситуација, и као такав представља предмет заштите, али је и
- средство које омогућава смањивање опасности, или олакшава, односно омогућава отклањање последица ванредних ситуација чиме се омогућује функционисање заједнице у таквим условима.

Када се имају у виду ове веома битне чињенице, дефинисани проблем се може посматрати и у тражењу одговора на још два значајна питања:

1. Да ли организоване и успостављене мере заштите критичне инфраструктуре обезбеђују несметано одвијање њихове основне делатности према устаљеном режиму рада и омогућују њихово функционисање у условима ванредних ситуација?

2. Да ли су ресурси критичне инфраструктуре спремни да што пре отклоне последице ванредних ситуација на својим системима и објектима и укључе се у активности заштите и отклањања последица ванредних ситуација на

погођеном подручју?

Овако дефинисан проблем истраживања јасно осликава потребу за анализом безбедносног аспекта функционисања КИ у условима ванредних ситуација.

Да би се успешно одговорило на ова питања, неопходно је истражити:

- квалитет постојећих организационо-функционалних компоненти и ресурса критичне инфраструктуре;
- потенцијалне изворе, носиоце и облике угрожавања критичне инфраструктуре;
- правце реорганизације, односно развоја и унапређења функционисања и заштите критичне инфраструктуре у измењеним околностима и то на бази уочених недостатака и иностраних достигнућа и искустава.

Одговором на ова питања створиће се основа за практично решавање проблема функционисања и заштите критичне инфраструктуре у Републици Србији.

1.2. ПРЕДМЕТ ИСТРАЖИВАЊА

Предмет истраживања у овој докторској дисертацији првенствено се односи на истраживање безбедносних аспеката функционисања критичне инфраструктре у условима ванредних ситуација. Овако дефинисан предмет истраживања се може посматрати у ужем и ширем смислу.

Шире одређење предмета истраживања усмерено је на анализу свих фактора који опредељују изградњу система заштите критичне инфраструктуре у Републици Србији, а уже одређење предмета истраживања усмерено је на истраживање спремности и могућности функционисања критичне инфраструктуре у условима ванредних ситуација.

У оквиру ужег предмета истраживања, тежиште рада усмерено је на истраживање безбедносних ризика којима је критична инфраструктура изложена, нормативну уређеност критичне инфраструктуре, организацију мера заштите критичне инфраструктуре, сагледавање квалитета ресурса

критичне инфраструктуре и организацију безбедносних служби у оквиру система критичних инфраструктура. Сви наведени индикатори који ће се истражити кроз теоријско и емпиријско истраживање, пружиће релевантне податке да се сагледа стање у области критичне инфраструктуре Републике Србије и да се на тим основама да предлог модела који би требало развијати у будућем периоду. Комплетно истраживање се посматра са аспекта ванредних ситуација и могућности безбедног функционисања критичне инфраструктуре у свим фазама развоја ванредне ситуације. Такође, посебно значајним се сматра и истраживање значаја критичне инфраструктуре у свакој појединачној фази управљања ванредним ситуацијама (припреми, одговору и санацији).

У циљу теоријског одређења предмета истраживања неопходно је дефинисање појмова: инфраструктура, критична инфраструктура и ванредне ситуације.

Инфраструктура (лат. infra под, испод, ниже, structura од *struere* слагати, склапати) темељ, основа, подлога; основа за привредни и друштвени развој, коју чине: саобраћајна мрежа (путеви, железничке пруге, канали и сл.), водне инсталације, извори електричне и др. енергије, објекти намењени јавним потребама (осветљење, паркови, тргови, домови здравља, болнице, школе итд.).[2]

Критична инфраструктура обухвата поједине институције јавног и приватног сектора, канале дистрибуције те „мреже“ особа и информација које гарантују несметан и континуиран проток људи, роба, сервиса, услуга, што је кључно за стабилност економског и безбедносног система земље. У групу „критичне инфраструктуре“ убрајају се телекомуникације, електропривреда, складиштење и пренос плина и нафте, банкарство и финансије, транспорт, водоснабдевање, хитна служба (укључујући медицинске, полицијске, ватрогасне и спасилачке службе) и друге институције.

[2]*Вујаклија, М., Лексикон страних речи и израза, Просвета, Београд, одредница инфраструктура, 2006.*

Критична инфраструктура постала је саставна компонента националне безбедности 1990-их година и данас представља један од приоритета сваке државе. Према закључку Одбора за цивилну заштиту Евроатланског већа *(Euroatlantic Partnership Council, Civil Protection Committee - EAPC CPC)* од 2002. године са годишњег заседања у Брасову, који је касније усвојио и Виши одбор за цивилно хитно планирање *(Senior Civil Emergency Planning Committee - SCEPC)* појам критична инфраструктура обухвата одговарајуће националне капацитете, службе и информацијске системе који су од виталног значаја да би њихова немогућност деловања или оштећење могли имати директан утицај на националну безбедност, националну економију, јавно здравље, сигурност становништва и ефикасност деловања власти.

Појам критичне инфраструктуре односи се на имовину која укључује физичке и компјутерске системе који су од есенцијалног значаја за обезбеђивање економске и политичке стабилности земље.[3]Оне заправо представљају оквир међузависних мрежа и система који обухватају одређене индустрије, институције (укључујући људе и процедуре) и капацитете за дистрибуцију који пружају поуздан проток производа и услуга који су неопходни за одбрамбену и економску сигурност земље, неометано функционисање власти на свим нивоима, и друштва у целини.

Критичне инфраструктуре обухватају, али нису искључиво ограничене на, енергетске системе, телекомуникације, саобраћај, воду, храну, банкарске системе и финансије, цивилну администрацију, укључујући и владин и приватни сектор.[4] Ниједна подела критичних инфраструктура није апсолутна и углавном је заснована на проценама стручњака и/или доносиоца политичких одлука.

Европска унија дефинише критичну инфраструктуру као скуп физичких ресурса, служби, уређаја, информационих технологија, економске и социјалне користи било: а) две или више земаља чланица, било б) три или више земаља

[3]*Radvanovsky, R., McDougall, A., Critical Infrastructure, Homeland Security and Emergency Preparedness, 2nd edition, CRC Press, Taylor&Francis Group, New York, 2010.*
[4]*Ibid.*

чланица.[5]

По дефиницији Европске уније, критична инфраструктура укључује оне физичке изворе, услуге и објекте информационе технологије, мреже и инфраструктурне комплексе чије уништење и оштећење има озбиљне последице на здравље, сигурност, економску и другу стабилност две или више земаља чланица.[6]

У САД, национални програм за заштиту критичне инфраструктуре је покренут 1998. године. На нивоу ЕУ, Европски савет је 2004. позвао Европску комисију да припреми свеобухватне стратегије за заштиту критичне инфраструктуре. Комисија је 2004. године усвојила програм заштите критичне инфраструктуре у борби против тероризма, који је изнео смернице о унапређењу превенције, приправности и одговора на терористичке нападе укључујући и ресурсе критичне инфраструктуре који су такође предмет терористичких напада.

Амерички речник термина дефинише кључну инфраструктуру као основне објекте, услуге, и инсталације потребне за функционисање заједнице или друштва, као што су превоз и комуникациони системи, водне и електричне инсталације, као и јавне институције, укључујући школе и поште.

У САД појам критичне инфраструктуре односи се на системе и средства, било физичка или виртуелна, од виталног значаја за националну безбедност земље, њиховим онеспособљавањем или уништењем угрозио би се ниво достигнуте безбедности, економска сигурност земље, јавно здравље или неки други значајан сегмент. На основу ове дефиниције, извршена је идентификација 17 критичних инфраструктура и кључних ресурса, и одређене улоге и одговорности за заштиту ових сектора *(Homeland Security Presidential Directive 7 (HSPD-7), December 2003).* Одељење за националну

[5]*Commission of the European Communities, Critical Infrastructure Protection in the fightagainst terrorism (Brussels, 20.10.2004), COM(2004)702 final, pp. 3, Извештај Комисије доступан је на интернет адресu:http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf17.11.2012.*

[6]*Commission of the European communities, Green paper on a European programe for critical infrastructures protection, Brussels, 2005.*

безбедност, у марту 2008. године, идентификовало је још један критичан сектор (сектор за производњу критичних производа). Уз могућност даље трансформације листе критичних сектора, следећи сектори су тренутно наведени као кључни за ефикасну заштиту критичних инфраструктура: информационе технологије; телекомуникације; хемијска постројења; пословна постројења; бране; комерцијални нуклеарни реактори, материјали и отпад; владина постројења; транспорт; хитне службе; поштанске и доставне услуге; пољопривреда и храна; јавно здравље и здравство; пијаћа вода и системи за пречишћавање обичних вода; енергија, укључујући производњу, прераду, складиштење и дистрибуцију нафте и гаса, електропривреду; банкарство и финансије; национални споменици и знаменитости; одбрамбена индустријска база; производња критичних производа.

Појам заштита критичних инфраструктура (ЗКИ) је први пут употребио председник Клинтон 1996. године, након терористичког акта на Федералну зграду Алфреда П. Мараха у Оклахоми 1995. године (Извршна наредба, јул 1996). Овом наредбом истакнуте су одређене националне инфраструктуре, које су од изузетног значаја за САД и чије би онеспособљавање или уништење имало велики утицај на одбрану, економску сигурност и благостање грађана.

Заштита критичних инфраструктура се односи на активности које се тичу заштите инфраструктура од круцијалног значаја. Ту спадају људи, физичка имовина и информационо-комуникациони системи који су неопходни за националну и наднационалну безбедност, економску стабилност и јавни и правни поредак и безбедност. Методе и средства заштите критичних инфраструктура одвраћају или ублажавају нападе на критичне инфраструктуре од стране људи (терористи, криминалци, хакери итд.), природних катастрофа (земљотреси, олујни ветрови, поплаве итд.), пожара и експлозија у нуклеарним или хемијским комплексима. У суштини, заштита критичних инфраструктура подразумева заштиту имовине од непроцењиве друштвене вредности.

У оквиру НАТО програма планирања за случај ванредних ситуација критичну инфраструктуру чине средства, објекти, мреже и услуге чије би повремено онеспособљавање или уништавање имало озбиљне последице по здравље, сигурност, стабилност, економско благостање или уобичајено функционисање државе. Ако се не заштити критична инфраструктура може страдати у случају природних и других катастрофа, укључујући и тероризам.[7]

Ванредне ситуације изазивају догађаји који нарушавају нормално функционисање служби и предузећа, угрожавају живот грађана, природна и материјална добра (животну средину) и представљају претњу по стабилност (одрживост) локалног, националног и глобалног развоја.[8]

Управљање ванредним ситуацијама подразумева пружање хитне помоћи и задовољење најприоритетнијих потреба које су се јавиле као директна последица незгоде. У те потребе спада обезбеђење воде, хране, санитарних услуга, основних здравствених услуга и смештаја. Адекватан смештај је важан као физички заклон од временских услова, као заштита од ризика по здравље, али, што је једнако важно и за очување достојанства човека и живота у оквиру породице.[9]

У сложеним ванредним ситуацијама отежавајућа околност представља урушавање критичне инфраструктуре. Када је нарушено или потпуно онемогућено функционисање болница, могу бити изгубљени животи људи који су могли бити спасени у овим установама. Сметње у рутинским службама могу такође утицати на губитке људских живота.[10]

Управљање ванредним ситуацијама је врло сложен процес. Озбиљност, сложеност последица ванредних ситуација захтева једнако такав приступ у управљању и организовању превенције, одговору, спасавању и отклањању насталих последица. Основу функционисања система критичне

[7]*NATO Public Diplomacy Division, Brusesels, Belgium, 2006.*
[8]*Wahle, T., Beaty, G., Emergency Management Guide for Business&Industry, Federal EmergencyManagement Agency (FEMA), Internet edition, pp. 29, 2004.*
[9]*Анђелковић, Б., Ризик технолошких система и професионални ризик, Југословенски савез друштава инжењера и техничара заштите, Ниш, стр. 121, 2002.*
[10]*Весић, Д., Менаџмент и кризни програм - аспект односа са јавношћу, Безбедност, Београд, бр. 3, стр. 345-354, 2000.*

инфраструктуре чине људски ресурси, простор, ресурси информација и знања, финансијски ресурси и време. Ови ресурси имају пресудну улогу на успешност одговора на изазове, ризике и претње на безбедност људи, материјалних добара, простора а тиме и на заштиту од свих видова ризика од било ког облика ванредне ситуације.

Основни појмови везани за угрожавање безбедности КИ су: претња, ризик, хазард, рањивост (вулнерабилност).

Претња безбедности је све оно што представља извор опасности и има могућност да нанесе озбиљну штету лицима, имовини, друштву или држави.[11]Претња је неко или нешто што има могућност да науди националним интересима једне државе и да оствари нежељени догађај. Када се ова могућност актуелизује, она престаје да буде претња и постаје догађај попут других. У тренутку када је претња уочена она постаје део ризика, а као таква и предмет расподеле њиховог времена и расположивих ресурса (људских, техничких, финансијских или других) ради супротстављања.[12]

Претња представља јасно и непосредно изражену намеру и/или способност да се неко или нешто повреди, уништи, казни итд.[13]Политика националне безбедности увек зависи од перцепције претњи које постоје у односу на националне интересе и представља развијање могућности заштите од истих.[14]

Бројне дефиниције појма ризик у домаћој и страној литератури указују да јеризик (итал. risico) могућа опасност. Ризиковати значи изложити се (излагати се) опасности.[15] Под ризиком се подразумева вероватноћа или могућност опасности, губитка, озледе или неке друге штетне последице.[16]

---

[11]*Baldwin, D.A., Thinking about Threats, Journal of Conflict Resolution, Vol. 15, No. 1, 70-78, 1971.*
[12]*Путник, Н., Сајбер простор и безбедносни изазови, Београд, Факултет безбедности, стр. 62, 2009.*
[13]*Daasse, C., Kessler, O., Knowns and Unknowns in the War in Terror: Uncertainty and the political contruction of danger.*
[14]*Milburn, T.W., Watman, K.H., On the Nature of Threat: A Social Psychological Analysis, New York: Praeger, 1981.*
[15]*Московљевић, М., Речник савременог српског књижевног језика с језичким саветником, Гутенбергова галаксија, Београд, стр. 577, 2006.*
[16]*Consise Oxford Dictionary, 9th edition, Claredon Press, Oxford, pp. 866, 1997.*

Ризик је и могућност да се одређени циљ не оствари у потпуности или да се оствари делимично. Могућност отклањања или смањења ризика зависи од нивоа познавања појаве у којој је садржан одређени ризик.

Појам ризик представља универзалан и специфичан облик опасности по безбедност било ког објекта безбедности, независно од тога да ли је у поседу субјекта безбедности или субјекта опасности. Наиме, извориште заштите (одбране) сваког објекта безбедности је у одлучивању, а доносити одлуке значи излагати се ризику. Таквој опасности излажу се обе стране у конфликту: субјект безбедности доноси одлуку ради оптималне заштите свог објекта безбедности, а субјект опасности доноси одлуку да на најефикаснији начин угрози безбедност, односно изазове промене на дотичном објекту безбедности.[17]

Анализа ризика пружа улазну информацију о оцени ризика и одлукама да ли ризици треба да се решавају и које су то одговарајуће (најприхватљивије) стратегије у третирању ризика. Анализа ризика обухвата разматрање узрока и извора ризика, њихових позитивних и негативних последица, као и вероватноћу појављивања тих последица. Такође, могу се идентификовати и фактори који утичу на појаву последица и вероватноћу њиховог појављивања. Ризик се анализира тако што се одређују последице и вероватноћа њиховог настанка, као и остале особине ризика.[18]

Идентификација и анализа ризика представљају део ширег процеса процене ризика *(risk assessment)*, односно управљања ризиком *(risk management)*. Процена ризика је саставни део процеса управљања ризиком и представља свеобухватни процес идентификовања потенцијалних опасности, анализе и оцене ризика.

Заједнички именитељ наведених дефиниција ризика јесте неизвесност и могућност губитка КИ. Неизвесност постоји онда када се не може са

---

[17]*Мијалковски М., Ђорђевић И., Ризик - специфичан облик угрожавања безбедности, Универзитет у Београду, Факултет безбедности, 2006.*

[18]*Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д., Процена ризика у заштити лица, имовине и пословања, Центар за анализу ризика и управљање кризама, Београд, стр. 108, 2011.*

сигурношћу знати исход одређеног догађаја. Када ризик постоји, морају постојати бар два могућа исхода. Најмање један од могућих исхода мора да буде непожељан.

То може да буде губитак у смислу да је нешто што је било у саставу КИоштећено (изгубљено), затим то може да буде губитак који је већи од пројектованог или пак добитак који је мањи од пројектованог. Уопштено, као битна карактеристика ризика може се навести могућност да се претрпи штета.

Хазард се дефинише као могући извор опасности, физичких или операционих услова, са потенцијалом који може да произведе одређену врсту негативних последица.[19] У стручној литератури среће се појам физичких хазарда, који представљају материјалне услове средине који утичу на учесталост и степен губитка имовине, као што су локација, конструкција и инсталације, као и начин коришћења објеката и опреме.[20]

Вулнерабилност је слабост одређене особе, групе или система, односно слабост критичне инфраструктуре или њених елемената услед које они постају изложенији ризику од наступања нежељеног догађаја који може резултовати нарушавање физичког или психичког интегритета појединаца односно стања система.[21]

Операционално одређење предмета истраживања

Операционално одређење предмета истраживања могуће је разматрати кроз следеће сегменте:

Први сегмент предмета истраживања односи се на теоријску анализу и разраду чињеница везаних за појам ванредне ситуације, критичне инфраструктуре чијом ће се анализом јасно сагледати следећа питања: теоријски приступ дефинисању појма ванредних ситуација и критичне инфраструктуре, последице ванредних ситуација, улога критичне

[19] *Ibid, 176.*
[20] *Ibid, 28.*
[21] *Bankoff, G., Maping Vulnerability, Earthscan, London, 2004.*

инфраструктуре у ванредним ситуацијама, облици угрожавања критичне инфраструктуре, заштита критичне инфраструктуре у ванредним ситуацијама. У овом истраживању, нагласак ће бити стављен на следеће инфраструктуре: енергетске системе, телекомуникације, саобраћај, воду и храну.

Теоријски ће се анализирати област заштите и функционисања критичне инфраструктуре у ванредним ситуацијама у земљама у региону.

Други сегмент предмета истраживања односи се на истраживање стања и проблема организовања и функционисања ресурса критичне инфраструктуре у Републици Србији. Посебно ће бити апострофирани нормативно-правни проблеми, функционални и организациони проблеми. У оквиру овог сегмента истраживања треба дати приказ реалног стања ресурса критичне инфраструктуре у измењеним условима.

Уз то је потребно поставити основне принципе и правце пројектовања логистичке подршке критичној инфраструктури како би она испунила своје задатке у ванредним ситуацијама.

Трећи део рада представља анализа резултата емпиријског истраживања. Истраживања која су спроведена у овој докторској дисертацији обухватила су анализу свих фактора који се односе на безбедносне аспекте функционисања критичне инфраструктуре у ванредним ситуацијама.

Истраживање је спроведено у форми анкетног упитника (Прилог 1.) који је садржао 35 питања. Истраживањем су обухваћене све релевантне установе које су везане за домен критичне инфраструктуре. Посебно је обрађена једно привредно предузеће - Термоелектрана „Никола Тесла“ чије је беспрекорно функционисање неизмерно важно у данашњем времену.

Четврти сегмент премета истраживања се односи на конципирање и представљање могућег унапређеног модела система заштите и функционисања критичне инфраструктуре Републике Србије, који би био усклађен са процењеним потребама за реаговање у ванредним ситуацијама.

Временско одређење предмета истраживања

Временско одређење предмета у потпуности се односи на проучавање овог проблема у нашој држави у прошлости (период уназад десет година), садашњости и будућој оријентацији.

Просторно одређење предмета истраживања обухвата простор Републике Србије и простор земаља које су предмет теоријске анализе.

Дисциплинарно одређење предмета истраживања

Предмет истраживања теоријски припада наукама одбране, заштите и безбедности. Посматрано у ширем контексту предмет истраживања има интердисциплинарни карактер и обједињује већи број научних дисциплина: техничке, правне, економске, организационе, социолошке, психолошке и сл.

Предмет овог истраживања су функција и заштита критичне инфраструктуре у ванредним ситуацијама. Наиме, позната је чињеница да су ванредне ситуације део свакодневног живота и да се са развојем државе и друштва повећавају извори, облици њиховог јављања као и губици људских живота праћених великим материјалним губицима. Такође је позната чињеница да је технолошки развијено друштво тако организовано да се због економских и других разлога снабдевања енергентима, храном, репроматеријалом, медицинским материјалом и низом других роба одвија редовно па је стварање великих залиха постало ванстандардно. Ванредне ситуације у највећем броју случајева прозрокују оштећења и застоје на инфраструктурним постројењима.

1.3. ЦИЉЕВИ ИСТРАЖИВАЊА

Основни циљ овог истраживања односи се на истраживање безбедносног аспекта функционисања критичне инфраструктуре у условима ванредних ситуација. Резултати истраживања треба јасно да укажу на правце којима се треба руководити при унапређењу система функционисања и заштите критичне инфраструктуре у Републици Србији.

Научни циљ

Научни циљ истраживања јесте да изврши научну дескрипцију (описивање) са елементима класификација и научно објашњење постојећег стања функције и заштите критичне инфраструктуре у ванредним ситуацијама,као и да применом системског приступа и искустава из праксе истражи и сагледа основу модела за побољшање напред наведеног.

Практични циљ

Практични циљ овог истраживања јесте да се на основу теоријских сазнања и емпиријских резултата:

- потпуније, реалније и објективније сагледају постојећи функционални и организациони аспекти савремених система заштите и спасавања са посебним акцентом на критичну инфраструктуру у погледу спречавања и отклањања последица од ванредних ситуација;
- предложе одређена практична решења у циљу доградње система заштите и функционисања критичне инфраструктуре у Републици Србији при чему се морају уважавати реалне потребе и могућности;
- постави структура модела за побољшање, унапређење и управљање системом критичне инфраструктуре.

1.4. ХИПОТЕТИЧКИ ОКВИР ИСТРАЖИВАЊА

Основна (општа) хипотеза

Имајући у виду да је ово истраживање превасходно експланаторног карактера, те да за циљ има стварање могућности за генерисање хипотеза будућих истраживања, то је његова основа хипотеза дефинисана кроз **општу хипотезу**: *Ванредне ситуације узрокују специфичне захтеве безбедносног функционисања критичне инфраструктуре који се испољавају у домену њихове превенције, одговора и санације.*

Прва посебна хипотеза: Ванредне ситуације нарушавају стални режим функционисања критичне инфраструктуре али истовремено захтевају и

ангажовање свих ресурса критичне инфраструктуре у заштити и спасавању људи, материјалних и културних добара и животне средине у отклањању последица ванредних ситуација.

Друга посебна хипотеза: Нормативно-правни оквир, обученост и потпуна опремљеност ресурса критичне инфраструктуре представља основ њеног ангажовања у условима мирнодопских ванредних ситуација.

Трећа посебна хипотеза: Функционална и организацијска специфичност система заштите и спасавања Републике Србије као и успостављени систем критичне инфраструктуре пружају основ за адекватан одговор на превенцију, одговор, санацију и последице ванредних ситуација.

Четврта посебна хипотеза: Ресурси критичне инфраструктуре у Републици Србији представљају значајну логистичку подршку свим субјектима ангажованим у превенцији, одговору и отклањању последица ванредних ситуација.

1.5. НАЧИН ИСТРАЖИВАЊА

Прелиминарно истраживање има карактер комбинованог теоријско-емпиријског поступка.

Методе истраживања

У овом истраживању су примењене следеће методе:

- Анализа садржаја,
- Историјска метода,
- Компаративна метода,
- Статистичка метода и
- Метода испитивања (коришћена је техника анкетирања).

Искуствена евиденција се прикупља на систематичан начин. Метод **анализе садржаја** коришћен је за проучавање домаће и стране литературе и истраживачких искустава: научно-стручних часописа, стручних књига, монографија, студија, приручника и чланака. Овај метод је незаобилазан и

при проучавању нормативно-правних аката, доступних службених докумената, извештаја и анализа.

Историјска метода је неопходна како би се добила „историјска позадина“ истраживаног проблема и како би се на основу проучаваних искустава у прошлости пронашла перспектива будућих решења.

Компаративна метода - примена ове методе ће омогућити упоредну анализу постојећег стања опремљености и спремности критичне инфраструктуре за деловање у ванредним ситуацијама. Компаративни метод ће омогућити извођење компарације постојећег модела са жељеним решењима која позитивно утичу на целокупан аспект деловања у условима измењених околности.

Статистички метод ће се користити у поступку прикупљања, класификације и статистичке обраде добијених резултата.

Метод **испитивања** користиће се за реализацију емпиријског истраживања, уз примену анкетног упитника.

Анкетирање је техника која ће омогућити да се сазнају многе значајне чињенице (познавање мера, активности, поступака и процедура које треба предузети у измењеним околностима (ванредним ситуацијама). Анкетирана ће бити лица из струке, одговорна лица, руководиоци и др., и то из: Сектора за ванредне ситуације МУП РС, ЈКП „Београдски водовод и канализација“, ЈП „Пошта Србије“, ЈП „Електропривреда Србије“, „Нафтна индустрија Србије а.д.“, ЈП„Електромрежа Србије“, ЈП „Путеви Србије“, ЈВП „Србија воде“ и ЈП „Железнице Србије а.д.“Анкетирање ће бити спроведеном у циљу прикупљања података по унапред припремљеним и формулисаним питањима.[22]

[22]*Истраживањем је било предвиђено анкетирање Министарства грађевинарства, саобраћаја и инфраструктуре, Аеродрома „Никола Тесла а.д.“ и Министарства пољопривреде и заштите животне средине, али је добијен одговор да наведене институције нису надлежне за област од интереса ове докторске дисертације.*

1.6. НАУЧНА И ДРУШТВЕНА ОПРАВДАНОСТ ИСТРАЖИВАЊА

Научна и друштвена оправданост овог истраживања приозилази из циљева који се желе постићи овим истраживањем. Они се огледају у проширивању и продубљивању сазнања о свим питањима везаним за предмет истраживања и имплементирању тих сазнања у теоријски фонд наука одбране, заштите и безбедности.

Научна оправданост истраживања институционалних решења и стварног стања на пољу заштите критичних инфраструктура и њихове заштите огледа се, пре свега, у чињеници да овај проблем није до сада детаљније истраживан у домаћој литератури. Његовим теоријским постављањем, наглашавањем значаја и могућих решења, учинио би се значајан помак у промишљању и заснивању почетног корпуса сопственог теоријског сазнања о критичној инфраструктури и њиховој заштити.

Дескрипција и објашњење класификације критичних инфраструктура, која до сада није постојала у домаћој литератури, такође указују на научну оправданост овог истраживања.

Чињеница да Република Србија у великој мери заостаје у односу на успешније земље у окружењу, при чему је свакодневно суочена са низом најразличитијих ванредних ситуација, праћена је непостојањем одговарајућег институционалног оквира и компаративног увида у најбољу праксу.

Из наведених разлога, успостављање институционалног и нормативног оквира на пољима заштите критичних инфраструктура и управљања ванредним ситуацијама је од круцијалног значаја за функционисање локалних заједница, државе и нормалан живот друштва. Позитивна (као и негативна) искуства појединих земаља у транзицији, уз неопходно прилагођавање условима и специфичностима Републике Србије, значајно би утицало на убрзање закаснелих транзиционих процеса, што је и више него довољан разлог за друштвену оправданост овог истраживања.

Реално је претпоставити да ће резултат овог истраживања представљати

подстрек истраживачима да свестраније истражују корелативност између ефикасног управљања ванредним ситуацијама, ризицима и заштите критичних инфраструктура, чиме ће предмет истраживања бити још свеобухватније сагледан у теорији и пракси.

Глобално, намена рада јесте да изгради реалну слику стања у овој области и пружи смернице за осмишљавање савременог, јединственог и одрживог система функционисања критичне инфраструктуре који ће у организационом и функционалном смислу обезбедити максималну координираност свих субјеката и остварити ефикасност у превенцији и одговору на измењене околности.

2. ТЕОРИЈСКО ДЕФИНИСАЊЕ И КЛАСИФИКАЦИЈА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

2.1. ПОЈАМ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Данас постоје многи радови који расправљају о критичној инфраструктури и сваки од њих наглашава да је она постала веома важан сегмент националне безбедности и безбедности у опште. Људи су постали свесни да не могу да штите све и увек, и да морају да одлуче, која инфраструктура је од кључног значаја за њих и зашто. Заштита критичне инфраструктуре је на раскршћу између политике, бизниса, технологије и ризика. Сви су свесни важности критичне инфраструктуре, али још увек не постоји јединствена листа или дефиниција критичне инфраструктуре и то доводи до различитих приступа када је у питању и сама заштита критичне инфраструктуре.

У последњих десет до двадесет година, питање критичне инфраструктуре је посебно постало значајно. Модерни стил живота и зависност људи и привреде од струје, горива, интернета (комуникације уопште) је сваким даном све већа и већа. Безбедност критичне инфраструктуре је кључно питање савремене националне безбедности[23], јер критична инфраструктура је основа за опстанак заједнице[24], а асиметричне претње постале су уобичајена ствар. Терористички напад од 11. септембра 2001. године у САД, дао је ново значење и нову димензију концепта заштите критичне инфраструктуре. Терористички напади у Мадриду, Лондону, Москви, Мумбаију и Исламабада су само потврдили потребу за новим приступом у заштити критичне инфраструктуре. Поред тога, ураган Катрина у САД, цунами у југоисточној Азији и цунами у Јапану су такође показали да природне катастрофе могу имати разорне последице на инфраструктуру[25].

[23]*Herga, M., Nacionalna kritična infrastruktura, Menadžment i sigurnost - M&S 2010: „Planiranje i сигурност“, стр. 311, 2010.*
[24]*Чемерин, Д., Управљање критичним инфраструктурама, Зборник радова, 4. међународна конференција, „Дани кризног управљања“, Велеучилиште Велика Горица, стр. 442, 2011.*
[25]*Jopling, L., The protection of critical infrastructure, http://www.nato-pa.int/default.asp?SHORTCUT=1165.*

Чак и политичке одлуке могу имати сличне ефекте[26]. Због тога, заштита критичне инфраструктуре је постала један од кључних приоритета Европске уније (ЕУ) у области безбедности. Такође, у Националној стратегији за унутрашњу безбедност САД, из 2007, управљање кризама у природним катастрофама је стављено на врх листе испред терористичких напада[27]. Иста је ситуација и широм света.

У зависности од критеријума а у циљу дефинисања критичне инфраструктуре, постоји потреба за бољим сагледавањем различитих типова критичне инфраструктуре. У принципу, критична инфраструктура може бити од интереса за: државне, регионе или свет, а то значи да можемо говорити о националној, регионалној (европској, афричкој, Евро-Азијској) и светској критичној инфраструктури. С друге стране, у неким државама је могуће говорити о критичној инфраструктури на локалном, регионалном (економског или културног региона у држави), државном (националном) и међународном нивоу.

У зависности од времена потребног за заштитом, критична инфраструктура може бити: стална, привремена или потенцијална. Стална критична инфраструктура је кључна инфраструктура за неке државе, прописана законом, а која мора бити у фокусу све време. У категорију привремене критичне инфраструктуре је могуће уврстити неке политичке или спортске догађаје који су кратки, али који су веома важни за државу или интернационално. За ове инфраструктуре је познато да ће бити важне у неко време године или током неких догађаја. Потенцијална критична инфраструктура је инфраструктура која није у фокусу, али у неким ситуацијама може бити веома важна. За ту инфраструктуру је познато да може постати критична инфраструктура у неким приликама, али ове ситуације се не планирају унапред.

---

[26]*Smedts, B., Disruptions of gas supply from Russia to East Europe during the winter of 2008-2009, Critical Infrastructure Protection Policy in the EU: state of the art and evaluation in the near future, Royal High Institute for Defense, Center for security and defense studies, Focus paper 15, стр.11., 2010.*

[27]*Зутер, Б., Стратешки кризни менаџмент Швајцарске - Поређење швајцарског модела са девет страних референтних држава, Војно дело, Београд, стр.37, 2011.*

Према неким ауторима, критична инфраструктура у односу на власништво унутар једне државе, може бити у поседу: државе, општине, приватног лица, лица за управљање имовиному државном власништву, у власништву правних лица чији су оснивачи локалне самоуправе[28]. С друге стране, то значи да може бити критична инфраструктура у јавним, приватним или јавнио-приватним рукама. Јавно-приватно партнерство је од суштинског значаја, јер се процењује да је преко 85 % од онога што се може класификовати као критична инфраструктура у САД у власништву приватног сектора, а такође се процењује да је у Немачкој преко 90% критичне инфраструктуре у рукама приватног сектора.

Дакле, то значи да су типови критичне инфраструктуре веома различити и зависе од различитих гледишта оних који одлучују шта је критична инфраструктура, као и од структуре и нивоа власти. Али у области заштите критичне инфраструктуре постоји потреба за свеобухватним приступом. То значи да сви нивои власти у држави морају да препознају своју критичну инфраструктуру и предузму мере да их заштите. Ако само један од нивоа није успео да препозна и заштити своју критичну инфраструктуру, то би могло довести до катастрофе, јер је критична инфраструктура међусобно повезана и зависна једна од друге.[29]

Све врсте критичних инфраструктура се морају узети у обзир када се планира заштита критичне инфраструктуре. Велики број врста критичне инфраструктуре значи да сви нивои власти у држави или у неким организацијама, па чак и на светском нивоу, треба да узме свој део посла на заштити критичне инфраструктуре. То је начин како да користе ресурсе на најбољи начин. Мора се успоставити нека врста система за заштиту критичне инфраструктуре, у зависности од нивоа власти и државне структуре. Заштита критичне инфраструктуре је дефинисана као стратегија, политика и спремност, да се заштити, спречи, а када је то потребно и

[28]*Херга, М., Национална критична инфраструктура, Менаџмент и сигурност - M&C 2010: „Планирање и сигурност“, стр. 314, 2010.*

[29]*Чемерин, Д., Трут, Д., Критерије за утврђивање хрватске критичне инфраструктуре, Зборник радова „Хрватска платформа за смањење ризика од катастрофа“, Државна управа за заштиту и спашавање, Загреб, стр. 33, 2010.*

одговори на нападе на ове кључне инфраструктуре и средства.[30]

Не постоји опште решење за све државе везано за заштиту критичне инфраструктуре. Она укључује неколико актера као што су: јавне власти - на државном и локалном нивоу, укључујући и јавне агенције, корисници критичне инфраструктуре, који су често из приватног сектора и становништво у целини. Заштита критичне инфраструктуре је такође све више стекла међународну димензију, која поставља питање међународне сарадње на заштите критичне инфраструктуре. Постоје различите институције одговорне за заштиту критичне инфраструктуре у различитим државама. Одговорност за националну заштиту критичне инфраструктуре у САД има Одељење за унутрашњу безбедност а у Великој Британији постоји слична агенција, Министарство унутрашњих послова, а у Немачкој Центар за заштиту критичне инфраструктуре који је у оквиру Савезне службе за цивилну заштиту и одговор на катастрофе (Министарство унутрашњих послова). Процес глобализације је довео до све веће међузависности и повезаности тржишта и мрежа у једном броју битних сектора као што су енергија, информације и комуникације, храна, превоз, што повећава осетљивост инфраструктуре у сваком од ових сектора. Већина критичних инфраструктура је данас у рукама приватног сектора, који стога сноси главну одговорност за заштиту своје инфраструктуре.

Критична инфраструктура обухвата поједине институције јавног и приватног сектора, канале дистрибуције те „мреже“ особа и информација које гарантују несметан и континуиран проток људи, роба, сервиса, услуга, што је кључно за стабилност економског и безбедносног система земље и има директан утицај на националну безбедност, националну економију, јавно здравље, сигурност становништва и ефикасност деловања власти.

Европска комисија дефинише критичне инфраструктуре као:

- средство, систем или његов део који се налази у државама чланицама који је неопходан за одржавање виталних друштвених функција, здравље,

[30]*Lewis, G.T., Critical Infrastructure Protection in Homeland Security - Defending and Networking Nation, Wiley-Interscience, New Jersey, cmp.8, 2006.*

безбедност, сигурност, економско или социјално благостање људи, као и нарушавање или уништење које би имало значајан утицај на државе чланице због неуспеха да одржавају те функције.

ОЕБС је дао две дефиниције термина „критичност“ и „инфраструктура“, које представљају покушај помирења различитих дефиниција које постоје у државама чланицама. Према овој дефиницији термин **„критична“** се односи на инфраструктуру која пружа кључну подршку за економско и социјално благостање, јавну безбедност и функционисање кључних владиних одговорности, тако да поремећај или уништавање инфраструктуре доводи до катастрофалних последица и велике штете.[31]

Националне дефиниције **„инфраструктура“** се углавном односе на физичку инфраструктуру, а често и нематеријална улагања и/или производњом или путем комуникационих мрежа. Ове дефиниције су веома широке, свакако шире од појма инфраструктуре које се уобичајено користе у другим областима политике (нпр. „суштински објекат“) и завршавају укључујући не само материјална средстава, него и нематеријалне вредности (нпр. софтвер, услуге итд.).

Критичне инфраструктуре су ресурси, системи и мреже, физички или виртуелни, чије уништавање или онеспособљавање може ослабити националну безбедност, економску стабилност и утицати на друге аспекте нормалног функционисања друштва.[32]У групу „критичне инфраструктуре“ убрајају се телекомуникације, електропривреда, складиштење и пренос плина и нафте, банкарство и финансије, транспорт, водоснабдевање, хитна служба (укључујући медицинске, полицијске, ватрогасне и спасилачке службе) и друге институције.

Постоји више дефиниција критичне инфраструктуре, али у принципу све се оне односе на средства и имовину која је кључна за неометано функционисање економије и друштва. Као пример наводе се следеће дефиниције:

[31]*http://www.oecd.org/dataoecd/2/41/40700392.pdf*
[32]*Rinaldi, S.M, Modeling and simulating critical infrastructures and their interdependencies, 2004.*

САД: *„Критична инфраструктура и основни ресурси (Critical Infrastructure and Key Resources - CIKR) је појам који се односи на широк опсег различитих средстава и имовине који су неопходни за свакодневно функционисање друштвених, економских, политичких и културних система у САД. Било какав прекид у елементима критичне инфраструктуре представља озбиљну претњу за правилно функционисање ових система и може довести до оштећења имовине, људских жртава и значајних економских губитака".*[33]

Европска Унија:

(а) *„Критична инфраструктура представља имовину, систем или његов део који се налази на територији земље чланице и који је неопходан за одржавање кључних друштвених функција, здравства, безбедности, сигурности, економског или социјалног благостања, а чије би ометање или уништење имало значајан утицај на земљу чланицу".*[34]

(б) *„Европска критична инфраструктура подразумева критичну инфраструктуру лоцирану на територији земље чланице, чије би ометање или уништење имало значајан утицај на бар две земље чланице. Значај поремећаја у функционисању елемената критичне инфраструктуре треба да се процени на основу критеријума међузависности. То подразумева ефекте настале као резултат међусекторске зависности од других типова инфраструктуре".*

У оквиру Европске уније под термином критичне инфраструктуре подразумевају се постројења, системи или одређене компоненте тих система, који су лоцирани у земљама чланицама и који су есенцијални за обављање основних функција држава и Уније, затим који су неопходни за функционисање здравства, за безбедност чланица и за економско и социјално благостање грађана, а чије би отказивање или ометање функционисања имало знатан негативан утицај на земље чланице, а

[33] *Critical Infrastructure and Key Resources, Cansas City Regional Tew, Interagency Analisys Center.*
[34] *Critical Infrastructure Protection in the Fightagainst Terrorism, Brussels, COM(2004)702, 2004.*

посредно и на читаву Европску унију.[35]

Критична инфраструктура се састоји од физичких и информационих технолошких објеката, мрежа, служби и материјалних добара, који, уколико буду урушени или уништени, могу имати озбиљан утицај на здравље, безбедност, сигурност и економско благостање или ефикасно функционисање власти. Ову дефиницију најчешће користе институције УН у образложењу садржаја појма - критична инфраструктура.

Критична инфраструктура се може схватити као објекат на коме се догађа ванредна ситуација, и као такав представља предмет заштите, али је и средство које омогућава смањивање опасности или олакшава, односно омогућава отклањање последица у ситуацијама када је опасност наступила.

НАТО такође дефинише појам „заштите критичне инфраструктуре“ који обухвата програме, делатности и деловање влада, власника, оператера или корисника предузете са циљем заштите властите критичне инфраструктуре. Осим НАТО, програме заштите критичне инфраструктуре покренули су и Европска унија, Уједињене нације, Клуб осам најразвијенијих земаља, низ регионалних организација и тако даље.[36]

Занимљива је дефиниција Гарба који сматра да *„критичну инфраструктуру представља разграната мрежа независних, већином у приватном власништву, система, капацитета и процеса, који синергијским деловањем омогућавају непрекидну производњу и дистрибуцију основних добара и услуга и чије уништење или квар може да проузрокује озбиљне последице по јавно здравство, безбедност, привредно стање, социјално благостање грађана и функционисање јавног сектора“*.[37]

Гарбова дефиниција се (изузевши концентрисаност на приватну имовину

[35]*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-L 345/82, 2008.*
[36]*Јаковљевић, В., Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама, Зборник радова ФЦО, Београд, 2010.*
[37]*Garb, G., Varnostno upravljanje kritične infrastructure, Magistrsko delo, Fakulteta za logistiko, Celje, 2009.*

која није потпуно разумљива и тиме коректна) приближава дефиницији критичне инфраструктуре у НАТО Савезу и у САД, (такође и у Канади, Финској, Великој Британији као и ОЕБС, која као последицу оштећења или уништења критичне инфраструктуре наводи директан негативни утицај на јавно здравство.

Табела 1. Дефиниције критичне инфраструктуре у различитим земљама

Канада	Критична инфраструктура подразумева систем од свих физичких и информационих технологија, објеката, мрежа, услуга и добара који ако је уништен или онеспособљен за рад може да има озбиљан утицај на здравље, безбедност и добробит Канађана и ефикасно функционисање владе у Канади.
Немачка	Критична инфраструктура обухвата организације и установе од великог значаја за заједницу, чији неуспех или оштећење може изазвати трајан недостатак залиха, велике поремећаје у јавном реду и друге драматичне последице.
Холандија	Критична инфраструктура обухвата производе, услуге и пратеће процесе који, у случају прекида рада или неуспеха, може да изазове велике социјалне немире. Прекид рада би довео до великог броја жртава и велике економске штете.
Енглеска	Национална критична инфраструктура састоји се од средстава, услуга и система који подржавају економски, политички и друштвени живот у Великој Британији чији значај је такав да губитак може да: 1) изазове велике губитке живота, 2) да има озбиљан утицај на националну економију, 3) имају и друге тешке социјалне последице за заједницу.
САД	Општа дефиниција критичне инфраструктуregласи: системи и средства било физички или виртуелни који су од виталног значаја за САД и њихова неспособност или уништење може имати утицај на безбедност, економску сигурност, јавно здравље или било коју комбинацију ових ствари.

Имајући у виду наведена дефинисања појма критичне инфраструктуре, може се закључити да не постоји широко прихваћена дефиниција за критичну инфраструктуру и још увек је то питање сваке државе засебно. Такође, постоје различити критеријуми селекције инфраструктуре за критичну инфраструктуру у зависности од земље порекла и практичног тумачења листе критичне инфраструктуре, а то зависи од саме методологије.

Свака држава или организација мора да дефинише и класификује своју

инфраструктуру и одреди која инфраструктура је критична. Према документима ЕУ критичне инфраструктуре морају бити дефинисане и наведене у свим земљама чланицама и у свим земљама које хоће да постану чланице ЕУ.

2.2. КЛАСИФИКАЦИЈА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Критична инфраструктура обухвата широк спектар виталних сектора, као што су саобраћај, транспорт, производња и дистрибуција енергије, информациони и комуникациони системи, здравствене службе, системи за снабдевање водом и храном, финансијске службе, државна инфраструктура (агенције и организације влада, административни сектор) итд. Делимично или потпуно отказивање ових инфраструктура може да угрози друштво, националну безбедност и да доведе до најразличитијих проблема. Развијене земље, а последњих година и оне мање развијене, настоје да идентификују и анализирају критичне секторе, потсекторе, процесе и објекте коришћењем различитих методолошких и политичких приступа. Невероватна комплексност инфраструктурних система је дефинитивно највећи заједнички проблем свих земаља које су се упустиле у анализирање и идентификовање критичне инфраструктуре, као и оних које покушавају да формирају политику заштите критичне инфраструктуре. О овој комплексности инфраструктурних система говоре многи стручњаци из области заштите критичне инфраструктуре.[38]

Повећана међузависност критичних инфраструктура и већа операциона комплексност учиниле су критичне инфраструктуре посебно рањивим на природне катастрофе и природне хазарде, људске грешке и техничке проблеме, као и на нове облике сајбер-криминала, тероризам и сајбер-ратове. Сваки од ових догађаја може да доведе до озбиљних последица по критичну инфраструктуру, па чак и до потпуног уништења критичне инфраструктуре.

[38]*Lewis, T.,Infrastructure Protection in Homeland Security, Defending a Networked Nation, Wiley Interscience, 2006.*

Велики је број инфраструктурних сектора који истовремено обухватају већи број подсектора, грана индустрије, служби, производних области и имају специфичну вертикалну структуру. Поједина мишљења указују на опасност идентификовања свих инфраструктура као критичних услед нејасних граница између критичне и *некритичне* инфраструктуре. Заједно указују на све јачу међуповезаност критичних инфраструктура (међусекторска повезаност). Све у свему, велики број стручњака је сагласно да бројне ризике, претње и рањивости треба идентификовати пре него што се пређе на идентификовање критичних инфраструктура.[39]

Анализирајући различите приступе дефинисања и класификовања критичне инфраструктуре, може се закључити да она обухвата посебно (не искључиво):

- храну,
- воду,
- пољопривреду,
- здравствене службе и службе хитне помоћи,
- енергију (електрична, нуклеарна, гас и нафта, бране),
- саобраћај (ваздушни, друмски, железнички, луке, пловне путеве),
- информације и телекомуникације,
- банкарство и финансије,
- хемијска постројења,
- одбрамбену индустрију,
- поште и дистрибуцију роба и
- националне споменике и друге културне вредности.

Када се расправља о појимању и класификацији критичне инфраструктуре, веома често се користи Извршна наредба 13010[40], коју је потписао председник Клинтон 1996. године, а која успоставља председничку комисију за заштиту критичне инфраструктуре, односи се на оно што одређену

[39]*Moteff, D.J., Parfomak,P., Critical Infrastructure and Key Assets: Definition and Identification, Congressional Research Service, Library of Congress, 2004.*
[40]*Executive Order 13010 - Critical Infrastructure Protection, Federal Register, Vol. 61, No. 138. pp. 37347-37350, 1996.*

инфраструктуру чини критичном: *„Одређене националне инфраструктуре које су толико виталне да би ометање њиховог рада или уништење имало ефекат слабљења одбрамбене или економске сигурности САД“*.[41]

Према овој извршној наредби, ове инфраструктуре су обухватале:

- телекомуникације;
- системе електричне енергије;
- складиштење и транспорт нафте и гаса;
- банкарство и финансије;
- транспорт;
- системе за снабдевање водом;
- хитне службе (медицинске, полицијске, ватрогасне и за спасавање) и
- континуитет власти.[42]

Уз употребу језика из ове извршне наредбе, коначни извештај комисије упућен председнику САД дефинише критичну инфраструктуру на следећи начин: *„Инфраструктура која је толико витална да би њено онеспособљавање или уништење имало ефекат слабљења одбрамбене или економске сигурности“.*[43]

Извештај комисије такође је дефинисао инфраструктуре сваког сектора који је споменут у извршној наредби:

Банкарство и финансије: Ентитети као што су малопродаје и комерцијалне организације, инвестиционе институције, брокерске куће, трговачке куће и системи резерви, и придружене оперативне организације, владине операције и активности подршке које су укључене у све аспекте монетарних трансакција, укључујући штедне улоге, инвестиције, безготовинске исплате и исплате у форми зајмова и других финансијских инструмената.

Системи електричне енергије: Електране и мреже за пренос и дистрибуцију који производе и снабдевају електричном енергијом крајње кориснике тако

[41] *Ibid. стр. 37347.*
[42] *Оп. Цит.*
[43] *President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructure, 1997.*

да они постижу и одржавају номиналну функционалност, укључујући транспорт и складиштење горива које је неопходно за овај систем.

Хитне службе: Медицинске, полицијске, ватрогасне службе и системи за спасавање, као и особље које је на располагању онда када су појединац или заједница суочени с ванредном ситуацијом. Ове услуге се углавном пружају на локалном нивоу. Осим тога, државни и федерални планови имају функцију у пружању подршке приликом реаговања на ванредне ситуације и санирања њихових последица.

Производња, складиштење и транспорт нафте и гаса: Постројења за производњу и складиштење природног гаса, сирове и прерађене нафте и нафтних деривата, постројења за рафинисање и прераду ових горива, и нафтоводи, бродови, камиони и железнички системи за транспорт ових производа до крајњих корисника.

Информације и комуникације: Компјутерска и телекомуникациона опрема, софтвер, процеси и људи који подржавају:

- прикупљање, обраду, складиштење и пренос података и информација;
- процесе и људе који од података стварају информације, а од информација знање.

Транспорт: Системи за физичку дистрибуцију који значајно доприносе националној безбедности и економском благостању, укључујући системе националног ваздушног саобраћаја, ваздушне линије, ваздухоплове и аеродроме; путеве и аутопутеве, копнена возила; луке, водене путеве и пловила; јавни саобраћај, железнички и аутобуски; цевоводе, укључујући оне за природни гас, нафту и друге опасне материјале; теретну и путничку железницу и сл.

Системи за снабдевање водом: Извори воде, резервоари и постројења за складиштење, водоводи и други транспортни системи, системи за филтрацију, чишћење и прераду воде, цевоводи, расхладни системи и други механизми испоруке који обезбеђују воду домаћинствима и индустријским потрошачима, укључујући системе за рад са отпадним водама и системе за

заштиту од пожара.

Као одговор на извештај комисије, председник Клинтон потписао је 22.05.1998. године председничку директиву бр. 63 (PDD-63).[44] Директива је дефинисала критичне инфраструктуре као „оне физичке и *cyber*(сајбер) системе који су витални за минимално функционисање привреде и владе“. Физичка безбедност обично значи заштиту физичких средстава (укључујући компјутерску опрему) од оштећења изазваног физичком силом као што су експлозије, ветар, ватра и сл.

Сајбер безбедност може такође да означава физичку заштиту сајбер средстава. Међутим, сајбер безбедност означава заштиту и физичких и сајбер средстава од оперативног пада, или од неовлашћеног компјутерског приступа (укључујући и удаљени приступ) оперативном софтверу или подацима. Пружање физичке и сајбер безбедности критичним инфраструктурама захтева широк опсег напора који могу да варирају (од уградње физичких баријера до *firewall* софтвера), док различити појединци или политике могу да говоре о другим активностима.

Према директиви критична инфраструктура обухвата телекомуникације, енергетику, банкарство и финансије, транспорт, системе водоснабдевања и хитне службе (али није било ограничено искључиво на побројане елементе).

Током 2004. године, група научника израдила је упоредну анализу критичне инфраструктуре у шеснаест земаља света, што се може приказати овако:

- банкарство, финансије, телекомуникације, енергија, информациони и телекомуникациони системи у својим листама наводи 14 земаља;
- превоз, логистику, расподелу у својим листама наводи 13 земаља;
- здравствене службе и водоснабдевање у својим листама наводи 12 земаља;
- централна власт/владине службе у својим листама наводи 11 земаља;
- хитне спасилачке службе у својим листама наводи 10 земаља;

[44] *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63, White Paper, May 22, 1998.*

- снабдевање нафтиним дериватима у својим листама наводи 9 земаља;
- информативне службе, медије (радио и ТВ), јавну администрацију у својим листама наводи 8 земаља,
- остала подручја - јачање законодавства, правосуђе, јавни реди национална безбедност, управљање отпадом, полиција, РХБ заштита, војска и војни објекти, системи осигурања, социјалне службе, управљање залихама воде, нуклеарне електране у својим листама наводи 6 до 1 земље.

Анализом ових осам група приоритета у погледу критичне инфраструктуре, лако је извући закључак да дефиниција критичне инфраструктуре и њен садржај не може бити идентичан у сваком делу света па је и логично да се та дефиниција и садржај мора утврдити на националном нивоу.[45]

[45] *Оп. Цит.*

Табела 2. Индикативна листа критичне инфраструктуре[46]

Канада	Велика Британија	Сад	Немачка	Шведска	Норвешка	Холандија	Швајцарска
Енергија (објекти електричне и нуклеарне енергије, природни гас производни и транспортни системи)	Енергија	Енергија	Енергија (електрична, нафта и плин)	Енергија	Енергија и објекти	Енергија и објекти	Објекти и службе
Комуникације	Телекому-никације	Информације и телекому-никације	Телекомуни-кације и Информацијска инфра-структура	Телекомуни-кације	Снабдевање нафтом и гасом	Телекомуни-кације	Телекомуникације
Сервиси (финансије, дистрибуција хране, јавно здравство)	Здравстве-не службе	Здравство	Здравство	Електронске информа-ционе службе	Телекомуни-кације	Здравство	Дистрибуција информација
Транспорт (ваздушни, морски, копнени)	Финансије	Храна	Банкарство и финансије	Здравство	Здравство	Храна	Здравство
Сигурност (нуклеарна сигурност, службе спашавања, хитне службе)	Транспорт	Пољопривре-да	Транспортни системи	Храна	Банкарство и финансије	Банкарство и финансије	Храна
Влада (службе, информац. системи и мреже	Хитне службе	Банкарство и финансије	Хитне и спасилачке Службе	Банкарство и финансије	Транспорт	Транспорт	Финансије
/	Средишња власт	Хитне службе	Властијавнеслу жбе (полиција, царина и оружане снаге)	Транспорт	Спасилачке службе	Јавнореди сигурност	Транспорт
/	Вода	Власт	/	Вода	Одбрана	Власт	Цивилна одбрана
/	/	Обрамбена индустрија	/	Друштвене вредности	Полиција	Одбрана	Администрација
/	/	Вода	/	/	Друштвена сигурност	Правосуђе	Војнаодбрана
/	/	Хемијска индустрија	/	/	/	Пијаћавода	Снабдевање водом
/	/	Поште и достава робе	/	/	/	Управљање водама	Социјална сигурност
/	/		/	/	/	Друштвени сектор	Индустрија
/	/	/	/	/	/	Објекти високог ризика у ванредним ситуацијама	Истраживање и образовање

[46]*Кљаић, З., Манцука, С., Шкорпут, П.,Примјена ICT у управљању критичном инфраструктуром у транзицијским земљама, 18. Телекомуникациони форум ТЕЛФОР 2010, Београд, 23.-25.11.2010. год.*

3. УГРОЖАВАЊЕ, ЗНАЧАЈ И МЕРЕ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

3.1. ПРЕТЊЕ И РИЗИЦИ У КРИТИЧНОЈ ИНФРАСТРУКТУРИ

Идентификација и процена ризика у критичној инфраструктури је најважнији корак у стварању успешне стратегије унапређења безбедности и њихове заштите.

Идентификовање ризика подразумева процес проналажења, прописивања и карактерисања елемената ризика релевантних за циљеве управљања, односно процену ризика. Неопходно је идентификовати изворе ризика, догађаје или низ околности, као и њихове потенцијалне последице. Свеобухватна идентификација и регистровање ризика је од суштинске важности јер се ризик, који у овом стадијуму није идентификован, искључује из даље анализе. Идентификација би требало да укључи све ризике без обзира на то да ли су под контролом или нису.[47]

Када говоримо о ризицима у критичној инфраструктури свакако треба обухватити чиниоце који могу довести до угрожавања безбедног функционисања критичне инфраструктуре и нормалног обављања дужности од стране оператера, као и власника КИ, социјалну климу и интерперсоналне односе између свих људи неопходних за функционисање КИ, као и обезбеђеност објеката, техничких и информационо-комуникационих система и осталих средстава, и правила функционисања самог процеса КИ. Такође, треба водити рачуна о томе да су ризици међусобно условљени и испреплетени и да промене временских, просторних и фактора средине, односно окружења доводе до појаве нових и промене постојећих ризика.

Другим речима, ризици су варијабилна категорија, тако да редуковање једне врсте ризика може да доведе до настајања новог или до повећања вероватноће остварења другог ризика, што не би требало занемарити у

[47] *Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д.,Процена ризика у заштити лица, имовине и пословања, Центар за анализу ризика и управљање кризама, Београд, 2011.*

процесу анализе, идентификације и класификације ризика. Треба напоменути да приступ идентификацији и класификацији ризика мора бити заснован на објективности, систематичности и непристрасности, с тим да је пожељно узети у обзир субјективне доживљаје свих одговорних за нормално функционисање КИ о степену и врсти угрожавања, па је препоручљиво процес идентификације и класификације ризика прилагодити специфичностима једне КИ, њеног окружења и локалне заједнице. У идентификовању и класификовању ризика врло су битне релевантне и ажуриране информације и посебна стручна знања.[48]

Могуће опасности и процена ризика од елементарних непогода и других несрећа разврставају се, у зависности од узрока настанка, на: сеизмичке, хидросферске, атмосферско метеоролошке, биосферске и техничко-технолошке. Евидентирање карактеристика потенцијалних опасности врши се за сваку потенцијалну опасност посебно, а према могућим величинама, према следећем:

- Величина 1 - минимална опасност,
- Величина 2 - мала опасност,
- Величина 3 - средња опасност,
- Величина 4 - велика опасност и
- Величина 5 - максимална опасност.

Након завршетка прелиминарне анализе потенцијалних опасности од елементарних непогода и других несрећа, врши се анализа ризика, која резултује детерминисањем нивоа ризика.

Ниво ризика, који може бити у границама од минимално 1 до максимално 25, добија се као производ степена вероватноће и степена последица.

Степеновање величине вероватноће које одговара степену вероватноће, врши се на следећи начин:

1 - немогуће, 2 - невероватно, 3 - вероватно, 4 - скоро извесно и 5 - сигурно.

[48] *Оп. цит.*

Степеновање последица које одговара величини последица, врши се према следећем:

1 - Минималне, 2 - Мале, 3 - Умерене, 4 - Озбиљне и 5 - Катастрофалне.

На основу одређеног **нивоа ризика** врши се класификација ризика у категорије од најниже (прва) до највише (пета) а потом одређује који су ризици прихватљиви, а који нису.

Прихватљиви ризици су ризици прве, друге и треће категорије док су ризици четврте и пете категорије неприхватљиви. На основу листе прихватљивих и неприхватљивих ризика дефинише се листа приоритета за третирање.

Класификација безбедносних претњи и ризика по критичну инфраструктуру може се извршити на више начина. Тако, на пример, могуће их је на основу порекла поделити у три изоловане категорије:[49]

Елементарне непогоде, грешке унутар система инфраструктуре, које се могу даље према пореклу узрока поделити на:

- оне до којих доводи људски фактор - лоше планирање активности у оквиру сектора, несмотреност оператера критичном инфраструктуром, неадекватна кооперација или координација активности и
- оне до којих долази из техничко-технолошких разлога - отказивања машина, дефектан драјвер или грешке у софтверу који се користи у оквиру неког инфаструктурног сектора.

Напади на систем критичне инфраструктуре се деле на физичке (директни терористички напади и саботаже) и виртуелне (сајбер-напади). Такође, у оквиру ове категорије могли би се као претња рачунати и могући ратни сукоби.

[49] *La Porte, T.R., Critical Infrastructure in the Face of a Predatory Future: Preparing for untoward surprise, Vol. 15, No.1, 2007.*

3.1.1. Природни облици угрожавања

Природне катастрофе све озбиљније угрожавају безбедност савременог човечанства. Не само да је, последњих деценија евидентан тренд повећања броја природних катастрофа, него је присутно и повећање њихове деструктивности. То за последицу има и повећане људске губитке, материјалну и нематеријалну штету. Уз то, угрожавањем критичне инфраструктуре онемогућава се или ограничава реализовање виталних државних функција (вршења власти, здравствене, просветне, енергетске, економске, социјалне и уопште безбедносне функције), што се додатно рефлектује на безбедност држава и грађана. И без обзира на технолошко напредовање човечанства, друштва су све угроженија. Јасно је да се ванредне ситуације и катастрофе и њихов утицај на људе и критичну инфраструктуру не могу спречити, али се могу унапредити механизми предвиђања и раног упозоравања на катастрофе, односно повећати отпорност и способност за бржу и ефикаснију ревитализацију угрожених вредности и добара.

Осим од степена деструктивности, стратегија реаговања у насталој ванредној ситуацији зависиће и од врсте катастрофе, али и од врсте критичне инфраструктуре и конкретних добара и вредности које су угрожене.

Поплаве, земљотреси, олујни ветрови, клизишта, снежне падавине, градитд. представљају природне облике угрожавања који своја негативна дејства могу да испоље својом великом природном снагом.

Природни извори који могу угрозити систем критичне инфраструктуре РС су и земљотреси чије је дејство испољено више пута у највећој разорности која је довела до оштећења.

Земљотрес спада у ред најразорнијих геофизичких природних катастрофа. То је изненадно подрхтавање земљине коре. Сам удар земљотреса је изненадан, скоро да не постоји упозорење, због чега га је немогуће предвидети. Услед њега долази до оштећења насеља, зграда, конструкција и инфраструктуре, нарочито мостова, надвожњака, железничких пруга, водних торњева, цевовода, објеката за производњу електричне енергије, те до

дестабилизовања власти, економије и друштвене структуре земље.[50] Накнадни удари земљотреса могу да узрокују већа оштећења већ ослабљених конструкција. Секундарни ефекти подразумевају пожаре, пуцање брана и одроне који могу да блокирају копнене и водне путеве и да узрокују поплаве. Може доћи до оштећења објеката у којима се користе или производе опасне материје, што резултује цурењем хемикалија. Такође, може доћи до кварова објеката за комуникацију. Последице земљотреса су разноврсне. Постоји велики број жртава због лошег пројектовања зграда и система критичне инфраструктуре. Од укупног броја лица која су погинула у земљотресима, њих 95 % је изгубило живот због рушења зграда.[51] При томе, огромне су штете у области јавног здравственог система, транспорта, комуникација и снабдевања водом у погођеним подручјима.

На пример, земљотрес који је јануара 1995. године погодио град Кобе у Јапану, изазвао је следеће последице по критичну инфраструктуру: 240.000 зграда је уништено; 1,3 милиона људи је остало без воде; 2,6 милиона људи је остало без електричне енергије; 860.000 људи је остало без снабдевања гасом; 300.000 телефонских уређаја је било уништено; ауто-путеви и железничке пруге су биле уништене; штета на мрежи за снабдевање гасом била је следећа: 26.459 станица средњег притиска је било уништено, било је потребно 15 часова да се заустави цурење система са гасом и 85 дана је утрошено на реконструкцију гасоводне мреже.[52]

Тако је и земљотрес, који је задесио Краљево 03.11.2010. године, озбиљно угрозио критичну инфраструктуру. Тог дана у граду није било грејања, а делимично и струје, вода се није препоручивала за пиће. Породилиште је било поплављено, у Клиничком центру „Студеница“ нису радиле операционе сале, док су у продавницама попадали рафови и полице, па је снабдевање грађана било веома отежано. Услед потреса, мобилна телефонија у Краљеву је била у прекиду. У селу Витановац је, од укупно 850 домаћинстава, страдало

[50] *Edward, B., Natural Hazards, 2nd Edition, Cambridge, University Press, 2005.*
[51] *Murray, T., Critical Infrastructure Protection: The VulnerabilityConundrum, Telematics and Informatics, Vol. 29, No. 1, 2012.*
[52] *Bimal, P., Environmental Hazards and Disasters Contexts, Perspectives and Management,Cansas State University, Wiley - Blackwell, 2012.*

око 70 % објеката. У Матарушкој Бањи неколицина кућа је било оштећено и напукло. У Краљеву су улице биле прекривене комадима стакла, бетона и малтера, што је онемогућило нормално одвијање саобраћај. Процењује се да је укупна штета била милион евра.

3.1.2. Спољни облици угрожавања

Оружана агресија као спољни облик угрожавања безбедности земље па представља озбиљан облик угрожавања.

Обавештајно извиђачка делатност - може бити и унутрашњи и спољни облик угрожавања а најчешће је комбинован. Изводе се са циљем прикупљања што више тачних података о стању привредног друштва, намерама руководећег кадра, свим слабостима у систему привредног друштва, процедурама за деловање у различитим ситуацијама, стање опреме, задовољство запослених, поделе међу запосленима, подаци о запосленима техничка документација о техничко-технолошком процесу делатности и сл. Остварују се преко страних обавештајних служби или дипломатских, привредних представника, разних добротворних, мировних, хуманитарних и других организација под формом сарадње са предузећем. Следећи начин је свакако и врбовање запослених за остварење тих циљева преко поткупљивања, уцењивања, условљавања, довођења пред свршен чин и сл. Имајући у виду веома разгранату мрежу оваквих служби као и ниску безбедносну културу наших радника процена је да су овакви видови деловања веома могући. Прибављање наведених информација поред наведеног може бити и насилним путем (проваљивање у просторе где се налазе информације, хакерисањем и скидањем података са рачунарске мреже) или разним врстама превара (лажно представљање, фалсификовање докумената и сл. јер су начини превара неисцрпни).

Диверзантско-терористичка дејства као најгрубљи облик субверзивне делатности против неке земље представљају добро осмишљене и припремљене активности које се изводе тајно са циљем наношења великих губитака противничкој страни како би се остварили сопствени политички,

војни или други циљеви. С обзиром на савремене карактеристике ДТД као и на значај ППВ у систему водоснабдевања исти је могућа мета ових активности.

3.1.3. Унутрашњи облици угрожавања

Саботажа представља смишљену прикривену делатност запослених појединаца или група са циљем изазивања материјалне штете привредном друштву.

Поред претходно поменутих мотива, у последње време великих међупартијских, синдикалних и многих других подела, мотиви могу бити и политичке или синдикалне природе са циљем слабљења условно речено противничке групације која је тренутно на власти.

Саботери те активности увек раде прикривено како би они остали неоткривени као извршиоци, а узрок застоја када се открије био приписан претходно поменутим разлозима. Као саботери могу се појавити радници који непосредно раде на тим пословима где се саботажа догодила али могу бити и други радници или руководиоци који имају приступ тим местима. Саботаже су могуће и на свим другим деловима система. Управо овде долази до изражаја основна карактеристика саботаже (најбољи извршиоци саботаже су најбољи познаваоци система), тако да су начини извођења и облици остварења препуштени машти и знању извршиоца.

Криминалитет као облик угрожавања, упркос различитим дефиницијама могли бисмо окарактерисати као негативно друштвено понашање које се манифестује као укупност свих кривичних дела у посматраном временском периоду. У претходној анализи појава из области криминала анализиране су крађе и разни облици инкриминисаних радњи као облици унутрашњег или спољног угрожавања. Без обзира о ком облику криминалитета или инкриминисане радње се ради начини остварења дела су исти и за њих се може рећи да теку по устаљеним правилима. Поред крађа које се врше насилним путем (обијање, коришћење специјалног алата за отварање брава и сл.) и које су само спорадично забележене у претходном периоду, све

остале крађе настале су као последица неодговорног односа запослених према имовини предузећа. Познато је да за незаштићеном имовином поред радника са таквим склоностима могу да посегну и они који то никада раније нису чинили. Мотиви свих ових дела су углавном прибављање имовинске и материјалне користи за извршиоце.

Извршиоци могу бити из свих структура запослених а посебно су интересантни радници на руководећим функцијама који својим чињењем чине много већу штету предузећу, а с обзиром да су постављени на та места од стране актуелног руководства.

Асоцијална - преступничка понашања представљају сва она понашања која изазивају негативну реакцију већине запослених и која су у супротности са обичајним и моралним нормама понашања и нису санкционисана законом. Оваква понашања се још називају и социо-патолошке појаве.

Асоцијална понашања су посебно опасна јер могу бити узрок многих кривичних дела, акцидената, пропуста у раду, пожара и многих других опасности којима могу бити угрожени.

Једну од тешкоћа приликом сваког покушаја класификације ризика за критичну инфрструктуру представља чињеница да је број претњи које могу угрозити КИ практично неограничен, због чега их је веома тешко све предвидети. Другим речима, свакој класификацији се може замерити одређени степен непотпуности. Зато идентификација претњи захтева наглашену опрезност будући да се претња која није била идентификована често може показати као катастрофална. Из тог разлога се поставља и питање избора адекватног методолошког приступа, посебно зато што у вези са овим проблемом ни на нивоу теорије још не постоји јединствено решење. Са друге стране, неизбежно је разврставање безбедносних претњи у групе које, у извесном смислу, представљају логичке целине јер то омогућава њихову анализу, што је неопходан корак за формулисање сваке политике заштите.

3.2. ЗНАЧАЈ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

Значај ресурса критичне инфраструктуре за живот модерног човечанства је неоспоран. У измењеним околностима у највећем броју случајева долази до оштећења и застоја на инфраструктурним постројењима, што ремети устаљен начин снабдевања становништва, привреде, и осталих корисника. С друге стране, застој у свакодневном функционисању инфраструктурних система може довести до ванредне ситуације. Приоритет у овим околностима јесте да се спаси живот на првом месту, али и нужност заштите критичне инфраструктуре.

Последице угрожавања и уништавања критичне инфраструктуре могу се огледати у следећем:

- губитак живота и имовине,
- прекид деловања значајних служби за производњу,
- губитак посла и основних средстава за живот,
- уништавање комуналне инфраструктуре,
- прекид уобичајеног начина живота и
- последице на животну средину, здравствене, социјалне и психолошке последице.

На питање зашто је заштита критичне инфраструктуре значајна и актуелна, одговор је следећи: екстремни ванредни догађаји су све учесталији, расте број потенцијалних облика угрожавања а пре свега објекти критичне инфраструктуре су све више повезани, међузависни и рањиви. У отклањању последица ванредних ситуација, великих несрећа као и терористичких напада, критична инфраструктура је кључни елемент на којем треба отклонити штету и оспособити за функционисање, елемент који представља инструмент за отклањање последица истих.

Критичне инфраструктуре од виталног су значаја за нормално функционисање друштва и држава. Инциденти, несреће или намерно ометање нормалног функционисања инфраструктура може да остави озбиљне последице по економију и да спречи на дужи или краћи период рад

инфраструктуре, што се може одразити на велики број људских делатности. Бројни су разлози због којих инфраструктура мора бити добро обезбеђена и заштићена.

Неки од разлога су ***терористички напади*** (ситуације кад једна особа или група људи намерно напада инфраструктуру из политичких или идеолошки разлога - напади на Светски трговински центар у САД 2001. године, бомбашки напади у лондонском метроу (2005. године) и у Мадриду (2004. године), бомбашки напад на аеродрому Домодедово у Русији (2011. године), бомбашки напади на главној железничкој станици у Мумбаију 2008. године), *саботаже* (ситуације када једна особа или организована група (нпр. бивши запослени на некој инфраструктури, политички противници Владе или групе за заштиту животне средине предузимају напад током ког преузимају контролу над функционисањем кртичне инфраструктуре), *информационо ратовање* (приватни корисници - хакери или пак читаве државе могу из различитих разлога да нападају информационе системе у разним земљама и да доведу до великих проблема не само у функционисању информационе инфраструктуре већ и многих других сектора, с обзиром на то да се многи ослањају на информационе системе - такви су били сајбер-напади током 2008. године, тј. током рата у јужној Осетији), *природне катастрофе* (урагани и природни догађаји оштећују инфраструктуру попут цевовода, мрежа снабдевања водом и храном и сл., такав је био ураган Катрина).

Посебно је важна улога објеката критичне инфраструктуре у ванредним ситуацијама:

- Производња и дистрибуција електричне енергије (хидро и термоелектране, далеководи, трафостанице);
- Производња и снабдевање енергентима (рафинерије, налазишта нафте, складишта гаса, нафтних деривата, магистарални нафтоводи и гасоводи);
- Телекомуникације (преносни путеви, фиксна и мобилна телефонија, централе);
- Производња и снабдевање питком водом (изворишта и фабрике воде, дистрибутивни центри);

- Производња и снабдевање храном (производни погони за производњу хране);
- Здравствена заштита (здравствене установе и објекти);
- Материјална и културна добра (музеји, позоришта, културно-историјски споменици) и
- Национални паркови.

Имајући у виду важност инфраструктуре једне државе, њену употребну вредност и значај за развој и унапређење сваке заједнице, као приоритетан задатак сваког друштва се намеће рационално и ефикасно управљање овим јавним добрима. То се може постићи само доследним поштовањем и спровођењем дугорочне државне стратегије развоја, унапређења и заштите инфраструктурних система.

Ефекат на друштво у случају прекида рада инфраструктуре може бити директан и индиректан. Директна штета односи се на моменталне ефекте отказивања инфраструктуре на становништво, економију, јавност и окружење. Процена штете врши се на основу три претпоставке: потпун прекид функционисања инфраструктуре, непостојање противмера, непостојање сценарија. Прва претпоставка је да се инфраструктура суочава са потпуним прекидом функције или са тоталним уништењем. У стварности то је скоро немогуће, али је с друге стране то једини добар начин да се утврди улога конкретне инфраструктуре за друштво.

Друга претпоставка је да процена треба да се обави без претходне примене мера заштите. У стварности и то је скоро немогуће и увек постоји одређени скуп мера заштите, које имају задатак да спрече претњу и отказивање инфраструктуре. Ипак, узимање у обзир свих могућих и потенцијалних мера заштите инфраструктуре учинило би процену значаја инфраструктуре по друштво немогућом.

Трећа претпоставка је да процена значаја неке инфраструктуре по друштво треба да се ради без разматрања било каквог сценарија. Процена претњи и рањивости у пракси је углавном заснована на процени различитих сценарија. Ипак, у овом конкретном случају се никакав сценарио не узима у обзир и није

важан. Важна је чињеница да је инфраструктура у потпуности престала да функционише. Процена негативних ефеката по друштво не укључује директне последице догађаја који су били окидач за престанак рада инфраструктуре, већ само последице нефункционисања инфраструктуре. На основу три наведене претпоставке добија се процена директне штете по друштво у случају престанка рада инфраструктуре, односно процена апсолутног друштвеног значаја одређеног инфраструктурног сектора.[53]

Колика је значајна КИ говори и то да националне КИ једне државе, у данашње доба су у све већој мери повезане са КИ тог истог типа у другим државама. Ефекти великих кварова и отказивања инфраструктура у једној држави могу да се пренесу на друге суседне државе, па чак и даље од тога. Стога, националне КИ представљају део јако комплексне међународне мреже. Баш из тог разлога се Европска унија током последњих пар године озбиљно бави питањима прекограничних ефеката отказивања и кварова КИ.

Улога КИ као и међузависност између сектора из дана у дан расте. Велики број истраживања указују на то да сектор енергетике и сектор информационих и телекомуникационих технологија играју најбитнију улогу међу критичном инфраструктуром и да скоро сва остала КИ зависи од ових сектора. Зимерманова база података из 2004. године[54] о крос-секторским инцидентима у САД за период од 1990. године до 2004. године показала је да неке КИ више и чешће утичу на функционисање других, него што друге КИ утичу на њих.[55]

Следећи типови инфраструктурних система су изузетно значајни током ванредне ситуације:

- јавне услуге (болнице, полицијске станице, ватрогасне станице, центри за снабдевање храном итд.);
- вода (извори воде и канализациона мрежа);

[53]*Lewis, T., Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley Interscience, 2006.*
[54]*Zimmerman, R., Decision-making and the Vulnerability of Interdependent Critical Infrastructure, IEEE Control Systems Magazine, pp. 23, 2004.*
[55]*Pereboom, J.,Infrastructure Interdependencies: Overviews of Concepts and Terminology, Infrastructure Assurance Center.*

- саобраћај (путеви, пруге, аеродроми и луке);
- телекомуникације и
- извори енергије (струја, гас, бензин итд.).

У оквиру једног инфраструктурног система, нема свака структура или подсистем исту важност за одржавање функционалности читавог система. Током катастрофе не мора сваки јавни сервис, тј. услуга да функционише у оном обиму као када су у питању нормални услови: нпр. за одржавање система јавног здравља у току ванредних периода нема свака болница исту важност или подједнаке капацитете када су у питању хитне или ванредне ситуације.

Физичка рањивост подразумева рањивост инфраструктурних елемената, као што су путеви, зграде, пруге итд. Уколико је посебно рањива инфраструктура сконцентрисана на једном месту, то може значајно да утиче на степен оштећења уколико дође до неког катастрофалног догађаја, било да су у питању последице природних хазарда или хазарда неког другог порекла. Ови догађаји могу имати различите потенцијалне утицаје на инфраструктуру, у зависности од врсте догађаја, његове локације, као и делова инфраструктуре који се налазе на том месту.

Витални друштвени сектори су међусобно повезани и зависе једни од других, што доводи до стварања нових рањивости. Ометање функционисања једног сектора може да утиче и на функционисање других сектора, а такође важи и обрнути случај (међузависност). Истраживања у овој области указују да таква међузависност између сектора из дана у дан расте, да та међуповезаност постаје хијерархијски структурирана и мултикатегоријска. Врсте међузависности су:

- Физичка међузависност (повезаност инпута и аутпута, производ једне инфраструктуре неопходан је за функционисање друге);
- Сајбер међузависност (стање једне инфраструктуре зависи од информација пренесених кроз информациону инфраструктуру);
- Географска међузависност (један или више елемената инфраструктура су физички близу тако да догађај као пожар ремети обе инфраструктуре);

- Логичка међузависност (реципрочни ефекти јављају се на две или више инфраструктуре без физичке, сајбер или географске међузависности, јављају се финансијски губици).

Међусекторски приступ заснован је на претпоставци да се идентификовање виталних инфраструктурних сектора може постићи испитивањем одређеног броја кључних критеријума који се постављају пред сваки сектор:[56]

- Перцепција претњи, рањивости и ризика од стране одговорних менаџера, власника и оператера инфраструктуре,
- Предвиђена штета по друштво коју би изазвало отказивање инфраструктурног сектора,
- Временски период који протекне од тренутка кад дође до престанка функционисања инфраструктуре до тренутка настанка ванредне ситуације,
- Прекограничне последице престанка функционисања инфраструктуре,
- Међузависност инфраструктурних сектора,
- Критични објекти и географска област у којој су концетрисани,
- Одговорност менаџера, власника и оператера инфраструктуре,
- Власништво над инфраструктуром,
- Законске основе,
- Спроведене и планиране безбедносне мере.

Ови критеријуми су заправо најважније карактеристике критичних инфраструктура које треба анализирати.

Подаци о овим критеријумима представљају за сваку државу кључне улазне податке на основу којих се формира политика заштите критичне инфраструктуре у ванаредним ситуацијама.

[56] *Rinaldi, S.M., Modeling and simulating critical infrastructures and their interdependencies, 2004.*

3.3. МЕРЕ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Заштита критичне инфраструктуре у ванредним ситуацијама се може посматрати као део јединственог процеса превенције и одговора на ванредну ситуацију.

У том контексту, организација успоставља, примењује и одржава процедуре за идентификовање потенцијалних инцидената који могу негативно утицати на неку организацију, њене активности, функције, услуге, заинтересоване стране и окружење. Ове процедуре имају за циљ заштиту живота, имовине, спречавање прерастања инцидента у ванредну ситуацију или катастрофу, скраћивање времена прекида операција или активности организације, опоравак најважнијих активности организације, повратак на редовне активности и заштита имица и репутације организације.

Последично, развијене земље улажу пуно ресурса у истраживање могућности и модела заштите. Заштита представља спремност, одбрану, умањење, одговор односно опоравак од поремећаја или уништења критичне инфраструктуре. То су активности власника, оператора, произвођача, корисника и регулаторних власти, са циљем очувања перформанси критичних инфраструктура. Методологија процеса заштите критичних инфраструктура може да садржи следеће елементе:

- прецизна идентификација критичних инфраструктура и њихова дефиниција;
- утврђивање опасности које прете датим критичним инфраструктурама;
- анализа рањивости/осетљивости оних инфраструктура којима прети опасност, и то оних које доприносе прекиду у случају:

а) намерних напада;

б) природног или случајног догађаја;

- процена ризика од деградације или губитка критичне инфраструктуре и приоритизација оних које су у опасности и рањиве;

- примена контра мера тамо где је ризик неприхватљив, како би се штитиле способности да инфраструктуре ефикасно обављају активности у хитним ситуацијама.[57]

Процедуре су прилагођене потребама организација и односе се на: природу хазарда; карактеристике окружења и хазарда са потенцијалним утицајем на организацију; највероватнији тип и размеру инцидента; одговарајући метод за ублажавање и одговор на инцидент да би се спречило његово прерастање у ванредну ситуацију или катастрофу; процедуре командовања и контроле у ланцу командовања, оперативном центру и резервним локацијама, процедуре и овлашћење за проглашавање ванредне ситуације, иницирање процедура, активирање планова и активности, процену штете и одлуке везане за финансије; планове комуникације; процедуре за обезбеђење медицинске помоћи; активности у циљу умањења људских, материјалних и других губитака; заштите виталних информација, информационих система; успостављање и евалуација корективних мера после инцидента; периодична увежбавања одговора на инциденте; обука персонала за управљање ванредним ситуацијама; листа и основне информације о кључном персоналу и агенцијама (службама) надлежним за пружање помоћи у ванредним ситуацијама.[58]

Карактеристике, бројност и последице ванредних ситуација на критичну инфраструктуру захтевају од друштва и државе спремност у предузимању контрамера за првенствено спречавање ванредне ситуације и елиминисање њихових последица уколико је могуће.

Заштита критичних инфраструктура се дефинише као стратегија, политика и спремност која је неопходна да се одврати или спречи напад, односно пружи одговор у случају да дође до напада на критичне инфраструктуре. Заштита критичних информационих инфраструктура представља програме и активности реализоване од стране власника, корисника, оператера, научно-

[57] *Ribeiro, S.L., Bezerra, E.K., Nakamura, E.T., Critical infrastructure in Brazil, 1st IEEE International Workshop on critical infrastructure protection, 3-4th Nov 2005, Darmstadt, 2005.*
[58] *Liscouski, R., Infrastructure Protection, Dept. of Homeland Security, Testimony before the House Select Committee on Homeland Security; Infrastructure and Border Security Subcommittee, 2004.*

истраживачких институција, влада, регулаторних тела с циљем одржавања перформанси критичних информационих инфраструктура у случају отказа, напада или инцидената и минимизирање последица и времена опоравка.

Политика заштите критичне инфраструктуре није ограничена искључиво на обезбеђивање непосредног и ефикасног одговора у случају прекида. Напротив, евидентно је постојање одређених фаза у циклусу заштите критичне инфраструктуре, које комбинују поступке превенције и одговарајућег третмана.[59] Уколико дође до одређених проблема у критичним инфраструктурама те мере би морале бити усмере ка осигурању благовремене реакције и ефикасно управљање кризама.[60]

Досадашња пракса у САД је довела до идентификације три главне фазе циклуса заштите критичне инфраструктуре, које се дешавају пре, за време и после неког догађаја који могу угрозити или деградирати инфраструктуру. Ове три фазе представљају оквир за свеобухватно решење за инфраструктуру квалитета:

- **фаза 1 (анализа и процена):** Анализа и процена фаза представља темељну активност и најважнија је фаза животног циклуса у заштити критичне инфраструктуре. Ова фаза идентификује имовину или функције које су апсолутно критичне за успех мисије и одређује средства/или функције слабе тачке, као и њихове међузависности, конфигурације и специфичне карактеристике. Таква процена садржи анализиране утицаје везане за губитак или деградацију одређене инфраструктуре.
- **фаза 2 (санација):** Фаза санације (ремедијације) подразумева превентивне мере и радње које се предузимају пре него што дође до нежељених догађаја. Засноване су на фиксирању свих познатих сајбер опасности и физичке рањивости које могу довести до прекида функција. На пример, поступци ремедијације могу обухватити области образовања, оперативне процесе, процедуралне промене и конфигурације система.

[59] *Infrastucture Protection, grupa autora, Springer a.g., Library of Congress Control Number 2007938897, ISBN 978-0-387-75461-1.*
[60] *MurrayT.G., Critical infrastructure protection: The vulnerability conundrum, Telematics and Informatics, Vol. 29, No. 1, 2012.*

- **фаза 3 (индикације и упозорења):** Фаза индикације и упозорења (пре и/или за време догађаја) подразумева праћење процене способности осигурања имовине критичне инфраструктуре. Индикације представљају припремне радње које указују да ли је догађај вероватан или се планира његово дешавање. Индикације су засноване на улазним подацима тактичког, оперативног или стратегијског нивоа.

3.4. КЉУЧНИ ФАКТОРИ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Током година, а посебно током протекле деценије, у области заштите критичне инфраструктуре се појавило више различитих и специјализованих субјеката, који имају веома важну улогу:

- **Влада.** Одговорност за координацију политика везаних за заштиту критичне инфраструктуре у првом степену је у надлежности владе. На националном нивоу, министри надлежни за унутрашњу безбедност су одговорни за координацију политике у тој области.
- **Специјализоване екипе за одговор.** Свака земља која има политику за заштиту критичне инфраструктуре поседује одговарајуће тимове за реаговање у ванредним ситуацијама. У зависности од земље, назив може бити замењен синонимима као што су: *CERT/CC* (*Computer Emergency Response Team/Coordination Centre*), *CSIRT*[61] (*Computer Security Incident Response Team*), *IRT* (*Incident Response Team*) и *SERT* (*Security Emergency Response Team*). Тако је *CERT* проширио своје капацитете до постизања пуне безбедносне услуге, укључујући и превентивне услуге: одговарајућа упозорења, сигурносни савети, обука и услуге управљања у области безбедности. Термин *CERT*је заштићена ознака *CarnegieMellonCERT*, првог *CERT*формираног у свету. Крајем 1990. године је дефинисан нови термин *CSIRT*. Тренутно су оба ова термина (*CERT* и *CSIRT*) синоними, с тим што је термин *CSIRT доста прецизнији у детерминолошком смислу*.

[61]*Computer Security Incident Response Team An Overview, Global Cyber Security Capacity Centre, University Of Oxford, 2014.*

4. ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ЕВРОПСКОЈ УНИЈИ И ДРУГИМ ДРЖАВАМА

Европска унија је један од кључних фактора на међународном нивоу кад је у питању заштита критичне инфраструктуре. Покренула је низ иницијатива и истраживачких програма како би се проучили различити аспектипретњи и заштите по критичну инфраструктуру, као и утицаји које оштећивање критичних инфраструктура има на образовање, привреду, здравство, комуникације и многе друге сегменте људске делатности. Терористички напади у Мадриду 2004. године и Лондону 2005. године, скренули су пажњу јавности на опасност од напада Европске критичне инфраструктуре. Као контра-одговор, Европски Савет је затражио од Европске Комисије да припреми целокупну стратегију и акциони план за побољшање заштите Европске критичне инфраструктуре - *European Critical Infrastructure (ECI)*.

Као резултат овог захтева, Комисија је предложила оснивање Европског Програма за заштиту критичне инфраструктуре - *European Programme on Critical Infrastructure Protection (EPCIP)*. Програм се састоји од три главна дела: Директиве за идентификацију и именовање *ECI*, Финансијског програма и Информационе Мреже критичне инфраструктуре - *Critical Infrastructure Warning Information Network (CIWIN)*.[62]

Извештај Комисије Европске уније о заштити критичне инфраструктуре у борби против тероризмадаје дефиницију критичне инфраструктуре,преглед идентификованих критичних инфраструктурних сектора и указује на критеријуме за проглашење одређених инфраструктурних сегмената критичним. У њему се наводи да се критичне инфраструктуре „састоје од оних физичких и информационих технологија, постројења, мрежа и служби, чије би ометање или уништење имало озбиљне негативне ефекте на здравље, безбедност или економско благостање грађана или на ефикасно функционисање влада држава чланица. Критичне инфраструктуре

[62]*Koubatis, A., Schonberger, J.Y.,Risk management of complex planning framework, Safety Science, 2001.*

обухватају и велики број економских сектора и кључне службе влада држава чланица".[63]

Након извештаја Комисије ЕУ донет је и Зелени документ о европском програму заштите критичне инфраструктуре (*Green Paper on a European Program for Critical Infrastructure Protection-Green Paper on* EPCIP).[64] У овом документу дата је и дефиниција заштите критичне информационе инфраструктуре, где се наводи: *„Сви програми и активности власника, оператера, произвођача и корисника инфраструктуре као и регулаторних органа, који за циљ имају обезбеђивање квалитетног функционисања, минимизирање штете и брз опоравак критичне информационе инфраструктуре у случају кварова или напада на критичну информациону инфраструктуру, представљају заједно програм заштите критичне информационе инфраструктуре"*.Заштита критичне информационе инфраструктуре би требало да се посматра у контексту међусекторске повезаности с обзиром на то да прожима скоро све остале критичне секторе и требало би да се координише са заштитом свих осталих критичних инфраструктурних сектора.[65]

Критичне инфраструктуре (КИ) су ресурси, системи и мреже, физички или виртуелни, чије уништавање или онеспособљавање може ослабити националну безбедност, економску стабилност и утицати на друге аспекте нормалног функционисања друштва.

Зелени документ о европском програму заштите критичне инфраструктуре даје и преглед критичних инфраструктурних сектора. У критичне инфраструктуре се према овом документу убрајају:[66]

- Енергетика (производња нафте и гаса, рафинисање, прерада и складиштење укључујући и гасоводе и нафтоводе; производња струје;

[63]*Commission of the European Communities, Critical infrastructure protection in the fightagainst terrorism (Brussels, 20 October 2004), COM(2004)702 final, pp. 3.*
[64]*Commission of the European Communities, Green Paper on a European Programme forCritical Infrastructure Protection (Brussels, 17.11.2005.), COM(2005) 576 final, pp. 19,http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf 17.11.2012.*
[65]*Ibid, pp. 19.*
[66]*Ibid.*

трансмисија струје, гаса и нафте; дистрибуција струје нафте и гаса),

- Информационе и комуникационе технологије - ИКТ (информациони системи и мрежна заштита; интернет; пружање услуга у области фиксне телефоније; пружање услуга у области мобилне телефоније; радио комуникација и навигација; сателитска комуникација),
- Вода (обезбеђивање и дистрибуција пијаће воде; контрола квалитета воде; контрола доступности пијаће воде),
- Храна (снабдевање храном и очување безбедности и квалитета хране),
- Здравство (медицинска и болничка нега; лекови, серуми, вакцине; био-лабораторије; био-агенси),
- Финансијски системи (службе исплате; владине финансијске службе),
- Органи јавног реда и мира, јавне безбедности и судство (очување јавног реда, мира, безбедности; судска администрација),
- Цивилна администрација (владини органи; оружане снаге; службе цивилне администрације; службе за реаговање у ванредним ситуацијама; поштанске и курирске службе),
- Саобраћај и транспорт (друмски саобраћај; железнички саобраћај; ваздушни саобраћај; речни саобраћај; поморски и океански саобраћај и транспорт),
- Хемијска и нуклеарна индустрија (производња, складиштење и прерада хемијских и нуклеарних супстанци; цевоводи за транспорт опасних материја) и
- Истраживање свемира.[67]

У одлуци Савета за унутрашње послове и правосуђе из децембра 2005. године од Комисије је затражен нацрт Европског програма за заштиту критичне инфраструктуре. Основни циљ европске политике јесте обезбеђење једнаког степена заштите за постројења одабране критичне инфраструктуре, што је изводљиво једино на основу заједничког европског оквира за заштиту критичне инфраструктуре. Овакав приступ проистекао је

[67] *Commission of the European Communities, Green Paper on a European Programme forCritical Infrastructure Protection (Brussels, 17.112005.), COM(2005) 576 final, pp. 24.*

из опасности да би разарање или поремећај одређене критичне инфраструктуре у једној земљи чланици могли непосредно утицати и на друге земље чланице. У овом смислу Европска унија дефинише тзв. Европску критичну инфраструктуру која се састоји од оних физичких ресурса, служби, уређаја, информационе технологије, економске или социјалне користи: било две или више земаља чланица, било три или више земаља чланица.

Директива Европског Савета 2008/114/ЕС из 2008. године представља саставни део EPCIP програма. Она дефинише критичну инфраструктуру, заједничке процедуре за идентификацију и означавање европске критичне инфраструктуре ЕКИ, заједнички приступ у процени потреба за побољшавање заштите, као и све ризичне приступе са првим приоритетом претње од тероризма.

Директива Европске Комисије 2008/114/ЕС је основа за наредне кораке у дефинисању критеријума за критичну инфраструктуру. У Анексу III истог документа наведене су процедура, које свака земља чланица треба да имплементира, кроз неколико консеквентних корака.

Кад је донета ова директива, она је представљала први корак у идентификацији и одређивању Европске критичне инфраструктуре - ЕКИ и потребе да се унапреди њихова заштита. У оквиру ње наглашено је да се односи на сектор енергетике и транспорта али и да је треба размотрити са посебним освртом на процену међуутицаја сектора, између осталог, посебно у односу на сектор информационих и комуникационих технологија. Прва ревизија Директиве почела је јануара 2012. године.

Истраживање постигнуто у процесу заштите критичне инфраструктуре на нивоу држава чланица ЕУ (2011. година) је показало да од 27 држава, 18 има дефинисану националну критичну инфраструктуру, док код 9 држава нема дефинисане националне критичне инфраструктуре. Међутим, већина тих држава предвиђа усвајање националне дефиниције критичне инфраструктуре у складу са принципима Европског програма за заштиту критичне инфраструктуре. Недостатак ове дефиниције значи да државе не спроводе специфичне заштитне мере заштите важних објеката и простора.

Што се тиче држава које имају дефинисану националну критичну инфраструктуру главна разлика у њиховим тумачењима је да поједине државе дефинишу критичне објекте и инфраструктуру, а друге се концентришу на *виталне* функције друштва. Као додатак томе, постоје и разлике у начину фокусирања држава чланица на спровођење ЗКИ. У појединим државама власти су фокусиране на заштиту важних објекта/инфраструктуре, док су у другим државама власти највише фокусиране на безбедност државе.[68]

Истраживање је даље показало да девет држава чланица ЕУ поседује списак јасно утврђене критичне инфраструктуре унутар своје територије. Све државе које имају дефинисану националну критичну инфраструктуру поделиле су их на секторе или подсекторе. Сектори који се најчешће јављају у националним програмима су: снабдевање енергијом, систем информација и телекомуникација, снабдевање храном, систем саобраћаја и дистрибуције, финансије и банкарство, здравство и снабдевање водом. Ово показује да су многе државе углавном фокусиране на заштиту оних сектора који се односе на основне животне потребе, а мање на тзв. симболичку инфраструктуру, као што су национални споменици (за разлику од САД, Аустралије и Канаде).[69]

Што се тиче организације система који је задужен за спровођење мера ЗКИ, она је иста или бар слична у свим државама чланицама ЕУ. У свакој држави, централно тело које спроводи ЗКИ је јасно дефинисано, иако се оно може разликовати у самој природи, дужностима или политичкој одговорности - у појединим државама координишуће тело нпр. може бити нека врста подршке и координатора, док у другим то исто тело може играти активну улогу у постављању стандарда и критеријума за оцењивање планова заштите. У појединим државама координишуће тело је део или је у надлежности Министарства унутрашњих послова или Министарства одбране, док је у другим део Центра цивилне заштите.[70] Такође, и друга

[68] *Ibid.*
[69] *Ibid, pp.21.*
[70] *UNISYS, табела 2, стр.25-26, преглед координишућих тела и законских/политичких оквираЗКИ у 25 држава чланица ЕУ, 2007.*

министарства и агенције могу бити надлежни за обезбеђивање критичне инфраструктуре унутар подсектора за које су задужене. У свакој држави приватни сектор је укључен у заштиту критичне инфраструктуре, јер је већи део инфраструктуре у приватном власништву.[71]

У пет земаља дефинисана је и законска обавеза за спровођење заштите критичне инфраструктуре. Од оних земаља које немају међусекторско законодавство или политику заштите критичне инфраструктуре, у току су радови на изради таквог законодавства или политике. У осам земаља ЗКИ се сматра делом националне стратегије за кризни менаџмент или антитерористичког плана.

Даље, у осам земаља не постоји законска обавеза да се заштити критична инфраструктура, нити је дефинисана политика заштите критичне инфраструктуре, али су неке стратегије усвојене на нивоу заштите појединих сектора. Три државе немају никакву законску или правну основу за спровођење.[72]

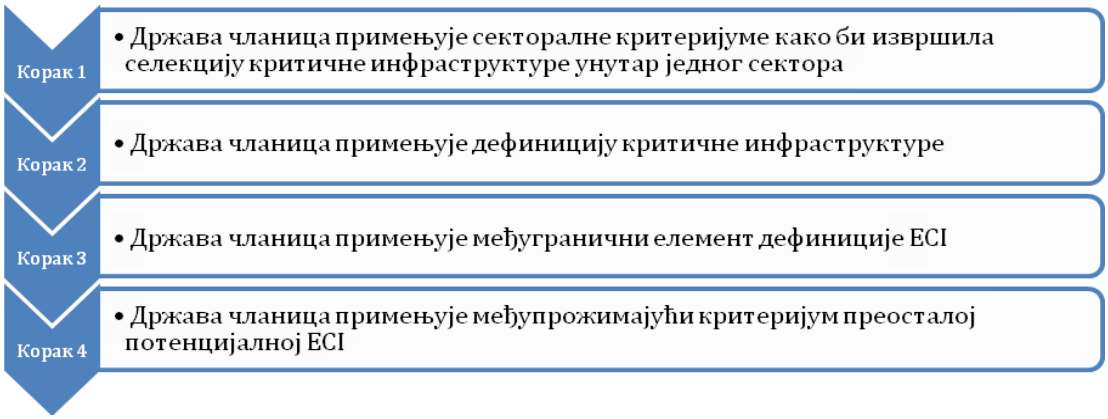
4.1. ИДЕНТИФИКАЦИЈА И ПРИМЕНА ПРОПИСА ВЕЗАНИХ ЗА ЕВРОПСКУ КРИТИЧНУ ИНФРАСТРУКТУРУ

Директива успоставља процедуру које се свака држава чланица мора придржавати, како би успешно идентификовала и применила Европску критичну инфраструктуру. Званична процедура идентификације може се илустровати процесом који садржи четири корака. Према директиви, свака држава чланица мора да идентификује потенцијалну ECI у сектору енергије и саобраћаја, а која испуњава секторалне критеријуме, а дефинисана је критичном инфраструктуром и ECI у члану 2 (а) и члану 2 (б) директиве (видети доле).[73] Као подршка државама чланицама усвојено је и необавезујуће упутство које би помогло при примени директиве.

У првом кораку свака држава чланица је у обавези да примени секторалне

[71] *Ibid.*
[72] *Ibid.*
[73] *Процедура идентификације је описана у члану 3 и Анексу III директиве Савета Европе (2008/114/EC).*

критеријуме како би извршила селекцију критичне инфраструктуре унутар једног сектора. Користе се четири различите врсте секторалних критеријума: традиционални критеријум који обухвата специјалне облике (нпр. димензије, капацитети и удаљеност критичне инфраструктуре); међутим, морају се утврдити „кључни елементи“ који морају бити директно именовани. Секторални критеријуми су поверљиви и нису доступни јавности. На слици 1. је приказана илустрација процедуре идентификације четири корака.



Слика 1. Илустрација процедуре идентификације четири корака

Важно је нагласити и разлике које постоје, а тичу се карактеристика *ECI*: док деоничари унутар једног сектора могу имати прецизне критеријуме на које могу да се ослоне, у другим секторима се јављају појединачне процене. Можемо закључити да одсуство прецизних критеријума у сектору, може довести до тенденције држава чланица да директно примењују међупрожимајући критеријум при процени и да мање или више искључе први „секторални корак“ унутар процеса идентификације. У пракси, ово може довести до ситуација у коме би процес идентификације могао да буде различит не само у државама чланицама, већ и у различитим секторима једне државе. Према томе, од велике је важности да државе чланице које се граниче, заједнички надгледају процес идентификације и заједно тумаче и примене добровољни критеријум. Чак и ако Комисија нема приступ информацијама који се тичу идентитета потенцијалне *ECI*, недостатак прецизних критеријума може довести до ситуације да државе чланице се

обрате Комисији за „помоћ“ око дефинисања националне *ECI*. То би довело до централизације којој су се противиле скоро све државе чланице током преговора о *EPCIP*.[74]

У другом кораку процеса идентификације, свака држава чланица мора да примени дефиницију критичне инфраструктуре *ECI*. Директива дефинише критичну инфраструктуру као: *...„објекте, системе или делове који се налазе у државама чланицама ЕУ, а који су важни за одржавање виталних животних функција, здравства, безбедности, заштите и економског или социјалног благостања људи, а чије нарушавање може имати катастрофалан утицај на све државе чланице“*.[75]

Другим речима, критична инфраструктура пружа услуге које су главне за наше друштво. Термин „критично“ је директно повезан са пружањем услуга и потенцијалним ефектима губитка таквих услуга. Тај термин „услуга“ је важан јер он ограничава инфраструктуре на оквир Директиве. Директива даље дефинише *...„за инфраструктуру која пружа главне услуге, доступност алтернативи и трајање нарушавања или опоравка мора бити узето у обзир“*. Као резултат другог корака, посматра се само инфраструктура која се сматра национално критичном.

Трећи корак у процесу идентификације пружа проверу нивоа нарушавања инфраструктуре и међуграничног утицаја на друге државе чланице: како би истраживали ово свака држава чланица мора применити дефиницију оног што се сматра *ECI*. Према члану 2 (б) Директиве, дефиниција *ECI* је: ...„критична инфраструктура је она која се налази у било којој држави чланици ЕУ, а чије би нарушавање угрозило најмање две државе чланице ЕУ. Значај овог утицаја мора бити процењиван у смислу међупрожимајућег критеријума. То укључује и ефекте који су настали као резултат међусекторске зависности од других врста инфраструктуре“.[76]

Уколико нарушавање инфраструктуре остане у националном оквиру, онда се

[74] *Lindstrom (2008б).*
[75] *Члан 2(а) директиве Савета Европе (2008/114/ЕС).*
[76] *Члан 2(б) директиве Савета Европе (2008/114/ЕС).*

критична инфраструктура не сматра *ECI*. Другим речима само међугранични утицај нарушену инфраструктуру чини *ECI*.

У четвртом и последњем кораку процеса идентификације, свака држава чланица се охрабрује да примени међупрожимајући критеријум преостале потенцијалне ECI. Међупрожимајући критеријум који је добровољан, мора бити узет у обзир: колики би опасан утицај имало нарушавање инфраструктуре; доступност алтернативе за замену нарушене инфраструктуре и колико је потребно да се нарушена инфраструктура опорави. Међупрожимајући критеријум се састоји од три фамилије: критеријума жртава, критеријум економских ефеката и критеријуми јавних ефеката.Сви наведени критеријуми су садржани у документима *ECI* као стандардизовани.

Доњи праг међупрожимајућег критеријума развијен је од стране Комисије у сарадњи са самим државама чланицама и то на добровољној основи; али ипак он се разликује од једне државе до друге државе чланице. Као и секторални критеријум, и међупрожимајући критеријум (ССС) је поверљив. Како би минимизирале ниво потребног рада државе чланице се охрабрују да отпочну са применом најрелевантнијег од три ССС (тј. оног који би се најлакше применио). Довољно је да један део међупрожимајућег критеријума задовољи корак 4 - процедуре идентификације. Уколико ниједан део ССС критеријума није задовољен инфраструктура се сматра „некритичном *ECI*".

Питање које се јавља у вези са проценом међупрожимајућег критеријума је да ли је могуће или не интегрисати ССС критеријум. На пример, да ли је могуће извршити процену целокупне инфраструктуре (на пример, ако је потенцијална критична инфраструктура веома близу економском критеријуму и такође близу критеријуму жртава можемо довести у питање њихову комплементарност). Представник Комисије је нагласио да критеријум зависи од тога да ли је критеријум основала сама држава чланица *(OMS)* или је он потекао из друге државе *(AMS)* која га је већ применила.Постоји такође и прилика за поновним оцењивањем претходног рада примене критеријума за различите учеснике или различите државе.

Међутим, примењивање критеријума се може спровести само уз одобрене државе; ако се држава не сложи инфраструктура се сматра „некритичном *ECI*“ чак иако је претходно идентификована као критична. Другим речима, сама држава има право „вета“ на примену *ECI*.

Процес идентификације и примене *ECI* мора се завршити у року од 24 месеца након ступања на снагу Директиве и мора се редовно надгледати. Не може се вршити процена броја потенцијалних *ECI* унутар целе ЕУ.

4.2. ОБАВЕЗЕ ПРЕМА ВЛАСНИЦИМА И ОПЕРАТЕРИМА КОЈИ ПРИМЕЊУЈУ ЕВРОПСКЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Директива наглашава три специфична захтева који власници и оператери *ECI* морају да испуне а то су: да осмисле План заштите оператера (*OSP*), да спроведу анализу ризика на основу сценарија претњи и да именују официра везе (*SLO*).

Први захтев обавезује државу да има *OSP* који идентификује процену критичне инфраструктуре *ECI*, као и мере заштите којим штити инфраструктуру.[77]*OSP* мора бити готов у року од годину дана након одређивања инфраструктуре и мора да се редовно надгледа.[78]

У вези са потребом осмишљавања *OSP*, друга обавеза је одређивање процене опасности.[79] Трећа обавеза је да власници и оператери Директиве морају у програму *ECI* именовати *SLO*. *SLO* ће комуницирати о безбедности са власницима/оператерима *ECI* и надлежним властима држава чланица. Штавише, свака држава чланица мора успоставити „механизам комуникације“ између власти држава чланица и *SLO*, како би се размениле информације о утврђеним ризицима и опасностима примене *ECI*.[80]

За све претходно наведене обавезе из Директиве надлежни су

[77]*Минимум захтева Плана заштите оператера је да се утврди Анекс II у директиви Савета Европе (2008/114/ЕС).*
[78]*Анекс II у необавезујућем упутству наводи постојање мере Заједнице које испуњавају захтеве постављених SLO и спроведених OSP.*
[79]*Видети члан 7.1 у директиви Савета Европе(2008/114/ЕС).*
[80]*Видети члан 6. у директиви Савета Европе (2008/114/ЕС).*

власници/оператери *ECI* и они морају проћи најбољу обуку тренинге и мењати информације о новим техничким односима *CIP*.[81]

Многе државе су већ идентификовале своје критичне инфраструктуре, а у оквиру њих и критичну телекомуникациону инфраструктуру (САД, Канада, Немачка, Шведска и Норвешка). Неке државе су покренуле пројекте из области КТИ (Бразил). У Републици Србији и региону се о овој теми веома мало дискутовало. Веће активности је предузела Хрватска док су БиХ и Црна Гора формирали тимове за одговоре на ванредне ситуације у области информационих технологија.

У Републици Србији се критична инфраструктура помиње само у оквиру поглавља 6.2. *„Стратегије развоја информационог друштва у Републици Србији до 2020. године“*,као: *„Потребно је развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, што поред ИКТ система могу бити и други инфраструктурни системи којима се управља коришћењем ИКТ, попут електро-енергетског система. У вези тога је потребно додатно уредити критеријуме за утврђивање критичне инфраструктуре са становишта информационе безбедности, критеријуме за карактеризацију напада применом информационих технологија на такву инфраструктуру у односу на класичне облике напада, као и услове заштите у овој области“*. Други релевантан документ којим су дефинисане активности у овој области је Упутство о методологији за израду процене угрожености и планова заштите и спасавања у ванредним ситуацијама.[82]

Следећи документи који би требало да обрађује питања КИ су Национална стратегија заштите и спасавања у ванредним ситуацијама и Закон о ванредним ситуацијама. Међутим у овим документима се ни не помиње критична инфраструктура, па тиме ни КТИ. У поглављу 24 је прописана обавеза доношења закона о критичној инфраструктури од стране СВС.

Треба нагласити да институционални оквири за дефинисање КИ постоје а то

[100] *Видети члан 8. у директиви Савета Европе (2008/114/ЕС).*
[82] *„Службени гласник РС“, 096/2012.*

су Сектор за ванредне ситуације, надлежна министарства као и надлежна регулаторна тела. Одређене мере заштите делова инфраструктуре су предузете од стране оператора, али нису донете ни стратегија, ни политика заштите на нивоу земље.

Потреба разматрања КИ препозната је у оквиру пројекта: *„Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору Републике Србије“*. Основни циљ пројекта је идентификација критичних инфраструктурних система чија је ефикасност кључна за неометан развој економије и друштва. Узимајући у обзир све факторе који могу негативно утицати на телекомуникациону инфраструктуру (природне непогоде, циљане нападе, ненамерне грешке) и мешовиту власничку структуру (државну и приватну), проблеми критичне телекомуникационе инфраструктуре постају комплексни и захтевају добро управљане регулаторне процесе.

У оквиру истраживања у поменутом пројекту предложена је следећа методологија у идентификовању КТИ:

- Формирање међусекторског тима (Сектор за ванредне ситуације, Надлежно министарство, РАТЕЛ, оператори, експерти);
- Дефинисање КТИ са свим критичним елементима у оквиру инфраструктуре;
- Идентификовање критичних тачака телекомуникационе инфраструктуре и процена ризика (Примена стандарда ISO 31000);
- Идентификовање веза са осталим КИ;
- Идентификовање националне КТИ као дела међународне КТИ у складу са међународним оквиром (ЕУ оквир);
- Предлагање препорука за спречавање инцидентних ситуација и осигуравање одржавања услуге и стабилности сервиса у случају да до таквих ситуација дође;
- Припрема стратегије и политике заштите телекомуникационе инфраструктуре;
- Припрема легислативног оквира за заштиту КТИ.

Подизање свести о потреби дефинисања КТИ и критичних система и мрежа и начина њихове заштите треба да буде део политике развоја КИ, у коме ће се јасно знати надлежности за дисеминацију информација о значају и заштити КИ. Истраживања из пројекта: *„Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и Железничком сектору Републике Србије“*, представљају полазишта у подизању свести о КТИ и идентификовању критичних елемената и њиховој заштити.

4.3. ПРОГРАМИ И МЕХАНИЗМИ ЕВРОПСКЕ УНИЈЕ У ОБЛАСТИ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

4.3.1. Информациона и комуникациона технологија

Област сигурности информационе и комуникационе технологије (ИКТ) се обимно развија на нивоу ЕУ задњих неколико година. Инфраструктура за комуникације, медије и информационе технологије се бави Комитет и постоји велики број закона, регулатива и програма унутар ЕУ. Сектор КИ који се бави ИКТ је дефинисан у Зеленом Папиру за *EPZKI* пошто садржи информационе системе и заштитне мреже; инструментацију аутоматизације и контролних система, интернет провизију фиксне телекомуникације, провизију мобилне комуникације; радио комуникацију и навигацију; сателитску комуникацију и емитовање.[83]

Унутар области мрежне и информационе сигурности (МИС) ЕУ има приступ који се састоји од три аспеката сигурности - специфичне мрежне и информационе мере сигурности контролног оквира за електронску комуникацију (укључујући и заштиту и приватности и података) и борбу против интернет криминала (марта 2002. године ЕУ је усвојила заједнички контролни оквир директиве за мрежу електронских комуникација и услуга. Ова директива Савета оснива оквир за регулацију мреже у услуга електронских комуникација, удружених капацитета и услуга. Такође, утврђује и скуп процедура у циљу обезбеђивања усклађених апликација

[83] *Jarlsvik, H., Castenfors, K., Security and Preparedness in the EU, Stockholm, 2004.*

контролног оквира кроз заједницу и дефинише задатке националних контролних ауторитета. Овај контролни оквир покрива све мреже електронске комуникације које дефинише ЕУ укључујући: *„Трансмисионе системе и опрему и друге изворе који дозвољавају пренос сигнала жицом, радиом, оптичким или другим електромагнетним средствима, укључујући и сателитске мреже, фиксне и мобилне мреже, системе електричних каблова, до степена коришћења тих услуга за пренос сигнала и мрежа које се користе за радио и ТВ емитовање, кабловске телевизијске мреже, без обзира на тип информација које се преносе"*.[84]

Унутар овог оквира једноставно је истакнуто да су државе чланице одговорне да осигурају очување интегритета и сигурности јавних мрежа комуникација - ниво сигурности и како је треба очувати још није детаљно изложено. Унутар оквира европског програма, који је део Лисабонске Стратегије, циљ је стварање заједничких спецификација на пример на личном интернету и контроли корисника, и развијање сигурне инфраструктуре. Европа дефинише сигурност унутар области која се састоји не само од технолошких питања већ и у великој мери од људског понашања и познавања претњи и помоћних средстава. Информациона сигурност бави се темама као што су приватност,интернационална трговина, права грађана и примена закона.

4.3.2. Вода

Унутар законодавства ЕУ не постоје прописи ни захтеви за државе чланице да гарантују грађанима приступ води за пиће, ни кроз заштиту система ни кроз очување акција.[85] Али ЕУ је дала неколико директива које се тичу квалитета воде. ЕУ је основала Оквирну Директиву на пољу политике воде за заштиту унутрашњих површинских вода, прелазних вода, природних и подземних вода. Глобални циљ је спречавање и смањење загађења, унапређење подршке употребе воде, заштита водене околине, унапређење

[84] *European Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C43/02).*
[85] *Jarsvik, H., Castenfors, K., Security and Preparednesa in the EU, Stockholm , 2004.*

статуса водених екосистема и ублажавање ефеката поплава и суша. Директива Савета из 1998. године дефинише основне стандарде квалитета вода намењене за људску употребу коју вода мора да има. Ова Директива има за циљ да заштити људско здравље постављајући захтеве о чистоћи пијаће воде који се морају испунити унутар заједнице. ЕУ такође има прописе који се тичу третмана отпадних вода у урбаним срединама а директива Савета из 1991. године тиче се сакупљања, пречишћавања и испуштања отпадних вода како из урбаних средина тако и из индустријских области. Њен главни циљ је заштита животне средине.

4.3.3. Храна

Безбедност хране је широка област политике у ЕУ. Она укључује теме као што су народно здравље, здравље животиња, исхрана и благостање, здравље биљака, етикетирање и паковање производа, хигијена хране, загађење и фактори околине, итд. У Зеленом Папиру *EPZKI* ЕУ је дефинисала сектор хране КИ а укључује припрему хране и заштиту и сигурност хране као и у случају воде не постоје законодавства, регулативности или захтеви ЕУ за гаранцију приступа хране грађанима. Међутим, заједничка пољопривредна политика је кроз историју била и може још бити инструмент осигурања залиха кроз производњу пољопривредних производа унутар ЕУ.

4.3.4. Здравље

Сектор КИ здравља дефинисан је у Зеленом Папиру *EPZKI* и укључује медицинску и болничку негу; лекове, серуме, вакцине и апотекарство као и биолабораторије.

4.3.5. Финансије

Област финансија је дефинисана у Зеленом Папиру као плаћање услуга и плаћање структура и финансијски задатак Владе. Систем финансије има најмање две карактеристике. То је функција основне друштвене вредности чиме подржава социјалну економију где ремећења која потичу из других области инфраструктуре морају бити узета у обзир јер је инфраструктура

сама по себи осетљива на ремећења. На европском нивоу регулативе које се тичу области финансија углавном се суочавају са заједничким оквиром који се тиче новчаних трансакција и сигурности као предуслов за функционисање заједничког тржишта. У области финансијских инфраструктура постоје два извештаја која се тичу инфраструктура и граница које постоје унутар њих са циљем елиминисања граница. Препорука која се тиче европских правила понашања у вези са електронским плаћањем је издата 1987. године и имала је за циљ да унапреди сигурност и погодност за потрошаче и већу сигурност и ефикасност за трговце и издаваче.

4.3.6. Цивилна администрација

Област цивилне администрације КИ је дефинисана у Зеленом Папиру и садржи владине функције; оружане снаге; услуге цивилне администрације, хитне службе и поштанске службе. Прве три компоненте ове области могу се посматрати као део европске спољне политике и одбране и безбедности. Владине функције, оружане снаге и цивилна администрација су традиционалног мишљења пошто су све у уставу државе и онога што је критично за њен опстанак. Уговором у Мастрихту ЕУ је ујединила циљеве заједничке спољне политике; одредбе заједничке спољне политике и сигурности (ЗСПС) биле су прилагођене Амстердамским Уговором који је ступио на снагу 1999. године. Чланови уговора 11-28 од тада су се држали главних принципа: обезбеђење сигурности уније; очување мира и јачање интернационалне сигурности, унапређење међународне сарадње и развијање демократије, законских права и људских права.

Европска Политика Одбране и Безбедности (ЕПОБ) има за циљ развој цивилних и војних капацитета уније за управљање ванредним ситуацијама и превенцију конфликата. ЕПОБ се значајно развила од 1999. године и има три главне компоненте. Прве две, управљају војним кризама и цивилним кризама, познати су као Петерсбуршки задаци. Превенција конфликата је трећа компонента. Јуна 1999. године европски Савет ставио је управљање кризом на основу процеса јачања ЕПОБ. Европски лидери коју су на врху су се

сложили да Унија мора да има капацитет за аутономне акције, подржане војним снагама, средства да одлучи да их употреби, као и спремност да их заврши, да би реаговала на међународне кризе.

Политика ЕУ у области хитних служби почела је средином 80-тих година и део је Еколошке политике пошто је иницијативно фокусирана на природне катастрофе. Данас постоји законодавни оквир који регулише европску цивилну заштиту и углавном је заснован на три дела европског законодавства. Први главни правни текст датира из 1999. године и основао га је Активни Програм Заједнице на пољу цивилне заштите. Одлуком Савета из 23.10.2001. године основан је Заједнички Механизам за Цивилну Заштиту, са циљем олакшања појачане кооперације у интервенцијама цивилне заштите, одлука Комитета од 23.12.2003. године, поставила је правила за спровођење механизма заједнице, дефинишући његове дужности и функције. Циљ је олакшање мобилизације неопходних средстава када природна или људска катастрофа погоди земљу, унутар или ван граница ЕУ.

Механизам Заједнице за цивилну заштиту има три главна оруђа за олакшање спремности и реаговања на катастрофу на нивоу заједнице. Центар за праћење и информисање је срце операције и служи као комуникациони центар на нивоу штаба. Заједнички резервни и информациони систем је алармна и обавештајан апликација креирана са циљем олакшања унапређења сарадње интервенција цивилне заштите. Овај програм укључује курсеве, обуке, организацију заједничких вежби и систем размене експерата.

4.3.7. Транспорт

Сектор транспорта је дефинисан у Зеленом Папиру као путни транспорт, железнички транспорт, ваздушни саобраћај, унутрашњи водени транспорт као и океанска и морска пловидба. Важно је напоменути да јавни транспорт није укључен у ову листу. Ово је посебно важно с обзиром на скорашње нападе, јер је у нападима у Мадриду и Лондону јавни транспорт коришћен као средство и циљ.

Инфраструктура за превоз људи и робе преко националних граница је

размотрена унутар „Транс-Европске Мреже-Транспорта“, чије су директиве усвојене јула 1996. године од стране Европског Парламента и Савета. Ове директиве укључују путеве, железницу унутрашње водене путеве, аеродроме, морске луке, унутрашње луке и системе управљањем саобраћаја које служе цео континент. Недостаје законодавност која се односи на функционалност система транспорта под притиском.

4.4. СТАЊЕ И ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ДРУГИМ ДРЖАВАМА

4.4.1. Сједињене Америчке Државе

Након распада СССР и пада Берлинског зида САД су остале једина војна, политичка и економска суперсила. Међутим, нестајањем „политике задржавања комунизма“ коју су водиле за време трајања стања биполарности, настале су претње друге врсте. САД су се суочиле са претњом тероризма. Због тога се требала редефинисати стратегија националне сигурности САД, с обзиром на то да развој тероризма не угрожава само у војној, него у великој мери и у економској и друштвеној сфери. Једна од последица тероризма свакако је и забрињавајуће стање на подручју енергетске сигурности и заштите инфраструктуре. САД су у великој мери укључене у светске сигурносне процесе.

Прекретница за националну сигурност САД били су догађаји након терористичких напада на америчком тлу. У САД се критична инфраструктура према Закону о уједињењу и јачању Америке кроз обезбеђивање одговарајућих средстава потребних за прекидање и спречавање тероризма. (USA PATRIOT ACT)[86] из 2001. године, у поглављу 1016е, дефинише на следећи начин: „термин *критична инфраструктура* означава системе, сервисе и постројења, физичке и виртуелне, који су толико витални за САД да њихово онеспособљавање или уништавање може да има врло негативан

[86]*USA PATRIOT ACT (пун назив на енглеском: Unitingand strengthening America by providing appropriate tools required to intercept and obstruct terrorism act), настао је као одговор на терористичке нападе који су задесили САД 11.09.2001. године. Донет је од стране америчког конгреса, а званично га је потписао и озваничиоЏорџ Буш 26.10.2001.*

утицај на безбедност, националну економију, јавно здравље, или комбиновани негативни утицај на све ове наведене области".[87]

На тренутној листи критичних инфраструктурних сектора у САД налазе се:[88]

- информационе технологије (ИТ),
- телекомуникације,
- хемикалије,
- комерцијалне установе,
- бране,
- нуклеарни реактори, нуклеарни материјали и нуклеарни отпад,
- институције Владе,
- саобраћајно-транспортни систем (који укључује инфраструктуру неопходну за функционисање масовног транспорта, авио-саобраћаја, водног, друмског и железничког саобраћаја и система цевовода),
- хитне службе (службе које реагују у ванредним ситуацијама),
- поштанске и шпедитерске службе и сервиси,
- пољопривреда и производња хране,
- јавно здравље и здравствена нега,
- вода за пиће и системи за третирање отпадних вода,
- енергетика (под чим се подразумевају постројења за производњу, рафинисање, складиштење и дистрибуцију нафте и гаса, електричне струје (осим за комерцијална нуклеарна постројења),
- банкарство и финансије,
- национални споменици и знаменитости,
- индустријска производња за потребе одбране земље и
- критична индустријска производња.[89]

Пошто је број актера који су укључени у заштиту критичне инфраструктуре у САД јако велик, америчка Влада развила је низ институција, иницијатива,

[87] *Macaulay, T., Critical Infrastructure - Understanding its component parts, Vulnerabilities, Operating Risks and Interdependencies, CRC Press, London, pp. 8, 2008.*
[88] *TheWhiteHouse, Nationalstrategyforhomelandsecurity, Washington, pp. 27; Документ о националној стратегији*: http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf17.11.2012.
[89] *Ibid, pp. 4.*

директива и правила реаговања како би се обезбедила координисана акција свих учесника, као што су:[90]

- *Председничка комисија за заштиту критичне инфраструктуре (Presidential Commissionon Critical Infrastructure Protection*-PCCIP*)*, је био први покушај да се укаже на рањивост инфраструктуре у САД.[91]
- *Председничке директиве 62 и 63 (Presidential Decision Directives (*PDD*) 62 and 63)*изнете су у мају 1998. године у склопу председничке одлуке.[92] Директивом 63 установљене су радне групе у оквиру Федералне Владе и позива се на дијалог између Владе и приватног сектора, како би се формирао Национални план обезбеђења инфраструктуре.[93]
- *Национални план за заштиту информационих система* представљен од председника САД 07.01.2000. године први је опсежни Национални план за заштиту критичне информационе инфраструктуре, чији је фокус био на обезбеђивању сајбер-компоненти критичне инфраструктуре. Пун назив овог плана био је Одбрана сајбер-простора Америке.[94] Овај план је указао на то да сајбер-безбедност представља заједничку одговорност Владе и приватног сектора.
- *Извршне наредбе о оснивању службе националне безбедности и Савета за националну безбедност*од 08.10.2001. године, првом наредбом председика (ЕО 13228), основана је Служба националне безбедности и са њом повезан Савет за националну безбедност.[95]Другом наредбом (ЕО 13231) под називом *Заштита критичне инфраструктуре у информационом добу*, установљен је Председнички одбор за заштиту критичне инфраструктуре. Задатак одбора јесте да „препоручује начин вођења политике заштите

[90]*Ibid.*
[91]*The President's Commission on Critical Infrastructure Protection (PCCIP),Critical Foundations: Protecting America's Infrastructures', Washington, 1997.*
[92]*William, J.C., Protecting America's Critical Infrastructures: Presidential Decision Directives 62 and 63, Washington, 1998.*
[93]*Ibid.*
[94]*William, J.C., Defending America's Cyberspace: National plan for information systemsprotectionversion1.0,AnInvitationto a Dialogue, Washington, 2010.*
[95]*George, W.B., Executive Order 13228, Establishing the office of homeland security and the homeland security council, Washington:http://www.fas.org/irp/offdocs/eo/eo-13228.htm 17.11.2012.*

критичне инфраструктуре и да координише извршења програма заштите информационих система битних за функционисање свих осталих сектора критичне инфраструктуре".[96] Овом наредбом такође је установљено Национално саветодавно веће за инфраструктуру[97] (*National Infrastructure Advisory Council* - NIAC), као председнички саветодавни орган састављен од власника и оператера критичне инфраструктуре државе.

- *Председничка директива Службе националне безбедности (HSPD-7)* од 17.12.2003. године издата је председничка директива Службе за националну безбедност (HSPD-7), која смењује председничку директиву 63 (PDD63) из маја 1998. године, као и све остале раније издате председничке директиве. Овом директивом установљен је став који сва одељења, све федералне службе и агенције треба да заузму кад је у питању заштита критичне инфраструктуре од терористичких напада.[98]
- Директивом се именује Секретар за националну безбедност који треба да буде „највиши федерални званичник који ће водити, интегрисати и координисати све акције везане за заштиту националне безбедности, критичне инфраструктуре и кључних ресурса и који ће активно сарађивати и подстицати сарадњу између федералних одељења и служби, затим између државне и локалних влада и приватног сектора".[99]
- *Национална стратегија* државне безбедности објављена је јула 2002. године и њоме је постављена основа за заштиту критичне инфраструктуре у САД. У фебруару 2003. године Бела кућа издала је две председничке националне стратегије - националну стратегију о обезбеђивању сајбер-простора и националну стратегију за физичку заштиту критичне инфраструктуре и кључних ресурса, оне представљају пратеће документе уз националну стратегију државне безбедности.

---

[96]*George W.B., Executive Order 1323, Critical Infrastructure Protection in the Informaion Age, Washington, http://www.fas.org/irp/offdocs/eo/eo-13231.htm 17.11.2012.*
[97]*Ibid.*
[98]*http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html 17.11.2012.*
[99]*Ibid.*

- *Национална стратегија Службе државне безбедности*[100] донета јула 2002. а ажурирана октобра 2007. године везана је за одбрану САД од терористичких напада.[101] Једна од шест *критичних мисија* које се налазе у Националној стратегији је и заштита критичне инфраструктуре и кључних ресурса.
- *Национална стратегија обезбеђивања сајбер-простора* (*National Strategy to Secure Cyber space* - NSSC)[102] указала је на важност изазова који представља обезбеђивање сајбер-простора. Стратегијом се сајбер-простор дефинише као *међузависна мрежа информационих инфраструктура* и сликовито указује на то да сајбер-простор представља *нервни односно контролни систем америчког друштва*. Стратегија настоји да прецизно дефинише националну политику на пољу заштите сајбер-простора.

У деловању САД важно место је чињеница да њихово деловање на глобалном плану у највећој мери утиче на цене енергената на светском тржишту. Тако су и њихови војни ангажмани у Авганистану и Ираку произвели велики пораст цена енергената. Власти САД својим грађанима настоје осигурати најниже цене енергената и у складу са тим питања енергетске сигурности, у смислу сигурног и стабилног увоза енергената, постају питања од националног интереса, а њихов ангажман на светском плану у осигуравању доступности извора енергије постаје питање националне сигурности.

Један од највећих потрошача енергената у свету су САД. Већину енергената увозе из других подручја, иако имају и властите залихе, а према неким подацима увозе чак 60 % нафте. Догађаји из 11.09.2001. године представљају прекретницу у деловању САД. Интервенције у Афганистану и Ираку одредиле су стање на тржишту енергената у свету, али и потребу редефинисања енергетске сигурности у светским размерима. Однедавно се почиње причати о енергетској кризи у коју САД полако улази. Велики

[100] *Papa, M., Shenoi, S., Critical infrastructure protection II, International federation for information processing, New York, pp. 21-22, 2008.*
[101] *Office of Homeland Security, National strategy for homeland security, Washington, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf 17.11.2012.*
[102] *TheWhiteHouse, NationalStrategytoSecureCyberspace, Washington,http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf 17.11.2012.*

потрошач енергената је америчка војска, што се оправдава одбраном нације. Без јасне стратегије САД се суочава са економским дефицитом узрокованим увозом енергената. САД највише користи нафту, чак 62 % од свих енергената. Америчка економија зависи од доступности количина нафте. Две трећине потрошње нафте одлази на транспорт, док је једна петина потребна за индустрију. Повећавањем цена нафте, уз повећање количине потрошње унутар САД, повећала се зависност од увоза енергената. За поређење, треба напоменути да становништво САД чини само 5 % светског становништва, а троши 45 % произведене нафте у свету. Како би се одржао раст економије САД, потрошња и доступност нафте требале би се следећих година повећавати.

Још од краја хладног рата подручја богата нафтом постала су занимљива за САД, па је тако Персијски залив, богат нафтом, сматран америчким виталним интересом, а у време председника Клинтона енергетска сигурност је проглашена фундаменталном компонентом националне сигурности. Бушова администрација наглашавала је да је очување америчког нафтног снабдевања национални приоритет. Тако је, примера ради, током инвазије на Ирак било неопходно заштитити нафтна поља и рафинерије у јужном Ираку.

Предвиђа се да ће америчка зависност од увозних енергената, нарочито од нафте, до 2020. године нарасти на 90 %, што ће америчку економију додатно ослабити. САД увози нафту из свих делова света, а чак 15 % из Африке. Предвиђа се да ће у скоријој будућности чак четвртина увоза нафте у САД бити из Африке, за што САД припрема политичку инфраструктуру. С обзиром на тешку ситуацију у афричким земљама и присутност терористичких група, САД гради војне базе и шаље дипломатске мисије са циљем заштите америчког приступа нафти на кризним подручјима попут Нигерије, Камеруна и Чада. Истовремено настоје ограничити приступ тим подручјима Кини и Индији или другим великим потрошачима нафте. Кина већ сарађује са афричким земљама, а чак четвртину нафте коју троши увози из тих земаља.

Проблем са којим се суочавају државе света, па тако и у највећој мери САД,

јесте одбрана енергетске инфраструктуре од терористичких напада. Критична инфраструктура се највећим делом налази на подручјима сукоба. Очување инфраструктуре у тим подручјима захтева повећане трошкове, што коначно утиче и на повећање цена енергената, посебно нафте. САД издваја и велике количине новца на заштиту инфраструктуре у Латинској Америци.

У САД се налазе четири велике нафтне рафинерије, стотине хиљада километара нафтовода и гасовода. Експерти упозоравају на опасности и рањивост америчког система инфраструктуре, а претње тероризма подстакле су на размишљање о њеној заштити. Међутим, највећи део нафте, а све више и природног гаса, у САД стиже из прекоморских земаља, а сигурност америчких нафтних прекоморских залиха у великој мери зависи од осигурања инфраструктуре одређеног подручја које извози енергенте.

4.4.2. Руска Федерација

Падом комунизма и распадом СССР настала је Руска Федерација, која је изгубила већину снаге и међународни положај какав је уживао СССР за време хладног рата. Иако је Русија кренула у процес транзиције, суочавала се, и још се суочава, с бројним економским, социјалним и политичким проблемима. Русија се од осамостаљења увлачила у сукобе на свом подручју или подручју бивших држава СССР, а њено је деловање на спољнополитичком плану изазивало многе контроверзе. Тако је још и данас присутна жеља дела политичког естаблишмента за рестаурацијом СССР, односно моћи и позиције које је бивша држава уживала. Не може се рећи да је Русија маргинализована с обзиром на њену позицију у тренутним међународним односима, али је њена моћ свакако умањена. Унутар саме Русије постоји политичка струја која заговара сарадњу са Западом, као нужну за обнову руске позиције једног од најзначајнијих актера, али је бројнија стара традиционалистичка струја против повезивања са западом.

Руска Федерација једна је од земаља произвођача енергената и самим тим енергетску сигурност поима на другачији начин. Таквим је земљама у циљу осигуравање стабилног и сигурног извоза уз остваривање својих интереса.

Русија као велики произвођач енергената настоји побољшати свој геополитички положај и повратити део некадашњег политичког утицаја. Прилика јој се пружа на подручју ЕУ где Русија извози највише својих енергената.

Енергетски сектор и политика у Русији неко време нису независни. Владимир Путин ставио је енергетику под власт државе, чиме је овај сектор постао витални национални интерес. Деловање енергетских компанија одвија се под контролом власти и не може се одвојити од политичког утицаја.

Русија од свог осамостаљења није изградила ефикасан систем сигурности, а тек су недавно донети одређени документи који унапређују стање националне сигурности. Поред тога, Русија пролази кроз фазу транзиције, која је у многим сегментима тешка и не даје очекиване резултате. Земља са великим енергетским потенцијалима наилази на препреке у остваривању енергетске сигурности. Највише извози на подручје ЕУ која, као што је претходно наведено, настоји елиминисати превелики руски утицај због увоза енергената на подручје ЕУ. Русији је потребна енергетска сарадња са ЕУ због додатних улагања у енергетски сектор, како би се отворила нова налазишта и побољшала продуктивност домаћих енергетских компанија.

За националну сигурност Русије, али и за сигурност Европе битно је оснаживање Русије и њено укључивање у светске развојне процесе. Ако Русија не спроведе нужне реформе, постаће претња за европску сигурност. Да би се спречили било какви облици угрожавања, предност у односима са Русијом треба дати економском и политичком, а не војном деловању.

Једно од најважнијих обележја Русије су бројна изворишта енергената, што Русију доводи у врло повољну позицију у којој може креирати своју спољну политику и повећавати моћ у свету на темељу енергетског сектора. Сам је концепт енергетске сигурности у случају Русије другачији него у државама увозницама енергената.

Руски председник Владимир Путин ставио је сектор енергетике под потпуну

контролу државе, што је додатно политизовало енергетски сектор и поставило га као инструмент спољне политике. Русија тренутно има неколико великих и врло утицајних нафтних компанија, попут „Газпрома“, које су већином у власништву државе те су у низу ситуација, попут ситуација са Украјином, Белорусијом и Грузијом коришћене као средство притиска у циљу што повољнијих услова пословања. Подручје ЕУ најважније је извозно подручје руских енергената. Чак 90 % енергената Русија извози на простор земаља ЕУ, а с низом земаља остварила је уговоре о сарадњи. Концепт енергетске сигурности за Русију означава сигурност у извозу енергената, а њен енергетски развој и сигурност зависе од развоја тржишта која захтевају руске енергенте.

Уз инфраструктуру, Русија покушава освојити европско тржиште и куповином удела у локалним европским енергетским компанијама. Истовремено отвара нова налазишта, али уговара и сарадњу са суседним земљама које обилују енергентима, стављајући тиме ЕУ у незавидну позицију. Тренутно не постоје знаци ширења извоза руских енергената на азијско подручје због захтевности изградње инфраструктуре и превеликих трошкова. Тако ће ЕУ остати највећи потрошач руских енергената, што се може сагледати вишедимензионално. Русија такву позицију може искористити за ојачавање своје моћи и демонстрацију снаге уценама и редукцијама, а са друге стране може осигурати великог, сталног и стабилног потрошача својих енергената.

4.4.3. Земље Европске уније

Економија земаља ЕУ све брже расте, а тиме расте и потреба за доступним енергентима. Европске земље немају додатне изворе енергената, па не могу задовољити потребе растуће економије. Велика потрошња енергената ЕУ чини и великим увозником. Највећи партнер у пословима енергетског снабдевања свакако је Русија. Зависност европског тржишта од руских енергената већ је видљива, што забрињава и саме европске државе. Поставља се питање природе политичког стања Руске Федерације, као и могућност

манипулације енергетским споразумима. Додатни проблем ЕУ је што се она не може одвојити од деловања својих чланица, а то може изазвати неспоразуме и компликације. До данас није створено јединствено енергетско тржиште, што отежава и стварање одређене јединствене енергетске политике. Због страха од Русије, ЕУ настоји отпочети сарадњу са подручјима на Кавказу, средишњој Азији и Блиском истоку. Међутим, та су подручја политички нестабилна, а улагање у њих својеврстан је ризик. Јасно је да ће у будућности Русија ипак бити највећи извозник енергената на подручје ЕУ, а у том циљу нужна је сарадња.

Руска енергетска инфраструктура је у лошем стању, а европске финансијске инвестиције биле би нужне у замену за гас и нафту. Међутим, ЕУ држи одређену дистанцу у сарадњи са Русијом због ситуације са Украјином, Белорусијом и Грузијом, где је Русија користила енергију као средство притиска. Русија, пак, види прилику за побољшање своје спољнополитичке позиције у енергентима, а тога се ЕУ боји. Ипак, према неким проценама, снабдевање ЕУ енергентима из Русије до 2020. године повећаће се на 70 %. Стога је ЕУ још 2006. године донела документ под називом *Green Paper - A European Strategy for Sustainable, Competitive and Secure Energy*, којим се настоји уредити заједничка стратегија око увоза енергената.

За разлику од САД, којима највећи проблем у будућности представља снабдевање нафтом, ЕУ је проблематично снабдевање природним гасом. Проблем са гасом је критична инфраструктура јер се једина испорука плина остварује гасоводима који на путу до европских одредишта пролазе кризним подручјима, а подложни су и уцењивањима од стране државе кроз коју пролазе. Како би смањила зависност о само једном добављачу, ЕУ реализује неколико пројеката који се односе на могућности дистрибуције енергената, при чему посебну важност имају подручја Кавказа и средње Азије.

Своју енергетску сигурност ЕУ дефинише као способност да се будуће потребе за енергијом задовоље било помоћу домаћих резерви или увозом по прихватљивим условима. Другим речима, енергетска сигурност означава сигурне изворе енергената по прихватљивим ценама. Европским

енергетским сектором доминира употреба нафте, природног гаса и угља, пуно мања употреба нуклеарне енергије и енергије из обновљивих извора. Ти подаци чине ЕУ једним од највећих увозника енергената у свету. ЕУ је један од највећих потрошача природног гаса, а добија га из Русије и Алжира.

Заштита критичне инфраструктуре у Европи односи се на осигуравање гасовода који од одредишта пролазе мноштво државних граница. Државе кроз које пролазе гасоводи очекују финансијске и политичке користи, као што су снабдевање гасом, запошљавање, транзитне накнаде и сл. Један од могућих проблема у будућности око критичне инфраструктуре биће и заштита гасовода од терористичких група, јер европске државе нису остале изван догађања након 11.09.2001. године. Како се гас не може доставити другим путевима осим гасоводом, у очувању енергетске сигурности биће неопходно успоставити добре споразуме са земљама извозницима како би се осигурала континуирана размена и сигурност од уцена. Стога стварање јединствене енергетске политике и енергетска сигурност постају приоритети деловања ЕУ, али и сваке државе појединачно.

Већина земаља ЕУ зависи од увоза енергената - тачније, увозе укупно 50 % свих потрошених енергената. Према неким проценама, увоз енергената у земље ЕУ до 2030. године нарашће на 70 %, што ће ЕУ учинити зависном од увозна енергената и биће подложна притисцима. Један од главних снабдевача на европском подручју је Русија, што у великој мери забрињава ЕУ. Европске земље енергетску сигурност доживљавају у економском и политичком контексту, иако ЕУ има своја политичка тела, у недостатку заједничке европске енергетске политике већина земаља делује самостално.

Европска унија у целини се може сврстати у земље претежне увознике енергената и у складу с тим енергетска сигурност означава сигурно и стабилно снабдевање енергијом. Као и за сваку земљу у истом положају и за земље ЕУ важно је да не постану зависне искључиво од једног добављача енергената, а подједнако је битно створити и јединствену европску енергетску стратегију. Кад се нагло суочила са проблемом недостатка извора енергената и све већим увозом, ЕУ је почела подстицати коришћење

алтернативних облика енергије. Године 2006. у документу названом *Green Paper - A European Strategy for Sustainable, Competitive and Secure Energy* најављено је стварање заједничке европске енергетске стратегије која би помогла у спровођењу енергетске политике ЕУ. Та стратегија узеће у обзир да енергетиком и енергетском сигурношћу у савременом свету управљају интереси и геополитичке позиције. Тренутна ситуација показује да ЕУ настоји смањити зависност од руских енергената изградњом енергетске инфраструктуре, изналажењем других добављача енергената или развојем других извора енергије. Постоји одређена несразмера у снабдевању и ценама енергената у земљама чланицама ЕУ, па су настојања европских структура јединствен приступ и политика енергетском сектору како би се остварили једнаки услови и погодности за све државе чланице ЕУ. Енергетска сигурност ЕУ у будућности ће зависити од њеног односа са добављачима енергената, па су настојања ЕУ да прошири мрежу добављача како евентуални проблеми у достави енергената не би угрозили развој, али и националну сигурност земаља чланица ЕУ.

Данас је већина држава чланица ЕУ уговорно везана за увоз енергената из Русије, па не желе захлађивати односе са Русијом, јер би то могло проузроковати проблеме у снабдевању енергентима. Зависност од енергената највећи је проблем за ЕУ. То значи зависност од добављача енергената која се може умањити добрим условима и сарадњом. Тренутно свака држава чланица ЕУ сама преговара и склапа споразуме о сарадњи на подручју енергетике. Тако, примера ради, Немачка увози преко 50 % енергената из Русије, а већина нових чланица које су ушле у Европску Унију 2004. и 2007. године, као земље бившег Источног блока кориснице су руских енергената, тачније природног гаса. Велики задатак за ЕУ биће усклађивање националних интереса земаља чланица у стварању јединствене енергетске сигурности. Истовремено ће бити потребно очувати и националну сигурност тих земаља, јер ће Русија неминовно бранити своје енергетске интересе у целини.

Приближавањем европским интеграцијама Република Србија мора отпочети

деловати и на плану енергетске сигурности. Као земља увозница енергената мора израдити флексибилну стратегију енергетске сигурности помоћу које ће редуковати потенцијалне енергетске опасности и успоставити добру сарадњу са извозницима енергената као предусловом за њен укупни развој. То захтева и редефинисање постојеће стратегије националне сигурности.

4.4.3.1. Бугарска

Према Закону о кризном менаџменту у Бугарској се критична инфраструктура дефинише као скуп добара, служби и информационих система, чије би отказивање, спречавање нормалног функционисања или уништење имало озбиљан негативан утицај на јавно здравље, безбедност грађана, животну средину, националну економију и функционисање државних институција".[103]

Иако се овом дефиницијом објашњава шта је критична инфраструктура, она не даје неки конкретан критеријум на основу кога би се вршила евалуација *критичности* одређених инфраструктура. Сама дефиниција није довољна ни када се жели утврдити да ли одређено добро, систем или служба могу да се третирају као *критични*. Бугарска је чланица Европске уније од 2007. године и као таква мора да прати активности и регулативу ЕУ у области заштите критичне инфраструктуре.

Велики број бугарских критичних инфраструктура екстремно су осетљиве на природне катастрофе као што су земљотреси, сурови временски услови, поплаве, олује исл. Чак и кад је елиминисан физички утицај непогода, нагло повећање потребе за критичним инфраструктурама током криза може да доведе до нпр. нестанака струје, што опет представља један облик отказивања критичне инфраструктуре. Слични сценарио је могућ и услед намерних или случајних људских акција. Критична информациона инфраструктура постала је рањива на активности хакера, криминалаца и терориста. Велику опасност по критичну информациону инфраструктуру

[103] *Дефиниција је донета на основу документа који је издала Комисија ЕУ, Green Paper on a European programme for critical infrastructure protection (COM 576 final), Brusels, 17.11.2005.*

представљају малициозни програми и кодови (компјутерски вируси, црви, логичке бомбе, тројанци), који за циљ имају модификовање и уништење информационих система или блокирање компјутерских система. Прислушкивање комуникације и крађа података који се размењују путем компјутерских мрежа, као и модификовање нормалних функција компјутерских мрежа и спречавање приступа разним информационим службама често су коришћени видови напада на критичну информациону инфраструктуру. Већина оваквих и сличних напада могу се реализовати путем интернета за свега неколико секунди, а починиоцима је често тешко ући у траг, па је стога неопходна континуирана и непрекидна заштита критичне информационе инфраструктуре.

У оквиру процеса формирања политике заштите критичне инфраструктуре у Бугарској постоји низ активности и процена које заједно чине целину. Најбитније активности везане за формирање политике заштите критичне инфраструктуре су:[104]

1. Идентификација главних сектора, подсектора и осталих елемената критичне инфраструктуре и утврђивање *најкритичнијих* међу њима (путем секторске анализе). Критичност се мери на основу очекиваног негативног утицаја који би имало отказивање или спречавање функционисања неког критичног сектора. Што је већи негативни утицај, већа је и *критичност* инфраструктуре. Критеријуми на основу којих се утврђује потенцијални негативни утицај инцидента и отказивања критичне инфраструктуре су:[105]

   a) Негативан утицај на јавност, тј. на становништво (број грађана који су угрожени отказивањем инфраструктуре - очекивани број погинулих, повређених, оболелих, евакуисаних људи),
   b) Економски утицај (утицај који отказивање инфраструктуре има на БДП, други економски губици, деградација производа и служби),

[104]*Engelbrekt, K., Förberg, M., Managing Crises in Bulgaria, Elanders Gotab, Stockholm, pp. 27-43, 2005.*
[105]*Dunn,M., Mauer, V., International critical information infrastructure protection handbook, ETH Center for conflict studies, Vol. I, Zurich, pp. 347, 2006.*

c) Утицај на животну средину,

d) Политички и психолошки утицај (нпр. утицај који отказивање инфраструктуре има на смањење поверења које грађани имају у Владу и друге државне институције у погледу решавања оваквих инцидената),

e) Временски аспект (дужина трајања негативног утицаја који изазива отказивање или спречавање нормалног функционисања критичне инфраструктуре - да ли је у питању инцидент чији ефекат се осећа само непосредно након што се догоди, инцидент чији се ефекат осећа дан или два након инцидента, недељу дана или неки дужи временски период).

2. *Идентификација, карактеризација и процена претњи по критичну инфраструктуру*. Претње по критичну инфраструктуру представљају намерни напади, природне катастрофе и људске грешке. У оквиру процене претњи, неопходно је утврдити способност могућих уљеза, нападача, терориста да успешно изврше нападе и извршити процену намера нападача.

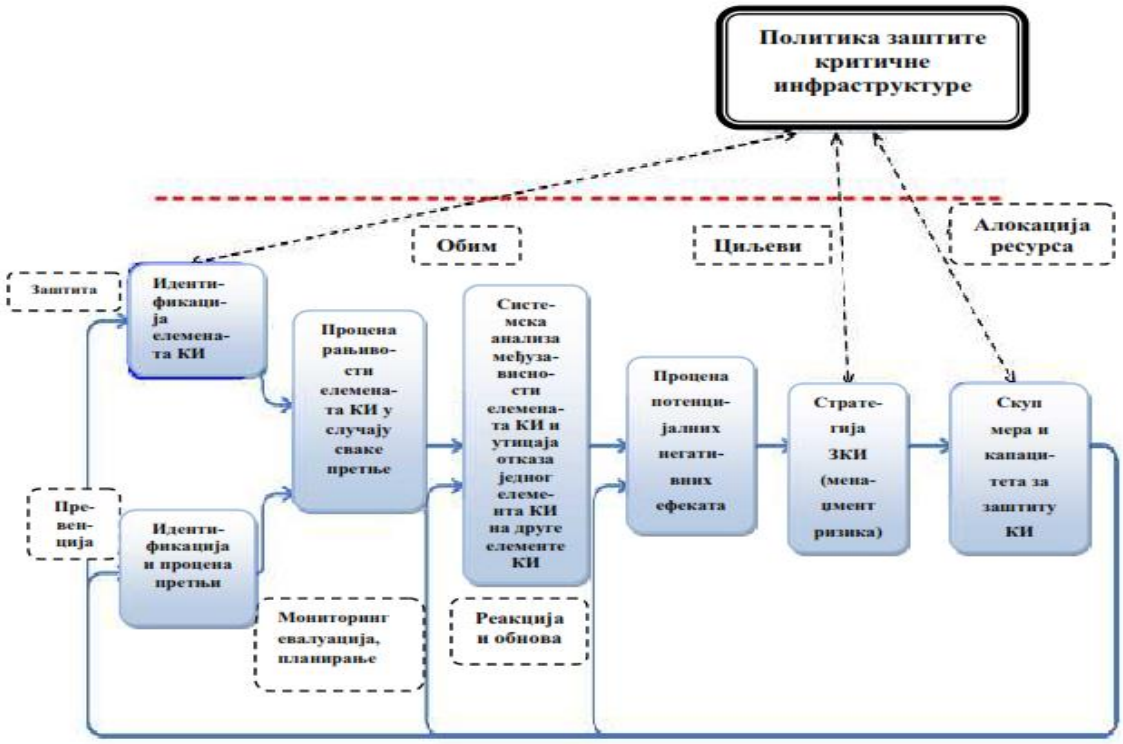
3. *Процена рањивости главних сектора критичне инфраструктуре у односу на специфичне претње.* Рањивост се може дефинисати као постојање слабости (осетљивих тачака), које могу бити изложене нападима, природним катастрофама исл.

4. *Процена међузависности између подсистема и инфраструктура*, уз фокусирање на оним међузависностима које потенцијално доводе до домино ефекта или сличних повезаних отказивања критичних инфраструктурних сектора. Међузависности и повезаност критичних инфраструктура су од суштинског значаја приликом доношења мера заштите критичне инфраструктуре, с обзиром на то да оштећење једног инфраструктурног сектора може последично да има ефекат на један или више других сектора (па чак и да више оштети неке друге секторе, него сектор на који је извршен напад, односно сектор који је први угрожен).

5. *Процена ризика (односно процена последица које се могу очекивати услед*

одређених напада на критичне инфраструктурне секторе, укључујући све типове негативних утицаја - губитак људских живота, економске губитке итд.). Процена ризика односи се на вероватноћу одређених инцидената. Резултати ових процена се након свега користе за идентификовање и приоритизацију стратегија и мера којима ће се смањити ризици и ублажити претње по критичну инфраструктуру.

6. *Разрада стратегије заштите критичне инфраструктуре*. Ова стратегија за циљ има ублаживање претњи по критичну инфраструктуру, смањење ризика и ублажавање евентуалних последица напада, природних катастрофа и непогода, људских грешака, по критичну инфраструктуру.
7. Формулисање мера и капацитета за заштиту критичне инфраструктуре и смањење ризика у оквирима стратегије.[106]



Слика 2. Приказ процеса заштите критичне инфраструктуре у Бугарској[107]

[106] *Engelbrekt, K., Förberg, M., Managing crises in Bulgaria, Elanders Gotab, Stockholm, pp. 27-43, 2005.*
[107] *Tagarev, T., Pavlov, N., Planning measures and capabilities for protection of critical infrastructures - study case of Bulgaria, pp. 42, 2007.*

Формирање политике заштите критичне инфраструктуре (ЗКИ) укључује одлуке о обиму критичних инфраструктура, затим одлуке о циљевима политике ЗКИ, одлуке о мерама за идентификовање и приоритизовање критичних инфраструктура и одлуке о алокацији ресурса за ЗКИ.

Процес заштите критичне инфраструктуре у Бугарској подразумева имплементацију седам корака приказаних на слици као и повратну информацију о резултатима мера заштите критичне инфраструктуре (представља интерактиван процес).

Оквири процеса планирања капацитета за заштиту критичне инфраструктуре морају да дефинишу и поставе баланс између четири кључне компоненте: циљева, стратегије и распореда улога између различитих државних и приватних организација, начина имплементирања стратегије и управљања ризицима.[108] Термин *капацитети за заштиту критичне инфраструктуре* се у бугарском Закону о кризном менаџменту дефинише као скуп ресурса којима се постиже мерљиви резултат у области заштите критичне инфраструктуре и остварује одређени квалитет резултата.[109]Сем четири главне компоненте за детаљније описивање процеса планирања заштите критичне инфраструктуре неопходно је дефинисати скуп могућих сценарија, као и скуп задатака који се требају обавити у случају ових сценарија.

Заштита критичне информационе инфраструктуре у Бугарској има три стратешка циља:[110]

- Превенцију сајбер-напада на критичне инфраструктуре,
- Смањење националне рањивости на сајбер-нападе,
- Минимизирање штете и времена опоравка од сајбер-напада који се догоде.

Како би се постигли ови циљеви, неопходна је нова стратегија, која укључује

[108]*Bartlett, H., Holman, G., Somes, E.T.,The art strategy and force planning, Strategy and force planning, Bartlett model, Naval War College Press, Newport, pp.17-33, 2004.*
[109]*Tagarev, T., The Art of Shaping Defense Policy: Scope, components, relationships (but no algorithms), The Quarterly Journal 5, No.1, pp. 15-34, 2006.*
[110]*Andreas,W., Metzger,J., Dunn,M., eds.,International CIIP Handbook center for security studies at the Swiss federal institute of technology, Zurich, 2004.*

следеће елементе:

- Предузимање превентивних мера на свима нивоима,
- Унапређење ране детекције и брзе реакције ради контроле штете и потраге за евентуалним нападачима,
- Лимитирање утицаја различитих напада на КИИ на друштво и државу,
- Брзо враћање угрожених (нападнутих) информационих система на нормалан режим рада.

Претње и рањивости састоје се од физичке, информационе и психолошке компоненте; Стога је неопходан отворени дијалог о новим рањивостима и претњама по КИИ. Такође, неопходно је дефинисање нових физичких, информационих и психолошких заштитних мера.

Спровођење мера заштите КИИ на националном нивоу врши се кроз пет националних приоритета Бугарске у области заштите КИИ, који се могу дефинисати на следећи начин:[111]

- Формирање националног система за сајбер-безбедност,
- Развој националног програма за редуковање претњи и рањивости у области сајбер-безбедности,
- Стварање и јачање свести грађана Бугарске о важности сајбер-безбедности и о мерама за очување сајбер-безбедности, као и формирање програма обуке у овој области,
- Обезбеђивање система државне управе,
- Јачање националне безбедности и међународне сарадње у области сајбер-безбедности.

*Проблеми заштите КИИ у Бугарској*са којима се Бугарска суочава у области заштите КИИ су:[112]

- Недостатак законских оквира - овај проблем у великој мери успорава и отежава сваки судски процес везан за сајбер-криминал,

[111]*Ibid.*
[112]*Nickolov, E., Critical information infrastructure protection: Analysis, evaluation and expectations - study case of Bulgaria, Information & Security, An International Journal, Vol.17, pp. 116-117, 2005.*

- Недостатак обученог особља,
- Недостатак неопходних техничких алата за одговор на сајбер-нападе,
- Недостатак поузданих система за интеракцију са специјалним организацијама из других земаља,
- Мањак националних организација на државном нивоу које би се бавиле координацијом активности у области заштите КИИ,
- Недостаци у националној стратегији везани за непостојање одредби на основу којих би се одређени финансијски ресурси државе усмеравали на развој организација које ће се бавити заштитом КИИ и координацијом активности у области заштите КИИ,
- Недостатак националног акционог плана на основу којег би се национални фондови повезивали са међународним пројектима на регионалном нивоу, на основу којих би се развијале организације које ће се бавити заштитом КИИ и координацијом активности у области заштите КИИ.

Бугарска ради на развоју законских оквира којима би се владине агенције овластиле да читају електронску пошту, пресрећу бежичну комуникацију (позиве и интернет комуникацију), да надзиру употребу рачунара, итд. Посебним законом су незаконитим проглашени чинови намерног неовлашћеног упада у рачунаре и намерно изазивање штете на другим рачунарима слањем малициозних програма путем интернета. Пре три године је и хаковање законом означено као кривично дело и уведен је појам сајбер-тероризма.

У области заштите КИИ Бугарска ради на неколико пројеката и унапређује заштиту своје КИИ у неколико сегмената:[113]

- Ради се на остварењу ефикасније сарадње између судских органа и специјалних служби за ЗКИИ балканских и европских земаља, и уопштено на развоју међународне сарадње,
- Бугарска ради на унапређењу националне стратегије за превенцију и

[113] *Tagarev, T., Pavlov, N., Planning measures and capabilities for protection of critical infrastructures in Bulgaria, pp. 46, 2007.*

борбу против сајбер-криминала,

- Ради се на развоју националне службе за борбу против сајбер-криминала и међународну сарадњу приликом транснационалних сајбер-инцидената,
- Проширује се међународна сарадња у области правосудне помоћи у борби против сајбер-криминала,
- Доносе се специјални закони из области телекомуникација и компјутерских мрежа у складу са тренутним међународним стандардима и са Конвенцијом Европске комисије о сајбер-криминалу.

Препорука бугарских стручњака у области заштите КИИ је и да се оформи једна контакт служба у коју би долазиле све релевантне информације везане за заштиту КИИ и за актуелне ванредне ситуације, и која би након пријема те информације прослеђивала свим релевантним службама. Тиме би се успоставила квалитетнија координација активности свих учесника у заштити критичне информационе инфраструктуре, а као последица боље координације, олакшало би се идентификовање извора напада, као и формирање и спровођење решења за одбрану од напада или за опоравак од сајбер-напада.

4.4.3.2. Република Словенија

Критична инфраструктура у Словенији је веома разноврсна и комплексна.Након стицања независности Словенија је успела релативно брзо да уђе у састав ЕУ, а уласком у ЕУ обавезана је и да своје законске регулативе усклађује са европским регулативама на свим пољима, па и на пољу ЗКИ.

У Републици Словенији 2006. Године установљена је међуресорна група за усклађивање припрема за заштиту критичне инфраструктуре са следећим задацима:

- Припрема прегледа организованости и нормативне уређености заштите критичне инфраструктуре према појединачним активностима, тј. подсистемима националне безбедности;

- Проучавање организације процедура, као и смерова развоја заштите критичне инфраструктуре на узорку чланица НАТО и ЕУ;
- Припрема оцене безбедносних околности, ризика и извора угрожавања државне инфраструктуре, као и оцена могућег опсега последица по становништво, економију и окружење;
- Одређивање унифицираног означавања виталне инфраструктуре државе;
- Обликовање предлога примерених мера и поступака за заштиту критичне инфраструктуре, узимајући у обзир усмерења и ставове НАТО и ЕУ;
- Припрема предлога органа и организација који би требало да планирају мере за заштиту критичне инфраструктуре.

Сектори критичне инфраструктуре у Републици Словенији утврђује се на основу основних критеријума за одређивање критичне инфраструктуре Републике Словеније.

На основу међусекторске анализе инфраструктуре може се формирати списак критичних инфраструктура Словенијеи утврдити који се сектори могу сматрати критичнијим у односу на друге.

Сектори критичне инфраструктуре Републике Словеније су:

- Сектор критичне инфраструктуре, који обезбеђује енергетску подршку,
- Сектор критичне инфраструктуре, која пружа саобраћајне везе,
- Сектор за критичне инфраструктуре, који обезбеђује храну,
- Сектор критичне инфраструктуре, који обезбеђује снабдевање питком водом,
- Сектор критичне инфраструктуре, која пружа медицинску негу,
- Сектор критичне инфраструктуре, који обезбеђује финансирање,
- Сектор критичне инфраструктуре, што осигурава заштиту животне средине,
- Сектор критичне инфраструктуре, која пружа информације и подршку комуникације.[114]

Одређивање приоритетних сектора које проистичу из рада међузависности и

[114] *gp.mo@gov.si.*

интеракције између сектора критичне инфраструктуре, као кварова у једном сектору могу имати значајан утицај на друге секторе. Према приоритетима деловања, директан утицај на другим критичним секторима инфраструктуре се класификује према следећем редоследу приоритета:

- снабдевање електричном енергијом,
- информације и комуникације подршка,
- снабдевање питком водом,
- снабдевање храном,
- пружање здравствене заштите,
- набавка нафтних деривата,
- железнички саобраћај,
- ваздушни саобраћај,
- речни саобраћај,
- снабдевање гасом,
- платни промет,
- обезбеђивање снабдевања готовином,
- функционисање државног буџета и
- заштита животне средине.[115]

У Словенији постоји интерес и иницијатива за увођењем још неких критичних инфраструктурних сектора као што су затворска инфраструктура (чије увођење предлаже Министарство правде) и инфраструктура културног наслеђа (чије увођење предлаже Министарство културе). Анализа свих критичних сектора у Словенији јасно указује на њихову велику повезаност. Ово је посебно приметно кад су у питању сектори саобраћаја и транспорта, енергетике, информационих и комуникационих технологија, финансија, воде и хране.

С обзиром на то да Словенија има малу инфраструктуру у односу на остале европске државе, као и у односу на Европску унију, она углавном зависи од страних инфраструктура, а мање сама утиче стабилношћу своје

[115] *Ибид.*

инфраструктуре на стабилност и нормално функционисање других земаља. Ово се јасно може увидети, како неки експерти из домена финансија тврде, на примеру евентуалног колапса финансијског система Словеније. Наиме, колапс финансијског система Словеније имао би мањи, скоро занемарљив ефекат на европски финансијски систем. Сви системи обављања међународних финансијских трансакција лоцирани су ван Словеније.

Географске области у којима су концентрисани критични објектимогу се разврстати у неколико категорија:[116]

- критични објекти,
- критичне везе (повезаности),
- критична укрштања инфраструктура и
- критични процеси који се дешавају у критичним објектима или у близини.

Традиционално се објекти критичне инфраструктуре посматрају као материјална категорија (физички објекти). Међутим, сем њих постоје још две категорије које се не могу сматрати материјалним: ваздушне и пловне руте. Ваздушна и поморска навигација заснивају се на коришћењу претходно утврђених рута (представљају везе између материјалних инфраструктурних објеката, као што су аеродроми и луке). И поред тога што руте не представљају физичке објекте, опште је прихваћен став да се посматрају као критични објекти, како у оквиру својих сектора тако у оквиру читавог друштва. Руте се сматрају критичним објектима јер њихово ометање може да доведе до проблема, па и криза у ваздушном и водном саобраћају.

Објекти критичне инфраструктуре асиметрично су дистрибуирани у оквиру Словеније. Критичне инфраструктуре у већој мери су смештене у урбаним срединама. Посебно су критичне мулти-инфраструктурне области тј. области у којима је лоциран већи број различитих типова инфраструктура. У Словенији постоје два примера таквих области: главни национални аеродром и национална лука. У оквиру главног националног аеродрома

[116]*Prezelj, I., Kustec Lipicer, S., Public and policy management of critical infrastructure: Lessons from Integral Nations Cross-Sectoral Scanning in Slovenia, IRSPM Conference, Panel: Risk and crisis management in the public sector, Berne, pp. 15, 2010.*

смештен је већи број инфраструктура као што су инфраструктура ваздушног саобраћаја, мреже информационих и комуникационих технологија, банке, мењачнице, агенције за шпедицију, пошта, нафтна компанија, војна инфраструктура, инфраструктура спасилачких служби, разни малопродајни објекти. Слична инфраструктура налази се и склопу главне националне луке. Критична инфраструктура је највећим делом смештена у главном граду Љубљани. Словенија је у извесној мери децентрализована држава у којој осим главног града (у коме живи око 13% становништва Словеније) одређени значај имају и други градови и индустријске зоне. Ипак, главна интернет чворишта, финансијске институције и објекти хемијске индустрије лоцирани су у главном граду. Љубљана се налази на споју два велика европска саобраћајна коридора (Коридор V и Коридор X), поред којих је такође смештен велики део инфраструктуре. Највећи део словеначке финансијске инфраструктуре лоциран је у градском центру, а у ширем подручју Љубљане (Љубљанска долина) налази се највећи део критичних објеката словеначке хемијске индустрије. Такође, много других типова инфраструктуре смештено је у главном граду (инфраструктура друмског и железничког саобраћаја, делови система за дистрибуцију воде и хране и инфраструктура службе хитне помоћи и медицинске неге. С друге стране, велики делови инфраструктуре сектора вода, хране и енергетике смештене су изван урбаних зона (нпр. системи за сакупљање воде, фарме и електране).

Критичне секторске међузависностипостоје између критичних сектора и осетљивих подсектора. У утицајне секторе од којих у већој мери зависи функционисање многих других инфраструктурних сектора убрајају се производња и дистрибуција струје, информационе и комуникационе технологије, нафта и гас, друмски саобраћај и транспорт и финансијска инфраструктура. Колапс и прекид функционисања ових инфраструктура имају снажан ефекат на функционисање осталих инфраструктура. С друге стране, у најосетљивије инфраструктуре убрајају се здравствени сектор, сектор производње и дистрибуције хране, хемијска индустрија, снабдевање водом и контрола квалитета воде.

4.4.3.3. Република Хрватска

Република Хрватска је током 2013. године донела прописе у подручју заштите критичних инфраструктура и то: Закон о критичним инфраструктурама, Правилник о методологији за израду анализе ризика пословања критичних инфраструктура и Одлуку о одређивању сектора из којих средишња тела државне управе идентификују националне критичне инфраструктуреи листе редоследа сектора критичних инфраструктура.[117]

У Републици Хрватској је 28.05.2013. године донет Закон о критичним инфраструктурама.[118] Овим Законом уређују се националне и европске критичне инфраструктуре, сектори националних критичних инфраструктура, управљање критичним инфраструктурама, израда анализе ризика, израда сигурносних планова власника, сигурносни координатор за критичну инфраструктуру, поступање са осетљивим и класификованим подацима, као и надзор над спровођењем овог Закона[119].

Овим се Законом у законодавство Републике Хрватске преузима правна тековина Европске уније садржана у Директиви Већа 2008/114/ЕС из 2008. године, која се односи на идентификацију и одређивање европских критичних инфраструктура и процени потребе за унапређењем њихове заштите.[120]

У овом документу Републике Хрватске националне критичне инфраструктуре су дефинисане као системи, мреже и објекти од националне важности, чији прекид деловања или прекид испоруке роба или услуга може имати озбиљне последице на националну сигурност, здравље и животе људи, имовину и околину, сигурност и економску стабилност и непрекидно

---

[117] *Закон о критичним инфраструктурама Републике Хрватске (Народне новине, бр. 56/13); Правилник о методологији за израду анализе ризика пословања критичних инфраструктура (Народне новине, бр. 128/13); Одлука о одређивању сектора из којих средишња тијела државне управе идентифицирају националне критичне инфраструктуре те листе редосљеда сектора критичних инфраструктура (Народне новине, бр. 118/13).*

[118] *Закон о критичним инфраструктурама Републике Хрватске, 28.05.2013. године.*

[119] *Деканић, И., Положај Хрватске у могућим енергетским и геополитичким кризама, у: Хрватска - како сада даље, Загреб, Центар за демократију и право Мико Трипало, 2008.*

[120] *Таталовић, С., Енергетска сигурност и критична инфраструктура, Загреб, Политичка култура, 2008.*

функционисање власти.[121]

Сектори националних критичних инфраструктура су подељени на следећи начин:

- енергетика (производња, укључујући акумулације, бране, пренос, складиштење, транспорт енергената и енергије, као и системи за дистрибуцију),
- комуникациона и информациона технологија (електронске комуникације, пренос података, информациони системи, пружање аудио и аудио-визуелних медијских услуга),
- промет (друмски, железнички, ваздушни, поморски и промет унутрашњим пловним путевима),
- здравство (здравствена заштита, производња, промет и надзор над лековима),
- храна (производња и снабдевање храном и систем сигурности хране и робних залиха),
- финансије (банкарство, инвестиције, системи осигурања и плаћања),
- производња, складиштење и превоз опасних материја (хемијски, биолошки, радиолошки и нуклеарни материјали),
- јавне службе (осигурање јавног реда и мира, заштита и спашавање, хитна медицинска помоћ),
- национални споменици и друге вредности.

Осим наведених сектора, Влада Републике Хрватске може одлуком одредити критичне инфраструктуре и из других сектора. Анализом ризика утврђују се укупни ефекти прекида рада критичне инфраструктуре, а спроводи се уз поштовање међусекторских и секторских мера.

Међу секторска мерила се примењују анализаи ризика свих критичних инфраструктура према следећем редоследу и укључују:

- људске губитке (процењује се могући број смртно страдалих или озлеђених због прекида рада поједине критичне инфраструктуре),

[121] *Стратегија националне сигурности Републике Хрватске, Народне Новине, бр. 32/2002.*

- привредне губитке (процењују се с обзиром на значај привредног губитка и/или умањење квалитета производа или услуга),
- утицај на јавност (који се процењује с обзиром на утицај на поверење јавности, телесне патње и ремећење свакодневног живота, укључиво и губитак основних и јавних услуга).

Ради успешне имплементације Закона о критичним инфраструктурама Републике Хрватске, успостављање Националног центра за критичне инфраструктуре (НЦКИ) представља важан задатак Владе РХ, надлежног тела државне управе, девет ресорних министарстава, власника/оператора критичних инфраструктура и других заинтересованих страна. НЦКИ би имао јасно дефинисане задатке, надлежности и одговорности у спровођењу прописа из области критичних инфраструктура, координисање и побољшану сарадњу свих учесника и хоризонтално и по вертикали. Што се устројства тиче, предлаже се избор једног од следећа два модела. Први, према којему би се НЦКИ устројио као самостални сектор, као служба унутар Сектора за цивилну заштиту или као одсек унутар Службе за превентиву, планирање и аналитику у оквиру Сектора за цивилну заштиту. Други, према коме би се НЦКИ устројио међусекторски као засебна агенција Владе РХ.

Што се његове функционалности тиче, НЦКИ би био задужен за: (1) Израду целовитог концепта заштите критичне инфраструктуре; (2) Ревизију, хармонизацију и унапређење референтног легислативног оквира и (3) Надзор спровођења тог легислативног оквира. У неке од важних краткорочних активности НЦКИ спадају: (1) Израда секторских и међусекторских мерила за идентификовање разреда критичности; (2) Дефинисање мера заштите које се морају примењивати у зависности о идентификованом разреду критичности; и (3) Спровођење поступка за идентификовање разреда критичности. Без обзира на будуће устројство, НЦКИ ће своје задатке испуњавати преко повереништва за заштиту критичне инфраструктуре (међуресорна радна група).

Чланови тог повереништва постали би већ именовани безбедносни координатори за критичну инфраструктуру. Основни задатак повереништва

састојао би се у верификацији документације и поступака израђених од стране НЦКИ. Такав приступ раду подразумева да НЦКИ има мандат за ангажовање одговарајућих стручних институција и појединаца са сврхом израде докумената и поступака везаних за успоставу система заштите критичне инфраструктуре. Рад повереништва не би захтевао нека значајна додатна средства.

Секторска мерила одређују надлежна средишња тела државне управе у сарадњи са регулаторним агенцијама и струковним удружењима за сваки појединисектор.

Средишња тела државне управе одређују сигурносног координатора за критичну инфраструктуру и његовог заменика за сваки сектор критичне инфраструктуре из свог делокруга рада.

Власници/управници критичних инфраструктура дужни су одредити сигурносног координатора за критичну инфраструктуру који је у спровођењу заштите критичне инфраструктуре одговоран за комуникацију у сигурносним питањима између власника/управника и надлежног средишњег тела државне управе у чијем је делокругу критична инфраструктура, како би се осигурала заштита и континуитет рада критичне инфраструктуре.[122] Примера ради, у овом закону је дефинисано да ће се новчаном казном од 500.000 до 1.000.000 куна казнити за прекршај власник/управник критичне инфраструктуре ако:

- не изради документацију везану за анализу ризика,
- не изради и не донесе сигурносни план власника/управника који обухвата мере заштите и осигурања наставка пословања критичне инфраструктуре, испоруке услуга/робе,
- не одреди сигурносног координатора за критичну инфраструктуру.

За прекршај из става 1. овога члана казниће се новчаном казном од 10.000 до 50.000 куна и одговорна особа власника/управника критичних инфраструктура.

[122]*Перинић, Ј., Кризно комуницирање на случају трагедије ватрогасаца на Корнату, Медианали, Свеучилиште у Дубровнику, Дубровник, стр. 47-66, 2007.*

5. ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

5.1. НОРМАТИВНО-ПРАВНИ ОКВИР ФУНКЦИЈЕ И ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

Нормативно-правни систем РС подразумева да домаћи правни акти буду у сагласности са Уставом РС.[123] Тим Уставом, поред осталог, утврђене су надлежности Републике и општина у области безбедности и јавног здравља. Према члану 97. Устава, Република обезбеђује „одбрану и безбедност РС и њених грађана; мере за случај ванредног стања“, као и „производњу, промет и превоз отровних, радиоактивних и других опасних материја“; ..и..„систем у областима здравства, социјалне заштите“ итд. Чланом 190. Устава, утврђено је да општине брину о заштити од елементарних и других непогода..., и о потребама грађана у области здравствене заштите.

Полазне основе за успостављање система леже у *Уставу Републике Србије* који дефинише да су основна права сваког човека: „...право на заштиту свог физичког и психичког здравља...“. Надлежност Републике Србије је да уређује и обезбеђује „одбрану и безбедност Републике Србије и њених грађана и мере за случај ванредног стања“; „систем заштите и унапређења животне средине; заштиту и унапређивање биљног и животињског света; производњу, промет и превоз отровних, запаљивих, експлозивних, радиоактивних и других опасних материја“ и „заштиту културних добара“. Надлежност општине је да се преко својих органа: „стара о заштити животне средине, заштити од елементарних и других непогода и заштити културних добара“.

Стратегија националне безбедности из 2009. године као најважнији стратешки документ који утврђује основе политике безбедности у заштити националних интереса, идентификује и дефинише 22 изазова, ризика и претњу по безбедност Републике Србије. Два ризика директно утичу на

[123] *Устав Републике Србије, „Службени гласник РС“, бр. 83/06, Београд, 08.11.2006., чл. 97.*

безбедност становништва и материјалних добара: 1) „Последице елементарних непогода и техничких и технолошких несрећа, као и угрожавање животне средине и здравља грађана услед радиолошке, хемијске и биолошке контаминације“ и 2) „Опасности повезане са појављивањем и ширењем инфективних болести код људи и зараза код животиња могао бити све израженији“. Један од основних циљева политике националне безбедности је и *унапређење безбедности грађана, друштва и државе,* кроз формирање „ефикасног система одбране“.

Након Стратегије националне безбедности из 2009. године, донети су Закон о ванредним ситуацијама (донет 2009, а допуњен је амандманима 2011. и 2012. године) и Национална стратегија заштите и спасавања у ванредним ситуацијама.

Законом о ванредним ситуацијама[124], регулишу се деловање, проглашавање и управљање ванредним ситуацијама, систем заштите и спасавања људи, материјалних и културних добара и животне средине од елементарних непогода, техничко-технолошких несрећа - удеса и катастрофа, последица тероризма, ратних и других већих несрећа, надлежности државних органа, аутономних покрајина, јединица локалне самоуправе и учешће полиције и Војске Србије у заштити и спасавању, затим права и дужности грађана, привредних друштава, других правних лица и предузетника у вези са ванредним ситуацијама, деловање организација и делатност цивилне заштите на заштити, спасавању и отклањању последица елементарних непогода и других несрећа, регулишу се финансирање, инспекцијски надзор, међународна сарадња и друга питања од значаја за организовање и функционисање система заштите и спасавања. Све горе наведено има за циљ изградњу јединственог система заштите и спасавања у складу са овим Законом и другим прописима, као и програмима, плановима и другим документима који се односе на заштиту и спасавање и цивилну заштиту.

Законом је предвиђено постојање система осматрања, раног упозоравања, обавештавања и узбуњивања. У Закону се наводи да је основни задатак

[124] *„Службени гласник РС“, бр. 111/09, 92/2011 и 93/2012.*

система осматрања, раног упозоравања, обавештавања и узбуњивања откривање, праћење и прикупљање података о свим врстама опасности које могу угрозити људе, животну средину, материјална и културна добра. Имаоци телекомуникационих система и средстава дужни су да служби 112 (112 је законом предвиђени интегрисани број свих хитних служби) омогуће приоритетно коришћење веза у ванредним ситуацијама.

У Закону се не помиње критична инфраструктура, али сам Закон представља јако добру основу за развој закона о заштити критичне инфраструктуре и свих осталих закона који из њега произилазе.

Национална стратегија заштите и спасавања[125] комплементарна је са Законом о ванредним ситуацијама. Као образложење за усвајање и спровођење стратегије наведено је да је регион југоисточне Европе све више угрожен разним врстама природних опасности (поплаве, суше, екстремно високе температуре, земљотреси, клизишта, олујне непогоде, итд.), техничко-технолошким несрећама, дејством опасних материја и другим стањима опасности. Глобалне климатске промене такође доприносе уништавању животне средине, са штетним утицајем на здравље људи, опстанак многих природних врста и културно наслеђе. Национална стратегија заштите и спасавања обухвата системе превенције, ублажавања, заштите и спасавања и обнове. Основ за спровођење Националне стратегије како се наводи у Стратегији „садржан је у Закону о ванредним ситуацијама којим је дефинисано успостављање интегрисаног система заштите и спасавања. Поред законодавног оквира, основ за израду Националне стратегије садржан је и у другим националним и међународним документима, као што су: Национални програм за интеграцију Републике Србије у Европску унију, Национална стратегија одрживог развоја, Стратегија националне безбедности Републике Србије, Миленијумски циљеви развоја, које су дефинисале чланице Уједињених нација и Хјого оквир за деловање

[125] *Стратегија је објављена у „Службеном гласнику РС“, бр. 86/2011 од 18.11.2011.*

2005 - 2015: Развој отпорности нација и заједница на катастрофе".[126]

Стратегија одбране Републике Србије[127] дефинише 10 (десет) изазова, ризика и претњи по одбрану Републике Србије, од којих се посебно издваја: 1) „елементарне непогоде и хемијске, биолошке, нуклеарне, техничке и технолошке несреће"; дефинише три основна циља политике одбране од којих је посебно важан: формирање *„ефикасног система одбране",* чији је циљ заштита одбрамбених интереса кроз реализацију војне и цивилне одбране. Носилац цивилне одбране су субјекти одбране (од Републике до општине), привредна друштва, јавне службе и остали субјекти и снаге система одбране. Тежишна мисије цивилне одбране је *заштита и спасавање* (ЗиС), првенствено *људи*, затим материјалних и културних добара, очување животне средине, са основном снагом одбране-цивилном заштитом.

Осим напред наведених наведених стратегија и закона везаних за националну безбедност, ванредне ситуације и заштиту и спасавање у Републици Србији постоји још законских оквира који су директно или индиректно везани за законски још недефинисану заштиту критичне инфраструктуре.[128]

Законом о безбедности и интероперабилности железнице[129] уређују се услови којима се омогућава да железница у Републици Србији буде безбедна и интероперабилна у циљу несметаног одвијања железничког саобраћаја.

Безбедност железнице, у смислу овог закона, обухвата услове које испуњава железнички систем и железнички радници, као и друге услове од значаја за остваривање безбедног и несметаног одвијања железничког саобраћаја. Интероперабилност железнице, у смислу овог закона, је способност железничког система да омогући безбедан и непрекинут саобраћај возова који испуњавају потребне захтеве за одређену мрежу. Та способност зависи

---

[126]*Mićović, M., Jakovljević, V., The system of critical infrastructure of the Republic of Serbia in response to emergencies - Opportunities and perspectives, V međunarodni stručno-znanstveni skup, Zaštita na radu i zaštita zdravlja, Veleučilište u Karlovcu, Zadar, Hrvatska, str. 900-906, 2014.*

[127]*„Службени гласник РС", бр. 88 од 28.10.2009.*

[128]*Мићовић, М., Специфичности заштите критичне инфраструктуре, Безбедност, стр. 165-174, бр. 3/2014.*

[129]*„Службени гласник РС", бр. 104/2013 и 66/2015.*

од свих регулаторних, техничких и експлоатационих услова који морају бити испуњени да би се задовољили основни захтеви за интероперабилност. У овом закону је посебно обрађена заштита железничке инфраструктуре и возила.

Влада РС је донела Стратегију[130] развоја железничког, друмског, водног, ваздушног и интермодалног транспорта у РС од 2008. до 2015. године, којом се утврђује стање у тим областима транспорта, успоставља концепт развоја инфраструктуре и транспорта, дефинишу дугорочни и краткорочни циљеви развоја транспортног система и акциони план за њихову реализацију. Унапређење транспортне инфраструктуре се, између осталог, односи на измештање транзитних токова из урбаних градских зона, а нарочито кад се транспортују опасни терети.

Стратегија је циљно оријентисана и заснована на визији за 2015. годину која узима у обзир друштвени развој, опредељење Републике Србије ка чланству у Европској унији, одрживи развој транспортног система и стабилне институције. Закон о водама[131] из 2010. године прописују мере заштите вода, правила прерађивања, правила утврђивања здравствене исправности воде, али и мере заштите од штетног дејства вода.

Закон о безбедности хране[132],који је ступио на снагу 01.01.2009. године, регулише се производња воћа и поврћа, употреба хемикалија, гајење стоке, контрола хране и уводи систем брзог обавештавања и узбуњивања уз примену хитних мера за управљање кризним ситуацијама.

У оквиру сектора информационих и комуникационих технологија постоји највећи напредак када је реч о усклађивању законске регулативе са европским законима. Тако су у оквиру овог сектора, за који је надлежно Министарство трговине, туризма и телекомуникација, усвојени следећи закони и стратегије:

---

[130] *„Службени гласник РС“, бр. 4/2008.*
[131] *Закон је објављен у „Службеном гласникуРС“,бр. 30/10, 07.05.2010.*
[132] *http://www.mpt.gov.rs/postavljen/123/bezbednost1.pdf10.02.2013.*

Закон о електронским комуникацијама[133]- овим Законом уређују се услови и начин за обављање делатности у области електронских комуникација, надлежности државних органа у области електронских комуникација, затим, уређује се положај Републичке агенције за електронске комуникације, прописују се начини спровођења јавних консултација у области електронских комуникација, уређује се управљање и коришћење адреса и бројева, управљање и коришћење и контрола радио-фреквенцијског спектра, дистрибуција и емитовање медијског садржаја, заштита права корисника и претплатника, безбедност и интегритет електронских комуникационих мрежа и услуга, тајност електронских података, законито пресретање и задржавање података, даље се уређују мере за поступање супротно одредбама овог Закона, као и друга питања везана за функционисање и развој електронских комуникација у Републици Србији.

Стратегија развоја електронских комуникација[134] у Републици Србији од 2010. до 2020. године - има велики стратешки значај и треба да постави главне правце и циљеве успешног развоја електронских комуникација у Републици Србији. Стратегија представља прагматичан скуп неопходних мера које би требало да Републици Србији обезбеде повољнију позицију у глобалној економији.

Стратегија развоја информационог друштва у Републици Србији до 2020. године[135]- У оквиру Европске уније ИКТ су препознате као главни фактор утицаја на економски раст и иновативност,[136] а међу седам водећих иницијатива економске стратегије Европа 2020[137] налази се *Дигитална агенда за Европу*, што показује значај који ИКТ имају у развоју модерне економије. Заједно са стратегијом у области телекомуникација, ова стратегија чини Дигиталну агенду за Републику Србију. Циљ Стратегије је да

[133]*Ступио на снагу 01.01.2012.*
[134]*„Службени гласник РС“, бр. 68/10, 02.09.2010.*
[135]*Усвојена 08.07.2010.*
[136]*Annual Information Society Report 2007 - Communication from the Commission to the European parlament, the Council, the European Economic and Social Committee and the Committee of the regions, Bruses, 30th March 2007.*
[137]*Europe 2020 - Astrategy for smart sustainable and inclusive growth, Communication from the Commision, Brusels, 03 March, 2010.*

развој информационог друштва усмери ка искоришћењу потенцијала ИКТ за повећање ефикасности рада, економски раст, већу запосленост и подизање квалитета живота свих грађана Републике Србије. Основне идеје развоја информационог друштва чине: отворен, свима доступан и квалитетан приступ интернету, развијено е-пословање, укључујући: е-управу, е-трговину, е-правосуђе, е-здравље и е-образовање.

Стратегија развоја електронске управе у Републици Србији за период од 2009. до 2013. године-стратегија је акт Владе којим се на целовит начин дефинишу основни циљеви, начела и приоритети унапређења стања у овој области и утврђују активности које треба предузети у наредном периоду. Под изразом *електронска управа* (е-управа), у смислу ове Стратегије, подразумева се примена информационо-комуникационих технологија којом се постиже ефикаснији и ефективнији рад органа управе и ималаца јавних овлашћења у функцији вршења власти, економског раста и смањења терета администрације.

Закон о електронском документу - Електронски документ јесте скуп података којим се уређују услови и начин поступања са електронским документом у правном промету, управним, судским и другим поступцима, као и права, обавезе и одговорности привредних друштава и других правних лица, предузетника и физичких лица, државних органа, органа територијалне аутономије и органа јединица локалне самоуправе и органа, предузећа, установа, организација и појединаца којима је поверено вршење послова државне управе, односно јавних овлашћења у вези са овим документом.

Законом о електронској трговини[138] уређују се услови и начин пружања услуга информационог друштва, обавезе информисања корисника услуга, комерцијална порука, правила у вези са закључењем уговора у електронском облику, одговорност пружаоца услуга информационог друштва, надзор и прекршаји.

[138] *„Службени гласникРС“, бр. 41/2009.*

Закон о електронском потпису- дефинише електронски потпис као скуп података у електронском облику који су придружени или су логички повезани са електронским документом и који служе за идентификацију потписника. Овим Законом уређује се употреба електронског потписа у правним пословима и другим правним радњама, пословању, као и права, обавезе и одговорности у вези са електронским сертификатима, ако посебним законима није другачије одређено.

Правилник о издавању временског жига[139] донет је на основну Закона о електронском документу, у ком се већ помиње коришћење временског жига. Правилником се прописују услови и поступак регистрације издаваоца временског жига, услови које мора да испуњава систем за формирање временског жига, садржина захтева за формирање временског жига, садржај структуре података временског жига, поступак означавања времена које је садржано у њему, као и садржај и начин вођења Регистра издавалаца временског жига у Републици Србији.

Законом о потврђивању Конвенције о високотехнолошком криминалу[140] се потврђује Конвенција о високотехнолошком криминалу, настала 23.11.2001. године у Будимпешти, којом се као криминални чинови класификују дела против поверљивости, целовитости и доступности рачунарских података и система, незаконит приступ, незаконито пресретање, ометање података, ометање система, злоупотреба уређаја и низ других дела из области превара и других криминалних радњи у оквиру ИКТ сектора, а за која се држава потписница обавезује да ће прописати одговарајуће законске казне.

Закон о приватном обезбеђењу[141] у члану 4. дефинише обавезно обезбеђене објекте као објекте од стратешког значаја за Републику Србију и њене грађане, као и објекти 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.

---

[139] *„Службени гласник РС“, бр. 112/2009.*
[140] *„Службени гласник РС“, бр. 19/2009.*
[141] *„Службени гласник РС“ бр. 104/13.*

5.1.1. Закон о министарствима

Законом о министарствима је омогућено да се образују министарства и посебне организације и утврди њихов делокруг[142]. У складу са овим законом делују следећа Министарства: Министарство финансија; Министарство привреде; Министарство пољопривреде и заштите животне средине; Министарство грађевинарства, саобраћаја и инфраструктуре; Министарство рударства и енергетике; Министарство трговине, туризма и телекомуникација; Министарство правде; Министарство државне управе и локалне самоуправе; Министарство унутрашњих послова; Министарство одбране; Министарство спољних послова; Министарство просвете, науке и технолошког развоја; Министарство здравља; Министарство за рад, запошљавање, борачка и социјална питања; Министарство омладине и спорта; Министарство културе и информисања.

5.1.2. Закон о полицији

Закон о полицији је конципиран је тако да се полицијски послови обављају као јединствени у РС[143]. Овим законом створене су законске претпоставке за даљу реформу полиције које су усклађене са најбољом европско-континенталном традицијом и савременим међународним и упоредно-правним изворима на којима се заснива полиција у демократском друштву. Доношењем овог закона створени су услови за успостављање новог концепта јавне безбедности и то на законском опредељењу да се безбедносна заштита осигура за све који су на територији РС, а не само за грађане (држављане Републике Србије). Та заштита је и шира и разноврснија и заснива се на пружању више врста помоћи, увођењу спасилачке функције, хуманих и других интервенција. Закон о полицији прописао је и обавезе у погледу сарадње са свима у интересу безбедности људи и са само организованим појединцима у заштити живота и безбедности људи у свако доба. Тако, полицијски службеници штите јавну безбедност без обзира да ли се ради о опасности за људе и имовину изазваној природним непогодама, епидемијама

[142] *Закон о министарствима, Службени гласник РС, бр. 44/2014.*
[143] *Закон о полицији, „Службени гласник РС“, бр. 101/2005, 63/2009 - одлука УС и 92/2011.*

и другим облицима угрожавања или се ради о сузбијању кривичних дела. Полицијски послови у смислу појма и врста утврђени су чланом 10. Закона о полицији. Полицијске послове који се односе на извршавање других задатака утврђених законом и подзаконским актима донетим на основу овлашћења и закона, сходно члану 4. Закона о полицији, обављају полицијски службеници који примењују полицијска овлашћења (овлашћена службена лица), као и запослени на посебним и одређеним дужностима чији су послови у непосредној вези са полицијским пословима и обухватају послове противпожарне заштите. Такође, Законом о полицији је дефинисано да су полицијски службеници који обављају послове противпожарне заштите они запослени, који раде на пословима на којима опасност по живот и здравље, одговорност и тежина, природа и посебни услови рада битно утичу на смањење радне способности.

У националном праву, а ни у стратегијским документима Републике Србије, не постоји одређење појма критичне инфраструктуре. Начелно, то су средства и имовина која је кључна за неометано функционисање економије и друштва.

Наиме, у документима Националне стратегије заштите и спасавања у ванредним ситуацијама, („Службени гласник РС“, бр. 86/2011), као и у Закону о ванредним ситуацијама („Службени гласник РС“, бр. 111/2009), критична инфраструктура се уопште и не помиње. Међутим, може се рећи да институционални оквири за дефинисање заштите критичне инфраструктуре постоје и да су то Сектор за ванредне ситуације Министарства унутрашњих послова Републике Србије, надлежна министарства, као и надлежна регулаторна тела. При томе, одређене мере заштите делова инфраструктуре постоје, али нису донесене ни стратегија ни политика заштите на нивоу земље. Потреба разматрања безбедности критичне инфраструктуре препозната је у оквиру пројекта „Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору

Републике Србије".[144]

Република Србија је последњих година учинила значајне напоре у стварању интегрисаног система заштите и спашавања како би се на адекватан начин одговорило у условима угрожавања критичних националних ресурса. Република Србија је децембра 2009. године добила Закон о ванредним ситуацијама[145] и у њему успоставила нормативну основу за један нови - интегрисани систем управљања ванредним ситуацијама.[146] Основним текстом Закона из 2009. године, држава се определила да Министарство унутрашњих послова буде надлежно за израду Процене угрожености од елементарних непогода и других несрећа. Истовремено, аутономне покрајине и јединице локалне самоуправе, министарства и други органи и организације израђују процену угрожености у делу који се односи на њихов делокруг и достављају је Министарству унутрашњих послова. Влада Републике Србије је на основу чл. 45, став 4. Закона о ванредним ситуацијама донела Уредбу о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама. Овим документом, поред већ наведене Процене угрожености, који су дефинисани у Закону о ванредним ситуацијама, предвиђа се да ће део Процене бити и процена критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа. У Републици Србији се овом уредбом први пут уводи појам критичне инфраструктуре али и даље без јасног дефинисања о којим је елементима или областима инфраструктуре реч. Такође, нису одређени субјекти који би сносили одговорност у заштити критичне инфраструктуре.

---

[144]*Gospić, G., Murić, D., Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia, International Conference on Applied Internet and Information Technologies, Zrenjanin, 2012.*

[145]*Основни текст закона у Службеном гласнику РС", бр. 111/09, Измене и допуне закона у Службеном гласнику РС бр. 92/2011 и„ Службеном гласнику РС" бр. 93/2012.*

[146]*Треба нагласити да је поред Закона о ванредним ситуацијама системски правни оквир за управљање ванредним ситуацијама у Србији одређен и Уставом Републике Србије (2006), Законом о државној управи(2010) Законом о министарствима (2011) Законом о локалној самоуправи, (2007) Законом о мерама за случај ванреднос стања (1991), Законом о полицији (2006), Законом о војсци Србије (2007), Законом о одбрани (2009) и стратешким документима: Стратегијом националне безбедности (2009) и Стратегијом одбране Републике Србије (2009).*

У погледу мера заштите критичне инфраструктуре, све државе, укључујући и Републику Србију, морају да утврде и редослед поступака: а)идентификацију критичне инфраструктуре, б) израда мапа критичне инфраструктуре, ц) размена информација, д) оспособљавање особља ангажованог на пословима и задацима у системима критичне инфраструктуре, е) увежбавање система за заштиту критичне инфраструктуре или опоравак у случају кризне или ванредне ситуације.[147]

Област ванредних ситуација свеобухватно је уређена Законом, који је матични за ту област. Поједина питања од значаја за област ванредних ситуација (безбедносна, еколошка и др) уређена су и посебним законима. Нпр. одредбама чл. 15 и 57. Закона о полицији[148] утврђене су посебне мере значајне за заштиту здравља и живота људи и за спречавање угрожавања безбедности изазваног елементарним непогодама или епидемијама. Те мере своде се на овлашћење државе да у изузетним случајевима, попут катастрофе 2014. године, ограничи или забрани кретање на одређеним подручјима, забрани настањивање на одређеном подручју, наложи евакуацију - напуштање одређеног подручја или објекта. И у целини посматрано, наведена и слична овлашћења државних и других органа пружају могућност за адекватно супротстављање катастрофи до које је дошло услед незапамћених поплава 2014. године.

Треба нагласити да институционални оквири за дефинисање КИ постоје**,** а то су постојање Сектора за ванредне ситуације, надлежних министарстава као и надлежних регулаторних тела. Одређене мере заштите делова инфраструктуре су предузете од стране оператера, али нису донесене ни стратегија ни политика заштите на нивоу земље.

Република Србија обезбеђује изградњу јединственог система заштите и спасавања у складу са Законом о ВС и другим прописима, као и програмима, плановима и другим документима. Овај јединствен систем се састоји од:

---

[147]*Национална стратегија заштите и спасавања у ванредним ситуацијама (Усвојена на седници Скупштине Републике Србије 18.11.2011.).*
[148]*„Службени гласник РС“, бр. 101/2005, 63/2009, одлука УС и 92/2011.*

1. Система заштите и спасавања који је део система националне безбедности и интегрисани облик управљања и организовања субјеката система заштите и спасавања на спровођењу превентивних и оперативних мера и извршавању задатака заштите и спасавања људи и добара од последица елементарних непогода, технолошких несрећа - удеса и катастрофа, последица тероризма, ратних и других већих несрећа, укључујући и мере опоравка од тих последица и

2. Цивилне заштите која је организован систем чија је, такође, основна делатност заштита, спасавање и отклањање последица елементарних непогода, техничко-технолошких несрећа и других већих опасности које могу угрозити становништво, материјална и културна добра и животну средину умиру али у и ванредном и ратном стању.

Данас се спроводи процес удруживања тих система са стварањем основног државног система заштите становништва и територија под општим називом „Систем заштите и спасавања у ванредним ситуација". Системом заштите и спасавања у ванредним ситуацијама, као делом система националне безбедности, руководи Савет за националну безбедност РС, на чијем челу је председник Републике. Основни систем заштите и спасавања у ванредним ситуацијама у РС обједињује снаге и средства органа државне управе, аутономних покрајина, градова и јединица локалне самоуправе, привредних друштва и других правних лица, грађана, групе грађана, удружења, професионалних и других организација које су овлашћене и оспособљене да решавају питања заштите и спасавања становништва и територија од ванредних ситуација.

Такође, у Републици Србији се критична инфраструктура помиње и у оквиру поглавља 6.2. „*Стратегије развоја информационог друштва у Републици Србији до 2020*"[149] кроз констатацију: „Потребно је развијати и унапређивати заштиту од напада применом информационих технологија на критичне инфраструктурне системе, што поред ИКТ система могу бити и други

[149]*Влада Републике Србије, Стратегија развоја информационог друштва у Републици Србији до 2020, 2010.*

инфраструктурни системи којима се управља коришћењем ИКТ, попут електро-енергетског система“.

Документи који би требало да обрађују питања КИ, осим Закона о заштити критичне инфраструктуре, су *Национална стратегија заштите и спасавања у ванредним ситуацијама* и Закон о ванредним ситуацијама. Друга два документа јесу усвојена, међутим, у њима се ни не помиње критична инфраструктура, барем не постоји као термин, мада се закони по својој природи баве питањима који су везани за заштиту КИ.

Као што је већ поменуто, на основу Закона о ванредним ситуацијама највећи део одговорности за спровођење и координацију активности свих релевантних служби током ванредне ситуације обавља Министарство унутрашњих послова. Релевантне службе чине професионалци из разних области делатности. Велики део ових релевантних служби интегрисан је у састав Министарства унутрашњих послова, ради лакше координације и успостављања јединственог система одговорности и данас представљају Сектор за ванредне ситуације при МУП. Без обзира на то што тренутно не постоји ресорни Закон о заштити критичних инфраструктура, као ни списак критичних инфраструктура Републике Србије. Овим документом се по први пут уводи појам критичне инфраструктуре који није јасно дефинисан и без прецизнијег одређења садржине појма критичне инфраструктуре. У нашој земљи појам и проблематика критичне инфраструктуре како у теорији тако и у пракси нису непознати већ су редефинисани. За време постојања СРЈ а на основу члана 36. став 3. Закона о одбрани[150], Савезна влада је донела Одлуку о одређивању великих техничких система од интереса за одбрану земље. Овом одлуком одређени су велики технички системи од значаја за одбрану земље као и техничка средства од значаја за функционисање тих система у области веза, информатике, електроенергетике, водоснабдевања, саобраћаја као и другим областима, при чијем су избору, изградњи и развоју те и набавкама техничких средстава за њихово функционисање, инвеститори дужни да их ускладе са потребама одбране земље и прописује се поступак

[150] *„Службени лист СРЈ“, бр. 43/94 и 28/96.*

обавештавања о избору, изградњи и развоју тих система, набавкама техничких средстава и постављању захтева за њихово усклађивање са потребама одбране земље. Такође, Влада РС је још 1992. године донела Уредбу о објектима и регионима од посебног значаја за одбрану РС[151]. Објектима од посебног значаја за одбрану РС у смислу ове Уредбе сматрају се објекти за које се проценом утврди да би њиховим оштећењем могле настати теже последице за одбрану и безбедност РС. У ове објекте спадају реони и објекти у области саобраћаја, телекомуникација, енергетике, водопривреде и индустрије.

У Републици Србији критичне инфраструктуре су у највећој мери у власништву државе, привредна друштва која имају монополски положај на тржишту роба и услуга, док је мали број привредних друштава у приватном власништву.

На основу Одлуке о одређивању великих техничких система значајних за одбрану[152] дефинисани су велики технички системи од значаја за одбрану и техничка средства од значаја за функционисање тих система у области телекомуникација, информатике, саобраћаја, енергетике, водоснабдевања и другим областима од значаја за одбрану и прописује се поступак обавештавања о избору, изградњи и развоју тих система, набавкама техничких средстава и начин обезбеђења техничких средстава и постављању захтева за њихово усклађивање са потребама одбране земље.

Великим техничким системом, у смислу тачке 1. ове одлуке, сматра се целина, односно скуп међусобно уређених делова и поступака који обезбеђују техничко-технолошко јединство и самосталност система или његову функционалну повезаност са другим техничким системима од значаја за одбрану.

Велики технички систем од значаја за одбрану на територији РС је: у области саобраћаја: Акционарско друштво за ваздушни саобраћај „JAT AIRWAYS“ а.д. Београд; Јавно предузеће Аеродром „Никола Тесла“; Агенција за контролу

[151] *„Службени гласник РС“, бр. 18/92.*
[152] *„Службени гласник РС“, бр. 15/2009, 54/2010, 4/2011 и 58/2011.*

летења Србије д.о.о.; Јавно предузеће „ПТТ саобраћаја Србија“ и Јавно предузеће „Железнице Србије“, Београд; у области енергетике: Јавно предузеће „Електропривреда Србије“, Београд и његова зависна привредна друштва основана за обављање делатности производње и дистрибуције енергије; Јавно предузеће „Електромреже Србије“, Београд; „НИС“ а.д. Нови Сад; Јавно предузеће „Србијагас“, Нови Сад; „Рафинерија нафте“ д.о.о., Београд; „ФАМ“ д.о.о. Крушевац и Јавно предузеће „Транс нафта“, Панчево; у области производње угља за потребе термоелектрана: Јавно предузеће „Рударски басен Колубара“, Лазаревац и Привредно друштво „Термоелектране и копови Костолац“ д.о.о. Костолац; у области водоснабдевања: Јавно водоводно предузеће „Србијаводе“, Београд; „Воде Војводине“, Нови Сад; Јавно комунално предузеће „Београдски водовод и канализација“, Београд; Јавно предузеће за водоснабдевање „Рзав“, Ариље; Јавно предузеће за водоснабдевање и за производњу и дистрибуцију електричне енергије „Ибар“, Зубин поток; Јавно комунално предузеће „Водовод и канализација“, Нови Сад и јавна комунална предузећа водовода и канализације у градовима.

У другим областима: Радио-дифузна установа „Радиотелевизија Србије“, Београд; Јавно предузеће Новинска агенција „Тањуг“; Јавно предузеће за газдовање шумама „Србијашуме“, Београд; Јавно предузеће за газдовање шумама „Војводина шуме“, Нови Сад; „Електронска индустрија“ а.д., Ниш; Јавно предузеће „Скијалиште“, Србије и градске топлане.

Овим истраживањем су обухваћени следећи велики технички системи од значаја у борби против ванредних ситуација:Нафтна индустрија Србије а.д., Јавно предузеће „Електропривреда Србије“, Јавно предузеће „Електромрежа Србије“, Јавно водопривредно предузеће „Србијаводе“, Јавно предузеће „Пошта Србије“, Јавно комунално предузеће „Београдски водовод и канализација“, Јавно предузеће „Путеви Србије“, Железнице Србије а.д. иСектор за ванредне ситуације МУП РС.

5.2. ЕЛЕМЕНТИ КТИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

5.2.1. Нафтна индустрија Србије а.д.

Нафтна индустрија Србије се бави прерадом нафте и продајом нафтних деривата, врши експлоатацију угљоводоника. Обим експлоатације НИС износи око милион тона нафтног еквивалента годишње.

НИС има рафинерије за прераду нафте у Панчеву и Новом Саду, укупног капацитета 7,3 милиона тона годишње. У саставу НИС налази се погон за производњу течног нафтног гаса у Елемиру.

Блок Сервиси компаније бави се геофизичким истраживањима, бушењем, ремонтом, испитивањем бушотина, хидросондирањем, пружањем транспортних, ремонтних и грађевинских услуга.

Компанија поседује сопствену малопродајну мрежу (460 јавних бензинских станица у функцији, 10 ауто пунилишта и 18 продавница боца), као и складишта нафте и водећи је снабдевач српског тржишта нафтним дериватима, који обезбеђује производњу око 85 % укупних потреба српског тржишта за нафтним дериватима. НИС извози моторна горива, бензол, толуол, битумен за асфалтирање и индустријски битумен у земље ЕУ, Украјину, Хрватску, Црну Гору, Босну и Херцеговину, као и керозин у државе у окружењу.

НИС поседује производне капацитете у Анголи и нафтне сервисе у Туркменистану, као и предузеће Јадран Нафтагас у РС, заједнички основано са фирмом Нефтегазинкор.

Стратешки циљ компаније је регионално лидерство и његова реализација до 2020. године подразумева раст основних показатеља вредности компаније: увећање обима производње нафте и гаса до 5 мил. тона, завршетак пројекта модернизације прерађивачког комплекса у Рафинерији Панчево и повећање обима прераде до 5 милиона тона, повећање обима продаје до 5 милиона тона, као и инвестиције у кључне правце бизниса до 2103. године у износу од 90 милијарди динара.

Подсећања ради, разарање постројења нафте у Новом Саду имало је размере еколошке катастрофе. Бомбардовање и разарање мостова, административних, стамбених као и других објеката инфраструктуре у ванредним ситуацијама.

5.2.2. Јавно предузеће „Електропривреда Србије“

Делатност ЈП ЕПС је енергетска делатност: снабдевање електричном енергијом. Такође, ЈП ЕПС може, у складу са законом којим се уређује област енергетике, обављати и делатност јавног снабдевања електричном енергијом купаца на територији Републике Србије.

Основна делатност ЈП ЕПС јесте:

- Производња електричне енергије и производња електричне и топлотне енергије у комбинованом процесу;
- Експлоатација лигнита;
- Дистрибуција електричне енергије и управљање дистрибутивним системом;
- Управљање економским субјектом;
- Кабловске телекомуникације;

5.2.3. Јавно предузеће „Електромрежа Србије“

Јавно предузеће Електромрежа Србије је енергетски субјект који према Закону о енергетици и одлуци Владе Републике Србије о оснивању овог предузећа обавља следеће енергетске делатности:

- пренос електричне енергије и управљање преносним системом и
- организовање тржишта електричне енергије.

Капацитете за пренос електричне енергије од произвођача до потрошача, односно за потребе прекограничне размене, обезбеђују далеководи и трансформаторске станице напона 400 kV, 220 kV и 110 kV.

5.2.4. Јавно водопривредно предузеће „Србијаводе“

Јавно водопривредно предузеће „Србијаводе“ је организовано као јединствена пословна и економска целина. У оквиру предузећа је успостављена територијална и функционална организација, која је утврђена Статутом и Правилником о унутрашњој организацији и систематизацији послова.

Унутрашњу организацију предузећа чине Дирекција, са седиштем у Београду, која координира и обједињује рад предузећа и три Водопривредна центра (ВПЦ). У Дирекцији предузећа и водопривредним центрима образоване су организационе јединице као сектори (Технички сектор, Сектор за економско-финансијске послове, Сектор за имовинско-правне и опште послове.

5.2.5. Јавно предузеће „Пошта Србије“

ЈП „Пошта Србије“, скраћено Пошта, јавно је предузеће коме је основна делатност пријем, пренос и достава поштанских пошиљки. Такође, обавља послове платног промета, а за рачун Поштанске штедионице обавља и послове штедње грађана. Регистровано је за вршење и других услуга. За Телеком Србија и Теленор врши продају СИМ Картица, а продаје и мобилне телефоне. Осим тога, пружа услуге као интернет провајдер, кабловски ТВ оператер и др[153].

Предузеће је 2002. године почело да користи лого (па и назив) Пошта, с тим што је службени назив предузећа ЈП ПТТ саобраћаја „Србије“ промењен у ЈП „Пошта Србије“ крајем 2013. године.

5.2.6. Јавно комунално предузеће „Београдски водовод и канализација“

Делатност водоснабдевања, одвођења и пречишћавања отпадних вода обавља око 100 јавних комуналних предузећа водовода и канализације у Републици Србији. Оснивачи ових предузећа су локалне самоуправе, које на основу Закона о комуналним делатностима, уређују њихове услове

[153]*Стратегија развоја поштанских услуга у Републици Србији за период од 2013. до 2016. године, Влада Републике Србије.*

управљања, организације и пословања.

Сви ови системи су сложени, деценијама грађени и веома скупи. У њихово функционисање и развој се највише улагало 60-тих и 70-тих година прошлог века и многи од њих и дан-данас раде са таквом превазиђеном технологијом и техником, инсталацијама, уређајима и опремом. Након тог периода, много мање се улагало у одржавање постојећих и проширење и изградњу нових, углавном секундарних, уличних водовода и канализације, чему је допринела велика економска криза, крајем прошлоги почетком овог века.

Недостајала су улагања и модернизација технологија третмана пијаће и отпадних вода, реконструкција магистралне и колекторске водоводне и канализационе мреже, примену информатичких технологија у управљању техником, у пословању и односима са потрошачима. Ова огромна материјална улагања превазилазе могућности градова и општина као оснивача ових предузећа. Многи од ових система данас тешко излазе на крај са обезбеђењем неопходног квалитета услуга.

Цена воде није на тржишним основама, као у земљама транзиције и земљама у развоју. Она не обезбеђује ни просту репродукцију, а камоли средства за развој у складу са потребама и интересима садашњих и будућих потрошача. Њен садашњи ниво, у сиромашној земљи каква јесмо, не подстиче потрошаче да се рационалније односе према потрошњи воде, која није неисцрпан ресурс. Такође, такав нештедљив однос према води доводи нас у ситуацију да улажемо велика средства у стално проширење капацитета, уместо да више пажње усмеримо ка систему управљања квалитетом производње, дистрибуције и другим услугама.

Између ових предузећа, која обављају исту делатност, раде у истим економско-социјалним условима и слично су организована, нема успостављене сарадње, нема размена информација, идеја, знања, метода и начина рада, коначно, нема ни заједничког наступа пред надлежним државним органима, организацијама и институцијама. То је нарочито значајно када се доносе кључна стратешка документа и закони, везани за ову област. Ово је значајно и због тога што је потребно на јединствени начин, на

националном нивоу, постићи и придржавати се норми и стандарда које су у области водовода и канализације прописани регулативом ЕУ. Те норме и стандарди допринеће ефикаснијем и квалитетнијем обављању ових делатности.

5.2.7. Јавно предузеће „Путеви Србије“

ЈП Путеви Србије обавља стручне послове који се односе на одржавање, заштиту, изградњу, реконструкцију, експлоатацију, развој и управљање јавним путевима I и II реда реда у Републици Србији.

Република Србија располаже путном мрежом државних путева I и II реда чија се вредност процењује на 4,2 милијарде евра. Путна мрежа се простире на надморским висинама од 30 m (Неготин) па до 1.700 m (Голија). Процена је да се 40 % дужине путне мреже простире на висинама преко 600 m. Асфалтни коловози државних путева првог и другог реда су изграђени у периоду од 1962. до 1985. године, при чему су многи правци задржали старе елементе трасе, тако да је асфалт положен преко постојећег туцаника. У истом периоду су најзначајнији правци изграђени по пројекту, па су те деонице добиле нове, боље елементе уздужног и попречног профила.

Путеви као добра у општој употреби су државна својина. На територији Републике

Сходно Закону о јавним путевима („Службени гласник РС“, бр. 101-05) основано је Јавно Предузеће „Путеви Србије“ за управљање државним путевима.

ЈП „Путеви Србије“ обавља послове који се односе на одржавање, заштиту, експлоатацију, развој и управљање државним путевима првог и другог реда у Републици Србији.

Уз заштиту и експлоатацију путева ЈП „Путеви Србије“ организује и обавља стручне послове на изградњи, реконструкцији и у управљању саобраћајем на државним путевима у Републици Србији.

5.2.8. Јавно предузеће „Железнице Србије“ а.д.

У Републици Србију ова област је дефинисана Законом о безбедности и интероперабилности железнице, који је објављен у „Службеном гласнику РС“ бр. 104 из 2013. године.[154]

Магистралне железничке пруге пролазе кроз све веће градове и укрштају се у зонама Београда и Ниша. Од укупне дужине железничке мреже у Републици Србији (3.809 km), 1.768 km представљају магистралне пруге, а електрифицирано је 1.247 km (32,7 %).

Само 7 % пруга (276 km) има два колосека. Просечно задовољавајућа густина мреже на нивоу Републике Србије веома је неравномерна и осетно опада ка југу.

Око 25 % магистралних пруга железничке мреже у Републици Србији налази се на Коридору X и његовим крацима Xb и Xc.

Само око 45 % пруга у Републици Србији има дозвољено осовинско оптерећење од 22,5 t док је на 30 % пруга то оптерећење испод 16 t.

Дозвољена брзина прелази 100 km/h на свега 3,2 % пруга, а највећи део (око 50 %) мреже дозвољава максималну брзину до 60 km/h. Са изузетком појединих секција пруга Београд-Шид и Велика Плана-Ниш, које су двоколосечне, електрифициране и на неким деоницама дозвољавају веће брзине, све остале пруге имају застареле техничке и технолошке параметре. Чак и на неким секцијама ових пруга има деоница у врло лошем стању тако да се брзина често привремено ограничава на 20 km/h или ниже.

ЈП „Железнице Србије“ располажу са око 480 локомотива, 8.500 теретних и 550 путничких вагона. Железничка возна средства су релативно стара и непоуздана. Просечна старост железничких возних средстава прелази 30 година, а стопа расположивости варира између 26 % и 61 %.

[154] *Закон о безбедности и интероперабилности железнице, „Службени гласник РС“ бр. 104, 2013.*

Недовољно улагање у основно одржавање на железници последица је општег привредног заостатка у претходном периоду, лоше организације, недостатка средстава, социјалне и кадровске политике.

Садашње стање железничке инфраструктуре карактерише потреба да се у пројектовано стање врати и модернизује још око 1.000 km магистралних пруга, тј. око 57 % главне мреже пруга, односно 26 % комплетне железничке мреже. За рехабилитацију и одржавање железничке мреже у наредних десет година према проценама биће потребно око 3,9 милијарди евра.

Управљање јавном железничком инфраструктуром, јавни превоз путника и робе и одржавање железничких возних средстава су претежне делатности ЈП „Железнице Србије“. Ово јавно предузеће је крајем 2000. године запошљавало близу 33.000 људи, а до краја децембра 2006. године број запослених је смањен за више од 37 %, на око 20.857.

ЈП „Железнице Србије“ суочене су са лошим стањем железничке инфраструктуре и недостатком савременог возног парка. Рехабилитација и побољшање потребни су на целој дужини Коридора X, који је окосница система (25 % мреже и преко 50 % транспортних активности).

5.3. МЕРЕ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

Управљање ризицима и ванредним ситуацијама на КИ, састоји се од следећих пет фаза:

- прелиминарно планирање,
- анализа ризика,
- спецификовање превентивних мера,
- имплементација система кризног менаџмента и
- евалуација свих фаза и резултата.

Прва фаза - прелиминарно планирање подразумева мере којима се стварају нужни предуслови за успостављање система управљања ризицима, као кризног менаџмента. Те мере укључују:[155]

[155] *Каровић С., Комазец Н., Управљање ризиком на системским основама, Војно дело, 2010.*

- дефинисање позиције новог менаџмент система у оквиру постојећег система управљања инфраструктуром,
- дефинисање улога, дужности и одговорности и
- дефинисање расположивих ресурса.

Анализа ризика, као друга фаза, интегрише разноврсне информације којима располажу и јавни и приватни сектор. У поступку анализе ризика процењују се различити процеси, појаве и елементи и упоређује се њихова ризичност по инфраструктуру. Када се говори о КИ, анализа ризика започиње структурним и системским сегментирањем организације на процесе и субпроцесе.

Сваки процес и подпроцес садржи елементе (материјалне или виртуелне), који могу бити угрожени или оштећени, чиме се функционисање процеса доводи у питање. Они се називају „ризичним елементима“ или елементима под ризиком, а то су:

- људи (запослени и други који се могу наћи у оквиру инфраструктуре или њеној непосредној близини),
- околина (путеви, паркинзи, зелене површине, суседни објекти),
- објекти (производне хале, пословне зграде, гараже),
- опрема (системи снабдевања енергијом, системи за грејање, снабдевање водом и сл, производне машине, комуникациона опрема, средства транспорта),
- специфична опрема (софтвер, медицинска опрема, системи обезбеђења) и
- подаци (документа, информације или складиштени подаци).

Циљ креирања и спровођења превентивних мера, као треће етапе је смањење потенцијала ризика да се оствари (реализује) и прерасте у ванредну ситуацију, као и да се у таквом случају последице минимизирају. Превентивне мере представљене су кроз инструменте, попут:[156]

- редукције ризика - смањење угрожености (опасности) или повредивости (осетљивости ризичних елемената);

[156]*Упутство о методологији за израду процене угрожености и планова заштите и спасавања у ванредним ситуацијама, „Службени гласник РС“, бр. 96/2012.*

- избегавања ризика - избегавање критичних подручја и локалитета, процеса, материјала;
- трансфера ризика - пребацивање дела или читавих ризичних процеса на друге системе (партнерске организације, државне институције);
- прихватања ризика - препознавање и третирање тзв. резидуалних ризика - проблема који се не могу решити претходно наведеним методама.

Ванредна ситуација представља девијацију или одступање у односу на уобичајено, свакодневно (подразумевано) стање и ситуацију у систему, а која се не може решавати спровођењем уобичајених активности. Кризе у критичним инфраструктурама могу имати озбиљне последице на дати систем, али и на друге структуре, јавне службе или друштво. Тиме, кризни менаџмент има кључну улогу у обезбеђивању стабилности система, припремљености на ризике и адекватне одговоре на кризе.

Кризни менаџмент *КИ* одвија се под специфичним околностима, у којима егзистирају и сами системи:

- мере се предузимају уз ограничене ресурсе (због величине система) и доступне информације (због специфичности система);
- нужна је екстерна подршка и сарадња и
- одлуке се морају доносити брзо, а на основу потпуних информација.

План кризног менаџмента, треба, као основно да садржи и дефинише следеће елементе:[157]

1) сврха и циљеви плана
2) правни основ
3) структура организације кризног менаџмента
   - тим за одговор на кризу
   - дефинисање улога и одговорности учесника менаџмент тимова
4) креирање специјалних процедура за управљање ванредним ситуацијама
   - командни ланац,

[157]*Завишић, Ж., Билић, И., Завишић, С., „Интерна комуникацијаукризнимситуацијама, Зборник радова „Дани кризног управљања“, Велика Горица, Хрватска, 2011.*

- модели ескалације и деескалације ванредне ситуације,
- мере опоравка и
- начини информисања

5) специфичне мере

- евакуација,
- редуковање напајања и
- ограничавање рада ИТ система.

Евалуација, као фаза управљања ризицима, подразумева анализу и оцену реализације свих претходних фаза и резултата. Евалуација треба да покаже адекватност мера које су планиране и спроводе се. Посебну евалуацију, у смислу ванредне анализе и тумачења, потребно је спроводити у следећим случајевима:

- након имплементирања појединачних и конкретних мера,
- након развоја или реструктурисања система и
- услед измене у стању или структури претњи.

Област заштите и спасавања у случају ванредних ситуација уређена је законима и великим бројем подзаконских прописа. Поред прописа чији је предмет регулисања поступање у појединој ситуацији која се може сматрати ванредном са аспекта ангажовања ресурса заштите и спасавања, као што је заштита од пожара, поплава, хемијског акцидента и сл., општи законски оквир чини **Закон о ванредним ситуацијама** који дефинише управљање ванредном ситуацијом, као и друге елементе неопходне за функционисање система заштите и спасавања. Ти елементи су пре свега прецизно дефинисана област примене (елементарна непогода и друга већа несрећа, техничко-технолошка несрећа, заштита и спасавање од последица терористичких напада и др.), затим дефинисани носиоци активности у случају ванредне ситуације, субјекти који доносе одлуке, и сви други субјекти који могу бити значајни у случају реаговања у ванредној ситуацији, али и за боље превентивно деловање и подизање отпорности друштва на ванредну ситуацију, као што су научно-истраживачке установе и сл.

5.3.1. Заштита критичне телекомуникационе инфраструктуре

Све више зависимо од информационих и комуникационих технологија (ИКТ). Личне и осетљиве податке преносимо на личне комуникационе уређаје или их чувамо на њима. Све више информација о себи поверавамо на чување онима који нуде различите ИКТ услуге. Из тих разлога, електронске комуникације и ИКТ постају једна од најрањивијих тачака заштите приватности појединаца.

Телекомуникационе мреже се на свим нивоима сматрају неодвојивим делом друштвене интеракције. Треба посебно нагласити да комплетна електронска комуникациона инфраструктура која се састоји од комуникационих мрежа, дистрибуираних рачунарских система, софтвера и апликација игра кључну улогу у унапређењу укупног знања и технологије. Захваљујући њеној могућности да окупи „критичну масу“ људи, идеја и инвестиција, она на различитеначине доприноси напретку на свим нивоима друштвеног и економског живота. Из тог разлога, телекомуникациона инфраструктура представља веома важну имовину и средство које мора бити заштићено и као таква је неопходно да се препозна као део националне критичне инфраструктуре. Заштита ових мрежа од напада и природних непогода, које могу довести до недоступности мрежних сервиса, је веома битан аспект који се не сме занемарити.[158]

Кроз разматрање процене ризика од различитих напада усмерених ка телекомуникационој инфраструктури (малициозних, природних катастрофа и сл.), указано је на неопходност регулисања КТИ и корака које треба предузети.

Телекомуникациона инфраструктура једне земље је комплексан скуп система који укључују велики број технологија и сервиса, а које се налазе у власништву више ентитета (државе, приватних компанија). Инфраструктура обухвата жичне, бежичне, кабловске и технологије за емитовање, мреже базиране на Интернет протоколу као и интерне информационе системе.

[158] *IT Governance Institute, Information Security Governance, 3rd edition, 2007.*

Многе телекомуникационе компаније/оператори које поседују и управљају телекомуникационом инфраструктуром су током времена имплементирале мерезаштите од природних катастрофа и незгода у оквиру својих архитектура уводећи редундантне чворове и системе, бизнис планове и стратегије за санацију након напада или природних непогода.

То указује да и поред данашњег веома конкурентног пословног окружења због повезаности и међузависности мрежа различитих оператора/сервис провајдера, сви чиниоци телекомуникационог сектора једне земље треба да сарађују, јер проблеми у функционисању мреже једног учесника на тржишту често могу да утичу на мрежу која је у власништву неког другог.

Како је највећи део телекомуникационе инфраструктуре у власништву приватног сектора, битно је установити заједнички стратешки оквир којим ће се осигурати заштита телекомуникационе инфраструктуре једне земље и осигурати њена безбедност.[159]

Вођени општом трансформацијом и конвергенцијом технологија почетком XXI века сектор телекомуникација и ИТ су постали практично нераздвојиви. Телекомуникациони сектор не укључује само физичке елементе као што су жичне, бежичне, кабловске и сл. технологије, већ и сервисе као што су Интернет саобраћај и рутирање, информационе сервисе и мреже кабловске телевизије. Компоненте комуникационе инфраструктуре које су у власништву државе и приватних компанија су нераскидиво повезане у оквиру ових физичко-логичких структура.

У дефинисању телекомуникационе инфраструктуре, уобичајено је да се за основу узима оно што је Међународна Унија за телекомуникације *(International Telecommunication Union - ITU)* дефинисала. Међутим, у оквиру фамилије *ITU* није дефинисана КТИ, иако многи документи *ITU* помињу потребу заштите КТИ (PP-10 Res. 130, PP-10 Res. 174, ITUCS/Art.38, ITUCS/Art.34, ITUCS/Art.35). Хармонизација која је урађена у оквиру ITU-T

[159]*Gospic, N., Muric, G., Bogojevic, D., Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia, International Conference on Applied Internet and Information Technologies, Zrenjanin, 2012.*

сектора серијама препорука Е.408-409 и Х.805 и Х.1051 дефинише захтеве за безбедност, оквире и смернице за идентификацију претњи, смањивање ризика, организацију у случају инцидента и архитектуру сигурности за системе који пружају крај-крај комуникацију. И друге стандардизационе организације као што су Међународна организација за стандардизацију *(International Standardisation Organization - ISO)*, 3GPPи 3GPP 2 *(Group for Partership for Third Generation)* такође не дају дефиниције КТИ већ само оквире за сигурност система мобилних комуникација и управљачких система.

Начин дефинисања КТИ у многоме зависи од контекста у ком се посматра не само КТИ већ и друге КИ у некој земљи. У том смислу КТИ се може дефинисати каојавна или приватна мрежа која преноси информације релевантне за националну безбедност или информације велике материјалне вредности. У физичком смислу КТИ може бити дефинисана као целокупна мрежа или део мреже преко које се преносе информације од велике важности.[160]

Изузетно брз развој и усвајање ИЦТ увеле су људско друштво у фазу трансформације из индустријског доба у информационо доба. Да би испунили своју улогу, комуникациони и информациони системи треба увек да буду поуздани и на располагању корисницима, поверљивост информација које се преносе и чувају не сме бити угрожена, а корисници морају бити сигурни и у идентитет пошиљаоца и у то да је примљена информација идентична послатој. Немогућност да се испуне ови захтеви умањује поверење корисника и њихову спремност да у пуној мери прихвате погодности нових пословних модела подржаних напредним информационим и комуникационим технологијама. Студија *„Друштвено-економски утицај Интернета у Србији*“, коју је 2009. године за Теленор израдила *The Boston Consulting Group*, уз ограду „уздржано“, прогнозира да учешће привредних активности базираних на коришћењу Интернета у Србији може порасти са

[160]*Public Switched Network Security Assessment Guidelines prepared by the office of the manager national communication systems, Arlington, VA, 2000.*

садашњих 1,7 % на 5,2 % 2020. године, да се укупни порески приходи државе из тих активности могу повећати до износа од 1,8 % и да се до 2020. године на основу тога може отворити 94.000 нових радних места. Уз то, не треба занемарити ни подједнако битну друштвену корист од оваквог тренда у областима као што су образовање, здравствена заштита, рурални и регионални развој, емисија CO_2 и другим. Наравно, све то под условом да се Интернет користи у пуном функционалном и технолошком капацитету и на начин који неће изазвати сумње и резерве код корисника. Наиме, истраживања спроведена последњих година показују да је између 70 и 80 % грађана у земљама ЕУ и САД озбиљно забринуто за заштиту своје приватности и безбедности у електронским комуникацијама, до те мере да то знатно утиче на сектор електронске трговине. Штавише, око две трећине анкетираних тврди да се из тих разлога уздржавају од куповине или новчаних трансакција (микроплаћања) преко Интернета, страхујући од могућности да би могли да постану жртве електронске интрузије, крађе идентитета и злоупотребе финансијских овлашћења. Незадовољавајућа безбедност и заштита приватности или чак само утисак недовољне безбедности и заштите приватности могу да имају не само негативан утицај на појединце, него и знатне економске и социјалне последице по друштво у целини.[161]

Када неко говори о приватности и безбедности, то чини из угла који у знатној мери зависи од његове перцептуалне и интересне позиције. Зато се неретко испоставља да, користећи се истим појмовима, говоримо о различитим стварима. Појмови као што су приватност, безбедност, заштита података о личности и сигурност информација, у свакодневном говору имају широк спектар значења, често се користе као синоними, а неретко су и предмет спорова различитих школа мишљења по питањима дефиниција, међусобног односа и хијерархије.

У изворном смислу, приватност означава жељу неке особе да не буде

[161] *Ђорђевић, Г., Утицаји ICT информационог друштва на друштвено-економски развој, Socioeconomica - The Scientific Journal for Theory and Practice of Socioeconomic Development Vol. 1, N°2, pp. 188-200. December, 2012.*

узнемиравана. У електронским комуникацијама уобичајено је да се приватност односи на прикупљање, обраду и давање информација о кориснику трећим лицима. Добро је поближе објаснити и појам поверљивости, који подразумева поверење у некога и веру у поделу неке тајне. Тајна задржана за себе је приватна, али подељена са неким другим постаје поверљива информација. Поверљивост у електронским комуникацијама односи се подједнако на садржај и на податке о обављеној комуникацији, а у овом случају поверење се даје осталим учесницима у комуникацији, али и пружаоцима услуге обраде и преноса. Приватност у електронским комуникацијама може се схватити као слобода од систематског посматрања и бележења активности и личних података, односно право појединаца да сами одређују када, како и у којој мери информација о њиховим комуникацијама треба и може да буде доступна другима. Атрибути приватности корисника у том контексту постају анонимност, слобода од узнемиравања, контрола доступности података о себи и интима (слобода од надзора), а компоненте приватности идентитет, подаци о личности, локација и кретање, (мета)подаци о обављеним комуникацијама и садржај комуникација. Поверљивост може бити компромитована, односно приватност корисника може бити повређена с намером, случајно или грешком, и то упадом у зону приватности (приступом, прикупљањем и обрадом), злоупотребом (одавањем или деловањем на основу доступне информације), пресретањем и уклапањем информација (профилисањем). Очигледно је да се питање приватности у електронским комуникацијама не може одвојити од питања заштите података о личности.[162]

Термин безбедност сам по себи је неодређен и може да има значења која обухватају: одсуство неке опасности и претње, гаранцију, осећај сигурности, скуп мера предострожности и заштите од криминала, саботаже и шпијунаже, али и организационе облике које све то треба да осигурају. Стављање појма безбедности у контекст електронских комуникација нимало не олакшава

[162]*Rajmohan, C., Subramanya, G., Sharma, N., Telecommunication Networks: Security Management, Tata Consultancy Services Limited, 2012.*

недоумицу око његовог значења. Без амбиције да буде свеобухватан или таксономски приказ безбедности и заштите приватности корисника електронских комуникационих услуга, овај текст ће размотрити три аспекта од посебног интереса за кориснике: изворни, у смислу заштите поверљивости комуникација и приватности корисника услуга, проширени, који обухвата преваре и компјутерски криминал, и имплицитни - надзор комуникација за потребе државних органа.

Изворно значење безбедности у електронским комуникационим мрежама се може најкраће дефинисати као обезбеђивање поверљивости, интегритета, аутентичности, расположивости комуникација, одговорности актера и непоречивости информација које се преносе. Очигледно је да је реч о својеврсном проширењу значења познате *CIA triade* (*Confidentiality, Integrity and Availability*), која представља кредо свих ИТ професионалаца. Оквир за овакву дефиницију утврђен је стандардом *ISO* 7498-25 који дефинише пет основних безбедносних сервиса (аутентификација, контрола приступа, поверљивост података, интегритет података и непоречивост комуникације) и осам механизама за имплементацију (криптозаштита, дигитални потпис, контрола приступа, интегритет пакета података који се преносе, размена креденцијала при аутентификацији, попуњавање кодованог сигнала у циљу маскирања саобраћајних образаца (*traffic padding*), контрола усмеравања саобраћаја (*traffic routing*) и бележење - нотаризација). Овако дефинисани сервиси и механизми разрађени су кроз детаљне техничке стандарде и спецификације, да би практично оживели у системима и уређајима који се данас користе. Пружаоци услуга електронских комуникација заинтересовани су најпре за контролисан приступ мрежним ресурсима, одговорност корисника, исправност података који се преносе, поверљивост и интегритет сигнализационих порука, непоречивост употребе и обрачуна услуга, спречавање злоупотребе ресурса, усаглашеност са законским и регулаторним оквиром и друго. Проблем је што сваки безбедносни механизам временом и напретком офанзивне технологије еродира и на крају бива компромитована. Нажалост, захваљујући раширености и мега

димензијама електронских комуникационих мрежа, што опет резултује њиховом инерцијом у односу на промене, нападачи су увек у предности и имају на располагању значајан временски прозор, од тренутка откривања слабости и компромитације система заштите до тренутка откривања напада и примене контрамера. Ситуацију додатно отежава и Интернет, који је постао идеалан канал за дистрибуцију информација, знања и алата за експлоатацију слабости безбедносних механизама електронских комуникационих мрежа, услуга и уређаја. Последица свега је да су електронске комуникације константно угрожене и да борба између нападача и чувара безбедности и интегритета мрежа непрекидно траје и стално поприма нове облике и тактике међусобног надмудривања. Суштина безбедности електронских комуникација је у очекивању корисника да ће систем одолети насртајима предвидивих нападача који имају предвидиве потенцијале и капацитете за његово угрожавање. Наравно да је у пракси немогуће обезбедити мрежу од свих могућих нападача, који имају сва могућа средства и знања, па је безбедност у суштини вештина спознаје стварних извора претњи, њихових реалних могућности и налажења компромиса између вредности које се штите и трошкова заштите тих вредности. Не постоји апсолутно безбедан систем електронских комуникација, већ само слабије или јаче штићени системи, што има директан утицај и на цену коју за то треба платити.[163]

5.3.1.1. Преваре у електронским комуникацијама

Појам преваре (*fraud*) има широко значење и може се односити на било који акт којим се друга страна намерно доводи у заблуду са циљем остваривања незаслужене или незаконите користи. Преваре у електронским комуникацијама (*telecommunications fraud*) изводе се везано за телекомуникационе услуге, услуге са додатом вредношћу, телекомуникациону инфраструктуру или системе за подршку пружању тих услуга, из забаве, престижа, ради стицања финансијске користи или из других нечасних или криминалних побуда. Жртве преваре у електронским

[163] *Peltier,T.R., Information Security Policies and Procedures, Auerbach Publication, 2006.*

комуникацијама могу бити оператори и корисници. У првом случају, починиоци преваре користе производе и услуге без намере да за то и плате оператору, лишавајући га на тај начин легитимног прихода, а у другом, производе и услуге користе како би преварили друге кориснике, при чему превара може, али не мора, нужно да нанесе финансијски губитак оштећеној страни.

У стручним круговима познато је више од 200 различитих метода извођења преваре на штету оператора. Узимајући у обзир и чињеницу да је веома често конкретан напад у ствари комбинација два или више основних метода, испоставља се да је простор за извођење ових операција изузетно широк. Друга важна чињеница јесте то да је већина великих операција прекогранична и има атрибуте криминалне организације, тако да се, ако се у обзир узму штете које настају, слободно може говорити о једном виду ненасилног организованог криминала. Превара изведена на штету оператора у суштини повећава трошкове његовог пословања, јер директно умањује приходе, али индиректно штети и држави јер умањује њене пореске приходе. Проблем са утврђивањем стварне висине губитака услед ових превара је двојак: због изузетно интензивне пословне активности оператора, комуникационе активности корисника и сталних промена у начину извођења операција, добар део превара остаје неоткривен, а из интерних разлога и сами оператори често теже да своје губитке услед превара задрже за себе. На основу истраживања које је спровело удружење за контролу превара у телекомуникацијама (*CFCA8*), губитак оператора по овом основу за 2008. годину на глобалном нивоу процењен је на између 72 и 80 милијарди долара, што одговара уделу од 4,2 до 4,5 % њиховог укупног прихода.

У односу на претходно истраживање спроведено 2005. године, када је процена била у оквиру 54-60 милијарди долара, ово указује на раст губитака оператора услед преварених активности од 34 % на глобалном нивоу. С обзиром на високу интегрисаност Србије у глобалну мрежу електронских комуникација и скромне одбрамбене капацитете, нема разлога да верујемо да би Србија могла бити поштеђена утицаја овог тренда. Напротив, проценат

губитака оператора и државе вероватно је и већи од светског просека.

У сценаријима преваре на штету корисника, електронске комуникације се користе као канал за пласирање главног напада, без обзира на то да ли су у питању индивидуални или корпоративни корисници. При том су главни циљеви починилаца: злоупотреба комуникационог сервиса, крађа личних података (нарочито идентитета и финансијских података) и повреда приватности. Познат је већи број сценарија злоупотреба услуга које наносе финансијску штету корисницима у мрежама за пренос говора. Најпознатији, свакако не и једини, јесу разне варијанте злоупотребе механизма услуга са повећаном тарифом (*premium rate*), пропуштени позиви са непознатог броја (*call-backscam*), пецање (*phishing, vhishing*) и сл. На овим примерима добро се види да телефонска и Интернет мрежа конвергирају не само у области технологије и услуга него, нажалост, и када је реч о техникама преваре корисника. Са интензивнијим коришћењем Интернета умножавају се разни видови онлајн превара подржаних социјалним инжењерингом (*phishing*), незатраженим порукама (*spam*), злоћудним програмима (вируси, тројанци, *botnets, spyware*), повредама права интелектуалне својине и сл.

Поред основне намене електронских комуникационих мрежа, услуга и комуникационе опреме за пренос порука и информација, оне неким корисницима служе да би прикрили своје активности (присуство, идентитет, кретање, податке о контактима, садржај комуникација), узнемиравали или уцењивали друге кориснике, крали, злоупотребљавали или препродавали личне податке, систематски пратили или бележили активности других корисника или, једноставно, користили услуге и инфраструктуру мрежа као техничку логистику у вршењу кривичних дела, прекршаја или других нечасних радњи које немају директне везе са електронским комуникацијама. Иако на тај начин не наносе непосредну финансијску штету, овакви видови ненаменског и злонамерног коришћења се могу сместити у шири контекст превара, али исто тако и у неку од категорија угрожавања безбедности информација, повреда приватности или злоупотребе података о личности, што само додатно илуструје органску повезаност ових појмова.

Када је у питању евентуална обавеза и одговорност оператора да заштити кориснике од превара, треба напоменути да су сами корисници одговорни за то како користе своје уређаје и мрежне услуге. Међутим, и оператори који држе до свог кредибилитета и позиције на тржишту улажу велике напоре да преваре на штету корисника сведу на најмању могућу меру. Проблем је у томе што су у корену ових превара најчешће незнање, несмотреност и немар корисника, неретко подложност изазовима „културе бесплатног“ и лаке добити, па чак и похлепа самих корисника, а има случајева иза којих стоји свесна намера да, у улози жртве, наводно преварени корисник оствари добит за себе. Могућности оператора да спрече овакве случајеве ограничене су на стално или кампањско подизање нивоа свести и обавештености корисника о потенцијалним претњама и опасностима. Иако је последњих година у Србији било неколико кампања информисања јавности, најчешће иницираних конкретним инцидентима и ограничених по обиму и трајању, тек кроз систематску и координирану акцију институција државе, свих значајнијих оператора и медија, могуће је очекивати значајније ефекте напора на превенцији превара у електронским комуникацијама.

5.3.1.2. Надзор електронских комуникација за потребе државе

Право на неповредивост тајности писама и других средстава комуницирања и право на заштиту података о личности гарантовани су Уставом Србије као основна људска права и слободе. Одступања од начела неповредивости тајности електронских комуникација дозвољена су само на одређено време и на основу одлуке суда, ако су неопходна ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (Устав Републике Србије, члан 41.). Такође, забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике Србије, на начин предвиђен законом (Устав Републике Србије, члан 42.). Када говоримо о електронским комуникацијама, треба подсетити да је Међународни суд за људска права у Стразбуру (*ECHR*), у случају

Coplandvs. The United Kingdom 2007. године пресудио да информације везане за време и дужину телефонског разговора, а посебно изабрани бројеви саговорника, представљају „интегрални део телефонске комуникације“. С обзиром на то да су пресуде *ECHR* обавезујуће за Републику Србију, јасно је да начело неповредивости тајности електронских комуникација и у Србији треба примењивати подједнако на садржај и податке о обављеним електронским комуникацијама.

Неспорно је да право на неповредивост тајности електронских комуникација није апсолутно право, нарочито ако се има на уму да их криминалци и терористи редовно користе као помоћно средство за остваривање својих циљева, било са намером да почине криминално дело или да избегну откривање. Због тога је ефикасан надзор електронских комуникација од виталног значаја и за државне органе задужене за откривање и гоњење починилаца, али и за грађане. Наравно, под условом да се надзор примењује пропорционално, у складу са легитимним циљевима и законом утврђеним предусловима, по правилима која су правно обавезујућа, јавно објављена, предвидљива, прецизна, недвосмислена, на начин у ком је простор за дискреционе одлуке извршне власти минималан и јасно прописан, уз одговарајућу заштиту од злоупотреба и одговарајуће методе независног надзора. С друге стране, државне службе, без обзира да ли је реч о службама за спровођење закона или тајним службама, по својој интерној логици (која није специфична само за Србију) понекад прешироко тумаче поверена овлашћења и стављају оно што доживљавају као „интерес службе“ изнад права појединаца, што у комбинацији са неодговарајућим механизмима екстерног надзора повећава ризик од повреде људских права и злоупотребе државне моћи. Због тога, демократски организоване земље непрекидно трагају за одговарајућим моделом успостављања деликатне равнотеже између права друштва да штити своје вредности и права појединаца на приватност.

Оперативно-истражне потребе државних служби које спроводе законом овлашћен надзор електронских комуникација, наведене по степену

задирања у приватност од лакшег ка тежем, односе се на: идентификацију корисника, личне и уговорне податке о корисницима, детаљне податке о оствареним и покушаним комуникацијама као што су време, место, трајање, други учесници, коришћени мрежни сервиси и друго (*Metering of Calls*), лоцирање комуникационих терминала у реалном времену (*Stealth Ping*), пресретање података о комуникацијама (статистички надзор) и пресретање комуникација у пуном капацитету (подаци о комуникацијама и садржај говорних, неговорних и сигнализационих порука).

У савременим мрежама електронских комуникација, ефикасан надзор електронских комуникација тешко је извести без одговарајуће инфраструктурне и оперативне подршке оператора и пружалаца услуга. Пошто оператори немају никакав комерцијални интерес да за те потребе додатно инвестирају у опрему, обавезе оператора да обезбеде техничке услове и државним органима омогуће надзор утврђују се законом.

5.3.1.3. Заинтересоване стране

У контексту заштите приватности и безбедности услуга, постављеном у претходном одељку, могу се идентификовати интересне групе корисника, оператора, комерцијалног сектора и државних органа. Свака од ових група има одређене интересе, који по правилу нису усаглашени, а није редак случај да су чак и интереси у оквиру једне групе контрадикторни.

Корисници од електронског комуникационог система очекују поуздану, квалитетну и поверљиву услугу, као и то да њихови лични подаци које су поверили оператору остану заштићени од сваке незаконите обраде. Укључујући се у мрежу, корисници уговором или имплицитно прихватају одређена правила понашања и постају одговорни за своје поступке, прихватају мере које оператор предузима ради њихове заштите као корисника, али и мере која држава може предузети ради заштите друштвене заједнице. Важно је нагласити да при сваком прикупљању и обради података за потребе заштите мреже, услуга и корисника од стране оператора, дужна пажња мора бити посвећена питању приватности. Оно мора бити строго

контролисано и ограничено на јасно дефинисане легитимне сврхе. При томе, треба напоменути да обрачун и наплата услуга није једина легитимна сврха, како се то неретко тумачи.

Оператори могу имати улогу оператора телекомуникационих мрежа, пружалаца услуга приступа телекомуникационој или Интернет мрежи, пружалаца услуге приступа мултимедијалним садржајима, пружалаца услуга са додатном вредношћу, пружалаца услуга инфраструктуре (хардвера, комуникација, апликација, похрањивања информација) и другим. Најчешће се један пословни ентитет јавља у неколико улога, па је у пракси тешко одредити јасне границе. Оператори имају посебно изражен интерес да обезбеде заштиту приватности корисника и безбедност услуга, пошто на тај начин освајају бољу позицију на тржишту, штите своје материјалне и нематеријалне вредности, задобијају и чувају поверење корисника и не излажу се опасности да прекршајно и кривично одговарају. Основа пружања електронских комуникационих услуга је у поверљивом управљању информацијама и подацима корисника, па је поверење корисника од кључног значаја за сам посао. Губитак поверења корисника, утемељен на стварним инцидентима или само на перципираној приватности без заштите, може у знатној мери да нашкоди угледу оператора и директно се одрази чак и на вредност компаније на берзи. Због тога су приватност корисника и безбедност услуга из угла оператора битни предуслови за обављање основног посла, а у крајњем исходу чак и компаративна предност у односу на конкуренцију.

Комерцијални сектор има бројне и различите интересе у погледу заштите приватности корисника и безбедности услуга, интересе који све више добијају на значају са развојем пословних активности у домену Интернета и електронског пословања. С једне стране, погодности информационог друштва комерцијални сектор види као прилику да, обрађујући информације о потрошачима, проникне у њихове потребе, развије нове маркетиншке стратегије, нове производе, унапреди кориснички сервис, повећа ефикасност својих интерних процеса и слично. И ту се отвара питање на које није лако

одговорити: када маркетиншке активности прерастају у нарушавање приватности појединаца? Истовремено, безбедна ИКТ инфраструктура, безбедне електронске трансакције и заштићени лични подаци постају кључни у опредељивању потенцијалних клијената за ступање у пословни однос са неком компанијом. Све интензивније укључивање већег броја партнера у пословне процесе (кроз *Outsourcing* услуге, *Cloud computing* и сличне пословне моделе) чини да се традиционални безбедносни оквир ИТ губи у сајбер простору, што не само да усложава задатак заштите, него и наглашава значај најслабије карике у ланцу, који год учесник то био.

Пошто се поверење пружалаца услуга са додатном вредношћу заснива на гаранцијама других учесника у ланцу да њихови приходи неће бити оштећени преварама или повредама права интелектуалне својине, глобални развој сектора електронских комуникација почиње све више да зависи и од међусобног поверења свих страна у процесу и поставља као императив да сваки од њих предузме све разумне мере заштите.

Са друге стране, комерцијални сектор се јавља и као послодавац који има природан интерес да контролише пословне процесе, а то лако може да се деформише и у злоупотребу приватности запослених. Ако, на пример, послодавац који дозвољава коришћење компанијских комуникационих средстава и у приватне сврхе без изричите сагласности запослених прикупља и анализира податке о телефонским комуникацијама или контролише садржину електронске поште (ради наводне контроле трошкова, заштите пословања или слично), могао би се наћи у озбиљном проблему због повреде приватности појединаца.

Државни органи, поред интереса да обезбеде услове за законит надзор у области безбедности електронских комуникација и заштите приватности имају јасан задатак да уравнотеже интересе и одговорности грађана, комерцијалног сектора, оператора и друштвене заједнице. Доношењем неопходних прописа и обезбеђивањем њихове примене, држава треба да осигура највиши ниво безбедности и заштите грађана, али истовремено мора избећи и претерано оптерећивање оператора и спутавање комерцијалног

сектора. На природно питање где повући границу, ЕУ у серији стратешких докумената *eEurope* даје одговор да, колико год је то могуће, тржиште треба да одреди који је ниво безбедности потребан корисницима, за шта је опет неопходно да се утврде добри индикатори и јасни критеријуми успешности.

5.3.2. Заштита критичне инфраструктуре у поштанском сектору

Развој и примена оптималних модела за управљање критичном инфраструктуром у поштанском сектору, који су, између осталог, и у складу са Европским програмом за заштиту критичне инфраструктуре треба да обухватају одговарајуће моделе за идентификацију критичне инфраструктуре, моделе за идентификацију и анализу опасности, моделе за креирање идеалног сценарија и моделе дијагностике критичне инфраструктуре. На тај начин стварају се предуслови да оператори у поштанском сектору даље унапреде своје пословање, односно да пружају сервисе најбољег квалитета уз истовремено постизање добрих финансијских резултата и унапређење односа са својим корисницима и партнерима. Такође, посредно на овај начин се у великој мери повећава и конкурентност услуга и добара Србије на глобалном тржишту, затим здравље, безбедност и благостање грађана, квалитет живљења у заједницама, потребно време путовања људи на посао или ка другим одредиштима и ефикасан транспорт роба и услуга, као и поузданост и брзина телекомуникација, односно преноса поштанских пошиљки.

Један основни (општи) модел за управљање критичном инфраструктуром у поштанском сектору састојао би се из две фазе:

- анализа стања управљања критичном поштанском инфраструктуром и
- дефинисање оквира за развој одрживог система критичне поштанске инфраструктуре.[164]

Фаза анализе стања управљања критичном поштанском инфраструктуром обухватају следеће активности:

[164] *Мацура, Д., Управљање критичном инфраструктуром за одрживи развој у поштанском и железничком сектору РС, Пројекат Министарства науке и технолошког развоја, 2011-2014.*

- анализа модела управљања критичном инфраструктуром у поштанском сектору у одабраним земљама и Србији;
- анализа технологија за контролу услова и перформанси критичне инфраструктуре поштанског сектора;
- анализа нових материјала за изградњу и одржавање компоненти инфраструктуре у поштанском сектору;
- анализа текућих иницијатива за унапређење националних критичних инфраструктурних система;
- анализа постојећих модела финансирања инфраструктуре у поштанском сектору;
- истраживање међуповезаности и међузависности критичне инфраструктуре саобраћајних сектора.

Фаза дефинисања оквира за развој одрживог система критичне инфраструктуре у поштанском сектору састојала би се од следећих послова и задатака:

- дефинисање визије и циљева развоја одрживог система критичне инфраструктуре у поштанском сектору;
- развој ефективне стратегије управљања критичном инфраструктуром у поштанском сектору са фокусом на процену ризика;
- развој модела за мерење перформанси критичне инфраструктуре у поштанском сектору;
- дефинисање одговарајућег модела финансирања критичне инфраструктуре у поштанском сектору;
- разрада процеса и методологија заштите критичне инфраструктуре у поштанском сектору;
- развој програма обуке кадрова за управљање критичном инфраструктуром у поштанском сектору;
- дефинисање модела конзистентног партнерства између власника (оператора) поштанске инфраструктуре и државе;
- развој програма за примену модела управљања критичном инфраструктуром у поштанском сектору.

Примена адекватне методологије за управљање критичном инфраструктуром даје могућност да се у овај процес интегришу различите иницијативе. Осим тога, на овај начин се обезбеђује константно анализирање резултата процеса и могућности за даља унапређења.

Управљање критичном инфраструктуром у поштанском сектору захтева релативно велике инвестиције, како у само одржавање система, тако и у одговарајуће аналитичке базе података и информационе системе. Са друге стране, већина савремених стратегија за инвестирање и доношење одлука, било у јавним или приватним секторима, углавном се фокусирају на једну врсту инфраструктуре, или на један објекат, као и у извесној мери на значајне разлике у циљевима власника и оператера инфраструктуре што директно утиче и на обиме и износе инвестиција у критичну инфраструктуру у појединим секторима.

Осим тога, у пракси постоји и значајна разлика да ли инвестирање у инфраструктуру врши приватни сектор или државни органи, односно органи локалне управе. У приватном сектору иде се само ка оправданим инвестиционим улагањима, односно улагања се врше само ако је циљ задржавање постојећих клијената, проширење тржишта и броја постојећих клијената, или корист за акционаре, уз известан ризик да се инвестиција неће исплатити. Насупрот томе, државна и локална управа морају да пруже услуге свим домаћинствима, чак иако то није финансијски исплативо. Јавне услуге морају реализовати него за владу посебан изазов представља и задржавање ниских такси и трошкова услуга.

Посебна специфичност већине инфраструктурних унапређења је да се период инвестирања креће од 15 до 30 година, тако да је неопходна не само подршка локалног изборног тела, већ и изналажење одговарајућих механизама финансирања, који укључују јавно-приватна удруживања, корисничке таксе, јавне фондове, па и приватизацију појединих инфраструктурних система и објеката.

Одређени модели инвестирања у КИ довели су до тога да се доношење одлука о инвестицијама у јавни и приватни сектор реализују на принципу

пројекат по пројекат, чиме се спроводи сегментација финансијских извора између различитих нивоа у влади и између организација у приватним секторима.На основу искустава из развијених земаља Европске уније и света, које су унапредиле систем управљања и одржавања критичне инфраструктуре у поштанском саобраћају, као и осталим саобраћајним секторима ове инвестиције су се враћале већ након неколико година, и то пре свега кроз стварање ефикасног заједничког саобраћајног система и хармонизацију међу операторима, чиме се стварају предуслови за сигурност и ефективност саобраћајне услуге.[165]

5.3.3. Заштита критичне инфраструктуре у сектору енергетике

Упоредо са све бржим индустријским развојем и откривањем нових технологија, почетком XX века порасла је потреба за осигуравањем доступности енергената. Преласком из аграрне производње у индустријску није се променила само економска структура света, већ и сам људски живот. Производи постају доступнији и траженији, расту производња и транспорт, а у складу с тим расте и потреба за изворима енергије.

Земље богате енергентима, нафтом, природним гасом и угљем, постају геостратешки врло битне, посебно за земље чије су индустрије захтевале велике количине енергената. Почетком хладног рата почела се развијати и нуклеарна енергија која је у великој мери утицала на прерасподелу постојећих природних енергената. Употреба енергената стога је у битној мери одредила развој савремених држава, што можемо пратити кроз фазе од почетка XX века преко раздобља хладног рата и постхладноратовског доба до данас.

Борба народа за контролу извора енергије, као и њихово поседовање и допремање, као предуслова развоја, постала је кључно питање, које је брзо прерасло економске оквире и ушло у сферу политичког и сигурносног. Такмичење у контролисању извора енергије постало је глобално питање које

[165]*Вешовић, В., Кнежевић, Н., Менаџмент пословних процеса у пружању поштанских и телекомуникационих услуга, XXIII Симпозијум о новим технологијама у поштанском и телекомуникационом саобраћају - PosTel 2005, Београд, 13.-14.12.2005.*

не укључује само и искључиво државе, него и мноштво организација, мултинационалних компанија, финансијских актера, али и терористичких група које отежавају ситуацију везану за енергенте последњих година. Посебно се то односи на заштиту критичне енергетске инфраструктуре. Стога је питање енергетске сигурности постало питање како међународне сигурности тако и националне сигурности већине земаља света. Данашња пракса показује да се све више земаља света индустријски развија, у зависности од ситуације на тржишту енергената које је прилично нестабилно и подложно политичким интервенцијама.

Важан проблем је и исцрпљивање светских извора енергената, нафте и природног гаса и њихове велике залихе на подручјима која су политички и економски нестабилна, што изазива проблеме у снабдевању енергентима, али и у њиховим ценама. Надаље, еколошка питања такође заокупљају јавност и научнике. Међутим, потребе за енергентима расту, а државе настоје осигурати стабилно снабдевање. Стога је нужно дефинисати сигурносне политике помоћу којих ће се спровести идеје сигурног снабдевања енергентима у сврху даљег просперитета, без угрожавања других друштвених подручја. Свака би држава требала енергетску сигурност имплементирати у систем националне сигурности, било у смислу снабдевача енергентима или у смислу потрошача, како би се створио сигуран и стабилан енергетски систем у светским размерама.

Енергетика је једна од инвестиционо најинтензивнијих грана привреде. Она имавишеструко дејство на економске резултате привређивања, као и на читаву технолошку основу друштва, и представља једну од основних подлога укупног развоја свакеземље. Сигурно и безбедно снабдевање енергијом, њена доступност и расположивост под транспарентним и недискриминаторним условима, производња и коришћење у складу са принципима одрживог развоја су предуслови за успешно функционисање сваког друштва, за подизање конкурентности националне привреде и коначно за благостање грађана. Ово је посебно битно у времену економске кризе у којој се Република Србија тренутно налази.

Стратегијом развоја енергетике Републике Србије за период до 2025. године, са пројекцијама до 2030. године предлаже се пут тржишног реструктурирања и технолошке модернизације енергетике Републике Србије, како би се боље припремила за период раста опште тражње добара и услуга.

Стратешки приступ енергетици подразумева да се процеси у привреди и држави, као и у животу грађана, одвијају уз ниже економске трошкове и виши степен социјалне и еколошке одрживости - виши стандард становништва уз смањење загађења и бољу заштиту природе. У том смислу, из примене Закона о енергетици и Стратегије развоја енергетике Републике Србије, треба да проистекне одговарајућа енергетска политика, која би уз адекватну економску и социјалну политику, као и политику у области заштите животне средине водила ка одрживом енергетском систему, ефикаснијој економији и већем друштвеном благостању, уз одрживе билансе природних ресурса и што ниже нивое загађења.

Енергетске ресурсе и потенцијале Републике Србије чине фосилна, конвенционална (угаљ, нафта и природни гас) и неконвенционална горива (уљни шкриљци), као и обновљиви извори енергије.

Република Србија је прихватила, потписала и ратификовала Уговор о оснивању Енергетске заједнице. Тиме је као један од својих приоритета поставила и успостављање регионалног тржишта енергије и његову интеграцију у енергетско тржиште Европске уније. Такво тржиште треба да омогући значајније инвестирање у сектор и да допринесе економском развоју и стабилности земље и региона. Функционисање тржишта се мора заснивати на имплементацији релевантног правног оквира и правних тековина Европске уније у области енергетике, заштите животне средине, конкуренције, коришћења обновљивих извора енергије и енергетске ефикасности. Енергетску безбедност релативно мале и увозно зависне економије је далеко лакше остварити у условима усаглашених принципа функционисања тржишта енергије у региону и шире, стварањем јединственог и отвореног енергетског тржишта.

Развијено национално и регионално тржиште отвара могућности за значајно веће инвестирање у сектор и доприноси економском развоју и стабилности земље. Изградња гасовода „Јужни ток", и нових електроенергетских и гасних интерконекција ће позиционирати Републику Србију као енергетски значајну транзитну земљу. За ефикасно функционисање унутрашњег и регионалног енергетског тржишта неопходан је рад на даљој изградњи и модернизацији електроенергетске и гасоводне инфраструктуре. Потребно је извршити регионално повезивање гасоводног система и завршити гасификацију Србије, а у области електроенергетике перманентно радити на ревитализацији постојећих и изградњи нових преносних и дистрибутивних капацитета. Развој енергетике Републике Србије треба да буде такав да његови ефекти по животну средину буду минимални. Међутим, енергетика Србије ће морати и да буде тржишно утемељена и економски ефикасна, у мери да генерише сопствени развој, али и да представља генератор и сигурну основу развоја земље.[166]

5.4. ПРОЦЕНА РИЗИКА ПО КРИТИЧНУ ИНФРАСТРУКТУРУ

Упутство о методологији за израду процене угрожености и планова заштите и спасавања у ванредним ситуацијама је садржано у „Службеном гласнику РС" бр. 96 из 2012. године. Овим упутством прописана је методологија за израду процене угрожености од елементарних непогода и других несрећа, плана заштите и спасавања у ванредним ситуацијама на нивоу Републике Србије и плана заштите и спасавања у ванредним ситуацијама органа државне управе, аутономних покрајина, јединица локалне самоуправе, привредних друштава, других правних лица и других организација.

Процена је документ којим се идентификују опасности, извори и облици угрожавања, могући ефекти и последице, процена угрожености - ризика, сагледавање снага, средстава и превентивних мера за одговор на опасности изазване елементарним непогодама и другим несрећама, заштиту и

[166] *Стратегија развоја енергетике Републике Србије до 2025. године, са пројекцијама до 2030. године, 2014.*

спасавање живота и здравља људи, животиња, заштите материјалних, културних добара и животне средине.

Проценом се дефинишу положај и карактеристике територије, могућа угроженост критичне инфраструктуре, идентификација опасности, процена ризика, процена потребних снага, средстава и превентивних мера за заштиту и спасавање од елементарних непогода и других несрећа.

Процена садржи:

- увод;
- положај и карактеристике територије;
- процену критичне инфраструктуре са становишта угрожености од елементарних непогода и других несрећа;
- идентификацију опасности и процену ризика од елементарних непогода и других несрећа;
- процену потребних снага, средстава и превентивних мера за спровођење заштите и спасавања и
- закључак.

Код процене врсте и интензитета опасности и могућих последица деловања елементарних непогода и других несрећа, потребно је идентификовати објекте критичне инфраструктуре и извршити процену могућих штетних последица на обављање њихове делатности и последица прекида обављања делатности по кориснике, и то нарочито у следећим областима:

- **Производње и дистрибуције електричне енергије:** хидроелектране, термоелектране, алтернативни енергенти, далеководи, трафо-станице;
- **Снабдевања енергентима (мрежа дистрибуције енергената):** складишта гаса, нафтних деривата и других енергената (магистрални нафтоводи, гасоводи и локална гасна мрежа);
- **Снабдевања водом:** систем дистрибуције воде и пречистача, изворишта воде за пиће, изворишта воде - бунари, могући загађивачи површинских и подземних вода;

- **Снабдевања становништва храном (производња, складиштење и дистрибуција):** производни објекти и капацитети, погони за производњу хране, складишне просторије прехрамбених производа, објекти и средства за дистрибуцију, обрадиве пољопривредне површине, плантаже воћа, објекти за узгој животиња и прераду меса;
- **Здравствена заштита:** здравствено обезбеђење и локације (здравствене установе, локације, капацитети, техничка опремљеност);
- **Материјална и културна добра и животна средина:** објекти од националног значаја (културно-историјски споменици, музеји, легати и др.), објекти за одржавање културних манифестација и верски објекти;
- **Заштићена природна добара:** национални паркови, резервати животињског света;
- **Телекомуникација:** преносни путеви (подземни каблови, ваздушни водови, бежични линкови), антенски стубови, антене базних станица за мобилну телефонију, телефонске централе, преносна емисиона опрема - радио и ТВ станица (техничка опрема за пренос и емитовање аудио-визуалног сигнала);
- **Саобраћај:** саобраћајна и путна мрежа, железничка мрежа, пловни речни путеви, мостови, вијадукти и тунели и
- **Производње опасних материја** (објекти за производњу, складиштење и промет опасних материја).

Процена се заснива на анализи потенцијалних опасности и последица по становништво, материјална и културна добра и то:

1) Од поплава: хидролошки показатељи - водотокови, језера и акумулације које могу бити узрок поплава, опасност од поплава река или бујичних вода, преглед угрожених насеља с бројем и структуром становништва, мере заштите у урбанистичким плановима и грађењу, хидрометеоролошки услови - водостај, лед, просечна годишња количина падавина, заштитна инфраструктура - насипи и други заштитни водопривредни објекти с

показатељима о броју, врстама, димензијама и сл., процењена величина угроженог подручја и степен изграђености површина - насељеност, индустрија, саобраћај, локације критичне за формирање ледених баријера у утицај на пловност, статистички показатељи о најкритичнијим месецима у години, проглашеним елементарним непогодама, насталим штетама и сл.;

2) Од померања тла, односно сеизмичких опасности:

Земљотрес: морфологија и састав земљишта, сеизмолошка карта, сеизмичке карактеристике терена, мере заштите у урбанистичким плановима и градњи, квалитет градње, учесталост, интензитети и епицентри потреса у задњих 50 година, последица потреса по сеизмичким зонама за стамбене, јавне, индустријске и друге објекте коришћењем MCS, могуће последице (могући број угроженог становништва, могућа оштећења и уништења материјалних и културних добара и могућа угроженост животне средине (ваздух, земљиште, вода, биљни и животињски свет), психолошки ефекти и могућа повређивања (појаве у објектима становања и другим објектима), промене у природи (подземне воде, тло и растиње), оштећење инфраструктуре и др.);

Клизишта, одрони и ерозије: мапиран рељеф са приказом удолина различитих површина и нагиба, режим подземних вода (осцилација нивоа подземних вода), густина и влажност тла, могућа оштећења на објектима, оштећења путне инфраструктуре и подземне инфраструктуре - цевоводи и мере заштите предвиђене урбанистичким плановима; ерозије (квалитет земљишта, узрок који проузрокује ерозију пустошење и крчење шума, непланске чисте сече, паша и брст стоке, коришћење камена, шљунка, песка, хумуса, земље и тресета, ветрови, обилне падавине, површина захваћена ерозијом, густина насељености и број објеката.);

3) Од осталих природних узрока, нарочито оних који припадају категорији екстремних временских услова (суша, олујни ветрови, град, снежне мећаве, падавине наноси и поледица), статистички подаци сушних периода (број месеци-дана без кише) за последњих 10 година, класификација јачине суше помоћу СПИ (стандард индекса падавина), могућности наводњавања (расположивост воде за наводњавање), интензитет олујних ветрова, правац

и смер струјања, висина снежних падавина, густина инфраструктурних и привредних објеката на подручју, постојање активне заштите од града, спецификација угрожених и најугроженијих подручја (насељеност, структура становништва, прилазни путеви животињски свет и др.) и статистички приказ последица за последњих 10 година, број проглашених ванредних ситуација због појаве елементарне непогоде у последњих 10 година, које су битно промениле свакодневно функционисање (могућност снабдевања виталним производима, прекид снабдевања електричном енергијом, прекид саобраћаја, онемогућавање пружања хитне медицинске помоћи и сл.) и могући утицаји на пољопривредне културе, здравље људе и животиње;

4) Од техничко-технолошких удеса и терористичких напада:

изазване несрећом у привредним - индустријским објектима: количина и врста опасних материја у постројењима, складиштима и у промету, карактеристике територије у окружењу објекта са опасним материјама (врста насеља, густина насељености, привредни и повредиви објекти, удаљеност, културна и материјална добра и др.; изазване несрећама у саобраћају: количина и врста опасних материја у саобраћају (месечни и годишњи промет по пуним правцима) инфраструктура - анализирати стање путне, железничке и водене инфраструктуре, ранжирних рампи, прелаза, да ли постоје посебна паркинг и зауставна места, путева кроз националне паркове и заштићена подручја, уређеност пристаништа и лука са аспекта претакања и манипулације и др.

Процена последица од тероризма израђује се на основу стратешких докумената Републике Србије, јавно доступних докумената министарства надлежног за одбрану и министарства надлежног за унутрашње послове, узимајући у обзир структуру, величину и процедуре оперативних снага за реаговање у ванредним ситуацијама у односу на захтеве за њиховим ангажовањем током отклањања последица тероризма. Процена од терористичког напада обухвата податке о: карактеристикама објеката, уређаја, савремених техничких средстава и физичко техничког обезбеђења, који могу бити мета терористичког напада, могућности и последице

терористичког напада, број настрадалих и погинулих, материјална штета, облици терористичке активности са аспекта примене средстава (експлозивна, хемијска, радиолошка и биолошка средства);

5) Од пожара и експлозија: број и врсту објеката угрожених од пожара (стамбених, индустријских, јавних и других), осетљивост објеката на пожаре, стање противпожарне заштите, зоне угрожености, број угрожених људи, животиња, материјалних добара, густину изграђености објеката по рејонима, врсту објеката (материјал, спратност, пожарна оптерећеност), ширину и проходност саобраћајница,врсту и стање инсталација (електроинсталација, гасоводи и др.), начин снабдевања водом (број и распоред хидраната, бунара, цистерни идр.), изворе топлоте, шумске комплексе (врсте шума, уређеност, проходност, начин експлоатације); складишта експлозивних средстава, производња муниције експлозивних направа и др., складишта експлозивних материјала, експлозивне прашине, заостала неексплодирана убојна средства (НУС), носиоца заштите од експлозија, место и локација уништења НУС, преглед субјеката у којима постоји великаопасност од експлозије;

6) Од рушења хидроакумулационих брана (могућа опасност заснива се на потенцијалима хидроакумулационих језера, односно на њиховој акумулацији због кога би услед рушења бране или насипа хидроакумулације било угрожено становништво и материјална добра на правцу кретања водног таласа), мере заштите у урбанистичким плановима и грађењу;

7) Од нуклеарних и радијационих акцидената: стање нуклеарних објеката као и објеката за заштиту од нуклеарних и/или радијационих акцидената на територији - анализирати број и квалитет стамбених и привредних објеката са аспекта могућности коришћења за склоништа, особине радиоактивних материја које настају у акциденту, могућност радиоактивне контаминације људи, животиња, воде,ваздуха, земљишта, пољопривредних површина засејаних пољопривредним културама, угроженост прекограничним ефектом (важно јеевидентирати најближа подручја која у случају потенцијалне опасности могу бити угрожена), уобичајене врсте несрећа које се догађају (са испуштањем у атмосферу, испуштањем у површинске воде,

водотокове, језера, испуштање у тло, односно у подземни водоток као и присуство радиоактивног отпада);

8) Од епидемиолошке и санитарне опасности (могуће последице заснивају се на проценама надлежних здравствених, санитарних, ветеринарских, агрономских и других служби и институција које у јединственом систему заштите и спасавања представљају основне носиоце који су, у оквиру редовних делатности, надлежни за реаговање у случајевима епидемиолошких и санитарних опасности), мере заштите у урбанистичким плановима и грађењу;

9) Од епидемије: Угроженост подручја епидемијама насталим без повезаности са другим појавама - подручје анализирати према следећем: могућност појаве нових заразних болести; могући поремећаји водоснабдевања; конзумирање намирница ван контроле; обухват имунизацијом.

Типови епидемија - Угроженост подручја епидемијама које настају као последица санитарно хигијенских услова и инфраструктуре територије - анализирати са аспекта: постојања различитих врста епидемија.

Санитарно хигијенско стање објеката и инфраструктурних инсталација - сагледати са аспекта: постојања депонија, локације, величине и стања; локално снабдевање водом; грађевинско-техничко стање постојећих објеката.

Здравствени и други капацитети у функцији збрињавања, смештаја, транспорта и друго, сагледати са аспекта - кадровски, смештајни и транспортни капацитети, лекови, медицинска и друга опрема;

10) Од епизоотија: параметри и карактер опасности - подручје анализирати са аспекта броја и врста угрожених животиња и карактеристика болести;

Површина и карактеристике угроженог подручја - подручје анализирати са аспекта: извора заразне болести, развоја, преношења и ширења болести, могућности предузимања превентивних и куративних мера;

Густина животињског фонда - извршити анализу густине животињског фонда са аспекта броја и врста животиња критичних на епизоотије;

Изграђеност система заштите од епизоотија - анализирати са аспекта постојања планова заштите од епизоотија, природних и вештачких баријера за ширење болести и капацитета за збрињавање;

11) Од биљних болести анализирати са аспекта врста угрожених биљака и карактеристика болести (извора, развоја преношења и ширења), површине и карактеристика угроженог подручја, посебно пољопривредних површина засејаних усевима, поврћем и воћем.

Могући ниво несреће одређује се на основу предвиђеног сценарија и анализе повредивости, а изражава се као I, II, III, IV или V ниво несреће:

I ниво несреће (објекта постројења) - негативне последице несреће су ограничене на део објекта- постројења или цео објекат - постројење на комплексу привредног друштва и другог правног лица и не очекују се негативне последице у околини.

II ниво несреће (објекта, постројења и комплекса) - негативне последице несреће могу захватити део објекта - постројења илицео комплекс привредног друштва и другог правног лица и не очекују се негативне последице у околини изван комплекса.

III ниво несреће (ниво јединице локалне самоуправе) - негативне последице несреће могу се пренети изван граница опасног објекта - постројења и комплекса привредног друштва и другог правног лица и очекују се последице на делу или целој територији јединице локалне самоуправе, односно града.

IV ниво несреће (национални ниво) - негативне последице несреће на објекту - постројењу и комплексу привредног друштва и другог правног лица, могу се проширити на део територије и целу територију Републике Србије.

V ниво несреће (међународни ниво) - негативне последице несреће на објекту - постројењу и комплексу привредног друштва и другог правног лица, могу се проширити ван територије Републике Србије.

5.4.1. Процена угрожености привредног друштва и другог правног лица

Процена се разрађује по елементима овог упутства, али прилагођено својим потребама, односно специфичностима и то:

Положај и карактеристике локације:

Објекти, постројења, инфраструктура, делатност, намена и коришћење површина, окружење, насељеност, повредиви објекти у окружењу, подаци о удесима и др.

- Социјална структура запослених: укупан број запослених (мушкарци и жене), квалификациона структура, оспособљеност са аспекта заштите и спасавања;
- Материјална добра;
- Водоснабдевање: бунари, хидрантска мрежа, црпне станице, објекти за прераду воде (градска водоводна мрежа), квалитет воде, потребне количине и дистрибутивна мрежа;
- Пољопривредне површине: земљишна површина по намени коришћења и сектору власништва, остварена сетвена структура у производњи у текућој години основних ратарских и повртарских култура, преглед појединих капацитета складишног простора на територији општине, капацитети хладњача на територији општине за ускладиштење меса и месних производа, силоси и сушаре;
- Објекти за склањање и здравствено збрињавање: објекти за збрињавање запослених (капацитети, локације, медицинска опремљеност, квалификациона структура запослених и др.), екстерне здравствене институције за потребе здравственог збрињавања запослених;

- Саобраћајно-технолошка инфраструктура: путна мрежа, железничка мрежа, пристаништа, канализација, гасна, системи за пречишћавање отпадних вода.

5.4.2. Процена критичне инфраструктуре са становишта угрожености од елементарних непогода и других несрећа

Проценом критичне инфраструктуре, потребно је идентификовати објекте и проценити последице од елементарних непогода и других несрећа са аспекта функционисања исте, и то у областима:

- Снабдевања енергијом (мрежа дистрибуције енергената): струјом, складишта нафтних деривата, гасна мрежа и др.;
- Снабдевања водом - властито (бунари);
- Здравствена заштита: објекти (локација);
- Материјална добра: складишта (готови производи, сировине), средства за рад по постројењима, помоћни објекти;
- Путна инфраструктура: интерна (путна, железничка), пристаништа.

5.4.3. Процена снага, средстава и превентивних мера за заштиту и спасавање

У Процени снага, средстава и превентивних мера за заштиту и спасавања потребно је утврдити постојеће снаге и средства, расположиве материјалне ресурсе који се могу ангажовати на спречавању настанка и отклањању поледица елементарних непогода и других несрећа.

Превентивне мере се предузимају ради спречавања или смањења вероватноће настанка несреће као и умањења последица од истог и то:

- мере које су предвиђене избором техничко-технолошких решења које обезбеђују безбедан транспорт опасних материја унутар привредног друштва;
- мере које обезбеђују квалитетно и правовремено одржавање техничко-технолошког нивоа објекта - постројења, нивоа знања, нивоа радне и технолошке дисциплине;

- мере које су предвиђене за одржавање комуникационих путева и пролаза у објектима, постројењима и погонима;
- мере које су предвиђене у систему безбедности: надзор, управљање системима безбедности и заштите, детекција и идентификација опасности.

Привредна друштва и друга правна лица овлашћена и оспособљена за спровођење мера заштите и спасавања у Републици Србији, посебно разрађују део Процене које се односе на снаге и средства планирана за извршавање задатака заштите и спасавања из Националног плана и Плана. Све наведене активности су садржане у Плану заштите и спасавања, тј. основном планском документу на основу кога се субјекти заштите и спасавања организују и припремају и учествују у извршавању мера и задатака заштите и спасавања угроженог становништва, материјалних и културних добара и животне средине.

Као једна од европских земаља у транзицији Република Србија покушава да успостави везу са модерним европским демократијама, развије концепт владавине права, реформише законску регулативу и укључи се у регионалне и светске токове. Стога се питање изградње адекватног система управљања ванредним ситуацијама и заштите инфраструктура од битног значаја намеће само по себи, како на државном нивоу тако и у јавним предузећима, профитном сектору, образовању, туризму, спорту и другим областима.

Концепт заштите критичних инфраструктура са аспекта националне безбедности РС, захтева усаглашавање националног законодавства са постојећим међународним стандардима.

С обзиром на кораке које РС чини како би постала чланица Европске уније и на убрзану информатизацију друштва, процес стандардизације у овој области намеће се као један од приоритетних задатака РС у блиској будућности.

5.5. УЛОГА СЕКТОРА ЗА ВАНРЕДНЕ СИТУАЦИЈЕ У ЗАШТИТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

По питању проблематике везене за ванредне ситуације, као и последице које остављају на критичну инфраструктуру основни субјект одговора је у надлежности Сектора за ванредне ситуације Министарства унутрашњих послова (у даљем тексту Министарства). Он је формиран 2009. године спајањем Сектора за заштиту и спасавање Министарства и Управе за ванредне ситуације Министарства одбране у јединствену службу.[167]

Главни задаци Сектора су: превентива; надзор; припрема грађана за ВС; обука оперативних јединица: набавка опреме за оперативне јединице; спасилачке активности; управљање у ванредним ситуацијама; координација између републичке и локалне управе са осталим организацијама на националном, регионалном и локалном нивоу; спровођење мера на отклањању последица ВС; размена информација; међународна сарадња.

У извршавању своје функције Сектор обавља следеће послове:

- нормативне, управне, организационо-техничке, превентивне, превентивно-техничке, образовне, информативно-васпитне и друге природе за организовање, планирање, спровођење, контролу мера заштите животне средине, здравља и материјалних добара грађана, очување услова неопходних за живот и припремање за превладавање ситуације у условима пожара, елементарних непогода техничко-технолошких незгода, дејства опасних материја и других стања, опасности већих размера које могу да угрозе здравље и животе људи и животну средину или да проузрокују штету већег обима и пружање помоћи код отклањања последица (смањивање и санацију) проузрокованих у ванредним ситуацијама, а посебно: израде и предлагање закона, норматива и препорука који испуњавају захтеве Европске уније у области заштите и спасавања у ВС у циљу потпуног правног уређивања за обављање послова; успостављање институционалних, организационих и персоналних услова

[167] *Више: сајт Сектора за ванредне ситуације МУП РС.*

за спровођење заштите и спасавања у ванредним ситуацијама; предузимање превентивних мера ради спречавања избијања пожара и ублажавања последица елементарних непогода, технолошких незгода и сл. Превенција у циљу спречавања угрожавања здравља грађана услед дејства опасних материја и других опасности и

- стручног оспособљавања припадника организационих јединица на пословима делокруга Сектора и др.

У извршавању напред наведених задатака Сектор остварује непосредну сарадњу и координацију са свим министарствима и органима државне управе (републички, покрајински и локална самоуправа), привредним друштвима и другим правним лицима, удружењима, професионалним и другим организацијама. Сектор за ВС у свом саставу има: управу за превентивну заштиту; управу за ватрогасно-спасилачке јединице; управу за управљање ризицима; управа за цивилну заштиту; национални центар за ВС, и управе и одељења за ВС у полицијским управама.

Управа за превентивну заштиту у свом саставу има: Одељење за спровођење превентивних мера при изградњи објеката, Одељење за спровођење превентивних мера при коришћењу објеката и Одељење за контролу промета и превоза опасних материја.

Управа за ватрогасно-спасилачке јединице у свом саставу има: Одељење за материјално - техничко опремање ватрогасних и спасилачких јединица, Одељење за контролу рада ватрогасних и спасилачких јединица, и Одсек за здравствено психолошку превенцију.

Управа за управљање ризиком у свом саставу има Републички центар за обавештавање (112), и Одељења за: осматрање, обавештавање, узбуњивање и телекомуникације, управљање ризиком од технолошких удеса и терористичких напада, и управљање програмима и пројектима.

Управа за цивилну заштиту у свом саставу има: Одељење за оперативно организационе послове цивилне заштите, Одељење за стратешко планирање и координацију и Одељење за техничку подршку и неексплодирана убојна

средства.

Функционисање система за заштиту и спасавање у ВС реализује се, у зависности од услова и обима прогнозиране или настале ВС у три режима - фазе:

- режим редовне делатности,
- режим приправности - повећане спремности и
- режим ванредних ситуација.

Важан део система за ВС су снаге и средства, која се деле на снаге и средства за надзор и контролу, и снаге и средства за одговор (локализацију и ликвидацију) ванредних ситуација.

Снаге и средства за надзор и контролу обухватају органе, службе и установе, који врше државни надзор, инспекцију, мониторинг, контролу, анализу стања животне средине, потенцијално опасних објеката, материјала, здравља људи.

Снаге и средства за одговор (локализацију и ликвидацију) ВС чине:

- ватрогасно-спасилачке јединице Сектора за ВС Министарства;
- специјализоване јединице цивилне заштите Сектора за ВС Министарства и других предузећа;
- службе хитне медицинске помоћи и мобилне екотоксиколошке лабораторије Министарства здравља;
- опште и специјализоване јединице Министарства (жандармерија, специјална антитерористичка јединица, против терористичка јединица, хеликоптерска јединица, речна полиција; полицијска бригада, интервентне јединице дежурних служби и др.);
- јединице за уклањање и уништавање НУС;
- противградне службе Републичке хидрометеролошке службе;
- ватрогасне јединице привредних друштава и добровољних ватрогасних друштава;
- јединице опште намене Цивилне заштите локалне самоуправе и привредних друштава;

- инжењеријске и друге јединице и јединице радијацијске, хемијске и биолошке заштите Министарства одбране, као и национални центар за контролу тровања (ВМА);
- Црвени крст Србије;
- рударско-спасилачке јединице и интервентне екипе „Србија гаса“ и електропривредних предузећа;
- ватрогасно-спасилачки возови и специјална шинска возила железница Србије;
- привредна авијација Министарства пољопривреде;
- хаваријско-спасилачке екипе и јединице у предузећима;
- јединице и специјалисти - добровољци друштвених удружења (ватрогасци, спелеолози, алпинисти, кинолози и др.).

6. ЕМПИРИЈСКА ИСТРАЖИВАЊА

Истраживања реализована у овој докторској дисертацији су обухватила анализу свих фактора који се односе на безбедносне аспекте функционисања критичне инфраструктуре у ванредним ситуацијама.

Истраживање је спроведено у форми анкетног упитника (Прилог 1.) који је садржао 35 питања. Истраживањем су обухваћене све релевантне установе које су везане за домен критичне инфраструктуре.

Питање 1: Старосна група анкетираног лица
Одговор: Старосне категорије анкетираних лица су приказане у табели 3.

Табела 3. Старосна група анкетираних лица

Р.бр.	Број година	Број лица	Проценат (%)
1.	до 35 година	14	14,9
2.	од 36 - 45 година	28	29,8
3.	више од 45 година	52	55,3

Евидентно је да највећи број анкетираних лица у овој области старости изнад45 година, што значи да је 55,3 % лица са највећим искуством је учествовало у овом истраживању. Резултати анкетирања су приказани у табели 4.

Питање 2:Пол анкетираних лица
Одговор: Истраживањем су обухваћена 94 лица, 64 мушкарца и 30 жена.

Табела 4. Институције у којима је спроведено анкетирање

Институције анкетираних лица	Мушкараца	Жена	Укупно
Сектор за ванредне ситуације МУП РС	28	14	42
Јавно комунално предузеће „Београдски водовод и канализација“	7	1	8
Јавно предузеће „Пошта Србије“	20	9	29
Јавно предузеће „Електропривреда Србије“	3	1	4
Нафтна индустрија Србије а.д.	3	/	3
Јавно предузеће „Електромрежа Србије“	1	1	2
Јавно предузеће„Путеви Србије“	1	/	1
Јавно водопривредно предузеће „Србијаводе“	1	1	2
Железнице Србије а.д.	/	3	3
УКУПНО	**64**	**30**	**94**

Додатне информације добијене анкетним упитником су садржане у табели5.

Табела 5. Степен образовања испитаника

Стручна спрема	Број лица
Средња стручна спрема	18
Виша стручна спрема	4
Висока стручна спрема	30
Мастер - Магистар	5
Доктор наука	3
УКУПНО	**60**

Питање 3: Наведите област радног/стручног ангажовања (реферат/послове које обављате.

Одговор: У оквиру овог питања анкетирана лица су навела дужности на којима се налазе, а анализом података је установљено да је њихово радно и стручно ангажовање везано за критичну инфраструктуру.

Питање 4: Наведите шта се подразумева под критичном инфраструктуром?

Одговор: У оквиру овог питања највећи број анкетираних лица (око 70 %) је

критичну инфраструктуру дефинисао као објекте који су најугроженији од ванредних ситуација (електроенергетски објекти, саобраћај ПТТ саобраћај, војни објекти, водовод и канализација итд.

Питање 5: Колико година се бавите пословима везаним за заштиту и спасавање?

Одговор: Добијени резултати су дати у табели 6.

Табела 6. Радно ангажовање на пословима заштите и спасавања

Р.бр.	**Број година**	**Број лица**	**Проценат (%)**
1.	до 5 година	28	29,8
2.	од 5 до 10 година	6	6,3
3.	од 10 - 20 година	31	32,9
4.	од 20 - 30 година	20	21,4
5.	више од 30 година	9	9,6

Стручно мишљење су дала и лица која поседују велико искуство у овој области (више од 30 година), као и почетници (до 10 година).

Питање 6: Оцените значај критичне инфраструктуре за управљање и превазилажење последица ванредне ситуације.

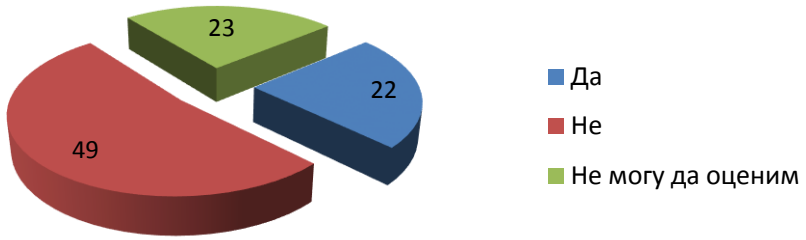
Одговор: Добијенирезултати су приказани у табели 7.

Табела 7. Значај критичне инфраструктуре

Р.бр.	**Значај**	**Број лица**	**Проценат (%)**
1.	Изузетно велики значај	61	64,9
2.	Велики значај	30	30,9
3.	Мали значај	1	1
4.	Нема значај	/	/
5.	Не могу да оценим	2	3,2

Питање 7: Да ли сматрате да је критична инфраструктура и њено функционисање у условима ванредне ситуације довољно нормативно-правно регулисано?

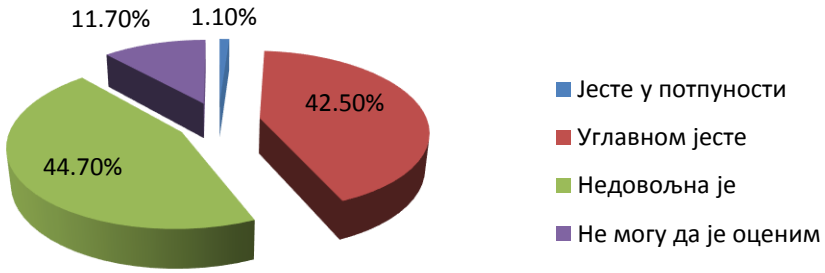
Одговор: Добијенирезултати су приказани на графикону 1.



Графикон 1. Мишљење о функционисању КИ у условима ванредних ситуација

Питање 8: Да ли је, према Вашем мишљењу, постојећа законска регулатива адекватна савременим опасностима и потребама заштите и спасавања у условима ванреднихситуација?

Одговор: Добијенирезултати су приказани на графикону 2.



Графикон 2.Усклађеност законске регулативе са савременим опасностима и потребама заштите и спасавања у условима ванреднихситуација

Питање 9: Да ли је по Вашем мишљењу неопходно (променити, усвојити) још неке законске прописе у области заштите и спасавања?

Одговор: Добијенирезултати су приказани у табели 8.

Табела 8. Потреба промене законских прописа

Р.бр.	Промена законских прописа	Број лица	Проценат (%)
1.	Да	28	29,8
2.	Не	5	5,3
3.	Делимично	49	52,2
4.	Не могу да се одредим по овом питању	12	12,7

Питање10: Да ли израда нормативно-правне регулативе у области заштите и спасавања треба да буде заједнички посао субјеката различитих профила (нпр. стручно-оперативни органи из области заштите и спасавања, здравствене службе, ватрогасно-спасилачких јединица МУП, Војске, стручњаци из области заштите животне средине, радници државних органа управе и безбедносних структура БИА, ВБА или ВОА)?

Одговор: Добијенирезултати су приказани у табели 9.

Табела 9. Потреба за сарадњом у процесу израденормативно-правне регулативе

Р.бр.	Заједничка израда нормативно-правне регулативе	Број лица	Проценат (%)
1.	Неопходна је сарадња међу њима	93	98,9
2.	Сарадња није неопходна	/	/
3.	Немам мишљење о овом питању	1	1,1

Питање11: Да ли је спроведена процена ризика у Вашем предузећу?

Одговор: Добијенирезултати су приказани у табели 10.

Табела 10. Реализација процене ризика у установи

Р.бр.	Процена ризика у установи	Број лица	Проценат (%)
1.	Да	24	25,5
2.	Не	21	22,3
3.	Делимично	29	30,9
4.	Не могу да се одредим по овом питању	20	21,3

Питање12: Наведите три потенцијална ризика који могу довести до ванредне ситуације у Вашем предузећу?

Одговор: Највећи број анкетираних лица је као потенцијалне опасности навео пожар, експлозије и епидемије.

Питање 13: Да ли постоји могућност угрожавања Вашег привредног субјекта од нуклеарних, хемијских или биолошких терористичких радњи?

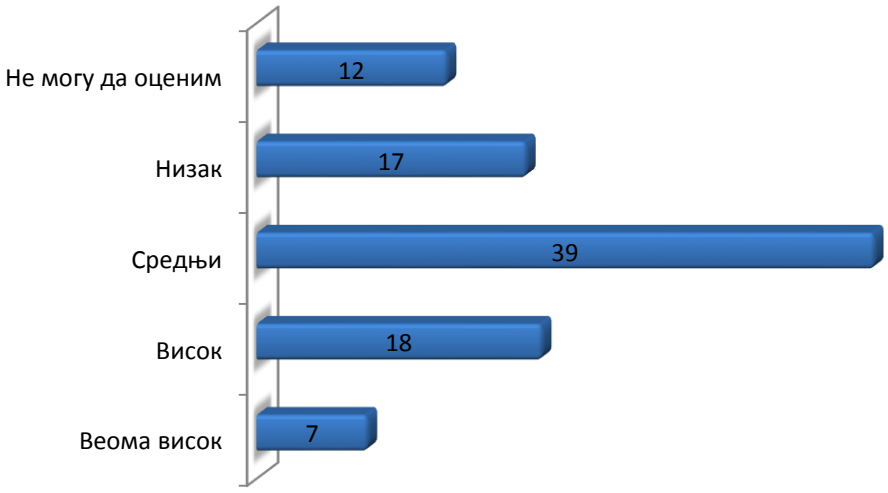
Одговор: Добијенирезултати су приказани у табели 11.

Табела 11. Могућност угрожавања привредног субјекта од нуклеарних, хемијских или биолошких терористичких радњи

Р.бр.	Процена ризика у установи	Број лица	Проценат (%)
1.	Да	57	60,6
2.	Не	9	9,6
3.	Не могу да оценим	28	29,8

Питање 14: Оцените степен опасности од природних и техничко-технолошких ризика у Вашој средини?

Одговор: Добијенирезултати су приказани на графикону 3.



Графикон 3.Степен опасности од природних и техничко-технолошких ризика

Питање 15: По Вашем мишљењу који од објеката критичне инфраструктуре су најугроженији у условима ванредне ситуације?

Одговор: Добијенирезултати су приказани на графикону 4.

Графикон 4. Степен опасности од природних и техничко-технолошких ризика

Питање 16: Да ли је критична инфраструктура изложена потенцијалним терористичким нападима и којим (која средства би била по вашем мишљењу употребљена)?

Одговор: Добијенирезултати су приказани у табели 12.

Табела 12. Изложеност критичне инфраструктуре потенцијалним терористичким нападима

Р.бр.	Процена ризика у установи	Број лица	Проценат (%)
1.	Конвенционална (класична)	50	53,2
2.	НХБ (нуклеарна, хемијска или биолошка)	24	25,5
4.	Импровизована	20	21,3

Питање 17: Можете ли навести шта садржи процена ризика?

Одговор: У оквиру овог питања највећи број анкетираних лица (око 75 %) је навео да процена ризика обухватаидентификацију, анализу, оцену ризика од природних непогода, техничко-технолошких удеса, терористичких напада, НХБ удеса на одређеном подручју.

Питање18: Који би се критеријуми, по Вашем мишљењу, могли користити за оцену степена ефикасности јединица за отклањање последица ванредне ситуације?

Одговор: Добијенирезултати су приказани у табели 13.

Табела 13. Критеријуми за оцену степена ефикасности јединица за отклањање последица ванредне ситуације

Р.бр.	Процена ризика у установи	Број лица	Проценат (%)
1.	Ефективност	23	24,5
2.	Економичност	11	11,7
3.	Координација	49	52,1
4.	Опремљеност	70	74,5
5.	Покретљивост	43	45,7
6.	Обученост	83	88,3
7.	Ефикасност	47	50

Питање 19: Наведите нека од Ваших искустава везаних за послове заштите и спасавање, тј. отклањања последица ванредне ситуације:

Одговор: Анкетирана лица су навела неколико карактеристичних примера, који се односе на спашавање лица из пожаром захваћених објеката, лица страдалих у поплавама у Републици Србији и неким техничко-технолошким несрећама.

Питање 20: Каква је образовна структура стручно-оперативног органа у коме сте радно (стручно) ангажовани?

Одговор:Највећи број испитаника (76 %) је констатовао да у институцијама у којима су запослени има подједнак број запослених лица са високом, вишом и средњом стручном спремом.

Питање 21:Колико је искуство Вашег стручно-оперативног органа у управљању ванредним ситуацијама?

Одговор:Највећи број испитаника је рекао да у свом саставу велики део лица поседује зависно радно искуство на овим пословима.

Питање 22:Каква је стручна оспособљеност чланова Вашег стручно-оперативног органа из области цивилне заштите?

Одговор:Највећи број испитаника је констатовао да стручно-оперативни органи који реализују активности из домена цивилне заштите поседује

задовољавајућу оспособљеност за обављање свих послова. Највећи број одговорних лица поседује одговарајуће дипломе, сертификате о завршеним курсевима/усавршавању.

Питање 23:Да ли су чланови Вашег стручно-оперативног органа образовани и обучавани за област одбране од ванредних ситуација?

Одговор: Добијенирезултати су приказани у табели 14.

Табела 14. Обученост стручно-оперативних органа

Р.бр.	Обученост стручно-оперативних органа	Број лица	Проценат (%)
1.	Да	60	63,8
2.	Не	18	19,1
3.	Не могу да проценим	16	17,1

Питање 24:Да ли се постојећим плановима предвиђа отклањање последица терористичких аката?

Одговор: Добијенирезултати су приказани у табели 15.

Табела 15. Планови отклањања последица терористичких аката

Р.бр.	Отклањање последица терористичких аката	Број лица	Проценат (%)
1.	Да	31	32,9
2.	Не	13	13,9
3.	Не могу да проценим	50	53,2

Питање 25: Да ли постојећи субјекти (нпр. Војска, Сектор за ванредне ситуације МУП, јавне службе) поседују адекватна средства и опрему за отклањање последица терористичких аката насталих конвенционалним оружјем?

Одговор: Добијенирезултати су приказани у табели 16.

Табела 16. Опремљеност за отклањање последица терористичких аката насталих конвенционалним оружјем

Р.бр.	Опремљеност	Број лица	Проценат (%)
1.	Да	25	26,7
2.	Делимично	35	37,2
3.	Не	/	/
4.	Не могу да оценим	34	36,1

Питање26: Да ли наведени субјекти у претходном питању поседују адекватна средства и опрему за отклањање последица терористичких аката насталих нуклеарним, хемијским или биолошким оружјем?

Одговор: Добијенирезултати су приказани у табели 17.

Табела 17. Опремљеност за отклањање последица терористичких аката насталих НХБ оружјем

Р.бр.	Опремљеност за НХБ околности	Број лица	Проценат (%)
1.	Да	9	9,6
2.	Не	9	9,6
3.	Само део адекватних средстава	36	38,3
4.	Не могу да оценим	40	42,5

Питање27: Да ли имате припремљене планове за управљање ванредним ситуацијама?

Одговор: Добијенирезултати су приказани у табели 18.

Табела 18. Поседовање планова за управљање ванредним ситуацијама

Р.бр.	Планови за управљање ванредним ситуацијама	Број лица	Проценат (%)
1.	Да	53	56,4
2.	Не	18	19,1
3.	Не знам	23	24,5

Питање28: Да ли имате посебне планове за управљање у условима испољених терористичких аката?

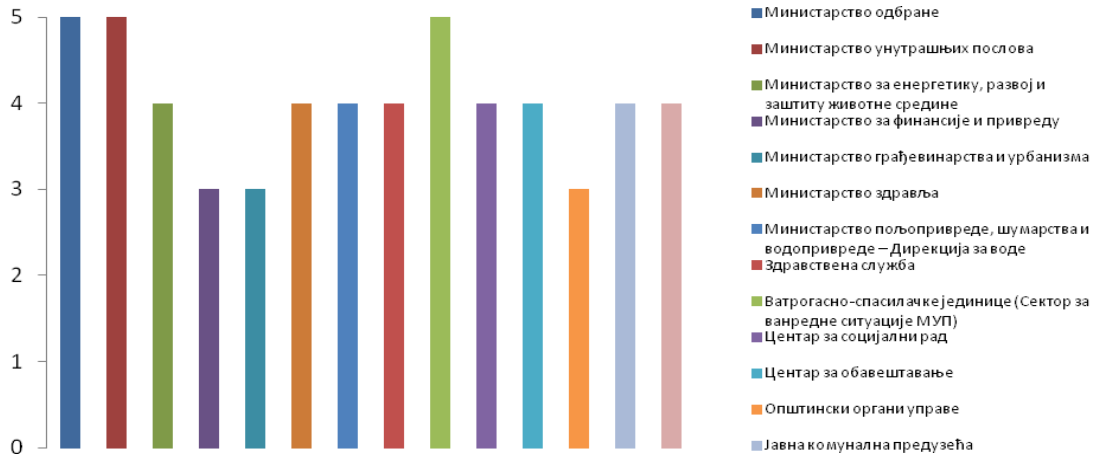
Одговор: Добијенирезултати су приказани у табели 19.

Табела 19. Поседовање планова за одговор на терористички акт

Р.бр.	Планови за управљање ванредним ситуацијама	Број лица	Проценат (%)
1.	Да	18	19,2
2.	Не	35	37,2
3.	Не знам	41	43,6

Питање 29:Оцените досадашњу сарадњу са институцијама у току ванредних ситуација од 1 до 5 (1 - најнижа оцена; 5 - највиша оцена)

Одговор: Резултати су приказани на графикону5.



Графикон5. Оцена сарадње са институцијама РС

Највишом оценом је оцењена сарадња са Министарством одбране, Министарством унутрашњих послова и Сектором за заштиту и спасавање МУП.

Питање 30: Да ли управљање системом интегрисане заштите у отклањању последица напада на критичну инфраструктуру треба да се заснива на (дати одговор)?

Одговор: Добијенирезултати су приказани у табели 20.

Табела 20. Интегрисана заштита КИ

Р.бр.	Интегрисана заштита КИ	Број лица	Проценат (%)
1.	Сопствени модел заштите и спасавања	9	9,6
2.	Страним искуствима у овој области	2	2,1
3.	Комбиновању страних искустава са сопственим	76	80,8
4.	Не знам	7	7,5

Питање31:Да ли се уз добро пројектован систем интегрисане заштите, који би био резултат ангажовања и координације субјеката различитих профила, последице од терористичких аката могу битно умањити?

Одговор: Добијенирезултати су приказани у табели 21.

Табела 21. Пројектовање система интегрисане заштите

Р.бр.	Пројектовање система интегрисане заштите	Број лица	Проценат (%)
1.	Да	74	78,7
2.	Не	3	3,2
3.	Не могу се одредити по овом питању	17	18,1

Питање32: Наведите ко треба да чини окосницу планирања и управљања системом интегрисане заштите?

Одговор: Највећи број испитаника је рекао да то треба бити Министарство унутрашњих послова Републике Србије.

Питање 33: Наведите стручно-оперативни орган који би руководио и спроводио координацију активности на отклањању последица неке ванредне ситуације?

Одговор: Највећи број испитаника је навео да то требају бити Штабови за ванредне ситуације.

Питање 34: Наведите Ваше виђење проблема/потешкоћа везаних за област управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре.

Одговор: Највећи број испитаника је као разлог лошег управљања у овој области навео слабу координацију министарстава и других надлежних органа Републике Србије.

Питање 35: Наведите Ваше сугестије у области управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре о неком питању које није обухваћено овим упитником.

Одговор: Највећи број испитаника је предложио да се унапреди превентивно деловање у области заштите и спасавања, да се унапреди планско деловање снага за интервенцију, уведе обавезна обука омладине у школама и обезбедити већа финансијска средства за јачање целокупног система.

6.1. ДИСКУСИЈА РЕЗУЛТАТА ИСТРАЖИВАЊА

Резултати емпиријских истраживања јасно указују да је стање у погледу функционисања и заштите критичне инфраструктуре у Републици Србији незадовољавајуће. Свеобухватна анализа презентираних резултата истраживања истиче следеће проблеме у први план.

Област заштите критичних инфраструктура је још увек законски неуређена, те је првенствено неопходно донети Закон о заштити критичне инфраструктуре чиме би се успоставио нормативни оквир за дефинисање, идентификацију, одређивање и заштиту националне критичне инфраструктуре. Након усвајања Закона о критичној инфраструктури биће потребно усвојити и подзаконска акта која ће обезбедити практична решења и критеријуме за идентификацију критичних инфраструктура и сектора критичне инфраструктуре.

Доношење Закона о заштити критичне инфраструктуре обавеза је Републике Србије у процесу придруживања Европској унији. Акциони план о поглављу 24 за придруживање ЕУ препознаје Министарство унутрашњих послова Републике Србије као носиоца будућег закона. У оквируСектора за ванредне ситуације Републике Србије је тело које је дужно да координира активности на успостављању међуресорне радне групе која ће имати за циљ дефинисање националне политике у области заштите критичне инфраструктуре.

Испитаници су истакли да у будући Закон о заштити критичне инфраструктуре треба преузети одредбе задржане у Директиви ЕУ о заштити критичних инфраструктура (Direktiva 2008/114/EC). У том смислу, неопходно је извршити измене и допуне Стратегије заштите и спасавања у ванредним ситуацијама и Закона о ванредним ситуацијама у делу који би се односио на област заштите критичне инфраструктуре. Такође, у постојеће референтне законе и подзаконска акта треба укључити нови термин „критична инфраструктура“ и ускладити их са Законом о заштити критичних инфраструктура када буде ступио на снагу.

Испитаници су велики значај указали на ризике којима су изложени критични инфраструктурни системи, превенцију и процену ризика критичних инфраструктура. То је сасвим оправдано ако се зна да отпорност критичне инфраструктуре означава способност система да настави извршавање критичних функција неопходних за испуњавање своје мисије у случају ванредних ситуација.

Незадовољавајуће стање је показано и у делу који се односи на планске активности и међуресорну сарадњу. Стога је неопходно у наредном периоду успоставити одговарајући систем јасног дефинисања надлежности и одговорности у области заштите критичне инфраструктуре. Поред тога, веома значајним се чини и успостављање адекватног система јавно-приватног партнерства и поверења између свих актера у области заштите критичне инфраструктуре.

Анализом резултата истраживања може се закључити да су испитаници изразили позитивне ставове о квалитету људских ресурса, а да су оцене о квалитету материјалних и финансијских ресурса незадовољавајуће. Када су у питању људски ресурси оцене су доста високе, међутим, оне се морају узети са резервом јер сви ти кадрови нису уско специјализирани за област заштите критичне инфраструктуре, већ су им ти послови придодати у склопу својих редовних активности. Такво стање захтева јачање квалитета људских ресурса и прилагођавање система образовања будућих стручњака за област заштите критичне инфраструктуре у Републици Србији. Ограниченост финансијских ресурса је потенцирано од стране испитаника, и тај моменат може бити значајан фактор за нормалан развој система заштите критичне инфраструктуре.

6.2. КОМПАРАТИВНА АНАЛИЗА РЕЗУЛТАТА ДРУГИХ ИСТРАЖИВАЊА

Истовремено када је реализовано емпиријско истраживање за потребе ове докторске дисертације извршено је емпиријско истраживање у оквиру међународног пројекта у RECIPE (Отпорност заштите критичне инфраструктуре у Европи) којим је обухваћена Република Србија и три

суседне земље региона (Босна и Херцеговина, Црна Гора и Македонија).[168] Циљ истраживања био је да се идентификују нормативно-правни аспекти организације заштите критичне инфраструктуре и најзначајнији практични проблеми у овој области.

Истраживање је реализовано путем анкетног упитника у којем су питања била сврстана у неколико целина.

- законодавство и пракса заштите критичне инфраструктуре Републике Србије;
- процена рањивости и идентификација претњи критичне инфраструктуре Републике Србије;
- применљивост постојећих метода и анализа за процену ризика критичне инфраструктуре;
- анализа међузависности критичних инфраструктура у Републици Србији;
- успостављање процедуралних стратегија за унапређење сарадње и комуникације између националних субјеката (државни сектор, приватни сектор и научна заједница).

Националне институције које су доставиле попуњен анкетни упитник су:

- Министарство рударства и енергетике (Сектор за електроенергетику, Сектор за нафту и гас, Сектор за геологију и рударство);
- Министарство грађевине, саобраћаја и инфраструктуре (Сектор за водни саобраћај и безбедност пловидбе, Сектор за железнице и интермодални транспорт;
- Министарство пољопривреде и заштите животне средине (Сектор за планирање и управљање у животној средини - Одсек за заштиту од великог хемијског удеса);
- Министарство унутрашњих послова (Сектор за ванредне ситуације) и
- Институт за јавно здравље Србије „Батут“.

[168] *Резултати ових истраживања су јавно саопштени од стране истраживачког тима Факултета безбедности Универзитета у Београду на панел дискусији одржаној 16. и 17.06.2015. године у Институту за међународну политику и привреду у Београду.*

Резултати који су саопштени на овом скупу јасно су указали на све проблеме који су идентификовани емпиријским истраживањем спроведеним за потребе ове докторске дисертације.

У теоријским и у емпиријским истраживањима се дошло до закључка да у Републици Србији не постоји јасна дефинисана политика заштите критичне инфраструктуре. То потврђују и резултати овог истраживања где је на питање *„Да ли у вашем Министарству/Сектору постоји политика заштите критичне инфраструктуре?*“ негативан одговор дао највећи број испитаника (n=8 или 88,8 %). Исти резултати су добијени и на питање *„Да ли постоји нормативно обавезан регулисан државни надзор заштите критичне инфраструктуре у вашем Министарству*/Сектору?“ (n=8 или 88,8 %). Сви испитаници су одговорили *да национална законска регулатива у области заштите критичне инфраструктуре није усклађена са нормама ЕУ (Директивом ЕК) у заштити критичне инфраструктуре.*

На питање *„Да ли је ваше Министарство/Сектор именовало тело за координацију активности спровођења политике заштите националне критичне инфраструктур*е?“ негативан одговор је дала већина испитаника (n=7 или 77,7%). Исти резултати су добијени у одговору на питање *„Да ли је њихово министарство/сектор на националном нивоу успоставио платформу или мрежу заинтересованих страна за заштиту критичне инфраструктуре*?“ (n=7 или 77,7 %). Посебним се чине значајан податак који је добијен, а односи се на то, где је највећи број испитаника дао одговор *да њихово Министарство/Сектор није идентификовало претње и ризике за критичне инфраструктуре.* Такође, већина испитаника дала је негативан одговор на питање: *„Да ли су у вашем министарству/сектору извршене анализе рањивости и ризика за критичну инфраструктуру?“* Највећи број испитаника (n=6 или 66,6 %) је одговорио *да у процесу менаџмента, сваки сектор критичне инфраструктуре није прихватио приступ заснован на „свим претњама“ и није развио планове специфичне за одређени сектор*. На питање *„Да ли Ваше Министарство/Сектор сарађује са другим институцијама у циљу развијања модела и методологије за управљање ризиком у критичној*

инфраструктури?“, пет испитаника је дало одговора да, док су четири испитаника дала одговор не.

Да у оквиру Министарства/Сектора не постоје смернице, тј. директиве или приручници за евалуацију заштите критичне инфраструктуре, већина испитаника је одговорила негативно (n = 8 или 88,8 %). Негативан одговор је добијен и на питање *да ли је управљање ризиком део пословне стратегије правних лица, односно власника и оператера инфраструктура који је у надлежности вашег министарства.* Негативан одговор на питање: *„Да ли је управљање континуитетом пословања до пословне стратегије правних лица, односно власника процеса у критичној инфраструктури која је у надлежности вашег министарства/сектора?“* дала је већина испитаника (n=5 или 55,5 %). Такође, негативан одговор на питање: *„Да ли у критичној инфраструктури која је у надлежности вашег Министарства/Сектора јавни и приватни сектор сарађују у управљању ризиком?“,* дало је 5 испитаника (55,5 %). Исти резултат добијен је и у одговору на питање да ли је безбедносна политика власника критичних инфраструктура усклађена са законском регулативом у области заштите критичних инфраструктура.

Презентирани резултати поменутог истраживања, су само део комплетног истраживачког опуса проведеног у оквиру наведеног истраживачког пројекта и који су значајни за компарацију са резултатима емпиријског истраживања у докторској дисертацији. Компаративном анализом, јасно се може закључити да стање у области заштите критичне инфраструктуре у Републици Србији је незадовољавајуће скоро у свим сегментима.

Имајући у виду наведене проблеме јасно је да се Република Србија у погледу идентификације, приоритизације, заштите, отпорности и правне регулативе налази на самом почетку. Уочени проблеми и изазови у области заштите критичне инфраструктуре, свакако неће се завршити доношењем новог закона.

Идентификација сектора критичних инфраструктура, идентификација и приоритизација објеката критичне инфраструктуре, усвајање методологије

за процену ризика критичне инфраструктуре, јавно-приватно партнерство и поверење у заштити критичне инфраструктре, међуресорна сарадња и размена осетљивих информација, као и евентуално успостављање Националног центра за критичне инфраструктуре, главни су, али и не једини изазови који би допринели ефикасном функционисању критичних инфраструктура у условима ванредних ситуација.

Ови изазови се могу превазићи доношењем подзаконских аката, хармонизацијом других релевантних закона (Закона о ванредним ситуацијама, Закона о одбрани, Закона о планирању и изградњи, Закона о јавно-приватном партнерству и сл.), затим едукацијом и подизањем свести власника и оператера критичних инфраструктура, усвајањем и применом међународних стандарда и чвршћом сарадњом са академским институцијама.

7. ПРЕДЛОГ КРИТИЧНИХ СЕКТОРА У РЕПУБЛИЦИ СРБИЈИ

Критична инфраструктура је релативно нов појам у Србији, будући да се као термин први пут помиње тек 2011. године у Уредби о садржају и начину израде плана заштите и спасавања у ванредним ситуацијама.[169] Наиме, Уредба у члану 8. истиче процену критичне инфраструктуре са гледишта елементарних непогода и других већих несрећа, али не пружа тумачење дефиниције овог појма.

Такође, Упутством о методологији за израду процене угрожености и планова заштите и спасавања утврђују се критеријуми за процену десет сектора критичних инфраструктура са становишта њихове угрожености од елементарних непогода и других несрећа. Иако методологија садржи најсвеобухватнији приступ у заштити критичних инфраструктура у домаћем законодавству, он је оријентисан на идентификовање извора опасности и последица које поремећаји и прекид у функционисању инфраструктура има по економију и екологију. Приступ садржан у методологији не обухвата процену рањивости и отпорности критичних инфраструктура на све врсте претњи, као и мере повећања отпорности које треба да умање штетне последице елементарних и других несрећа на саме инфраструктуре, укључујући и ефекте међузависности. Посебно се указује потреба да се развију модели и методе за подизање отпорности система критичних инфраструктура у циљу унапређења капацитета којима се амортизују ефекти претњи на штићене вредности. Из наведеног разлога, потребно је дефинисати критеријуме заидентификацију потенцијалних претњи, тј. опасности и генерисање опасности и међузависности прилагођене различитим секторима критичних инфраструктура у складу са међународним, европским и националним стандардима.

Дакле, област ЗКИ је још увек законски неуређена, те је првенствено неопходно донети Закон о заштити критичне инфраструктуре, чиме би се успоставио нормативни оквир за дефинисање, идентификацију, одређивање

[169] „Службени гласник РС“, бр. 8/2011.

и заштиту националне и европске критичне инфраструктуре. Након усвајања Закона о КИ биће потребно усвојити и подзаконска акта која ће обезбедити практична решења и критеријуме за идентификацију КИ и сектора КИ.

Закон о приватном обезбеђењу („Службени гласник РС“, бр. 104/2013), у члановима 4 и 5 дефинише појам „обавезно обезбеђених објеката“, као „објеката од стратешког значаја за Републику Србију и њене грађане, као и објеката од посебног значаја, чијим оштећењем или уништењем би могле наступити теже последице по живот или здравље људи или који су од интереса за одбрану земље“.

Такође, под обавезно обезбеђеним објектима подразумева се и простор на коме се они налазе, као и пратећи објекти. Поред ова два закона, други најважнији закони и стратешки документи којима се директно и индиректно штити КИ су: Закон о ванредним ситуацијама („Службени гласник РС“, бр. 111/2009), Национална стратегија заштите и спасавања у ванредним ситуацијама, („Службени гласник РС“, бр. 86/2011), Закон о заштити животне средине („Службени гласник РС“, бр. 135/2004, 36/2009, 36/2009 - др. закон, 72/2009 - др. закони 43/2011 - одлука УС), Закон о тајности података („Службени гласник РС“, бр. 104/2009), Закон о планирању и изградњи („Службени гласник РС“, бр. 72/2009), Закон о водама („Службени гласник РС“ бр. 30/10 , 93/12) и други релевантни документи.

Као следеће кораке потребно је извршити приоритизацију идентификоване КИ, а затим регулисати оне аспекте заштите критичне инфраструктуре који су се у досадашњој европској и глобалној пракси показали као нарочито проблематични, а то су јавно-приватно партнерство и размена осетљивих информација.

Анализом међународних искустава у области идентификовања и заштите критичне инфраструктуре утврђено је да дефиниција критичне инфраструктуре и њен садржај не могу бити идентични у свакој држави понаособ, па је логично да се та дефиниција и садржај морају утврдити на националном нивоу, што важи и за Републику Србију.

Да бисмо били сигурни на који садржај појма КИ се ослањамо и које су његове оквирне границе, потребно је донети Закон о заштити критичне инфраструктуре, чиме би се успоставио нормативни оквир за дефинисање, идентификацију, одређивање и заштитунационалне и европске критичне инфраструктуре; као и подзаконских аката који ће обезбедити практична решења и критеријуме за идентификацију КИ. Доношење Закона о ЗКИ обавеза је Републике Србије у процесу придруживања Европској унији. Акциони план о поглављу 24 за придруживање ЕУ препознаје Министарство унутрашњих послова Републике Србије као носиоца будуће гзакона. У оквиру МУП, Сектор за ванредне ситуације Републике Србије је тело које је дужно да координира активности на успостављању међуресорне радне групе која ће имати за циљ дефинисање националне политике у области заштите критичне инфраструктуре.

У будући Закон о ЗКИ, али и у друге законе релевантне за ЗКИ треба преузети одредбе садржане у Директиви ЕУ о заштити критичних инфраструктура. У том смислу, неопходно је извршити измене и допуне Стратегије заштите и спасавања у ванредним ситуацијама и Закона о ванредним ситуацијама у делу који би се односио на област ЗКИ. Ради ефикасне заштите критичне инфраструктуре и свеобухватног правног регулисања ове области биће потребно имплементирати постојећи Закон о тајности података, који по мишљењу стручњака, постоји само на папиру. Затим, треба коначно донети Закон о информационој безбедности (на чијем се нацрту ради већ више од три године), Уредбе о криптозаштити, као и Стратегије сајбер-безбедности.

Приликом идентификације критичних инфраструктура и сектора критичних инфраструктура пожељно би било кренути од међународног, у најмању руку од регионалног нивоа. Иако један број развијених земаља идентификује преко десет сектора (укључујући Републику Хрватску, која је идентификовала једанаест сектора) треба бити реалистичан и не правити превише детаљан попис објеката услед ограничености буџета, који се услед тога не би могли заштитити на оптималан начин. У наредном кораку,

практично би било идентификовати КИ на различитим нивоима, осим регионалног и националног. КИ се могу идентификовати и на градском, локалном, па и на секторском нивоу. Прелиминарну идентификацију и класификацију КИ могуће је урадити и без важећих законских аката, уколико се дефинишу критеријуми и ресорне секторске анализе.

Издвајањем оних инфраструктура које се појављују у скоро свим земљама са дефинисаном политиком заштите критичне инфраструктуре добија се следећи предлог ширег списка критичних инфраструктура у Србији:

- Енергетика (производња, пренос дистрибуција и складиштење енергената (гаса и нафте) и електричне енергије),
- Информационе, дигиталне и комуникационе технологије (електронска комуникација, пренос података, информациони системи, пружање аудио и мултимедијалних услуга),
- Транспорт (друмски, железнички, ваздушни, водни),
- Здравство (болнице, производња лекова),
- Воде (снабдевање пијаћом водом, бране, обрада отпадних вода, заштита вода),
- Храна (производња, снабдевање храном, безбедност хране, робне залихе),
- Финансије (банкарство, инвестиције, системи осигурања и плаћања) и
- Јавне службе (очување јавног реда и мира, заштита и спасавање, хитна медицинска помоћ).

Различита министарства, сектори и ресори поседују засебне критеријуме и класификације објеката под њиховом ингеренцијом. Закон о одбрани даје дефиницију објеката од посебног значаја за одбрану, за које се сматрају: велики техничко-технолошки системи, објекти у којима се производе, складиште или чувају предмети или врше услуге за потребе одбране, објекти у којима су смештени државни органи и правна лица од посебног значаја за одбрану земље, као и одређени инфраструктурни објекти. У Плану одбране донетом крајем 2013. године наведено је на стотине техничко-технолошких система, и за све њих постоје планови одбране, а Упутство о изради планова одбране 2013. године даје методологију на основу које су ти техничко-

технолошки системи идентификовани.

Стога је могуће да се будући планови заштите критичних инфраструктура уврсте у планове одбране. Поред закона и планова одбране за будућу идентификацију и класификацију КИ у Србији релевантна су и следећа подзаконска акта:

- 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 и 35/2015),
- Одлука о одређивању производа и услуга од посебног значаја за одбрану Републике Србије („Службени гласник РС“, бр. 58/2008) и
- Одлука о врстама инвестиционих објеката и просторних и урбанистичких планова значајних за одбрану земље („Службени гласник СРЈ“, бр. 39/95).

Наведена документа пре свега помињу одбрамбену (наменску) индустрију Србије, али и друге индустријске и инфраструктурне објекте који за време ратног или ванредног стања, као и при мобилизацији Војске Србије првенствено врше услуге које утврди Министарство одбране.

Република Србија у односу на земље из непосредног окружења ужива доста висок степен безбедности у релативно нестабилном регионалном и међународном окружењу. Стога се систем кризног менаџмента у функцији заштите КИ земаља из непосредног окружења (БиХ, Црна Гора, БЈР Македонија и Албанија) није могао узети као референтни оквир за избор и предлагање модела заштите КИ у Републици Србији.

С друге стране, Бугарска и Словенија су, због просторно-географских, политичких, друштвено-економских и културолошких сличности, као и у погледу доношења и спровођења политике заштите КИ, добра референтна тачка за извлачење поука из искустава која би се могла применити у Републице Србији.

Словенија и Бугарска су извршиле истраживање критичних инфраструктура

уз непосредну стручну и материјалну помоћ Шведске. Истраживања су обавиле владине координационе групе за заштиту КИ заједно са свим релевантним министарствима и уз примену критеријума међусекторске анализе, са циљем идентификације најважнијих критичних инфраструктурних сектора, њихових функција и задатака, као и дефинисања организација, агенција и других државних и приватних удружења која су одговорна за функционисање и заштиту КИ.

Следећи поменуту добру праксу, Републике Србија би свој систем кризног менаџмента и заштите КИ могла да осмисли и примени у складу са досадашњим искуствима Словеније и Бугарске. Тим пре, што се Република Србија, исто као и Републике Словенија и Бугарска, налази на раскршћу неколико важних коридора друмског, железничког, водног и ваздушног саобраћаја, а инфраструктура информационих и комуникационих технологија и енергетике још увек нису саставни део европске инфраструктуре.

Готови модели Словеније и Бугарски се, са друге стране, не могу преузети и имплементирати у Републици Србији без одређених модификација, јер свака држава има своје специфичне особености. Објекти критичне инфраструктуре асиметрично су дистрибуирани у оквиру Словеније - критичне инфраструктуре у већој мери су смештене у урбаним срединама.

Посебно су критичне мулти-инфраструктурне области, тј. области у којима је лоциран већи број различитих типова инфраструктура. Ометање нормалног функционисања једног типа инфраструктуре у оваквим областима брзо би посредно утицало и на функционисање других инфраструктура у тој области.

У Републици Србији су, пак, објекти критичне инфраструктуре равномерно дистрибуирани на целој територији државе (по чему је наша земља слична Бугарској). Осим тога, Република Србија нема нуклеарну инфраструктуру какву поседују Словенија и Бугарска (Кршко и Козлодуј).

7.1. АНАЛИЗА ПРОБЛЕМА И ПРЕДЛОГ ЗА МОДИФИКАЦИЈУ ИЗАБРАНИХ МОДЕЛА

Док су многе развијене државе идентификовале своје критичне инфраструктуреу Републици Србији и региону се о овој теми мало дискутовало.[170] Мисао о кризама, посебно на нашим просторима, је још увек на зачетку, а практично поступање у кризним ситуацијама је на граници неосмишљеног и *ad hoc* реаговања. По мишљењу неких теоретичара личи на инстинктивну реакцију. Практичари у разним областима, почевши од политике, економије до заштите животне средине, и на различитим нивоима, од државног преко регионалног до локалног, на кризе најчешће одговарају реактивно, ситуацијски и исхитрено, без стратешке визије и било каквог краткорочног или дугорочног плана.[171] Потреба динамичког, проактивног и стратешког приступа нарочито је неопходна у процесу планирања заштите критичне инфраструктуре у условима различитих типова кризних и ванредних ситуација.

Систем за управљање ванредним ситуацијама постављен је тако да сваки ниво политичко територијалне организације има одговорност и за припрему и за одговор на ванредне ситуације у оквиру свог уставног и законског мандата и оперативних капацитета. Локални ниво има више оперативну улогу, регионални ниво је нека врста медијатора[172] од локалног нивоа ка покрајинској односно републичкој влади. Улога националног/државног нивоа је пре свега бављење стратегијом и укупним дизајнирањем система, као и координација, мониторинг и исправљање грешака и пропуста у функционисању система.[173]

Према Закону о ванредним ситуацијама Република Србија обезбеђује

---

[170]*Кљаић, З., Примена ИКТ у управљању критичном инфраструктуром у транзицијским земљама, ТЕЛФОР, Београд, 2010.*

[171]*Funda, D., Majić, T., Upravljanje krizom, International Conference "Crisis Management Days", Velika Gorica, 2011.*

[172]*Улога региона у управљању ванредним ситуацијама није у потпуности јасно дефинисана у Закону о ванредним ситуацијама.*

[173]*Kešetović, Ž., Country study Serbia, report within ANVIL project - European Union's 7th Framework Programme FP7/2007-2013 under grant agreement N°28467, 2013.*

изградњу јединственог система заштите и спасавања у складу са овим законом и другим прописима, као и програмима, плановима и другим документима који се односе на заштиту и спасавање и цивилну заштиту, Народна скупштина усваја Националну стратегију заштите и спасавања у ванредним ситуацијама док је Влада одговорна за све аспекте система за управљање кризним ситуацијама (усвајање планова, процене угрожености и других докумената, наређивање опште мобилизације јединица ЦЗ, надзор над припремама за ванредне ситуације итд.).

У погледу мера заштите критичне инфраструктуре, све државе, укључујући и Републику Србију, морају да утврде и редослед поступака: а) идентификацију критичне инфраструктуре, б) израда мапа критичне инфраструктуре, ц) размена информација, д) оспособљавање особља ангажованог на пословима и задацима у системима критичне инфраструктуре, е) увежбавање система за заштиту критичне инфраструктуре или опоравак у случају кризне или ванредне ситуације.[174]

Област ванредних ситуација свеобухватно је уређена Законом, који је матични за ту област. Поједина питања од значаја за област ванредних ситуација (безбедносна, еколошка и др) уређена су и посебним законима. На пример, одредбама чл. 15 и 57. Закона о полицији[175] утврђене су посебне мере значајне за заштиту здравља и живота људи и за спречавање угрожавања безбедности изазваног елементарним непогодама или епидемијама. Те мере своде се на овлашћење државе да у изузетним случајевима, попут катастрофе 2014. године, ограничи или забрани кретање на одређеним подручјима, забрани настањивање на одређеном подручју, наложи евакуацију - напуштање одређеног подручја или објекта. И у целини посматрано, наведена и слична овлашћења државних и других органа пружају могућност за адекватно супротстављање катастрофи до које је дошло услед незапамћених поплава 2014. године.

Нема сумње да ће сепитањима адекватних мера непосредно пре, за време и

[174]*Национална стратегија заштите и спречавања у ванредним ситуацијама (Усвојена на седници Скупштине РС 18.11.2011.).*
[175]*„Службени гласник РС“, бр. 101/2005, 63/2009 - одлука УС и 92/2011.*

после катастрофе, многе струке и науке, још дуго бавити и по изучавању ових катастрофалних поплава извести бројне закључке. Било би добро да ти закључци у далеко већој мери послуже будућности и превенцији (предвиђању) него да се по традиционалном приступу ограниче само на објашњење протеклих догађаја и већ установљених феномена.

Доношење једног броја од недостајућих прописа условљено је и претходним стварањем потребних материјалних и других услова за њихову примену, што се може закључити из још увек актуелног приказа стања из области ванредних ситуација, садржаног у „Националној стратегији заштите и спасавања у ванредним ситуацијама“.[176] Према том приказу, а и практично, указује се да је неопходно „веће техничко иновирање и опремање, као и унапређење инфраструктурног, информационог и технолошког система уз примену савремених технологија и стандарда Европске уније“. Ваља нагласити да су у овој стратегији и други недостаци постојећег система заштите и спасавања објективно препознати, а нарочито и то да су стратешки циљеви добро постављени. Требало би убрзати њихово остваривање.

Размере катастрофе која је 2014. године задесила Републику Србију захтевају да се узме у обзир и чињеница да се еколошка ситуација на планети Земљи погоршава. Због те чињенице политика је прихватила екологију и настала је еколошка политика, која се развија у многим државама. Два принципа заступљена су у тој политици, и то принцип *еластичности* који се своди на предузимање акција после настанка проблема и принцип *предострожности* који подразумева да се потенцијалне опасности отклањају одмах, пре прерастања у катастрофу. Велике расправе воде се о предностима и недостацима ових принципа. Према једном мишљењу „оба принципа су за креирање еколошке политике апстрактна, пошто су општи. Кључно питање јесте шта подразумевају када влада треба да донесе конкретне одлуке у различитим сферама. Ако се деси огромна катастрофа да је мало тога могуће урадити да се побољша *ex post* ситуација, онда је принцип еластичности под

[176] *„Службени гласник РС“, бр. 86/2011.*

великом сумњом. С друге стране, за идеју предострожности велики изазов представља дефинисање нивоа ризика за различите људске пројекте који се не може толерисати. Ако се уско тумачи, онда би уклањање свих ризика могло да значи уклањање свих могућности".[177]

Наведени цитат можда неће бити од помоћи онима који „све знају" о узроцима и последицама катастрофалне поплаве у Републици Србији маја 2014. године, али је чињеница да тек предстоји тежи пут да се до правих сазнања дође и да се она у предстојећем периоду искористе за спречавање нових катастрофалних поплава које би могле да угрозе Републику Србију и њене грађане.

У Републици Србији се критична инфраструктура помиње иу оквиру поглавља 6.2. „*Стратегије развоја информационог друштва у Републици Србији до 2020*"[178] кроз констатацију: „Потребно је развијати и унапређивати заштиту од напада применом информационих технологија накритичне инфраструктурне системе, што поред ИКТ система могу бити и други инфраструктурнисистеми којима се управља коришћењем ИКТ, попут електроенергетског система. У вези са тим је потребно додатно уредити критеријуме за утврђивање критичне инфраструктуре састановишта информационе безбедности, критеријуме за карактеризацију напада примениоминформационих технологија на такву инфраструктуру у односу на класичне облике напада,као и услове заштите у овој области".

Документи који би требало да обрађују питања КИ, сем самог Закона о заштити критичне инфраструктуре, су *Национална стратегија заштите и спасавања у ванредним ситуацијама* и Закон о ванредним ситуацијама. Друга два документа јесу усвојена, међутим, у њима се ни не помиње критична инфраструктура, барем не постоји као термин, мада се закони по својој природи баве питањима који су везани за заштиту КИ.

Треба нагласити да институционални оквири за дефинисање КИ постоје, а то

[177]*Lane, J.E., Државно управљање, разматрање модела јавне управе и јавног управљања, Београд, стр. 173, 2012.*
[178]*Влада Републике Србије, „Стратегија развоја информационог друштва у Републици Србији до 2020", 2010.*

су постојање Сектора за ванредне ситуације, надлежних министарстава као и надлежних регулаторних тела. Одређене мере заштите делова инфраструктуре су предузете од стране оператера, али нису донете нистратегија, нити политика заштите на нивоу земље.

Потреба разматрања КИ препозната је у оквиру пројекта „Управљање критичном инфраструктуром за одрживи развој у поштанском, комуникационом и железничком сектору Републике Србије“. Основни циљ пројекта је идентификација критичних инфраструктурних система чија је ефикасност кључна за неометан развој економије и друштва.

7.2. СЕКТОРИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ У РЕПУБЛИЦИ СРБИЈИ

Пошто у Републици Србији још увек не постоји закон о критичним инфраструктурама и оне нису јасно дефинисане може се предложити модел заснован напостојећим поделама критичних инфраструктура у суседним земљама, у складу са просторно-географским, привредним, економским и демографским карактеристикама. Издвајањем оних инфраструктура које се појављују у Бугарској и Словенији, земљама са дефинисаном политиком заштите критичне инфраструктуре, добија се следећи предлог критичних инфраструктура у Републици Србији.

Наравно, ово је само предлог заснован на искуствима других држава. Да би се са сигурношћу оформила листа критичних инфраструктура неопходно је да се, на основу једног од модела који су претходноописани, кроз сарадњу са свим релевантним секторима и институцијама (приватним и државним) утврди степен критичности сваке инфраструктуре, па након тога оформи и коначна листа критичних инфраструктура.

Енергетску привреду Републике Србије[179] у најширем смислу сачињавају нафтна и гасна привреда, рудници угља, електроенергетика и децентрализовани системи градских топлана и индустријске енергетике.

У оквиру енергетског система обавља се експлоатација домаће примарне

[179] *Егзактни подаци преузети су из Стратегије за развој енергетике Републике Србије до 2015.*

енергије, увоз примарне енергије (пре свега нафте и природног гаса), производња електричне и топлотне енергије, експлоатација и секундарна прерада угља, као и транспорт и дистрибуција енергије и енергената до крајњих потрошача финалне енергије. Према већ наведеном, енергетску привреду Републике Србије у најширем смислу чине:[180]

Сектор нафте у оквиру којег се врши експлоатација домаћих резерви нафте, обавља увоз, транспорт и прерада сирове нафте и нафтних деривата, као и дистрибуција и продаја/извоз деривата нафте. У области домаћег истражног и екплоатационог простора нафте и гаса присутан је стални пад производње који је последица малог нивоа улагања у одржавање постојеће производње, као и малог интензитета истражних радова због недостатка сопствених средстава. Транспорт нафте се доминантно врши магистралним нафтоводом (Јанаф) од Омишља у Хрватској до рафинерија нафте у Панчеву и Новом Саду. Укупни инсталисани прерађивачки капацитет домаћих рафинерија износи 7,8 милиона тона годишње (4,8 милиона тона у Панчеву и 3 милиона тона у Новом Саду).

Сектор природног гаса у оквиру кога се осим увоза гаса, обавља експлоатација домаћих резерви природног гаса, њихова примарна прерада, сакупљање, транспорт и дистрибуција до крајњих потрошача гаса. На главни магистрални гасовод, укупне дужине око 400 km, који се простире од границе Мађарске до Ниша, повезан је већи број дистрибутивних мрежа преко којих се врши снабдевање потрошача природним гасом. Велика већина ових мрежа изграђена је на територији Војводине.

Сектор угља у оквиру којег се врши експлоатација и прерада угља из рудника са површинском експлоатацијом у три рударска басена: Колубарски, Костолачки и Косовско-Метохијски, који не функционише у саставу енергетског система Републике Србије. Преко 95 % укупне производње угља на површинским коповима користи се за производњу електричне енергије. За финалну потрошњу користи се угаљ из осам рудника са подземном експлоатацијом, у којима се врши експлоатација каменог и мрког угља, као и

[180] *Ibid.*

знатно квалитетнијег лигнита (у односу на лигните из рудника са површинском експлоатацијом угља).

Електроенергетски сектор сачињавају објекти/системи:

- Електроенергетски извори, у које спадају електране (термоелектране на лигнит, термоелектране на мазут и природни гас),
- Системи за пренос електричне енергије, са око 10.200 km далековода и са трафостаницама, преко кога се врши пренос електричне енергије произведене у земљи и обавља размена са суседним системима,
- Електродистрибутивни системи, лоцирани у потрошачким центрима преко којих се врши испорука електричне енергије крајњим потрошачима у секторима потрошње енергије.

Систем градских топлана постоји у 45 градова Републике Србије, чине га децентрализовани топлотни извори и одговарајуће дистрибутивне мреже. Систем се користи за загревање стамбеног и пословног простора, обима од око 450.000 еквивалентних станова (површине 66 m^2).

Основна карактеристика свих наведених делова енергетског система је у великом броју случајева технолошка застарелост и ниска енергетска ефикасност, као и тренутно забрињавајуће и дугорочно неприхватљиво технолошко стање са становишта заштите животне средине.

Сектор информационе и комуникационе технологије, односно ИКТ сектор чине *предузећа којима су ИКТ доминантна делатност* и која су по својој структури претежно мала и средња приватна предузећа. Ту су информациони центри у великим привредним системима са израженом развојном функцијом у области информационо комуникационих технологија. У прошлости су управо ти велики информациони центри у великим системима били ослонац информатизације у Републици Србији. Касније, у процесу транзиције дошло је до стварања низа других малих и средњих приватних предузећа у тој области.

Битан елемент ИКТ сектора су и *универзитети и институти, као и научно-истраживачки центри*, *технолошки паркови и инкубатори* итд. који

представљају спој универзитета и имплементације у привреди.

Оно што је упечатљиво јесте да је број предузећа, претежно приватних, која се баве софтверским услугама врло велик, што на неки начин разбија уобичајено мишљење о стању ИКТ у Републици Србији. Подаци потписани и уговор о сарадњи са Мајкрософтом, и низ договора са представницима компанија *Cisco*, *IBM*, *Hewlett Packard*, *Oracle*, *Apple* и *Google Enterprise* показују да је ИКТ врло важан сегмент српске привреде. Битан је развој софтвера, развој рачунарских машина, производња рачунарских машина, систем интеграције и хардвера и софтвера. Наравно, телекомуникације такође играју важну улогу у оквиру ИКТ сектора, као и сви сегменти, подгрупе у области телекомуникационих технологија.

Кад је у питању област увоза и извоза, извоз у ИКТ сектору у Републици Србији наглорасте из године у годину још од 2000. године, што значи даје извозни потенцијал ИКТ сектора огроман. Извештај тржишне анализе кретања ИКТ сектора у Републици Србији, извршене од стране компаније *IDC*, говори о врло високој годишњој стопи раста ИКТ сектора од 18,3 % и пројектованом петогодишњем расту од 16,8 % годишње.[181]

Интересантна је регионална расподела ИТ сектора у Републици Србији. Концентрација ИТ фирми је пре свега у Београду, Војводина је заступљена са 15 % (мада Војводина има јако високу стопу раста броја фирми ИКТ сектора), Ниш - као некада традиционални и основни центар развоја информатике у Републици Србији - заступљен је са 13 %, а остали градови са 16 %.[182] Предности ИКТ сектора у Републици Србији су, пре свега, квалитетни кадровски ресурси који су још увек присутни у Републици Србији, затим висок технолошки ниво, који не заостаје за светским трендовима, висок степен знања и вештина коришћења ИКТ технологија. Чињеница је и да стране компаније сматрају да су српски кадрови креативни, флексибилни и врло пријемчиви за савремене трендове у информационим технологијама. Оно што је јако важно јесте међународна конкурентност индустрије

[181] *http://www.idc.com 10.02.2013.*
[182] *Медаковић, Р., ИТ сектор Привредне коморе Србије, ИКТ индустрија као доминантна привредна грана у Србији, часопис Е-волуција, 2007.*

софтвера: неценовна конкурентност, базирана на квалификованој радној снази, и ценовна конкурентност.

С обзиром на то да у свету више не важи подела на Исток и Запад, него подела на дигитално развијене, односно на информациона друштва и она друга, Република Србија у овом сегменту не заостаје за светом. Развој и примена информационих технологија је у пуној експанзији и ефекти и сви елементи глобализације директно се осликавају и бивају потпомогнути применом информационо-телекомуникационих технологија. У свету је нормално да компјутерски писмени људи имају могућност квалитетнијег запошљавања, тј. постоји потреба коришћења технички високообразованог кадра и радне снаге. Чињеница је да мала почетна инвестициона улагања за разлику од других сектора привреде иницирају појаву нових иновативних фирми старт-ап компанија. Ничу мала предузећа која су флексибилна и која могу да одговоре на захтеве једног фрагментираног и разноврсног тржишта. То је тржиште наменског софтвера и услуга које управо омогућава широк спектар могућности за рад малим фирмама односно компанијама. Такође, светске прилике омогућавају да чак и малим предузећима буду доступна страна тржишта управо коришћењем веза, канала и контаката на међународном тржишту посредством интернета и информационих технологија.

С друге стране, велике и мултинационалне компаније имају другу филозофију, која се заснива на томе да одржавају своју конкурентност и рејтинг на тржишту, користећи се решењима која су врло рестриктивна и квалитетна, али по нижој цени. Да би то постигли, фокусирају се на земље у транзицији, као што је Република Србија,[183] где по релативно нижим ценама могу да *аутсорсују* своју производњу уз постизање жељеног квалитета. Тренутно је у Републици Србији присутан знатан број великих мултинационалних компанија из ИКТ сектора, које врше и значајну улогу

[183]*Пример је поменути уговор који је потписан са Мајкрософтом, као и разговори са водећим светским фирмама из ИКТ сектора:http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:433144-Dacic-u-SAD-sa-predstavnicima-najvecih-svetskih-IT-kompanija 10.02.2013, као и: http://www.novosti.rs/vesti/naslovna/drustvo/aktuelno.290.html:433290-Dacic-Promenjena-slika-o-Srbiji-u-svetu10.02.2013.*

трансфера технологије.

ИКТ тржиште у Републици Србији има тренд раста који се може поредити са било којом земљом у региону. Чињеница је да главно ИКТ тржиште у Републици Србији представљају, односно највећа очекивања су од Владе као и од локалне самоуправе. Затим, ту су *инфраструктурни привредни системи, јавна предузећа, успешни привредни системи, али и мала и средња предузећа* која су оријентисана на савремене пословне моделе пословања.

Саобраћај и транспорт у најширем смислу чине:[184]

Друмски транспорт са укупном дужином путева од око 38.000 km. Мрежа путева у Републици Србији је добро развијена, мада је њен квалитет лош због недостатка инвестиција и недовољног одржавања. На територији Републике Србије се налази 792 km путева Коридора 10 са његовим крацима - 10b и 10c.

Рехабилитација путева започета је 2001. године и процењује се да је за започету реконструкцију мреже потребно још око 600 милиона евра. За рехабилитацију и одржавање мреже државних и локалних путева у наредних десет година биће потребно око 6,2 милијарди евра.[185] Недостатак средстава за модернизацију и одржавање путне мреже уз застарео возни парк утицао је на значајно смањење безбедности саобраћаја на путевима.[186]

Друмски транспорт у Републици Србији представља динамичан и доминантан вид саобраћаја који учествује са око 80 % у укупном обиму превезеног терета, односно са око 74 % у укупном броју превезених путника. Привредни субјекти који обављају друмски транспорт, а који су били у друштвеној својини, углавном су приватизовани и функционишу у условима слободне конкуренције, а улога државних органа је ограничена на уређивање

[184]*Највећи део нумеричких података преузет је са сајта Министарства саобраћаја (http://www.ms.gov.rs, 10.02.2013.) и из званичних докумената (Актуелни Закони о саобраћају и стратегија развоја транспорта до 2015). Међутим, документи се врло често позивају на податке који су још из '90-их година (вероватно јер се од тад није озбиљно радило на модернизацији саобраћајне инфраструктуре) па је под великим знаком питања колико и у којим сегментима су подаци релевантни данас. Ово се посебно односи на водни и на железнички транспорт, делимично на друмски.*

[185]*Стратегија развоја друмског, железничког, водног, ваздушног и интермодалног транспорта у Републици Србији 2008-2015.*

[186]*Ibid.*

ове области у смислу издавања лиценци, дозвола за друмски превоз, надзор итд. Међународни друмски транспорт у Републици Србији, односно приступ међународном транспортном тржишту, већим делом се обавља у режиму квота билатералних и мултилатералних ЦЕМТ дозвола што додатно, у условима постојања значајних административних и физичких препрека (нпр. још увек неоповољан визни режим за професионалне возаче, застоји на граничним прелазима и сл.), има негативан утицај на конкурентност наших превозника на међународном транспортном тржишту.

Управљање мрежом државних путева је претежна делатност Јавног предузећа *Путеви Србије*, док мрежом општинских путева и улица управљају органи јединица локалне самоуправе.

Јавни градски и приградски превоз путника обухвата друмски, железнички и водни превоз. Уређивање јавног градског и приградског превоза путника је у надлежности органа јединице локалне самоуправе.[187]

Јавни превоз путника у градским подручјима је значајно већи у односу на ванградска подручја. Око две трећине путовања обавља се средствима јавног градског и приградског превоза путника док само трећину чине међумесна путовања. Више од трећине становништва Републике Србије живи у шест највећих градских насеља и у њима се реализује око 95 % путовања. Значајније учешће у јавном градском и приградском превозу путника железница има само у Београду (Беовоз).

Железнички трансорт преко магистралне железничке пруге пролази кроз све веће градове и укршта се у зонама Београда и Ниша. Од укупне дужине железничке мреже у Републици Србији (3.809 km), 1.768 km представљају магистралне пруге, а електрифицирано је 1.247 km (32,7 %).

Само 7 % пруга (276 km) има два колосека. Просечно задовољавајућа густина мреже на нивоу Републике Србије веома је неравномерна и опада ка југу.

Недовољно улагање у основно одржавање на железници последица је општег привредног заостатка у претходном периоду, лоше организације, недостатка

[187] *Ibid.*

средстава, социјалне и кадровске политике. Садашње стање железничке инфраструктуре карактерише потреба да се у пројектовано стање врати и модернизује још око 1.000 km магистралних пруга, тј. око 57 % главне мреже пруга, односно 26 % комплетне железничке мреже. За рехабилитацију и одржавање железничке мреже у наредних десет година према проценама биће потребно око 3,9 милијарди евра.

Управљање јавном железничком инфраструктуром, јавни превоз путника и робе и одржавање железничких возних средстава су претежне делатности ЈП *Железнице Србије*.

Дирекција за железнице је образована као посебна организација ради обављања стручних, регулаторних и других послова у области железничког транспорта утврђених Законом о железници.[188]

Водни транспорт. Република Србија има повољне економске и географске карактеристике за теретни, путнички и туристички водни транспорт. Потенцијалирека и канала су значајни, али стање инфраструктуре није задовољавајуће. После 1990. године дошло је до великог застоја у одржавању унутрашњих водних путева и пратеће инфраструктуре.

За рехабилитацију и одржавање система унутрашњег водног транспорта у наредних десет година према проценама биће потребно око 290 милиона евра, а додатних око 220 милиона евра потребно је за развој интермодалног транспорта.

Превоз путника на унутрашњим пловним путевима у Републици Србији има пре свега туристички карактер. Број путника-туриста који на својим речним крстарењима посећују Републику Србију значајно расте сваке године и представљаће основу за развој значајне привредне активности у областима транспорта, туризма, трговине и других услуга.[189]

---

[188] *„Службени гласник РС“, бр. 18/05.*

[189] *Податак је преузет из стратегије развоја транспорта до 2015. године, међутим, оно што противречи логици је чињеница да туризам тешко може да буде „основ за развој значајне привредне активности у областима транспорта, туризма, трговине и других услуга“, већ би могао да буде само основ за развој туризма, док је за прави развој привреде, транспорта и*

Очекује се да ће са обнављањем и повећањем производње у великим индустријским постројењима у Републици Србији (челичане, хемијска индустрија, цемент и нафта) тражња за водним транспортом робе значајније порасти због његових компаративних предности.

Ваздушни транспорт у Републици Србији посматран је у односу на *аеродроме*, *авио-компаније*, *Директорат цивилног ваздухопловства Републике Србије* и *Агенцију за контролу летења.*

Авио-компаније. Јавно предузеће *AIR Serbia*[190] основала је Република Србија, са компанијом *Etihad* из Уједињених арапских емирата, за обављање делатности превоза путника и робе.

Директорат цивилног ваздухопловства државе Србије и државе Црне Горе основан је у октобру 2003. године ради обезбеђивања услова за несметано обављање послова од значаја за остваривање права и дужности у области ваздушног транспорта и примене међународних стандарда и препорука у тој области. Након престанка државне заједнице Србија и Црна Гора, Република Србија је преузела оснивачка права у Директорату и промењен му је назив у Директорат цивилног ваздухопловства Републике Србије.

У току 2005. године Србија је примљена у чланство EUROCONTROL и JAA (*Joint Aviation Authorities*). У току 2006. године потписани су Мултилатерални споразум о успостављању Заједничког европског ваздухопловног подручја и Споразум о одређеним аспектима ваздушног транспорта, тзв. *хоризонтални споразум*.

У циљу развоја и унапређења безбедности ваздушног саобраћаја наставља се интензивна сарадња са међународним организацијама у области цивилног ваздухопловства, тј. са ICAO (*International Civil Aviation Organization*), EUROCONTROL, ECAC (*European Civil Aviation Conference*) и JAA.

трговине неопходан развој лука, опремање лука за руковање контејнерима и карго теретом уопште и развој индустрије.

[190]*Од 08.08.2003. године име националног авиоревозника није акроним од Југословенски аеротранспорт, већ пуно име компаније (назив JAT задржан је тада као бренд): http://www.jat.com/active/sr-latin/home/main_menu/about_us/history.html 10.02.2013.*

Агенција за контролу летења Србије има задатак контроле летења изнад територија Србије у циљу безбедног, редовног и ефикасног одвијања ваздушног транспорта. У оквиру Агенције послују Центар за обуку контролора летења и другог стручног особља, за сопствене потребе као и за потребе других провајдера, и Служба за калибражу која пружа услуге провере исправности рада навигационих уређаја из ваздуха.

Агенција пружа навигацијско, метеоролошко и техничко обезбеђење ваздушног транспорта у ваздушном простору Републике Србије, Републике Црне Горе, 55 % горњег ваздушног простора Босне и Херцеговине, као и међународних вода јужног дела Јадранског мора.

Интермодални транспорт. Поред чињенице да је током деведесетих година интермодални транспорт био у прекиду, постоји делимично изграђена инфраструктура, како на железници - железнички интегрални транспорт, тако и у лукама (луке у Новом Саду, Београду, Панчеву и Прахову) за претовар контејнера. Код постојећих терминала присутна су значајна ограничења условљена постојећом локацијом, застарелом опремом и расположивим инвестицијама за развој. Такође, више пута дефинисана мрежа терминала и стратешки планови развоја нису реализовани.

Комбиновани друмско-железнички транспорт на железници се последњих година постепено обнавља и у благом је порасту.

Промет интермодалних транспортних јединица у лукама је протеклих година био мали, од четири луке које располажу контејнерским терминалима у 2003. години забележен је промет контејнера само у луци Београд (2200 TEU[191]) и у луци Дунав Панчево (500 TEU).

Здравство је веома значајно, посебно токомратних конфликта, масовних миграција, политичке и економске нестабилности. Међутим, квалитет здравствене заштите као и инфраструктуре везане за здравство у Републици Србији постао је неадекватан. Ни промена власти 2000. године, као ни све

[191]*TEU - Twenty-foot equivalent unit, Јединица еквивалента двадесет стопа - Један ТЕУ представља капацитет робе стандардног ИСО контејнера, 20 стопа (6,1 m) дугачког и 8 стопа (2,44 m) широког.*

што се након тога издешавало до данас, није довело до неких значајних побољшања ситуације у здравству.

Здравствени систем у Републици Србији пати од недостатка средстава и инвестиција, али обезбеђује основну услугу грађанима.[192]

Приватни здравствени сектор је развијен, али није и инкорпориран у национални здравствени систем.

Вода. Проблем заштите воде као критичног инфраструктурног сектора у Републици Србији је све већи, а степен загађења речних токова и пијаћих извора се из дана у дан повећава.

Растуће потребе за водом у претходним деценијама допринеле су ставу да ће вода бити ограничавајући фактор развоја човечанства, али и опстанка људи у водом најсиромашнијим деловима света. Већина река у развијеним земљама постале су само канали отпадних вода, које чак и превазилазе капацитете самог воденог тока. Разградња отпадних материја веома је успорена, па је количина кисеоника потребног живим бићима у њој вишеструко смањена. Код нас је све већи број *одумирућих* река, док је на неким токовима стање толико лоше да живота у њима готово и да нема.

Кључни извори загађења река у Републици Србији су непречишћене индустријске и комуналне отпадне воде. Око 50 % загађења испуштеног у реке долази од индустријских постројења, а само 13 % комуналних отпадних вода се третира пре испуштања.[193]

Велики загађивач вода Републике Србије су и неуређене депоније. Вода и отпад су чврсто повезани, јер сваки отпад доспева и до подземних вода. Последице небриге због неодговарајућег одлагања отпада све се више осећају, а бројни извори су већ загађени.

Основни начин да се повећа квалитет вода и да се воде заштите је елиминисање и контролисање њихових загађивача, док би истовремено

[192]*Списак свих здравствени установа у Србији може се наћи на сајту Републичког фонда за здравствено осигурање: http://www.rfzo.rs/10.02.2013.*
[193]*Податак са сајта јавног водопривредног предузећа СРБИЈАВОДЕ, http://www.srbijavode.rs 10.02.2013.*

велики произвођачи морали да поведу рачуна о својим отпадним водама и адекватно их пречисте пре испуштања у природу.

Пошумљавање планинских површина би значајно помогло у очувању здраве воде, а веома ефикасан начин је и изградња површинских акумулација и малих брана.

Храна и пољопривреда. Република Србија[194] се налази на површини од укупно 8.840.000 ha. Површина пољопривредног земљишта обухвата 5.734.000 ha (0,56 ha по становнику), а на око 4.867.000 ha те површине простире се обрадиво земљиште (0,46 ha по становнику). Око 70 % укупне територије Републике Србије чини пољопривредно земљиште, док је 30 % под шумама.

Финансије. Као главни актери у финансијском сектору Републике Србије означени су: банке, друштва за осигурање, брокерско дилерска друштва, даваоци финансијског лизинга, друштва за управљање добровољним пензијским и инвестиционим фондовима, затворени и приватни инвестициони фондови и друге финансијске институције. Главни носиоци финансијског система су банке, што је, између осталог, последица недовољне развијености сектора осигурања и тржишта капитала, као и оскудног коришћења лизинга као облика финансирања.[195]

Јавне службе. У контексту овог сектора могао се и већи део организација које обављају послове државне управе означити као критичан, што се у неким државама и ради, али се овде због једноставности разматрања узимају само службе које су апсолутно неопходне за функционисање друштва у кризним ситуацијама и које су битан интегрални део кризног менаџмента. Јавна служба је организована делатност у државном или приватном власништву која служи за задовољење важних животних потреба шире

[194] *У свим земљама са дефинисаном политиком заштите критичне инфраструктуре се као подсектор у оквиру сектора хране појављује и пољопривреда, а у САД читав критични инфраструктурни сектор носи назив храна и пољопривреда. Подаци у бројкама налазе се насајту Владе Републике Србије: http://www.srbija.gov.rs/pages/article.php?id=55,10.02.2013.*

[195] *http://www.economy.rs/finansije/9790/Poslovanje-finansijskih-institucija-u-Republici-Srbiji-2012-godine.html.*

социјалне заједнице.[196]

У модерним, развијеним земљама појам јавних услуга обично обухвата:

- образовање,
- дистрибуцију електричне енергије и гаса,
- заштиту од пожара,
- здравство,
- полицију,
- чистоћу и
- производњу и дистрибуцију воде.

У највећем броју случајева јавне услуге су услуге, тј. оне не подразумевају производњу добара. Могу их пружати локални или национални монополи и то нарочито у областима у којима постоје природни монополи. Њихови резултати тешко се могу приписати одређеном индивидуалном напору и тешко их је оценити по квалитету. Оне обично подразумевају висок ниво обучености и образовања запослених.

Пошто у Републици Србији још увек не постоји закон о критичним инфраструктурама и оне нису јасно дефинисане може се предложити модел заснован напостојећим поделама критичних инфраструктура у суседним земљама, у складу са просторно-географским, привредним, економским и демографским карактеристикама.

Да би се са сигурношћу оформила листа критичних инфраструктура неопходно је да се, на основу једног од модела који су претходно описани кроз сарадњу са свим релевантним секторима и институцијама (приватним и државним) утврди степен критичности сваке инфраструктуре, па након тога оформи и коначна листа критичних инфраструктура.

[196]*Управно право Републике Србије.*

ЗАКЉУЧАК

Свет се суочавамо са великим претњама и ризицима који доводе до различитих врста ванредних ситуација. Ванредне ситуације представљају тренутке смањене сигурности становника услед великих природних катастрофа, прометних, хемијских и других угрожавања инфраструктурних постројења. Пратећи трендове и штете изазване оваквим ванредним ситуацијама нужно се намеће захтев за технолошким и организацијским решењем.

Ванредне ситуације су део свакодневног живота и са развојем друштва повећавају се извори, облици њиховог јављања као и губици људских живота, праћени огромним материјалним штетама. Комплексност ванредних ситуација, посебно чињеница да се њиховом појавом угрожавају критични капацитети који су суштински у редовном процесу функционисања друштва, навеле су већину држава да развију акције које су имале за циљ да: схвате елементе критичности рањивости различитих инфраструктура државе, дефинишу мере за смањење тих рањивости, осмисле и развију планове за кризне и ванредне ситуације и накнадни опоравак, подстакну развој сензибилитета код јавних и приватних оператера у погледу проблема заштитекритичне инфраструктуре и подрже међународну сарадњу.

Зашто је критична инфраструктура као и њена заштита актуелна? Расте број деструктивних активности (вандализам, саботаже, тероризам, неодговорно понашање и сл.), а објекти критичне инфраструктуре су све више повезани, зависни међусобно и високорањиви, а екстремни временски догађаји су све учесталији.

Прекид функционисања у једном сегменту или систему инфраструктуре може довести до прекида или нефункционисања у другим системима, те комбиновано изазвати дугорочне последице на систем власти, економију, јавно здравље и сигурност, националну сигурност и поверење јавности.

Инфраструктура обухвата комплексе и објекте које користе организације за потребе заштите и спасавања (стамбене објекте и друге објекте значајне за

заштиту и спасавање). У кључне инфраструктуре за обезбеђење оптималних услова за спровођење мера заштите и спасавање у случају ванредних ситуација укључује телекомуникациону инфраструктуру, саобраћај и транспорт и остале елементе. Информациона инфраструктура обухвата сву инфраструктуру у одређеној организацији која на било који начин утиче на кључна својства поверљивости, доступности или интегритет података у оквиру које подаци настају, обрађују се или чувају.

Информациона и комуникациона инфраструктура су осовина сваке организације у функцији размене података. У свом најширем смислу, она укључује жичне и бежичне (радиокомуникације) комуникације. Радио комуникације се могу поделити на земаљске и сателитске, унутар којих је смештен велики број разних служби (фиксне и мобилне телефоније, радиодифузија итд.).

Посебан значај за управљање у ванредним ситуацијама има примена информатичких технологија рачунарске мреже, периферије, софтверске услуге и апликације, базе података, електронски записи, итд. Ова инфраструктура омогућује брзо, једноставно и јефтино складиштење информација, повраћај, пренос и обраду дигитализованих података у форми говора, података, видеа, анимација итд.

За успешно функционисање система размене података неопходно је обезбедити одговарајућу инфраструктуру за реализацију интероперабилности, које подразумева мрежну инфраструктуру (хардвер и софтвер), али и људе, организацију и активности, прописе и правилнике, неопходне за обезбеђивање услова за интероперабилност и размену информација. Оваква инфраструктура је у надлежности организација, тако да представља резултат ангажовања свих нивоа у систему одлучивања које ће омогућити размену информација преко стандардних, Интернет и Web протокола.

Са порастом проблема у области заштите цивилног становништва, материјалних и културних добара и животне средине у условима ванредних ситуација, постало је евидентно да многи, ако не и сви, проблеми везани за

ову проблематику не могу да се решавају изолованим активностима појединих земаља. Ово се посебно односи за случај када су у питању проблеми који имају прекогранични или глобални карактер.

Државе су принуђене да сарађују по питању усклађивања стандарда у области система управљања ванредним ситуацијама, како би тиме олакшале и учиниле ефикаснијим активности заштите и спасавања становништва, материјалних и културних добара и животне средине у условима ванредних ситуација. Неопходно је да државе међусобно сарађују на усвајању наднационалних мера политике (нпр. подрегионалне, регионалне и глобалне), на развијању међународне регулативе и међународних стратегија, програма и планова с циљем да координирају изградњу и јачање система заштите и спасавања у условима ванредних ситуација.

Тема критичне инфраструктуре постаје, посебно последњих неколико година, незаобилазна у стручној литератури, од превенције ризика и катастрофа до могућих штетних учинака људске активности. Елементи критичне инфраструктуре су присутни у свим сферама наших свакодневних активности.

Примера ради, САД су прве покренуле иницијативу и акције на нивоу владе на тему заштите критичних инфраструктура доневши, 1998. године Председничку директиву о заштити критичних инфраструктуре (*President Decision Directives - PDD* 63). Након тога су многе друге земље развиле акције које су имале за циљ да:

- схвате елементе критичности и рањивости различитих инфраструктура државе;
- дефинишу стратегије за смањивање тих рањивости;
- подстакну развој сензибилитета код јавних или приватних оператера у погледу проблема заштите критичних инфраструктура;
- осмисле и развију планове за ванредне ситуације и опоравак;
- да подстакну развој суштински сигурних технологија и

- подрже међународну сарадњу.[197]

Наведене мере и поступци обавеза су државних органа, власника, оператера или корисника и морају се континуирано припремати и спроводити. У спровођењу мера заштите критичне инфраструктуре неопходно је утврдити редослед делатности:

- идентификација критичне инфраструктуре,
- израда мапа критичне инфраструктуре,
- размена информација,
- оспособљавање особља (менаџера, специјалних служби, радника) ангажованих на пословима и задацима у системима критичне инфраструктуре,
- увежбавање система за заштиту критичне инфраструктуре или опоравак у случају настанка ванредне ситуације.

Такође, у погледу мера заштитекритичне инфраструктуре, све државе, укључујући и Републику Србију, морају да утврде и редослед поступака: идентификација критичне инфраструктуре, израда мапа критичне инфраструктуре, размена информација, оспособљавање особља ангажованих на пословима и задацима у системима критичне инфраструктуре, увежбавање система за заштиту критичне инфраструктуре или опоравак у случају ванредне ситуације.

Заштита критичне инфраструктуре је препозната као основа одржавања функционалности друштвене заједнице у ванредним ситуацијама, као што су природне катастрофе. Главни циљ заштите критичне инфраструктуре од утицаја природних катастрофа је да се у таквим ситуацијама одржи континуитет у њеном функционисању.

Заштита критичне инфраструктуре у ванредним ситуацијама се може посматрати као део јединственог процеса превенције и одговора на ванредну ситуацију. У том контексту, организација успоставља, примењује и одржава процедуре за идентификовање потенцијалних инцидената који могу

[197]*Путник, Н., Сајбер простор и безбедносни изазови, Факултет безбедности, Београд, стр. 171, 2009.*

негативно утицати на неку организацију, њене активности, функције, услуге, заинтересоване стране и окружење. Ове процедуре имају за циљ заштиту живота, имовине, спречавање прерастања инцидента у ванредну ситуацију или катастрофу, скраћивање времена прекида операција или активности организације, опоравак најважнијих активности организације, повратак на редовне активности и заштита имица и репутације организације.

Смањење утицаја природних катастрофа на људе и критичну инфраструктуру обухвата интервенције са циљем спречавања или смањивања могућности физичког угрожавања и социјалног ремећења. Додуше, два су доминантна типа смањења утицаја природних катастрофа. Структурно смањење подразумева дизајнирање, конструисање, одржавање и реновирање физичких структура и инфраструктура како би се одупрли физичким силама и ударима природних катастрофа. Неструктурална смањења обухватају напоре за смањење изложености људске популације, физичких структура и инфраструктура условима опасности. Приступи неструктуралног смањења укључују законски донете урбанистичке мере које узимају у обзир могуће ударе катастрофа; регулисање развоја у зонама високе опасности као што су терени под нагибом који су склони клизиштима и приобалне зоне као мета олујних таласа; и чак у неким случајевима откуп и измештање заједница или делова заједница, што је мера која се сада користи за области које су искусиле поновне губитке од поплава.

Заједнички циљ којем теже све државе када је у питању заштита критичне инфраструктуре јесте израда адекватног механизма који ће спречити стварање услова који могу довести до отказивања одређене инфраструктуре услед несреће или напада на било који елемент система. Сходно томе, политика заштите критичне инфраструктуре представља један веома сложен склоп различитих стратегија, методологија, планова усмерених ка превенцији ризика и претњи, као и спречавању већих последица услед кризних ситуација. Комплексни проблеми захтевају мултидисциплинарни приступ и примену наменски израђених алата кризног менаџмента ради ефикасног идентификовања потенцијалних ризика и претњи.

Што се тиче политике заштите КИ на наднационалном нивоу, Европска унија представља једног од кључних актера, придајући велики значај овом питању. Од 2004. године, након терористичког напада у Мадриду, државе чланице Европске уније су покренуле низ иницијатива и истраживачких програма како би се испитали различити аспекти заштите и претњи по критичну инфраструктуру, као и утицаји који оштећење критичних инфраструктура може имати на образовање, привреду, здравство, систем комуникација и друге сегменте људске делатности. Функционисање и координација између држава чланица регулисана је Директивом ЕУ о заштити критичних инфраструктура из 2008. године, која представља добар модел и пружа могућност за преузимање одређених решења, посебно у области регулисања јавно-приватног партнерства.

Када је реч о заштити КИ на националном нивоу, највећи напредак на том пољу постигле су САД које улажу велике напоре и издвајају значајна финансијска средства намењена изградњи ефикасног система заштите КИ. Оно што је заједничко у свим стратегијама технолошки развијених земаља, јесу јасно идентификовани извори и облици угрожавања критичних инфраструктура, прецизна класификација критичних сектора, ефикасно регулисано јавно-приватно партнерство и стална модернизација информационе инфраструктуре. Међутим, ове земље суочене су са проблемом комплексности инфраструктура који иницира покретање сложенијих механизама за успостављања њихове ефикасне заштите. Поменути проблем, често може бити узрок грешке у функционисању система, о чему најбоље сведоче догађаји од 11.09.2001. године.

Интезитет свих врста штета и поремећаја који су изазвани екстремним природним катастрофама, може бити умањен усвајањем безбедносних мера за ублажавање и одговор на такве догађаје, на различитим нивоима. Ове мере би обухватиле регулацију коришћења земљишта и структуралну изградњу објеката, како би се онемогућило дејство подрхтавања тла, надирање воде и јаких ветрова на конструкције објеката С друге стране, припреме би обухватиле и доношење планова за одговор на последице

природних катастрофа, прикупљање свих неопходних залиха, тренирањем припадника интервентно-спасилачких служби, образовањем осталих снага заштите и спасавања од катастрофа и мерама за смањење последица.

Утврђено је да утицај природних катастрофа на витална добра не зависи само од физичких карактеристика таквих догађаја, већ и од способности људи да апсорбују утицај и опораве се од њихових последица.Тако појединци зависе од добијања одређених услуга у месту пребивалишта.Њихова угроженост се често повећава или смањује у зависности од природе ових услуга. На пример, уместо да се градови ослањају на један велики водоводни систем, пожељно је да постоји серија малих и самосталних постројења за водоснабдевање. У случају поплава, мало је вероватно да ће сва постројења за водоснабдевање бити уништена или оштећена (*Parker et all*, 1997). У том случају, непогођена постројења ће неопходно снабдевање водом пружити становницима у местима која су погођена поплавом.[198]

Смањење угрожености и повећање отпорности критичне инфраструктуре су компатибилни са циљевима одрживог развоја. Заједнице које су одрживе, истовремено су и отпорне и у стању су да минимизирају ефекте незгода; у исто време, имају способност да се брзо опораве од екстремних догађаја. Схватање значаја критичне инфраструктуре за људску и националну, па и међународну безбедност услов је за изналажење адекватних стратегија њихове заштите; адекватним стратегијама заштите критичне инфраструктуре постиже се прихватљив ниво губитака и оштећења у условима природних катастрофа, док је систем безбедности ефикаснији у превенцији и превазилажењу таквих ситуација.

Да би се постигао први циљ неопходно је предузети мере превенције, ублажавања и минимизације ефеката природне катастрофе. Стога, фазе које претходе природним катастрофама - превенција, ублажавање и припремљеност су од кључне важности.

Управљање ванредним ситуацијама подразумева анализе условљености

[198]*Bimal, P., Environmental Hazards and Disasters Contexts, Perspectives and Management, Kansas: State University, Wiley Blackwell, 2012.*

догађаја и последица, предузимање одговарајућих мера за спречавање или смањење појава ванредних ситуација или пак, санације ако је дошло до ванредне ситуације. Увођењем општег система за подршку ванредним ситуацијама, обезбеђује се боља комуникација и размена података између служби одговорних за управљање ванредним ситуацијама и на тај начин се управљање ванредним ситуацијамапобољшава и ставља под већу контролу.

За потребе израде ове докторске дисертације спроведено је истраживање у форми анкетног упитника. Он је садржао 35 питања, а анкетирана су лица из струке, одговорна лица и руководиоци организационих целина. Обухваћена су лица из составаСектора за ванредне ситуације МУП РС, Јавног комуналног предузећа „Београдски водовод и канализација“, Јавног предузећа „Пошта Србије“, Јавног предузећа „Електропривреда Србије“, Нафтне индустрије Србије а.д., Јавног предузећа „Електромрежа Србије“, Јавног предузећа „Путеви Србије“, Јавног водопривредног предузећа „Србијаводе“ и Железнице Србије а.д. Прикупљени су подаци по унапред припремљеним и формулисаним питањима.

Резултати ових истраживања су недвосмислено указали на постојеће проблеме везане за за управљање и превазилажење последица ванредне ситуације на пољу критичне инфраструктуре. Анализирана је нормативно-правна и законска регулитива, потреба усвајања нових законских прописа у области заштите и спасавања.

Идентификовани су проблеми/потешкоће везани за област управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре. Дефинисани су и критеријуми, који би се могли користити за оцену степена ефикасности јединица за отклањање последица. Поред тога сублимиране су и многобројне сугестије у области управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре.

ЛИТЕРАТУРА

I Монографије и научно-стручни радови

1. Adger, W.N., Vulnerability, Global Environmental Change 16, 2006.
2. Adizes, I.K., Kako upravljati u vrijeme krize (i kako je prije svega izbjeći), ASEE d.o.o., Zagreb, 2009.
3. Aguilar, F.J., Scanning the Business Environment, New York,The Macmillan Company, 1967
4. American Energy Security, The Southern States Energy Board, Norcross, Georgia, 2006.
5. Andreas, W., Metzger, J., Dunn, M., eds., International CIIP Handbook Center for Security Studies at the Swiss Federal Institute of Technology, Zurich, 2004.
6. Анђелковић, Б., Ризик технолошких система и професионални ризик, Југословенски савез друштава инжењера и техничара заштите, Ниш, 2002.
7. Ansof, H.I., Managing Strategic Surprise by Response to Weak Signals, California Management Review, Vol. VIII,No. 2,1975.
8. Annual Information Society Report 2007 - Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the regions, Brussels, 2007.
9. Association of Metropolitan Sewerage Agencies, Protecting wastewater Infrastructure Assets - Asset Based Vulnerability Checklist for Wastewater Utilities, 2002.
10. Bahgat, G., Europe's energy security -Challenges and opportunities, International Affairs, Vol. 82, 2006.
11. Baker, G.H., A vulnerability assessment methodology for critical infrastructure sites, Department of Homeland Security symposium: R&D partnerships in homeland security, Boston, Massachusetts, 2005.
12. Baldwin, D.A., Thinking about Threats, Journal of Conflict Resolution, Vol. 15,

No. 1, March, 1971.

13. Bankoff, G., Maping Vulnerability, Earthscan, London, 2004.
14. Bartlett, H., Holman, G., Somes, E. T.,The Art Strategy and Force Planning, Strategy and Force Planning, Bartlett model, Naval War College Press, Newport, 2004.
15. Bimal, P., Environmental Hazards and Disasters Contexts, Perspectives and Management. Kansas: State University, Wiley Blackwell, 2012.
16. Božidar, N., Krizno komuniciranje, Binoza press, Zagreb, 2001.
17. Благојевић, М., Улога специјалних јединица МУП Републике Србије у условима мирнодопских ванредних ситуација, Магистарска теза, Факултет безбедности, Београд, 2009.
18. Благојевић, М., Милановић З., Еколошка безбедност у функцији изградње капацитета система безбедности, Тематски зборник радова „Транзиција и економски криминал“, КПА, Београд, 2013.
19. Boin, A., McConnell, A., Hart, P., Governing after Crisis - The Politics of Investigation, Accountability and Learning, CambridgeUniversity Press, Cambridge, 2008.
20. Botan, C. H., Public Relations Theory, Hillsdale, New York, 1989.
21. Brecher, M., Winkenfield J., A study of crisis, Michigan Press, 2000.
22. Brunner, E.M., Elgin, M., Sutter, M., International CIIP Handbook 2008/2009, An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies, Centerfor Security Studies, Zurich,2009
23. Buble, M., Strateški menadžment, Sinergija, 2005.
24. Carl, A. Roper, Risk Management for Security Professionals, Butterworth-Heinemann, 1999.
25. Cavelty, M., Critical information instractructure: Vulnerabilities, Threates and Responsis, UNIDIR, Diaarmamenr Forum, No.3, 1999.
26. Cisco: Annual Security Reports 2008, 2009.
27. Communication from the Commission on fighting spam, spyware and malicious software, COM, 688 final, 2006.

28. Coombs, W.T., Ongoing crisis communication: planning, managing, and responding, Sage Publications, Thousand oaks, 1999.
29. Cornell, S.E., Nillson, N., Europe's Energy Security, Gazprom's Dominance and Caspian Supply Alternatives, Central Asia - Caucasus Institute & Silk Road Studies Program, Washington DC, 2008.
30. Consise Oxford Dictionary, 9th edition, Claredon Press, Oxford, 1997.
31. Country Analysis Briefs, Russia, Energy Information Administration, Washington DC, 2008.
32. Covey, S.R., Sedam navika uspješnih ljudi, Zagreb, Mozaik knjiga, 1998.
33. Criminal Intelligence Analysis, Development of Inferences Anacapa Sciences, Inc., USA, 1982-2003.
34. Crisis management, Proceedings No.2, Center for Crisis Management of the Republic of Macedonia, Skopje, 2008.
35. Critical infrastructure emergency risk management and assurance - Handbook, Emergency Management Australia, Infrastructure handbook, 2003.
36. Critical Infrastructure Emergency Risk Management and Assurance, Emergency Management Australia, A Division of the Attorney-General's Department, 2003.
37. Critical Infrastructure Protection II, izdavač Springer, grupa autora, Library of Congress Control Number 2008936479, 1995.
38. Critical Infrastructure Protection in Homeland Security, Ted G. Lewis, John Wiley & Sons, 2009.
39. Curtin, T., Hayman, D., Husein, N., Managing a Crisis, Palgrave Macmillan, New York, 2005.
40. Cutlip, S.M., Center, A.H., Broom, G.M., Effective public relations, osmo izdanje, Prentice Hall, Upper Saddle River, New York, 2000.
41. Cutlip, S.M., Center, A.H., Broom, G.M., Odnosi s javnošću, Mate d.o.o., Zagreb, 2003.
42. Cvjetković, B., Terorizam - sredstva i posljedice, Laus, Split, 2002.

43. Daasse, C., Kessler, O., Knowns and Unknowns in the War in Terror: uncertainty and the politicalconstruction of danger, 2007.
44. Деканић, И., Положај Хрватске у могућим енергетским и геополитичким кризама, Хрватска - како сада даље, Загреб, Центар за демократију и право Мико Трипало, 2008.
45. Deutsch, J., Future United States Energy Security Concerns, MIT Joint Program on the Science and Policy of Global Change, Report No. 115, Massachusetts Institute of Technology, 2004.
46. Douglas, M., Wildavsky, A., Risk and Culture: An Essay on the Selection of Environmental Dangers, CaliforniaUniversity Press, Berkeley, 1982.
47. Douglas, M., Risk and blame: essays in cultural theory, Rutledge, London, 1992.
48. Dozier, D.M., et. al., Manager's Guide To Excellence In Public Relations and Communication Management, Lawrence Erlbaum, New Jersey, 1995.
49. Drabeck, T., Quarantelli E., Scapegoats, Villains and Disasters, Transaction, No.4, 1967.
50. Dresner, H., Performance Management Revolution. NY: John Wiley & Sons Inc., 2008.
51. Дробњак, С., Утицај флексибилности и реактивности предузећа на ефикасност и ефективност кризног менаџмента, докторска дисертација, Факултет теничких наука, Нови Сад, 2015.
52. Drucker, P., Tudor, G., Učinkoviti menadžer, Menadžerski priručnik, M.E.P. Consult, Zagreb, 2004
53. Dunn, M., Mauer, V., International Critical Information Infrastructure, Protection Handbook, ETH Center for Conflict Studies,Vol. I, Zurich, 2000.
54. Edward, B., Natural Hazards, Second Edition. Cambridge, University Press, 2005.
55. Elliot, D., McGuiness M., Public inquiry: panacea or placebo, Journal of Contingencies and Crisis Management 10(1), 2002.
56. Energy Security to Energy Independence, Meeting report, Current Science,

Vol. 89, prosinac, 2005.

57. Engelbrekt, K., Förberg, M., Managing Crises in Bulgaria, Elanders Gotab, Stockholm, pp. 27-43, 2005.
58. Engdahl, F.W., Stoljeće rata, AGM, Zagreb, 2000.
59. EUROPOL: Strategic Intelligence Analysis Course, Reading Material, File No: 2520-47 Rev 1., 2002.
60. Ezell, B.C., Infrastructure Vulnerability Assessment Model (I-VAM), Risk Analysis, 27(3), pp. 571-583, 2007.
61. Čendo, M., Menadžment poduzeća i kriza, Zbornik radova II međunarodne konferencije „Dani kriznog upravljanja“, str. 34-41, 28.-29.05.2009. godine, Veleučilište Velika Gorica, Velika Gorica, 2009.
62. Černiček, I. Tot, T., Otkrivanje novih struktura i ponašanja u organizacijama, u Zborniku radova „Na putu ka dobu znanja“, Fakultet za menadžment, Novi Sad, 2004.
63. Džin, M., Bao, Y.T., Modelling of incentives for sustainable critical infrastructure systems, Technological and Economic Development of Economy 16(3), 365-379, 2010.
64. Fearn-Banks, K., Crisis Communications: A Casebook Approach, Lawrence Erlbaum Associates, Malwah, New York, 1999.
65. Fearn-Banks, K.: Crisis communications, A Casebook Approach, Third Edition, University of Washington, 2007.
66. Flinders, M.V., Smith M., Quangos, accountability and reform, Basingstoke's, UK: Palgrave Macmillan, 1999.
67. Funda, D., Majić, T., Upravljanje krizom, International Conference ''Crisis Management Days'', Velika Gorica, 2011.
68. Garb, G., Varnostno upravljanje kritične infrastrukture. Magistrsko delo, Fakulteta za logistiko, Celje, 2009.
69. George W.B., Executive Order 1323, Critical Infrastructure Protection in the Informaion Age, Washington, http://www.fas.org/irp/offdocs/eo/eo-13231.htm 17.11.2012.

70. George, W.B., Executive Order 13228, Establishing the office of homeland security and the Homeland Security Council, Washington: http://www.fas.org/irp/offdocs/eo/eo-13228.htm 17.11.2012.
71. Gilad, B., Early Warning: Using Competitive Intelligence to Anticipate Market Shits, Control Risk, and Create Powerful Strategies, AMACOM, 2003.
72. Gorodetsky, G., Russia between East and west: Russian Foreign Policy on the Threes-hold of the Twenty-First Century, London, Rutledge, 2003.
73. Gospić, G. Murić, D. Bogojević, Managing critical infrastructure for sustainable development in the telecommunications sector in the Republic of Serbia, International Conference on Applied Internet and Information Technologies, Zrenjanin, 2012.
74. Grunig, J.E., Two Way Symmetrical Public Relations: Past, Present and Future
75. Grunig, J.E., Hunt, T., Managing Public Relations, Holt, Rinehart and Winston, New York, 1984.
76. GSMA: SG.07, The Potential Misuse and a Threat Analysis of the GSM System, 2007.
77. Habermas, J., Javno mnjenje, Kultura, Beograd, 1969.
78. Hampel, R., Wagenknecht M., Chaker N, Fuzzy Control: theory and Practice. Heidelberg, Germany.
79. Harmon, C.C., Terorizam danas, Golden marketing, Zagreb, 2002.
80. Harrington, L.S.B., Vulnerability and Sustainability Concerns for the US High Plains in Rural Change and Sustainability: Agriculture, the Environment and Communities, Cambridge, MA: CABI Publishing, 2005.
81. Heath, R., Coombs, T., Today's Public Relations, Thousand Oaks, London, 2006.
82. Heath, R., Handbook of Public Relations, Thousand Oaks, Sage Publications, 2001.
83. Herga, M., Nacionalna kritična infrastruktura, Menadžment i sigurnost - M&S 2010: "Planiranje i sigurnost", стр. 311, 2010.
84. Hill, F., Energy Empire: Oil, Gas and Russia's Revival, London, The Foreign

Policy Centre, 2004.

85. Hofer, C.V., Turnaround Strategies, The Journal of Business Strategy, Vol. 1 (1), 1980.
86. Hood, C.,The Risk Game and the Blame Game, Government and Opposition, 37(1), pp. 15-37, 2002.
87. Huntington, S.P., Sukob civilizacija i preustroj svjetskog poretka, hrvatsko izdanje, Izvori, Zagreb, 1998.
88. Infrastucture Protection, grupa autora, Springer a.g., Library of Congress Control Number 2007938897, ISBN 978-0-387-75461-1.
89. Ivanovski Z., Development of cooperative crisis management capacities in Southeast Europe, Collection "Managing the Crisis in Macedonia", Associate number of Contemporary Macedonian Defense, Ministry of Defense of the Republic of Macedonia, Skopje, 2005.
90. ITU-D Study Group 1, Question 22/1: Report on Best Practices for a National Approach to Cyber security: A Management Framework for Organizing National Cyber security Efforts, ITU Secretariat Draft, 2008.
91. IT Governance Institute, Information Security Governance, 3rdedition, 2007.
92. Јаковљевић В., Ресурси критичне инфраструктуре и њихов значај за управљање ванредним ситуацијама, Зборник радова ФЦО, Београд, 2010.
93. Јаковљевић, В., Гачић, Ј., Заштита критичне инфраструктуре у кризним ситуацијама, Међународна научна конференција Менаџмент 2012, Младеновац, 2012.
94. Jarlsvik, H, Castenfors, K., Security and Preparedness in the EU, Stockholm, 2004.
95. Jantol, T., Politička javnost, Birotisak, Zagreb, 2004.
96. Jones, M.D., The hiker's Toolkit, Fourteen Powerful Techniques for Problem Solving, Three Rivers Press, 1998.
97. Jopling, L., The protection of critical infrastructure, http://www.nato-pa.int/default. asp? SHORTCUT=1165, 31.07.2013.

98. Karović, S., Komazec, N., Управљање ризиком на системским основама, Vojno delo, 2010.
99. Кековић, З., Савић, С., Комазец, Н., Милошевић, М., Јовановић, Д., Процена ризика у заштити лица, имовине и пословања, Центар за анализу ризика и управљање кризама, Београд, 2011.
100. Kešetović, Ž., Toth, I., Problemi kriznog menadžmenta, znanstvena monografija, Veleučilište Velika Gorica, Visoka škola za sigurnost sa pravom javnosti, Centar zamеđunarodne i sigurnosne studije, Fakulteta političkih nauka u Zagrebu, Velika Gorica, 2012.
101. Khalsa, S., Forecasting Terrorism: Indicators and Proven Analytic Techniques. Scarecrow Press, Inc., 2004.
102. Khandwalla, P., Turnaround Excellence: Insights from 120 cases, Response Books, New Delhi, 2001.
103. Klepac, G., Kopal R., Korkut D., Sustavi ranog upozorenja temeljeni na metodama poslovne inteligencije, Sборник радова „Дани кризног управљања“, Велика Горица, Хрватска, 2011.
104. Klimke, R., Die kunst der krisen-PR, Junfermann Verlag, Padeborn, 1993.
105. Kopal, R., Korkut, D., Knežević, H., Primjena analitičkih tehnika u poslovnim istraživanjima, Zbornik Visoke poslovne škole Libertas, Zagreb, godina II, 2009
106. Kopal, R., Stanić N., Bereček B., Uloga poslovne inteligencije u kriznom menadžmentu, Zbornik Visoke poslovne škole Libertas. Zagreb, godina, 2008.
107. Koubatis, A., Schonberger, J.Y., Risk Management of Complex Planning Framework, Safety Science, 2005.
108. Kulić, S., Strategija nasilja kao strategija razvoja, Naprijed, Zagreb, 1996
109. La Porte, T.R., Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise, Vol. 15, No. 1, March, 2007.
110. Larsson, R. R., Russia's Energy Policy: Security Dimensions and Russia's Reliability as an Energy Supplier, FOI - Swedish Defense Research Agency, Stockholm, 2006.

111. Lewis, T.,Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley Interscience, 2006.
112. Lewis, G.T., Critical Infrastructure Protection in Homeland Security - Defending and Networking Nation, Wiley-Interscience, New Jersey, 2006.
113. Liscouski, R., Infrastructure Protection, Dept. of Homeland Security, Testimony before the House Select Committee on Homeland Security; Infrastructure and Border Security Subcommittee, 2004.
114. Luecke, R., Upravljanje kriznim situacijama, Harvard Business Essentials and Zgombić i Partneri, Zagreb (in Croatian), 2005.
115. Lukić, S., Živanović N., Bakić R., Upravljanje rizikom kao zaštita od potencijalne krize tvrtke, Zbornik radova III međunarodne konferencije „Dani kriznogupravljanja", Veleučilište Velika Gorica, Velika Gorica, 2010.
116. Macaulay, T., Critical Infrastructure - Understanding Its Component Parts, Vulnerabilities, Operating Risks and Interdependencies, CRC Press, London, 2008.
117. Мацура, Д., Управљање критичном инфраструктуром за одрживи развој у поштанском и железничком сектору РС, Пројекат Министарства науке и технолошког развоја, 2011-2015.
118. Mahwah, W., Lanwence Erlbaum Associates, 1996.
119. Mannila, H., Hand, D., Principles of Data Mining, Cambridge, Massachusetts: the MIT Press, 2001.
120. Manual - System for Crisis Management, Project for strengthening the capacities of the Center for Crisis Management, funded by the Government of Japan and the Program for Development of the United Nations, UNDP, Skopje, 2010.
121. McGraw K., Managing Blame: An Experimental Test of the Effects of Political Accounts, American Political Science Review 85, 1991.
122. Mitrevska, M., Crisis Management, Macedonian treasury, Skopje, 2005.
123. Michel-Kerjan, E., New Challenges in CI: A US Perspective, Journal of Contingencies and Crisis Management, Vol.11, No.3, 2003.

124. Михалинчић, М., Важност управљања комуникацијским процесима у кризним ситуацијама, Зборник радова „Дани кризног управљања“, Велика Горица, Хрватска, 2011.
125. Milburn, T.W., Watman, K.H., On the Nature of Threat: a Social Psychological Analysis, New York: Praeger, 1981.
126. Михаљевић Б., Михалинчић М., Кризна ситуација, опасност или повољна прилика, Гласник, АКД Училиште, бр. 9, 2011.
127. Мијалковски, М., Ђорђевић, И., Ризик - специфичан облик угрожавања безбедности, Универзитет у Београду, Факултет безбедности, 2006.
128. Milburn, T.W., Watman, K.H., On the Nature of Threat: a Social Psychological Analysis, New York: Praeger, 1981.
129. Мићовић, М., Специфичности заштите критичне инфраструктуре, Безбедност, бр. 3/2014.
130. Mićović, M., Jakovljević, V., The system of critical infrastructure of the Republic of Serbia in response to emergencies - Opportunities and perspectives, V međunarodni stručno-znanstveni skup, Zaštita na radu i zaštita zdravlja, Veleučilište u Karlovcu, Zadar, Hrvatska, 2014.
131. Murray T., Critical infrastructure protection: The vulnerability conundrum, Telematics and Informatics, Vol. 29, No. 1, 2012.
132. Monaghan, A., Russian Oil and EU Energy Security, Conflict studies research centre, DefenseAcademy of the UK, 2005.
133. Московљевић, М., Речник савременог српског књижевног језика с језичким саветником, Гутенберговагалаксија, Београд, 2006.
134. Moteff, D.J., Parfomak, P., Critical Infrastructure and Key Assets: Definition and Identification, Congressional Research Service, Library of Congress, 2004.
135. Најзначајнији резултати МУП Републике Србије у 2010. години, МУП РС, Београд, 2010.
136. Namid, R.N., Christopher, D.B., Organizational Data Mining: Leveraging Enterprise Data Resources for Optimal Performance: Idea Group, 2004.

137. National Infrastructure Protection Plan, Homeland Security, 2009.
138. NATO Public Diplomacy Division, Brusesels, Belgium, 2006.
139. Nickolov, E., Critical information infrastructure protection: Analysis, evaluation and expectations - study case of Bulgaria, INFORMATION & SECURITY, An International Journal, Vol. 17, 2005.
140. Novak, B., Krizno komuniciranje i upravljanje opasnostima, Binoza Press, Zagreb, 2001.
141. Oackl, a., PR-Praxis: Der Schlüssel zur Öffentlichkeitsarbeit, Econ, Düsseldorf, 1976.
142. OECD, Computer Viruses and Other Malicious Software - A threat to the Internet Economy, 2009.
143. Oeckl A., Handbuch der Public Relations: Theorie und praxis in der öffentlichkeitsarbeit in Deutschland und in der Welt, Süddeutscher Verlarg, München, 1964.
144. Olson R.S., Toward a Politics of Disaster: Losses, Values, Agendas, and Blame, International Journal of Mass Emergencies and Disasters, 18(2), 2000.
145. Osmanagić, N., Kriza kao šansa: kroz poslovnu krizu do poslovnog uspjeha, Školska knjiga, Zagreb, 2003.
146. Osmanagić, N., Bedenik, N.: Kontroling; Abeceda poslovnog uspjeha, Školska knjiga, Zagreb, 1998.
147. Osmanagić, N., Bedenik, N.: Kriza kao šansa, Školska knjiga, Zagreb, 2007.
148. Papa, M., Shenoi, S., Critical Infrastructure Protection II - Emergent Risks in Critical Infrastructures, International Federation for Information Processing, New York, 2008.
149. Peltier, T.R., Information Security Policies and Procedures, Auerbach Publication, 2006.
150. Pescatore, J., Young, G., Allan, A., Girard, J., Feiman, J., IT Security Threat Projection Timeline, 2008.
151. Pereboom, J., Infrastructure Interdependencies: Overviews of Concepts and Terminology, Infrastructure Assurance Center, Argonne, 2001.

152. Pedrycz, W., Gomide, An Introduction to Fuzzy Sets: Analysis and Design of Complex Adaptive Systems. Cambridge, Massachusetts: MIT Press, 1998.
153. Perinić, J., Mogući utjecaj medija u kriznim situacijama na javno mnijenje oblikovanjem sadržaja, Zbornik radova III Međunarodna konferencija „Dani kriznog upravljanja“, Veleučilište Velika Gorica, Velika Gorica,2010.
154. Perinić, J., Barović, V., Društvena odgovornost medija u izvještavanju o akcidentima i kriznim situacijama, Zbornik radova međunarodnog znanstvenog skupa „Mediji i turizam“, Zadar-Nin, 20.-22.03.2009, Sveučilište u Zadru.
155. Perinić, J., Žlof, K., Hadžić, S., Vjerodostojnost tiskanih medija u studiji slučaja „svinjska gripa“, Zbornik međunarodne znanstvene konferencije “Vjerodostojnost medija“, Fakultet političkih znanosti Zagreb, Sveučilište u Zagrebu.
156. Perrow, C., Normal Accidents: Living with High-Risk Technologies, Princeton University Press, Princeton, p. 351, 1999.
157. Physica-Verlag Jones, M.D., The honker’s Toolkit, Fourteen Powerful Techniques for Problem Solving, Three Rivers Press, 1998
158. PolitisD., KozyrisP., IglezakisI., Socioeconomic and Legal Implications of Electronic Intrusion, Zbornik radova, 2009.
159. Plenković, M., Holistička analiza odnosa s javnostima (javnošću), Informatologia 34, 1-2, 2001.
160. Plenković, M., Krizno komuniciranje i teorija odnosa s javnostima, Media, culture and public relations, br. 1, Zagreb, 2001.
161. Plenković, M., Teorija i praksa javnog komuniciranja, Izdavačko instruktivni biro, Zagreb, 1983.
162. Portnoy, M., Goodman,S., Global Initiatives to Secure Cyberspace, Springer 2009.
163. Prezelj, I., Kustec Lipicer, S., Public and policy management of critical infrastructure: Lessons from Integral Nations Cross-Sectoral Scanning in Slovenia, IRSPM Conference, Panel: Risk and crisis management in the public

sector, Berne, 2010.

164. Public Switched Network Security Assessment Guidelines prepared by the office of the manager national communication systems, Arlington, VA, 2000.
165. Путник, Н., Сајбер простор и безбедносни изазови, Београд, Факултет безбедности, 2009.
166. Pyle, D., Data preparation for Data Mining. San Francisco, Morgan Kaufmann, 1999.
167. Quarantelli, E.L., Disaster Crisis Management: A Summary of Research Findings, Journal of Management Studies, Vol. 25, 1988.
168. Radvanovsky, R., McDougall, A., Critical Infrastructure, Homeland Security and Emergency Preparedness, 2nd edition, CRC Press, Taylor&Francis Group, New York, 2010.
169. RAND Europe: Benchmarking Security and Trust in the Information Society in Europe and the US, IST-26276-SIBIS project (SIBIS Statistical Indicators Benchmarking the Information Society), 2003.
170. Rajmohan, C., Subramanya, G., Sharma, N., Telecommunication Networks: Security Management, Tata Consultancy Services Limited, 2012.
171. Rashed, T., Weks, J., Assessing vulnerability to earthquake hazards through spatial multicriteria analysis of urban areas, International Journal of Geographical Information Science, 2003.
172. Ray, S.J., Strategic Communications in Crisis Management: Lessons from the Airline Industry, Quorum Books, London, 1999.
173. Ribeiro, S.L., Bezerra, E.K., Nakamura, E.T., Critical Infrastructure in Brazil, 1st IEEE International Workshop on Critical Infrastructure Protection, 3-4th Nov 2005, Darmstadt, 2005.
174. Rinaldi. S.M, Modelling and Simulating Critical Infrastructures and Their Interdependencies, 2004.
175. Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing threats, Vulnerabilities and Consequences, Report to Congress, John Motef Specialist in Science and Technology Policy

Resources, Congress Research Service, Science, and Industry Division, Order Code RL32561.

176. Roper, C., Risk Management for Security Professionals, Butterworth-Heinemann, 1999.
177. Rosentha, U., Boin Arien, R., Comfort Louis. K. (eds.) Managing Crises: Threats, dilemmas, opportunities, Charles C. Thomas, Springfield, 2001.
178. Rothstein, H., The Institutional Origins of Risk: A New Agenda for Risk Research, Health, Risk&Society, vol. 8, No. 3, 2006.
179. Security Management, Tata Consultancy Services Limited, 2012.
180. Sapriel, C., Effective Crisis Management: Tools and Best Practice for the New Millennium, Journal of Communication Management, Vol. 7, No. 4, 2003.
181. Seeger, M., Robert R., Julie M., Sellnow Timothy, Post-crisis discourse and organizational change, failure and renewal, Journal of Organizational Change Management, Vol. 18, No. 1, pp.78-95, 2005.
182. Seymour, M., Moore, S., Effective Crisis Management: Worldwide Principles and Practice, Chassell, London, 2000.
183. Siler, W., Building Fuzzy Expert Systems, 2001.
184. Siler, W., Buckley J., Fuzzy expert systems and fuzzy reasoning. NY: John Wiley & Sons Inc., 2005.
185. Smedts, B., Critical Infrastructure Protection Policy in the EU: state of the art and evaluation in the (near) future, Royal High Institute for Defense, Center for Security and Defense Studies, Focus paper 15, 2010.
186. Solano, E., Methods for Assessing Vulnerability of Critical Infrastructure, Institute for Homeland Security Solutions, 2010.
187. Slatter, S., Lovett, D.: Corporate Turnaround, Penguin Books, London, 1999.
188. Slonjinski, R., Fuzzy Sets in Decision Analysis, Operations Research and Statistics. New York: Kluwer, 1998.
189. Субошић, Д., Концепције сложености као фактор одлучивања о посебним безбедносним задацима, Зборник радова „Дани кризног управљања“, Велика Горица, Хрватска, 2011.

190. Suchman, E.A., A conceptual analysis of the accident problem, Social Problems, Vol. 8, pp. 243, 1961.
191. Šoštarić, E., Amonijak i klor mogu ubiti sve stanovnike Zagreba, Nacional br. 426, 2004.
192. Tagarev, T., Pavlov, N., Planning measures and capabilities for protection of critical infrastructures in Bulgaria, pp. 46, 2007.
193. Tagarev, T., The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms), The Quarterly Journal 5 No. 1, Spring-Summer, 2006.
194. Tafra-Vlahović, M., Upravljanje krizom, VPŠ Zaprešić, Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing threats, Vulnerabilities and Consequences, Report to Congress, Order Code RL32561, 2011.
195. Taylor M., Horgan J., Terorizam u budućnosti, Golden marketing, Zagreb, 2003.
196. Traynor P., McDaniel, P., Security for Telecommunications Networks, Springer 2008.
197. The National Security Strategy of the United States of America, 2002.
198. Toft, B., Reynolds, S., Learning from disasters: A management approach, 3rd ed. Perpetuity Press, Leicester, UK, 2005.
199. Trapans, J., Fluri,P., Defence and Security Sector Governance and Reform in South East Europe: Insight and Perspectives - Self Assessment Study, Vol. I-II, 2003.
200. Tobin, A. Montz, E., Natural hazards and technology: vulnerability, risk, and community response in hazardous environments. In Geography and Technology (ed. S.D. Brunn et al.). Dordrecht: Kluwer, 2007.
201. Twigg, J., Bhatt M.R., Understanding Vulnerability: South AsianPerspectives, 1998.
202. Vanous, J., Security of Energy Supplies: Some Thoughts on the Concept and Key Related Issues, Prague Security Studies Institute Wiley&Sons Inc, 2004.

203. Van Santen W., Jonker C., Wijngaards N., Crisis Decision Making Through a Shared Integrative Negotiation Mental Model, Crisis Decision Making through a Negotiation Mental Model, Proceedings of the 6th International ISCRAM Conference - Gothenburg, Sweden, 2009.
204. Vešović V., Knežević N., Menadžment poslovnih procesa u pružanju poštanskih i telekomunikacionih usluga, XXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2005, Beograd, 13. - 14.12.2005.
205. Весић, Д., Менаџмент и кризни програм - аспект односа са јавношћу, Безбедност, Београд, бр. 3/ 2000.
206. Вујаклија М, Лексикон страних речи и израза, Просвета, Београд, 1996.
207. Вукадиновић, Д., Fuzzy Control Systems, Сплит, Хрватска, 2012.
208. Иванова, Ј.Т, Приходко, И.В, Теорија организације, друго стереотипно издање, Факултет заштите на раду, Ниш, 2007.
209. Пирц-МусарН., Водич кроз Закон о заштити података о личности, издање Повереника за информације од јавног значаја и заштиту података о личности Републике Србије, 2009.
210. Перинић, Ј., Кризно комуницирање на случају трагедије ватрогасаца на Корнату, Свеучилиште у Дубровнику, Дубровник, 2007.
211. Путник, Н., Сајбер простор и безбедносни изазови, Београд, Факултет безбедности, стр. 62, 2009.
212. Prezelj, I., Lipicer K.S., Public and Policy Management of Critical Infrastructure: Lessons from Integral Nations Cross-Sectoral Scanning in Slovenia, IRSPM Conference, Panel: Risk and Crisis Management in the Public Sector, Berne, 2010.
213. Rashed T., Weks J., Assessing vulnerability to earthquake hazards through spatial multicriteria analysis of urban areas, International Journal of Geographical Information Science, 2003.
214. Sapriel, C., Effective Crisis Management: Tools and Best Practice for the New Millennium, Journal of Communication Management, Vol. 7, No. 4, 2003.

215. Симонов, К., Глобални енергетски рат - тајне савремене политике, Москва, 2007.
216. Стевановић, О., Руковођење у полицији, Полицијска академија, Београд, 2003.
217. Стратегија националне сигурности Републике Хрватске, Народне Новине, бр. 32/2002.
218. Стратегија развоја информационог друштва у Републици Србији до 2020, Влада РС, 2010.
219. Стратегија развоја поштанских услуга у Републици Србији за период од 2013. до 2016. године, Влада Републике Србије.
220. Субошић, Д., Организација и послови полиције, Криминалистичко-полицијска академија, Београд, 2010
221. Tagarev, T., The Art of Shaping Defense Policy: Scope, Components, Relationships (but no algorithms), The Quarterly Journal 5, No.1, Spring-Summer, 2006
222. Таталовић, С., Енергетска сигурност и критична инфраструктура, Загреб, Политичка култура, 2008
223. Twigg J., Bhatt M. R., Understanding Vulnerability: South Asian Perspectives, 1998.
224. Wahle, T., Beaty, G., Emergency Management Guide for Business&Industry, Federal Emergency Management Agency (FEMA), Internet edition, 2004.
225. Water Critical Infrastructure and Key Resources Sector - Specific Plan as Input to the National Infrastructure Protection Plan, Homeland Security, Environmental Protection Agency, May, 2007.
226. William, J.C., Protecting America's Critical Infrastructures: Presidential Decision Directives 62 and 63, Washington, 1998.
227. William, J.C., Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0, An Invitation to a Dialogue, Washington, 2010.
228. Đorđević G., Uticaji ICT informacionog društva na društveno - ekonomski

razvoj, Socioeconomica - The Scientific Journal for Theory and Practice of Socioeconomic, 2012.

229. Завишић Ж., Билић И., Завишић С., Интерна комуникација у кризним ситуацијама, Зборник радова „Дани кризног управљања“, Велика Горица, Хрватска, 2011.
230. Зутер, Б., Стратешки кризни менаџмент Швајцарске - поређење швајцарског модела са девет страних референтних држава, Војно дело, јесен/2011, Београд, 2011.
231. Zimmerman, R., Decision-making and the Vulnerability of Interdependent Critical Infrastructure, IEEE Control Systems Magazine, 2004.
232. Чупић Е.М, Тумала Р.М.В, Савремено одлучивање - метода и примена, Научна књига, Београд, 1991.
233. Чемерин, Д., Управљање критичним инфраструктурама, Зборник радова, 4. међународна конференција, „Дани кризног управљања“, Велеучилиште Велика Горица, 2011.
234. Чемерин, Д., Трут, Д., Критерије за утврђивање хрватске критичне инфраструктуре, Зборник радова „Хрватска платформа за смањење ризика од катастрофа“, Државна управа за заштиту и спашавање, Загреб, 2010.

II ЗАКОНСКИ И ПОДЗАКОНСКИ ПРОПИСИ

1. 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, pp. 345-375, 2008
2. Council of Europe Convention on Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108.
3. Council of Europe: Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines, Project report, 2008.
4. Council of Europe: ETS 185, Convention on Cybercrime, 2001.
5. 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, 23.12.2008., L 345/75-L 345/82.
6. Council Conclusions of 9-10 June 2011 on the development of the external dimension of the European Programme for Critical Infrastructure Protection
7. Council of Europe: Special investigative means in South-eastern Europe, PACO SIMS Project report, 2003.
8. Directive 2002/58 of the European Parliament and Council concerning the processing of personal data and the protection of privacy in electronic communications networks and services
9. Directive 2006/24 of the European Parliament and Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58.
10. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
11. ETSI ETR 237: Baseline security standards; Features and mechanisms, 1996.
12. ETSI TS 101 331 V1.1.1 (2001-08) Lawful Interception; Requirements of Law Enforcement Agencies.

13. ETSI TS 102 656 V1.1.2 (2007-12) Requirements of Law Enforcement Agencies for handling Retained Data.
14. European Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C43/02).
15. European Council Resolution of 18 February 2003 on the implementation of the Europe 2005 Action Plan (2003/C 48/02).
16. European Commission, Commission staff working document on the review of the European Council Resolution of 18 February 2003 on European approach towards a culture of network and information security (2003/C 48/01).
17. European Programme for Critical Infrastructure Protection (EPCIP), European Commission, 2012.
18. European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications.
19. Executive Order 13010 - Critical Infrastructure Protection, Federal Register, July 17, 1996. Vol. 61, No. 138. pp. 37347-37350.
20. ISO/IEC Guide 73, Risk Management - Vocabulary - Guidelines for use in standards, 2002.
21. Национална стратегија заштите и спасавања у ванредним ситуацијама, „Службени гласник РС“, бр. 86/2011.
22. Одлука о одређивању великих техничких система од значаја за одбрану „Службени гласник РС", бр. 15/09.
23. Правилник о садржини и обрасцу захтева за издавање водних аката и садржини мишљења у поступку издавања водних услова, „Службени гласник РС“, бр. 74/2010.
24. „Службени гласник РС“, бр. 104/2013 и 66/2015.
25. „Службени гласник РС“ бр. 104/13.
26. „Службени гласник РС“, бр. 101/2005, 63/2009, одлука УС и 92/2011.
27. „Службени гласник РС“, бр. 101/2005, 63/2009, одлука УС и 92/2011.
28. „Службени гласник РС“, бр. 18/92.

29. „Службени гласник РС“, бр. 86/2011.
30. „Службени гласникРС“, бр. 111/09, 92/2011 и 93/2012.
31. „Службени гласник“ РС, бр. 112/2009.
32. „Службени гласник“ РС, бр. 19/2009.
33. „Службени лист СРЈ“, бр. 43/94 и 28/96.
34. „Службени гласник РС“, бр. 4/2008.
35. „Службени гласник РС“, бр. 88 од 28.10.2009.
36. „Службени гласник РС“, бр. 15/2009, 54/2010, 4/2011 и 58/2011.
37. „Службени гласник РС“, бр. 68/10, 02.09.2010.
38. „Службени гласник РС“, бр. 18/05.
39. Стратегија развоја енергетике Републике Србије до 2025. године, са пројекцијама до2030. године, 2014.
40. Закон о безбедности и интероперабилности железнице, „Службени гласник РС“ бр. 104, 2013.
41. Закон о водама, „Службени гласник РС“, бр. 46/91, 53/93, 53/93-др. закон, 67/93 - др. закон, 48/94 - др. закон, 54/96 и 101/05 - др. Закон.
42. Закон о државном премеру и катастру, „Службени гласник РС“, бр. 72/09 и 18/2010.
43. Закон о заштити животне средине, „Службени гласник РС“, бр. 135/04, 36/09, 36/09 - др. закон и 72/09 - др. закон.
44. Закон о заштити од пожара, „Службени гласник РС“, бр. 111/2009.
45. Закон о здравственој заштити, „Службени гласник РС“, бр. 107/2005.
46. Закон о јавним предузећима и обављању делатности од општег интереса, „Службени гласник РС“, бр. 25/00, 25/02, 107/05, 108/05 - испр. и 123/07
47. Закон о јавном здрављу, „Службени гласник РС“, бр. 72/2009
48. Закон о метеоролошкој и хидролошкој делатности, „Службени гласник РС“, бр. 88/10.
49. Закон о министарствима, „Службени гласник РС“, бр. 44/2014.
50. Закон о општем управном поступку, „Службени лист СРЈ“, бр. 33/97 и

31/2001 и Службени гласник РС, бр. 30/2010.

51. Закон о полицији, „Службени гласник РС“, бр. 101/2005, 63/2009 - одлука УС и 92/2011.
52. Закон о превозу експлозивних материја, запаљивим течностима и гасовима, Службени гласник РС, бр. 44/77, 45/85 и 18/89 и „Службени гласник РС“, бр. 53/93, 67/93, 48/94 и 101/2005 - др. закон.
53. Закон о Републичком сеизмолошком заводу, „Службени гласник РС“, бр. 71/94.
54. Закон о слободном приступу информацијама од јавног значаја, „Службени гласник РС“, бр. 120/04, 54/07, 104/09 и 36/2010.
55. Закон о средствима у својини РС, „Службени гласник РС“, бр. 53/95, 3/96, 54/96, 32/97, 101/05 - др. закон.
56. Закон о транспорту опасног терета, „Службени гласник РС“, бр. 88/10.
57. Закон о заштити становништва од заразних болести, „Службени гласник РС“, бр. 125/04.
58. Закон о ванредним ситуацијама и цивилној заштити, „Службени гласник РС“, бр. 111/09.
59. Закон о заштити животне средине, „Службени гласник РС“, бр. 135/04, 36/09, 72/9.
60. Закон о полицији, „Службени гласник РС“, бр. 101/05.
61. Закон о државној управи, „Службени гласник РС“, бр. 101/07.
62. Закон о стечају, „Службени гласник РС“, бр. 104/09.
63. Закон о ванредним ситуацијама, „Службени гласник РС“, бр. 111/09 и 92/11.
64. Закон о заштити од пожара, „Службени гласник РС“, бр. 111/09.
65. Закон о јавним набавкама, „Службени гласник РС“, бр. 116/08.
66. Закон о заштити животне средине, „Службени гласник РС“, бр. 135/2004, 36/2009, 36/2009 - др. закон, 72/2009 - др. закон и 43/2011 - одлука УС.
67. Закон о министарствима, „Службени гласник РС“, бр. 43/07.

68. Закон о Влади, „Службени гласник РС“, бр. 55/05, 71/05 - исправка, 101/07 и 65/08.
69. Закон о планирању и изградњи, „Службени гласник РС“ бр. 72/09, 81/09, 64/2010-одлука УС и 24/2011.
70. Commission Decision (2008/324/EC) of 25 March 2008 setting up the “Platform of Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime” group of experts.
71. Закон о критичним инфраструктурама Републике Хрватске, 28.05.2013. године.
72. Закон о водама, „Службени гласник РС“, бр. 30/10.
73. Упутство о методологији за израду процене угрожености и планова заштите и спасавања у ванредним ситуацијама, „Службени гласник РС“, бр. 96/2012.
74. Устав РС, „Службени гласник РС“, бр. 98/2006.

III ИНТЕРНЕТ АДРЕСЕ

1. http://www.asisonline.org
2. http://www.cip.gmu.edu
3. http://www.cscic.state.ny.us
4. http://www.dhs.gov
5. http://www.ec.europa.eu
6. http://www.fema.gov
7. http://www.gao.gov
8. http://www.mod.gov.rs
9. http://www.mup.gov.rs
10. http://www.nap.edu
11. http://www.nfpa.org
12. http://www.oecd.org
13. http://www.oecd.org
14. http://www.sarma.org
15. http://www.steelcityre.com
16. http://www.tisp.org
17. http://www.toffler.com
18. http://www.transition.fcc.gov
19. http://www.un.org/en/ecosoc
20. http://www.unece.org
21. http://www.unep.org
22. http://www.vma.mod.gov.rs
23. http://www.vs.rs/
24. http://www.westgov.org
25. http://www.whitehouse.gov
26. http://www.who.int/en

ПРИЛОЗИ

Прилог 1. Анкетни упитник

1. Пол: М Ж

2. Старосна група којој припадате је у интервалу:

- до 35 година
- од 36 до 45 година
- више од 45 година

3. Наведите област радног/стручног ангажовања (наведите реферат/послове које обављате):

_____

_____

4. Наведите шта се подразумева под критичном инфраструктуром?

_____

_____

5. Колико година се бавите пословима везаним за заштиту и спасавање?

_____

_____

6. Оцените значај критичне инфраструктуре за управљање и превазилажење последица ванредне ситуације:

- Изузетно велики значај
- Велики значај
- Мали значај
- Нема значај
- Не могу да оценим

НОРМАТИВНО-ПРАВНА РЕГУЛАТИВА У ОБЛАСТИ ЗАШТИТЕ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

7. Да ли сматрате да је критична инфраструктура и њено функционисање у условима ванредне ситуације довољно нормативно-правно регулисано?

- Да
- Не

- Не могу да оценим

8. Да ли је, према Вашем мишљењу, постојећа законска регулатива адекватна савременим опасностима и потребама заштите и спасавања у условима ванреднихситуација?

- Јесте у потпуности
- Углавном јесте
- Недовољна је
- Не могу да је оценим

9. Да ли је по Вашем мишљењу неопходно (променити, усвојити) још неке законске прописе у области заштите и спасавања?

- Да, навести које

_____

- Не
- Делимично
- Не могу да се одредим по овом питању

10. Да ли израда нормативно-правне регулативе у области заштите и спасавања треба да буде заједнички посао субјеката различитих профила (нпр. стручно-оперативни органи из области заштите и спасавања, здравствене службе, ватрогасно-спасилачких јединица МУП, ВС, стручњаци из области заштите животне средине, радници државних органа управе и безбедносних структура БИА, ВБА или ВОА)?

- Неопходна је сарадња међу њима
- Сарадња није неопходна
- Немам мишљење о овом питању

ПРОЦЕНА ОПАСНОСТИ КРИТИЧНЕ ИНФРАСТРУКТУРЕ

11. Да ли је спроведена процена ризика у Вашем предузећу?

- Да
- Не
- Делимично
- Не могу да се одредим по овом питању

12. **Наведите три потенцијална ризика који могу довести до ванредне ситуације у Вашем предузећу?**

a) _____

b) _____

c) _____

13. Да ли постоји могућност угрожавања Вашег привредног субјекта од нуклеарних, хемијских или биолошких терористичких радњи?

- Да
- Не
- Не могу да оценим

14. **Оцените степен опасности од природних и техничко-технолошких ризика у Вашој средини?**

- Веома висок
- Висок
- Средњи
- Низак
- Не могу да оценим

15. **По Вашем мишљењу који од објеката критичне инфраструктуре су најугроженији у условима ванредне ситуације?**

- Енергетски објекти
- Индустријски објекти
- Објекти водопривреде
- Телекомуникације
- Војни објекти
- Аеродроми
- Објекти државних институција
- Путне комуникације (путеви, железничке пруге, мостови)
- Метрои и станице подземне железнице
- _____

16. **Да ли је критична инфраструктура изложена потенцијалним терористичким нападима и којим (која средства би била по вашем мишљењу употребљена)?**

- Конвенционална (класична)
- НХБ (нуклеарна, хемијска, биолошка)
- Импровизована

17. Можете ли навести шта садржи процена ризика?

_____

_____

18. Који би се критеријуми, по Вашем мишљењу, могли користити за оцену степена ефикасности јединица за отклањање последица ванредне ситуације:

а) ефективност
б) економичност
в) координација
г) опремљеност
д) покретљивост
ђ) обученост
е) ефикасност

19. Наведите нека од Ваших искустава везаних за послове заштите и спасавање, тј. отклањања последица ванредне ситуације:

_____

_____

СТРУКТУРА И ОРГАНИЗАЦИЈА СТРУЧНО-ОПЕРАТИВНИХ ОРГАНА

20. Каква је образовна структура стручно-оперативног органа у коме сте радно (стручно) ангажовани?

- Висока стручна спрема _____ члан(ов)а
- Виша стручна спрема _____ члан(ов)а
- Средња стручна спрема _____ члан(ов)а

21. Колико је искуство Вашег стручно - оперативног органа у управљању ванредним ситуацијама?

- 0 – 10 година _____ члан(ов)а
- 11– 20 година _____ члан(ов)а
- 21– 30 година _____ члан(ов)а
- преко 30 година _____ члан(ов)а

22. Каква је стручна оспособљеност чланова Вашег стручно-оперативног органа из области цивилне заштите?

- Завршен факултет из наведених области _____ члан(ов)а
- Завршена специјализација из наведених области _____ члан(ов)а
- Мастер, Магистратура, докторат из ових области _____ члан(ов)а
- Завршен курс/семинар/радионица _____ члан(ов)а

23. Да ли су чланови Вашег стручно-оперативног органа образовани и

обучавани за област одбране од ванредних ситуација?

- Да
- Не

24. Да ли се постојећим плановима предвиђа отклањање последица терористичких аката?

- Да
- Не
- Не могу да оценим

СРЕДСТВА И ОПРЕМА ЗА ОТКЛАЊАЊЕ ПОСЛЕДИЦА ТЕРОРИСТИЧКИХ АКАТА

25. Да ли постојећи субјекти (нпр. Војска, Сектор за ванредне ситуације МУП, јавне службе) поседују адекватна средства и опрему за отклањање последица терористичких аката насталих конвенционалним оружјем?

- Да
- Делимично
- Не
- Не могу да оценим

26. Да ли наведени субјекти у претходном питању поседују адекватна средства и опрему за отклањање последица терористичких аката насталих нуклеарним, хемијским или биолошким оружјем?

- Да
- Не
- Само део адекватних средстава
- Не могу да оценим

ФУНКЦИОНИСАЊЕ И САРАДЊА СА ИНСТИТУЦИЈАМА

27. Да ли имате припремљене планове за управљање ванредним ситуацијама?

- Да
- Не
- Не знам

28. Да ли имате посебне планове за управљање у условима испољених терористичких аката?

- Да
- Не
- Не знам

29. Оцените досадашњу сарадњу са институцијама у току ванредних ситуација од 1 до 5 (1 - најнижа оцена; 5 - највиша оцена)

На државном нивоу	Оцена	На локалном нивоу	Оцена
Министарство одбране		Здравствена служба	
Министарство унутрашњих послова		Ватрогасно-спасилачке јединице (Сектор за ванредне ситуације МУП)	
Министарство за енергетику, развој и заштиту животне средине		Центар за социјални рад	
Министарство за финансије и привреду		Центар за обавештавање	
Министарство грађевинарства и урбанизма		Општински органи управе	
Министарство здравља		Јавна комунална предузећа	
Министарство пољопривреде, шумарства и водопривреде – Дирекција за воде		Медији	

30. Да ли управљање системом интегрисане заштите у отклањању последица напада на критичну инфраструктуру треба да се заснива на:

- Сопственом моделу заштите и спасавања
- Страним искуствима у овој области
- Комбиновању страних искустава са сопственим
- Не знам

31. Да ли се уз добро пројектован систем интегрисане заштите, који би био резултат ангажовања и координације субјеката различитих профила, последице од терористичких аката могу битно умањити?

- Да
- Не
- Не могу се одредити по овом питању

32. Наведите ко треба да чини окосницу планирања и управљања системом интегрисане заштите?

_____

_____

33. Наведите стручно-оперативни орган који би руководио и спроводио координацију активности на отклањању последица неке ванредне ситуације?

- Штабови за ванредне ситуације? Који чине

_____

_____

Штаб цивилне заштите више не постоји (њихове ингеренције је преузео Сектор за ванредне ситуације МУП), последице терористичких аката отклања држава, односно влада која формира штабове за ванредне ситуације које чине (Војска, Сектор за ванредне ситуације МУП, Жандармерија, Црвени крст, Здравствене службе, Горска служба спасавања и сви остали субјекти друштва за заштиту грађана који могу да помогну у зависности од последица терористичког акта).

34. Наведите Ваше виђење проблема/потешкоћа везаних за област управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре:

_____

_____

35. Наведите Ваше сугестије у области управљања системом интегрисане заштите у отклањању последица нарушавања критичне инфраструктуре о неком питању које није обухваћено овим упитником:

_____

_____

ПОТПИС:

_____

Прилог 2. Приказ модела процене угрожености критичне инфраструктуре у ванредним ситуацијама

За потребе израде ове докторске дисертације спроведена је анализа реализоване процене угрожености привредног друштва „Термоелектране Никола Тесла“. Основни разлог зашто је изабрано ово привредно друштво се огледа у чињеници да је од виталног значаја за нормално функционисање енергетског система Београда и околине и да је битан део укупног система критичне инфраструктуре.

ОПИС, ПОЛОЖАЈ И КАРАКТЕРИСТИКЕ ЛОКАЦИЈЕ ПРИВРЕДНОГ ДРУШТВА „ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА“

Географски положај-окружење

Привредно друштво „Термоелектране Никола Тесла“ д.о.о. Обреновац („ТЕНТ“ д.о.о.).
Адреса седишта (дирекције): Богољуба Урошевића Црног 44
Место: Обреновац
Организациона подела: број организационих целина: 5 (пет)
Укупна површина територије коју покрива ПД је 1.472 ha

Називи организационих целина

1) ТЕНТ доо Обреновац - Термоелектрана Никола Тесла А - огранак (**ТЕНТ А**),
2) ТЕНТ доо Обреновац - Термоелектрана Никола Тесла Б - огранак (**ТЕНТ Б**),
3) ТЕНТ доо Обреновац - ТЕ Колубара-огранак (**ТЕ „Колубара“**),
4) ТЕНТ доо Обреновац - ТЕ Морава-огранак (**ТЕ „Морава“**) и
5) ТЕНТ доо Обреновац - Железнички транспорт - огранак.

Локације организационих целина у Републици Србији

ТЕНТ А

Термоелектрана „Никола Тесла А“ лоцирана је на десној обали реке Саве на око 40 km узводно од Београда, у непосредној близини Обреновца. На локацији ТЕНТ А смештено је седиште целог ПД као и центар управљања железничким транспортом угља и низ заједничких служби. Локација ТЕНТ А налази се на западном ободу Колубарског басена. Депонија пепела и шљаке налази се поред реке Саве узводно од главног погонског објекта електране уз одбрамбени насип реке Саве, заузима површину од око 400 ha и насипима је подељена на три касете.

Термоелектрана „Никола Тесла Б“ је лоцирана на десној обали Саве 59 km узводно од Београда између насеља Скела и Ушће, на подручју Ворбис на 15 km одОбреновца и око 18 km узводно од ТЕНТ А. Локација ТЕНТ Б заузима простор од 108 ha. Депонија пепела и шљаке налази се на локацији „Бивољача“, ненасељеном простору између насеља Ушћа, Дрен, Грабовац и Скела, 4,5 km удаљена од термоелектране. Заузима површину од 600 ha и насипима је подељена на 3 касете.

ТЕ „Колубара“

Локација ТЕ Колубара А налази се код места Велики Црљени, у долини реке Колубаре. ТЕ је удаљена око 45 km од Београда, у правцу југозапада. ТЕ „Колубара“ обухвата подручје општине Лазаревац.

ТЕ „Морава“

ТЕ Мораве налази се на десној обали Велике Мораве, на 2,8 km од града Свилајнаца и на удаљености од 110 km од Београда. Објекти ТЕ Морава се налазе на више катастарских парцела у КО Дубље и КО Црквац.

Железнички транспорт

Железнички транспорт (ЖТ) снабдева ТЕНТ „А“, ТЕНТ „Б“ и ТЕ „КОЛУБАРА“

угљем са површинских копова рударског, колубарског угљеног басена, док се ТЕ „МОРАВА“ снабдева угљем из површинских копова рударског, колубарског угљеног басена и подземне експлоатације ресавског угљеног басена.

Метеоролошко-климатске карактеристике локације

ТЕНТ А и ТЕНТ Б

Одлике климе

Обреновац се налази готово у средишту северног умерено топлог појаса, са климом блажом од типичне панонске, континенталне. Због потпуне отворености према северу и северозападу и непостојања изразитијих ортографских препрека, територија општине Обреновац се често налази под утицајем хладних ваздушних маса које преко северне и средње Европе лако продиру на југ. На временске прилике ове територије снажно утичу циклони који долазе из Ђеновског залива, крећу се долином Саве и даље, долином Дунава одлазе према Црном мору. Долине Дрине и Колубаре имају веома битну улогу у оријентацији ваздушних струјања за овај део Србије. Ваздушне масе обогаћене влагом, које долазе са северозапада, у суштини прате правац пружања Динарида. Међутим, бројни огранци главне струје, пратећи најповољније пролазе увлаче се у речне долине десних притока Саве које су углавном оријентисане у правцу север-југ.

Врсте и карактеристике ветрова

За општину Обреновац је карактеристичан ветар кошава. Лети је доминантан ветар из западно-северозападног правца, а у пролеће су подједнако заступљени источно-југоисточни и северозападни ветар. Зими и у јесен доминира источни ветар.

Годишњи број дана са јаким ветром у просеку износи 124, са максимумом у

марту (15 дана) и минимумом у августу (7 дана). Ветрови из северног и јужног квадранта у Обреновац ретко доносе падавине. На основу руже ветрова може се уочити да са аспекта ширења загађујућих материја највећи значај имају северозападни и западни ветрови, при чему ни они из југоисточног квадранта нису ништа мање опасни.

Просечне годишње температуре

Средња годишња температура ваздуха износи 11,2 °C. Најхладнији месец је јануар са средњом температуром ваздуха од -0,2 °C, а најтоплији јули са 21,6 °C. Апсолутно максимална температура ваздуха забележена је 6. јула и износи 42 °C, док је апсолутни минимум регистрован 10.01.1893. године и било је -26,2 °C, тако да апсолутно годишње колебање температуре износи чак 68,2 °C.

Падавине

Средња годишња количина падавина износи 686,7 mm. Месец са највише падавина је јун (91,9 mm), док је у просеку најсушнији октобар (43,6 mm).

ТЕ „Колубара“

Одлике климе

Клима је у овом подручју умерено континентална уз тридесетак дана у години са средњом дневном температуром испод нуле. За потребе површинских копова угља редовно се прикупљају подаци у метеоролошким станицама у Зеокама и Каленићу.

Врсте и карактеристике ветрова

Од ветрова у овој области преовлађују северно-источни ветрови. У почетку пролећа обично дува југо који често наноси штете воћу, јер се јавља у време цветања воћњака.

Просечне годишње температуре

На основу вишегодишњих мерења установљено је да су средње дневне температура ваздуха у току зиме 1,7 °C, током пролећа, 10,1 °C, лети 19,5 °C и током јесени 10,6 °C.

Средња месечна температура ваздуха најнижа је у јануару - пола степена изнад нуле, а највиша у јулу и августу када у просеку достиже 19,8 °C. Апсолутна минимална температура од минус 28,5 °C регистрована је на мерној станици Тамнава у јануару, а максимална у августу 1998. године, када је температура износила 39 °C.

Падавине

На овом подручју годишње пада око 750 mm воденог талога, највише у јуну а најмање у зимским месецима. Са 910 mm падавина, рекордер је 1977. година, док је водени талог 1983. године износио само 539 mm. Годишња осунчаност креће се између 1.900 и 2.300 сати. У касну јесен и зими дувају северозападни и источни ветрови, почетком пролећа југо, а у спарним летњим данима освежења али и непогоде може да донесе западњак који стиже из Посавине.

Планине у ширем окружењу - Авала, Космај, Букуља, Венчац, Рудник, Сувобор и Маљен - као природна брана, знатно утичу на климатске прилике у Лазаревачком крају.

ТЕ „Морава“

Одлике климе

Клима је умерено континентална, зиме хладне, а мразни период релативно дуг. Ово подручје се одликује великом учесталошћу кошаве.

Врсте и карактеристике ветрова

Ветар је најважнији елемент за транспорт примеса гасова и честица у атмосфери, па је, уз стабилност атмосфере, од изузетног значаја за транспорт

загађујућих материја и незаобилазни параметар у свим математичким моделима за процену дистрибуције аерозагађења. Максимална јачина ветра такође је од значаја за прорачун стабилности високих објеката (димњака, стубова и сл.). Типични параметри који се користе за карактеризацију струјања ваздуха на неком локалитету су честе смерова ветра (ружа ветра), средње брзине честине појединих класа брзина и честе појаве тишина.

Најучесталије дува северозападни ветар са особином да доноси главне количине падавина под утицајем ваздушних струја са Атлантског океана и Јадранског мора. Други по учесталости је југоисточни ветар - кошава. Трећи по значају је хладни северац. Основна карактеристика овог подручја је велика учесталост појаве кошаве. Кошава дува у просеку око 200 дана годишње и има веома јаке ударе.

Просечне годишње температуре

Просторна расподела температуре је од значаја за разумевање дистрибуције загађујућих материја у ваздуху. Средња годишња температура износи 11,2-11,7 °C. Средње месечне температуре ваздуха се крећу од 0,6 у јануару до 21,6 °C у јулу. Мразних дана, просечно годишње има око 80, а ледених 19. Највећа појава мразних и ледених дана је у јануару и фебруару, а тако је и у децембру. Ван зимског периода појава јаких приземних мразева најучесталија је у пролеће и знатно мање у јесен. Учесталост топлих дана са максималном температуром изнад 25 °C највећа је у јулу и августу, а веома топлих дана са максималном температуром изнад 30 °C највише има у августу.

Падавине

Падавине су метеоролошки елемент чије се вредности јако мењају на малом растојању, а такође и јако варирају од године до године. Расподела по годишњим добима показује да је највише падавина у летњем периоду са просечном количином од 176,8 mm. После лета најкишовитије је пролеће са 170,5 mm, јесен 148,8 mm, а најмање падавина има зими 135,8 mm.

ДЕЛАТНОСТ ПРИВРЕДНОГ ДРУШТВА „ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА“

ПД ТЕНТ је највећи произвођач електричне енергије у Југоисточној Европи. Има 14 блокова чија је укупна инсталисана снага 3.288 MW, што је једна трећина инсталисаних капацитета „Електропривреде Србије“, и годишње произведе више од 50 % српске електричне енергије.

Основна делатност ПД ТЕНТ је дефинисана у складу са Законом о енергетици „Службени гласник РС“, бр. 145/2014 од 29.12.2014. године.

Основни параметри пословања

Прву деценију овог века ПД ТЕНТ је посветило модернизацији са ревитализацијом постројења и сталним активностима на повећању енергетске ефикасности. Блоковима ТЕНТ А-6 и А-5 и Б-1 је повећана снага. Захваљујући највише ревитализацији постројења, ПД ТЕНТ је у 2011. години произвело рекордних 20 милијарди 205 милиона kWh електричне енергије. То је највише што су икада заједно произвеле 4 термоелектране у саставу ПД ТЕНТ. Железнички транспорт је, такође, оборио рекорд у довозу угља - више од 29 милиона тона.

Намена и коришћење површина

Намена и коришћење површина се односи на:

ТЕНТ А

У оквиру комплекса **ТЕНТ А**, а на основу ПГР земљиште је подељено на јавно грађевинско и остало грађевинско. Цео простор је подељен на 4 целине:

Целина 1- погонски објекти,

Целина 2 -складишни простор,

Целина 3 - административни садржај,

Целина 4 - депонија пепела и шљаке.

ТЕНТ Б

У оквиру комплекса **ТЕНТ Б**, а на основу ПГР земљиште је подељено на јавно грађевинско и остало грађевинско. Цео простор је подељен на 3 целине:

Целина 1 - круг **ТЕНТ Б**,
Целина 2 - инфраструктурни коридор од круга до депоније,
Целина 3 - депонија пепела и шљаке.

ТЕ „Колубара“

ПГР за објекте ТЕ Колубара обухваћени су: круг ТЕК, депонија пепела и шљаке (касете 1,2), шума на локацији Волујак, црпна станица Пештан, насеље ТЕК, спортски центар, постројење за прераду питке воде, водозахват, изворište и бунари, исправљачка станица Вреоци, као и простор уз постојећу депонију планиран за њено проширење (Касета Ц). У оквиру наведеног извршена је подела на целине и подцелине.

ТЕ „Морава“

Простор на коме се налази ТЕ Морава обухваћен је ПГР за насеље Свилајнац. Овим планом простор ТЕМ дефинисан је као индустријска зона где је дозвољена изградња.

Укупан број запослених у ПД ТЕНТ

- Мушкарци 2025,
- Жене 328,
- Укупно 2353,
- Инвалиди 48,

Квалификациона структура

- магистри 4,
- инжењери 425,

- техничари 1231,
- монтери 689,
- помоћно особље 104,

Оспособљеност са аспекта заштите и спасавања

- заштита од пожара:2353
- прва медицинска помоћ861
- заштита на раду 2353
- опште реаговање у ванредним ситуацијама 2353

Повредиви објекти у окружењу

ТЕНТ А

1. СТАМБЕНИ ОБЈЕКТИ

- 29 насеља на територији ГО Обреновац: Баљевац, Барич, Бело Поље, Бргулице, Бровић, Дражевац, Дрен, Грабовац, Јасенак, Конатице, Кртинска, Мала Моштаница, Мислођин, Обреновац, Орашац, Пироман, Пољане, Љубинић, Ратари, Рвати, Скела, Стублине, Трстеница, Уровци, Ушће, Велико Поље, Вукићевица, Забрежје и Звечка.

2. ПРИВРЕДНИ ОБЈЕКТИ У ОКРУЖЕЊУ

- ЈП „Електромрежа Србије“,
- Комбинат „Драган Марковић“,
- „Биопротеин - Уљарица“,
- „Силос“.

ТЕНТ Б

- РЕИК,
- индустријски комплекс „Прва Искра“ Барич.

3. ШКОЛЕ И ПРЕДШКОЛСКЕ УСТАНОВЕ

- ОШ „Јован Поповић“ у Обреновцу,
- ОШ „Јован Јовановић Змај“ у Обреновцу,
- ОШ „Посавски партизани“ у Обреновцу,
- ОШ „Живојин Перић“у Стублинама,
- ОШ „Дражевац“ у Дражевцу,
- ОШ „14. Октобар“ у Баричу,
- ОШ „Скела“ у Скели,
- ОШ „Душан Полексић“ у Грабовцу,
- ОШ „Ратари“ у Ратарима,
- Гимназија у Обреновцу,
- Пољопривредно-хемијска школа у Обреновцу,
- Техничка школа у Обреновцу,
- ПУ „Перка Вићентијевић“ (5 вртића).

4. ЗДРАВСТВЕНЕ УСТАНОВЕ

- Дом Здравља Обреновац

Здравствене станице:

- Стублине бб,
- Грабовац бб,
- Дражевац бб,
- Кртинска, Младост бб,
- Ушће, Дуго поље 1,
- Скела, Шабачки пут бб,
- Звечка, Д. Вуковића Корчагина бб,
- Забрежје, Радничка 1,

- Мала Моштаница.

Дом за старе

- Установа за ометене у развоју

5. СПОРТСКИ И РЕКРЕАТИВНИ ПРОСТОРИ

- Дом културе Обреновац

6. ПРИРОДНА И КУЛТУРНА ДОБРА

Културна добра од великог значаја

Споменици културе

- Чесни дом породице Михаиловић, Маршала Тита 184, Обреновац (Одлука, „Сл. гласник СРС“ бр. 14/79)

Културна добра

Споменици културе

- Црква брвнара у Орашцу, Обреновац (Решење Завода бр.654/5 од 22.12.1965),
- Црква Св. Духа у Обреновцу, ул. Мила Марића, Обреновац (Решење Завода бр. 739/2 од 15.08.1975.),
- Кућа у којој се родио Народни херој Влада Аксентијевић, Маршала Тита 27 (по решењу бр. 147), Обреновац (Решење Завода за заштиту и научно проучавање споменика културе НРС бр. 372/50 од 07.04.1950.),
- Кућа у селу Дражевцу, Обреновац, (Решење Завода заштиту и научно проучавањеспоменика културе НРС, бр. 525/49 од 28.04.1949.)
- Механа Узун Мирка Апостоловића, Мислођин, Обреновац (Решење Завода бр.627/1 од 05.07.1966.),
- Споменик стрељаним таоцима у Скели, Обреновац (Одлука о проглашењу,

„Сл.лист града Београда“, бр. 16/87),

- Стара механа у Ушћу, Обреновац (Решење Завода бр. 638/2 од 16.07.1968.)
- Стара основна школа у Конатицама, к.б.217, Обреновац (Решење Завода бр. 553/3 од 19.06.1969.),
- Стара варошка кућа у Обреновцу, Маршала Тита 188 (Решење Завода бр. 1129/2 од 16.8.1975.),
- Стара задружна кућа Ранковића у Дражевцу, Обреновац (Одлука о проглашењу, „Сл.лист града Београда“, бр. 16/87)
- Манастир Грабовац (Одлука, „Службени гласник РС“, бр. 115/05)
- Црква Св. Вазнесења у Дрену (Одлука, „Службени гласник РС“, бр. 115/05),
- Црква Покрова Пресвете Богородице у Баричу, Обреновачки пут 134, (Одлука, „Сл.гласник РС“, бр. 115/05),
- Соколски дом, Војводе Мицка 228, Обреновац,
- Зграда Старог касационог суда, Мила Манића 14, Обреновац,
- Зграда Старе гимназије, Мила Манића 12, Обреновац,
- Зграда железничке станице, Обреновац,
- Зграда отправника возова, Обреновац,
- Стари млин, Обреновац,
- Основна школа у Обреновцу, Обреновац,
- Црквине у селу Мислођину, Обреновац (Решење Завода за заштиту споменика културе града Београда бр. 1098/1 од 30.12.1968.),
- Ушће реке Вукодраже, Обреновац, (Решење Завода за заштиту и научно проучавање споменика културе НРС бр. 279/50 од 16.02.1950.),

Добра која уживају статус претходне заштите

Објекти градске архитектуре

- Соколски дом, Војводе Мицка 228, Обреновац,
- Зграда Старог касационог суда, Мила Манића 14, Обреновац,
- Зграда Старе гимназије, Мила Манића 12, Обреновац,
- Зграда железничке станице, Обреновац,

- Зграда отправника возова, Обреновац,
- Стари млин, Обреновац,
- Основна школа у Обреновцу, Обреновац,

Објекти сакралне архитектуре

- Манастир Грабовац са црквом Св. Николе, Обреновац
- Црква покрова Богородице, Стублине
- Црква Рођења Богородице, Звечка

Археолошка налазишта

- Црквине у селу Мислођину, Обреновац (Решење Завода за заштиту споменика културе града Београда бр. 1098/1 од 30.12.1968.),
- Ушће реке Вукодраже, Обреновац, (Решење Завода за заштиту и научно проучавањеспоменика културе НРС бр. 279/50 од 16.02.1950.).

Природна добра

- Резервати природе - Обедска бара, Кључ, Шаранка, Горње њиве,
- Резервати природе Кључ, Шаранка и Горње њиве,
- Споменик природе ботаничког карактера - Група стабала храста лужњака код Јозића колибе.

7. ПОВРШИНСКЕ И ПОДЗЕМНЕ ВОДЕ

- реке Сава, Колубара и Тамнава,
- водотоци Баричка река, Црквиште, Дубоко, Елаб, Царевац и Јашовица.

ТЕНТ Б

1. СТАМБЕНИ ОБЈЕКТИ:

- 29 насеља на територији ГО Обреновац: Баљевац, Барич, Бело Поље,

Бргулице,Бровић, Дражевац, Дрен, Грабовац, Јасенак, Конатице, Кртинска, Мала Моштаница, Мислођин, Обреновац, Орашац, Пироман, Пољане, Љубинић, Ратари, Рвати, Скела Стублине, Трстеница, Уровци, Ушће, Велико Поље, Вукићевица, Забрежје и Звечка.

2. ПРИВРЕДНИ ОБЈЕКТИ У ОКРУЖЕЊУ

- ЈП „Електромрежа Србије“,
- комбинат „Драган Марковић“,
- „Биопротеин-Уљарица“,
- „Силос“,
- ТЕНТ А,
- РЕИК,
- индустријски комплекс „Прва Искра“ Барич.

3. ШКОЛЕ И ПРЕДШКОЛСКЕ УСТАНОВЕ

- ОШ „Јован Поповић“ у Обреновцу,
- ОШ „Јован Јовановић Змај“ у Обреновцу,
- ОШ „Посавски партизани“ у Обреновцу,
- ОШ „Живојин Перић“ у Стублинама,
- ОШ „Дражевац“ у Дражевцу,
- ОШ „14. Октобар“ у Бариу,
- ОШ „Скела“ у Скели,
- ОШ „Душан Полексић“ у Грабовцу,
- ОШ „Ратари“ у Ратарима,
- Гимназија у Обреновцу,
- Пољопривредно-хемијска школа у Обреновцу,
- Техничка школа у Обреновцу,
- ПУ „Перка Вићентијевић“ (5 вртића).

4. ЗДРАВСТВЕНЕ УСТАНОВЕ

- Дом Здравља Обреновац

Здравствене станице:

- Стублине бб,
- Грабовац бб,
- Дражевац бб,
- Кртинска, Младост бб,
- Ушће, Дуго поље 1,
- Скела, Шабачки пут бб,
- Звечка, Д. Вуковића Корчагина бб,
- Забрежје, Радничка 1,
- Мала Моштаница,
- Дом за старе,
- Установа за ометене у развоју.

5.СПОРТСКИ И РЕКРЕАТИВНИ ПРОСТОРИ

- Дом културе Обреновац

6.ПРИРОДНА И КУЛТУРНА ДОБРА

У широј околини (радијус 25 km) ТЕ „Никола Тесла“- Б налазе се следећи објекти који се налазе у надлежности Завода за заштиту споменика културе града Београда:

Културна добра од великог значаја

Споменици културе

- Чесни дом породице Михаиловић, Маршала Тита 184, Обреновац (Одлука, „Сл. гласник СРС“ бр. 14/79).

Културна добра

Споменици културе

- Црква брвнара у Орашцу, Обреновац (Решење Завода бр. 654/5 од 22.12.1965.)
- Црква Св. Духа у Обреновцу, Ул. Мила Марића, Обреновац (Решење Завода бр. 739/2 од 15.08.1975.)
- Кућа у којој се родио Народни херој Влада Аксентијевић, Маршала Тита 27 (Решење бр. 147), Обреновац (Решење Завода за заштиту и научно проучавање споменика културе НРС бр. 372/50 од 07.04.1950.)
- Кућа у селу Дражевцу, Обреновац, (Решење Завода заштиту и научно проучавање споменика културе НРС, бр. 525/49 од 28.04.1949.)
- Механа Узун Мирка Апостоловића, Мислођин, Обреновац (Решење Завода бр. 627/1 од 05.07.1966.)
- Споменик стрељаним таоцима у Скели, Обреновац (Одлука о проглашењу, „Службенилист града Београда“, бр. 16/87)
- Стара механа у Ушћу, Обреновац (Решење Завода бр. 638/2 од 16.7.1968.)
- Стара основна школа у Конатицама, к.б. 217, Обреновац (Решење Завода бр. 553/3 од 19.6.1969.)
- Стара варошка кућа у Обреновцу, Маршала Тита 188 (Решење Завода бр. 1129/2 од 16.8.1975.)
- Стара задружна кућа Ранковића у Дражевцу, Обреновац (Одлука о проглашењу, „Службени лист града Београда“, бр. 16/87)
- Манастир Грабовац (Одлука, „Службени гласник РС“, бр. 115/05)
- Црква Св. Вазнесења у Дрену (Одлука, „Службени гласник РС“, бр. 115/05)
- Црква Покрова Пресвете Богородице у Баричу, Обреновачки пут 134, (Одлука, „Службени гласник РС“, бр. 115/05)
- Соколски дом, Војводе Мицка 228, Обреновац
- Зграда Старог касационог суда, Мила Манића 14, Обреновац
- Зграда Старе гимназије, Мила Манића 12, Обреновац
- Зграда железничке станице, Обреновац
- Зграда отправника возова, Обреновац

- Стари млин, Обреновац
- Основна школа у Обреновцу, Обреновац
- Црквине у селу Мислођину, Обреновац (Решење Завода за заштиту споменика културе града Београда бр. 1098/1 од 30.12.1968.)
- Ушће реке Вукодраже, Обреновац, (Решење Завода за заштиту и научно проучавање споменика културе НРС бр. 279/50 од 16.2.1950.)

ДОБРА КОЈА УЖИВАЈУ СТАТУС ПРЕТХОДНЕ ЗАШТИТЕ

Објекти градске архитектуре

- Соколски дом, Војводе Мицка 228, Обреновац,
- Зграда Старог касационог суда, Мила Манића 14, Обреновац,
- Зграда Старе гимназије, Мила Манића 12, Обреновац,
- Зграда железничке станице, Обреновац,
- Зграда отправника возова, Обреновац,
- Стари млин, Обреновац,
- Основна школа у Обреновцу, Обреновац.

Објекти сакралне архитектуре

- Манастир Грабовац са црквом Св. Николе, Обреновац,
- Црква покрова Богородице, Стублине,
- Црква Рођења Богородице, Звечка.

Археолошка налазишта

- Црквине у селу Мислођину, Обреновац (Решење Завода за заштиту споменика културе града Београда бр. 1098/1 од 30.12.1968.),
- Ушће реке Вукодраже, Обреновац, (Решење Завода за заштиту и научно проучавање споменика културе НРС бр. 279/50 од 16.2.1950.).

Природна добра

- Резервати природе - Обедска бара, Кључ, Шаранка, Горње њиве,

- Резервати природе Кључ, Шаранка и Горње њиве,
- Споменик природе ботаничког карактера - Група стабала храста лужњака код Јозића колибе.

7. ПОВРШИНСКЕ И ПОДЗЕМНЕ ВОДЕ

- реке Сава, Колубара и Тамнава,
- водотоци Баричка река, Црквиште, Дубоко, Елаб, Царевац и Јашовица.

ТЕ „Колубара“

1. СТАМБЕНИ ОБЈЕКТИ:

Најближа насељена места су Велики Црљени, који се налазе непосредно уз ТЕ и Соколово, на удаљености од око 2 km од ТЕ у правцу исток-североисток. На удаљености до 5 km налазе се места Степојевац, Лесковац, Бељина, Арнајево, Рожанци, Араповац, Јунковац, Вреоци и Цветовац.

2.ШКОЛЕ И ПРЕДШКОЛСКЕ УСТАНОВЕ

- ОШ „Војислав Вока Савић“ у Лазаревцу,
- ОШ „Дуле Караклајић“ у Лазаревцу,
- ОШ „Кнез Лазар“ у Лазаревцу,
- Гимназија у Лазаревцу,
- Техничка школа у Лазаревцу,
- Раднички Универзитет.

2. ЗДРАВСТВЕНЕ УСТАНОВЕ

- Дом здравља „Др Ђорђе Ковачевић“ у Лазаревцу

Здравствене станице:

- Велики Црљени,
- Рудовци,

- Вреоци,
- Јунковац,
- Степојевац,
- Антитуберкулозни диспанзер у Лазаревцу,
- Породилиште у Лазаревцу.

3. СПОРТСКИ И РЕКРЕАТИВНИ ПРОСТОРИ

- КУД „Димитрије Туцовић”

4. ПРИРОДНА И КУЛТУРНА ДОБРА

- Спомен црква са костурницом у Лазаревцу,
- Библиотека „Димитрије Туцовић“.

5. ПОВРШИНСКЕ И ПОДЗЕМНЕ ВОДЕ

Реке:

- Колубара,
- Оњег,
- Љиг,
- Пештан,
- Турија,
- Бељаница,
- Лукавица.

ТЕ „Морава“

1. СТАМБЕНИ ОБЈЕКТИ:

- У општини Свилајнац има 22 насеља (један град и двадесет једно село).

2. ПРИВРЕДНИ ОБЈЕКТИ У ОКРУЖЕЊУ

- Tri Stan Fresh Produce,

- Green Only.

3. ШКОЛЕ И ПРЕДШКОЛСКЕ УСТАНОВЕ

Високе и више школе:

- Висока пословна школа струковних студија Чачак,
- Факултет еколошке пољопривреде Едуконс.

Средње школе у Свилајнцу:

- Пољопривредно-ветеринарска школа са домом ученика „Свилајнац“,
- Гимназија Свилајнац,
- Средња школа Свилајнац.

Основне школе у Свилајнцу:

- ОШ Јован Јовановић Змај Свилајнац

Остале основне школе у општини Свилајнац:

- ОШ Вожд Карађорђе Кушиљево,
- ОШ Бранко Радичевић Седларе,
- ОШ Стеван Синђелић.

4. ЗДРАВСТВЕНЕ УСТАНОВЕ

- Дом Здравља Свилајнац

5. ПРИРОДНА И КУЛТУРНА ДОБРА

- Споменик Мари Ресавкињи,
- Споменик Стевану Синђелићу,
- Алеја палих бораца,
- Кућа Стевана Синђелића.

Манастири:

- Манасија,
- Томић,
- Златенац,
- Миљков манастир.

6. ПОВРШИНСКЕ И ПОДЗЕМНЕ ВОДЕ
- реке Ресава и Велика Морава

Подаци о удесима

Хаварије

Подаци о хаварији:

- Локација: ТЕНТ д.о.о.
- Датум: 15/16.05.2014. год.
- Узрок: Поплава
- Последице: прекид процеса производње
- Висина материјалне штете: 440.654.725,96 дин.

Количине опасних материја

ТЕНТ А

Термоелектрана користи релативно малу количину опасних материја. Основне хемикалије које се користе у ТЕНТ А су:

- хлороводонична киселина - HCl 30-36 % (1341,6 t/год.),
- натријум хидроксид - NaOH 42 %, (773,1 t/год.),
- хидразин - N_2H_4 2 % (46,0 t/год.),
- амонијум хидроксид - NH_4OH 25 % (30,2 t/год.).

Као средства за одмашћивање се користе: фамин, трихлоретилен, петролеј и друго. Ова средства су смештена у затвореном простору складишта уља које је пројектовано за одређене количине.

ТЕНТ Б

Основне хемикалије које се користе у ТЕНТ Б су:

- хлороводонична киселина - HCl 30-36 % (416,5 t/год.),
- натријум хидроксид - NaOH 42 % (340 t/год.),
- хидразин - N_2H_4 2% и (26,4 t/год.),
- амонијум хидроксид - NH_4OH 25 % (17 t/год.).

ТЕ „Колубара“

ТЕ Колубара је у 2010. години извршила идентификацију количина опасних материја (ОМ) на својој локацији у складу са Правилником о Листи опасних материја и њиховим количинама и 18 критеријумима за одређивање врсте документа које израђује оператер Seveso постројења, односно комплекса („Службени гласник РС“ 41/10) и израдила „Обавештење о Seveso постројењу“ у складу са Правилником о садржини обавештења о новом Seveso постројењу односно комплексу, постојећем Seveso постројењу, односно комплексу и о трајном престанку рада Seveso постројења, односно комплекса („Службени гласник РС“, бр.41/2010). Након анализе количина свих присутних опасних материја у ТЕ Колубара, њихових особина ињихове класификације у одређене класе опасности, закључено је: ТЕ Колубара је Seveso постројење и сврстава се у групу постројења за која се израђује Политика превенције удеса, у смислу токсичности, у смислу запаљивости и у смислу еко-токсичности. ТЕ Колубара нема обавезу израде Извештаја о безбедности и Плана заштите од удеса. „Обавештење о Seveso постројењу“ за ТЕ Колубара је достављено Министарству животне средине и просторног планирања на сагласност 24.12.2010. године.

На основу Закона о заштити животне средине („Службени гласник РС“, бр. 135/04, 36/09 и 72/09) ТЕ Колубара спада у Seveso постројење нижег реда због коришћења хидразин хидрата. У складу са Правилником о садржини Политике превенције удеса и садржини и методологији израде Извештаја о безбедности и Плана заштите од удеса („Службени гласник РС“, бр. 41/10) фирма „Деконта“ је урадила „Политику превенције удеса за ТЕ Колубара

Велики Црљени.

У ТЕ Колубара се користе различите материје које би могле штетно утицати на човека и његову околину уколико би дошло до њиховог неконтролисаног испуштања у животну средину. Из тог разлога у електрани су предвиђене различите мере које обезбеђују безбедно коришћење ових материја, а истовремено делују и као превенција могућих хаваријских догађаја. Из тог разлога, неопходно је било сагледати потенцијалне изворе загађења, тј. врсте и количине штетних и опасних материја које се налазе у кругу електране.

На простору ХПВ се складиште следеће хемикалије:

- Хлороводонична киселина, HCl, се налази у резервоару запремине 37 m^3;
- Натријум-хидроксид, NaOH, се налази у резервоару запремине 37 m^3;
- Фери-хлорид, $FeCl_3$, се налази у резервоару запремине 63 m^3.

ТЕ „Морава“

Термоелектрана користи релативно малу количину опасних материјала. Хемикалије се користе за производњу декарбонисане и деминерализоване воде и то су: хидратисани креч, хлороводонична киселина 33 % и натријум хидроксид 45 %, а за технолошку обраду погонских вода користи се левоксин 15 или хидразин хидрат. Хидратисани креч смештен је у силос, киселине и лужине у четири гумирана челична резервоара капацитета 4×25 m^3. Левоксин 15 или хидразин хидрат смештен је у пластичну бурадод 200 L и налази се у магацину. По две цистерне са киселином и лужином смештене су у бетонским кадама и заштићене су епокси бојом. У случају хаварије бетонске каде могу да прихвате целокупну количину хемикалија које се могу пребацити у базен за неутрализацију. Претакање хемикалија врши се из ауто цистерни у доње цистерне, када је могуће изливање из истакачког места и загађење атмосферске канализације.

Водоник се користи за хлађење генератора. У употреби су боце (батерије) од 25 комада. Две батерије су смештене поред главног погонског објекта. Једна батерија је у употреби (прикључена на систем за допуну генератора), а једна је у резерви. Остале батерије су смештене у обезбеђени складишни простор.

Потрошња водоника на годишњем нивоу за 2014. годину износи 300/162 боца/kg.

Поред водоника, у употреби су и други гасови који се користе за заваривање и за избацивање водоника из генератора и то:

- Кисеоник (364 боце у 2014. год.),
- Ацетилен (160 боца у 2014. год.),
- Угљен диоксид (51 боца у 2014. год.),
- Аргон (15 боца у 2014. год.),
- Бутан (2 мале и 69 великих боца у 2014. год.).

Ови гасови су смештени у боцама, а боце које нису у употреби налазе се у обезбеђеном складишном простору.

Мазут и нафта

Мазут и нафта се користе за покретање блока (потпалу ватре у котлу) и за подршку ватре у току погона. У 2014. години потрошено је 1328 t мазута и 288 t нафте.

Складиштење мазута се врши у једном надземном резервоару капацитета 600 t смештеном у бетонску каду која, у случају хаварије, може да прими сву количину истеклог мазута. У оквиру помоћне котларнице, која се користи за старт погона, постоје два резервоара за мазут капацитета 2×25 t. Ови резервоари су повезани са главним резервоаром цевоводом који се налази у бетонском каналу. Мазут се до електране транспортује железничким или ауто цистернама и преко претакалишта и пумпи пребацује у главни резервоар.

Нафта се складишти у три надземна резервоара. Највећи резервоар је капацитета 200 t и смештен је у бетонску каду која, у случају хаварије, може да прими сву количину истекле нафте. Ова бетонска када није спојена ни са каквом канализацијом. Поред овог резервоара постоје још два надземна резервоара капацитета 6 t и 10 t, у које се складишти нафта која се користи као гориво за грађевинске машине и дизел локомотиве.

У оквиру помоћне котларнице, постоји један резервоар за нафту капацитета 25 t. Овај резервоар је повезан са надземним резервоаром цевоводом који се налази у заштићеном бетонском каналу.

Минерална уља

Нова и стара уља одлажу се у цистернама за турбинско уље капацитета 2 × 30 m^3 и у бурадима капацитета 200 L. Нова уља су смештена у хангару, а стара и рабљена на привременој депонији отпада. Бурад су постављена на дрвене палете, а палете на старе гумене траке и покривена су пластичном фолијом.

Средства за одмашћивање

Ова средства су смештена у затвореном простору складишта.

Водоснабдевање

ТЕ „Морава“

Бунари, црпне станице:

- број бунара: 2,
- број црпних станица: 1.

Хидрантска мрежа: 1407 (укупно ПД ТЕНТ)

- спољна хидрантска мрежа:
  - ТЕ Никола Тесла А: 74
  - ТЕ Никола Тесла Б: 102
  - ТЕ „Колубара“: 100
  - ТЕ „Морава“: 25
  - Железнички транспорт: 13
- унутрашња хидрантска мрежа
  - ТЕ Никола Тесла А: 257
  - ТЕ Никола Тесла Б: 573
  - ТЕ „Колубара“: 197

- ТЕ „Морава“: 18
- Железнички транспорт: 48

Објекти за склањање и здравствено збрињавање

Објекти за склањање у случају РХБ контаминације и техничко-технолошких несрећа:

- објекти за склањање људи основне и допунске заштите:

Локација ТЕНТ А и ЖТ

Укупно два склоништа основне заштите, укупног капацитета 400 места која се налазе у кругу електране. (склониште основне заштите 1 - зграда магацина опреме цивилне заштите, капацитета 200 места и склониште основне заштите 2 - зграда гардеробе допреме угља, капацитета 200 места), а сви путеви који воде до склоништа су увек проходни (нису закрчени). Склоништа су у добром стању, редовно се одржавају, а користе се двонаменски. Тренутно се у њима налазе архивски и други материјали али се у случају потребе склоништа доводе у стање потпуне употребљивости за три сата, по посебном наређењу директора ТЕНТ д.о.о.

Локација ТЕНТ Б

Укупно два склоништа основне заштите, укупног капацитета 400 места која се налазе у кругу електране. (склониште основне заштите 1 - зграда Ресторана друштвене исхране са склоништем основне заштите, капацитета 200 места и склониште основне заштите 2 - зграда гардеробе допреме угља, капацитета 200 места), а сви путеви који воде до склоништа су увек проходни (нису закрчени). Склоништа су у добром стању, редовно се одржавају, а користе се двонаменски. Тренутно се у њима налазе архивски и други материјали али се у случају потребе склоништа доводе у стање потпуне употребљивости за три сата, по посебном наређењу директора ТЕНТ д.о.о.

Локација ТЕ „Колубара“

Склањање радника није организовано на адекватан начин обзиром на значај објекта и производњу која се одвија. Не постоји одређен склонишни простор, нити су аналогно томе одређени руководиоци склоништа, па ће се користити природни и рововски заклони (2 заклона, 300 места). Могућа локација приручних склонишних простора био би канал цевовода испред техничке зграде који ако би се прекрио облицама стабала могао користити у краћем периоду. Проблем представља кишни период и могућност потапања. Као приручни објекти могу послужити и монтажне бараке и административна зграда.

Локација ТЕ „Морава“

Склањање радника није организовано на адекватан начин обзиром на значај објекта и производњу која се одвија. Не постоји одређен склонишни простор, нити су аналогно томе одређени руководиоци склоништа, па ће се користити природни и рововски заклони (2 заклона, 200 места).

Локација ТЕНТ А и ЖТ

Капацитети за РХБ деконтаминацију су: Купатила - број купатила 19; број тушева - број тушева 123. Цистерне са водом или резервоар - број цистерни 2, капацитет 4.000 L. Перионице - број перион. 1, капацитет 30.

Локација ТЕНТ Б, капацитети за РХБ деконтаминацију су:

Купатила - број купатила 8; број тушева - број тушева 51.
Цистерне са водом или резервоар - број цистерни 20, капацитет 10.000 L. Перионице - број перионица 1, капацитет 20 лица.

Локација ТЕ „Колубара“, капацитети за РХБ деконтаминацију су:

Купатила - број купатила 6,
Тушеви - број тушева 30 (вршиће се и деконтаминација возила, испред

гараже електране водом из хидранта).

Локација ТЕ „Морава“

Капацитети за РХБ деконтаминацију у Огранку ТЕМ су 4 купатила са тушевима.

Интерни објекти за здравствено збрињавање

Локација ТЕНТ А

Прва медицинска помоћ је организована на амбулантном принципу. Наиме, у ТЕНТ А постоји једна амбуланта у кругу електране. Капацитет тријаже 50 особа по сату (санитетом превоз 4 тешке и 20 лаких повреда у сату).

Локација ТЕНТ Б

Прва медицинска помоћ је организована на амбулантном принципу. Наиме, у ТЕНТ Б постоји једна амбуланта у кругу електране. Капацитет 10 особа по сату (санитетом превоз 1 тешке и 5 лаких повреда у сату).

Локација ТЕ „Колубара“

У кругу електране не постоји амбуланта, односно интерни објекат за здравствено збрињавање.

Локација ТЕ „Морава“

У кругу термоелектране постоји зграда здравственог центра (амбуланта), али нема запосленог особља.

Локације за екстерно збрињавање

Локација ТЕНТ А и ЖТ

За сложеније и масовније повреде или обољења ангажоваће се Дом здравља у Обреновцу или ће се пацијенти транспортовати у болнице града Београда. Капацитет транспорта ДЗ Обреновац санитетом 60 особа у сату.

Локација ТЕНТ Б

За сложеније и масовније повреде или обољења ангажоваће се Дом здравља у Обреновцу или ће се пацијенти транспортовати у болнице града Београда.

Локација ТЕК

Прва медицинска помоћ је организована преко амбуланте у Великим Црљенима Дома здравља из Лазаревца. Амбуланта је добро технички, материјално (санитетски материјал и лекови) и кадровски опремљена и може удовољити потребама радника ТЕК. Сви пацијенти који се не могу амбулантно санирати, упућују се за Београд на даље лечење у болничке центре. Апотекарска установа у Лазаревцу има и апотеку у Великим Црљенима која је солидно снабдевена.

Локација ТЕМ

За сложеније и масовније повреде или обољења ангажоваће се Дом здравља у Свилајнцу или ће се пацијенти транспортовати у медицинске центре у Ћуприји и Јагодини.

Опремљеност медицинским материјалом:

- санитетски материјал - локација ТЕНТ А и ЖТ и ТЕНТ Б, капацитети за 40 особа у датом моменту.

Саобраћајно-технолошка инфраструктура

Железничке станице и стајалишта:

ПРУГА (деоница): Обреновац - Стублине

ПРУГА (деоница): Стублине - Бргуле

ПРУГА (деоница): Бргуле - Вреоци

ПРУГА (деоница): Стублине - Ворбис

ПРУГА (деоница): Бргуле - Тамнава

ПРУГА (деоница): Сушара - ТЕК уплетени колосек.

Дужина пруга и станичних колосека индустријских железница:

- Укупна дужина пруга (km): 79,9
- Укупна дужина станичних колосека (без главних пролазних) (km): 16,3

Канализација и систем пречишћавања отпадних вода

Фекална канализација

ТЕ „Морава“

Прикључена на град Свилајнац

Технолошка канализација

Кишна канализација

ТЕНТ А

Техничка вода за производњу деми воде обезбеђује се из локалног изворишта подземних вода. Изворište има 14 бунара, тренутно укупног капацитета око 140m^3/L. Резерве изворишта су процењене на 52 L/s.

Систем расхладне воде је проточни, а потребне количине воде обезбеђују се захватањем воде из реке Саве. Захваћена вода се претходно пречишћава, најпре на грубој решетки а затим на тракастом ситу (фино пречишћавање).

Вода из реке Саве се користи за: хлађење паре у кондензаторима, хлађење разних уређаја, сакупљање и транспорт пепела и шљаке, противпожарну мрежу и хидрантску мрежу. За рад свих шест блокова ТЕНТ А потребно је 52 m^3/s расхладне воде.

Пијаћа вода обезбеђује се из ЈКП „Водовод и канализација Обреновац“. Потрошња ове воде је око 15 m^3/h.

Водовод и канализација

Изградња нових инфраструктурних објеката и реконструкција и одржавање постојећих мора се изводити у складу са условима наведеним у Плану генералне регулације.

Планом је обухваћен систем расхладне воде (захватање и испуст), систем техничке воде за ХПВ, систем пијаће воде и систем отпадних вода.

ТЕНТ Б

Низводно од локације ТЕ, на обали реке Саве налазе се рени бунари који се користе за водоснабдевање водом за пиће овог подручја и града Београда.

Канализациона мрежа

Системи за пречишћавање отпадних вода

На **ТЕНТ Б** је у плану изградња постројења за пречишћавање отпадних вода.

Систем за пречишћавање отпадних вода у кругу ТЕ „Никола Тесла Б“ представљаће сложени систем који ће обухватити већи број међусобно повезаних постројења и јединица.

ТЕ „Колубара“

Комплекс ТЕ „Колубара“ снабдева се водом из градске водоводне мреже. Предвиђене су спољне инсталације водовода за санитарне и противпожарне сврхе. На хидрантској мрежи постоје 4 надземна хидранта. Унутрашње

инсталације водовода предвиђене су портирници и објекту за одржавање возила за унутрашњи транспорт.

ТЕ „Морава“

Канализациона мрежа

У технолошком процесу производње електричне енергије настају:

- отпадна санитарна вода,
- отпадна вода из Главног погонског објекта (ГПО),
- отпадна вода из неутрализационог базена хемијске припреме воде (ХПВ) ,
- отпадна вода од прања пешчаних филтера из ХПВ,
- отпадна расхладна вода, преливна и дренажна вода са депоније пепела,
- атмосферска вода и
- отпадна вода од одводњавања допреме угља.

Отпадне воде из базена мешавине пепела и воде пумпама се транспортују на депонију пепела и шљаке, а истакање се врши у каду, а преливање се врши у суседну каду, која је због конфигурације терена нижа, одакле се гравитационо испушта у језеро. Вода из језера се потапајућом пумпом пребацује у тунел повратне расхладне воде односно реку Велику Мораву.

У **ТЕ „Морава“** санитарне отпадне воде се одводе системом градске канализације. Отпадне воде које садрже минерална уља из дренажних јама машинске хале се гравитационо испуштају у таложницу која је подељена на два дела. Из првог дела воде се пумпом која ради по нивоу претаче у други део таложнице, а одатле се гравитационо испушта преко прекидне коморе у повратни тунел расхладне воде који је повезан са реком Великом Моравом.

Контролу квалитета отпадних и пречишћених вода, вода реке Велике Мораве и подземних вода редовно врши овлашћена и акредитована лабораторија четири пута годишње. Последња испитивања је извршила овлашћена и акредитована лабораторија „А“ Београд.

Снабдевања водом - властито (бунари)

За одвијање технолошких процеса користи се вода са водозахвата на реци Великој Морави као и подземне воде из бунара. Највећа потрошња воде у **ТЕ „Морава“** је за хлађење кондензата. Водозахват се налази око 0,5 km западно од објекта електране. Вода се транспортује помоћу цевовода ø 1800 mm са две пумпе контролисане фреквентним регулаторима.

ТЕ „Морава“ се водом за пиће снабдева се из водовода Свилајнац. Поред тога термоелектрана поседује аутомате са питком водом постављене у својим просторијама, а користи се и флаширана вода за пиће.

Гасне мреже:

ТЕ „Морава“

Гасна мрежа налази се на 1 km од **ТЕ „Морава“**.

ИДЕНТИФИКАЦИЈА КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Критична инфраструктура представља најважније елементе система привредног друштва, чијим би нарушавањем функционисања основне делатности била угрожена функција предузећа. Проценом критичне инфраструктуре идентификују се објекти и процењују последице од елементарних непогода и других несрећа са аспекта функционалности које се односе на снабдевање енергијом, снабдевање водом, здравствену заштиту, материјална добра и путну инфраструктуру.

Снабдевање енергијом

ПД ТЕНТ је највећи произвођач електричне енергије у Југоисточној Европи. Има 14 блокова чија је укупна инсталисана снага 3.288 MW, што је једна трећина инсталисаних капацитета „Електропривреде Србије“, и годишње произведе више од 50 % српске електричне енергије.

Објекти и постројења за снабдевање електричном енергијом

ТЕНТ А располаже са 6 блокова укупне снаге 1.650 MW, у које су инсталирани уређаји и опрема који су неопходни за производњу електричне енергије.

ТЕНТ Б располаже са Трансформаторским станицама:

1 ком. 35/6 kV, 14 ком. 6,6/0,4 kV и 1 ком. 6/0,4 kV

ТЕ „Колубара“ располаже са **Разводним постројењима**:

1 ком. 110 kV, 1 ком. 35 kV, 15 ком. 6kV

ТЕ „Морава“ располаже са **Трансформаторским станицама**:

T1 13,8/110 kV
T2 110/35/0,6 kV
T3 13,8/6 kV
T4 110/6 kV
T5 110/35 kV
T23 6/0,4 kV
T24 6/0,4 kV
T25 6/0,4 kV
T13 6/0,4 kV
T14 6/0,4 kV

Мрежа за снабдевање електричном енергијом

Мрежа за снабдевање електричном енергијом се односи на надземне и подземне електроенергетске водове.

Могуће последице по функционисање

Услед хаварија или оштећења на појединим постројењима у дистрибутивном електроенергетском систему може доћи до прекида снабдевања потрошача електричном енергијом на појединим деловима територије Републике Србије на којим се налази хаварисано постројење.

Хаварије и оштећења могу настати због екстремно лоших временских прилика као што су поплаве, олујни ветрови, велике количине ледених наслага, земљотреса, пожара или друге елементарне непогоде.

Хаварије генератора електричне енергије, трансформаторских станица, електроразводних водова или других уређаја и опреме од којих зависи производња и дистрибуција електричне енергије, изазивају прекид напајања на свим трансформаторским станицама које се напајају са тих станица, као прекид напајања у нисконапонској мрежи на више насељених територија, чиме се угрожава:

- напајање домаћинстава и пословних објеката електричном енергијом,
- одвијање трамвајског и тролејбуског саобраћаја,
- рад јавне расвете,
- производни процеси у погонима за производњу,
- одвијање телекомуникационог саобраћаја,
- рад пумпних постројења у систему централног грејања или климатизације објеката и
- прекид функционисања заштитиних система који за рад користе електричну енергију.

Случајеви хаварије или оштећења на постројењима за производњу електричне енергије, у дистрибутивном електроенергетском систему или прекид на електроразводној мрежи могу значајно угрозити функционисање ПД ТЕНТ које се односи на потпуни прекид снабдевања електричном енергијом на ограниченој територији и то у дужем времену до успостављања редовног снабдевања.

Снабдевање водом

Низводно од локације ТЕНТ А и ТЕНТ Б, на обали реке Саве налазе се рени бунари који се користе за водоснабдевање водом за пиће овог подручја, као и подручја града Београда.

Здравствена заштита

Здравствене установе у Обреновцу:

- Дом Здравља Обреновац

Здравствене станице:

- Стублине бб,
- Грабовац бб,
- Дражевац бб,
- Кртинска, Младост бб
- Ушће, Дуго поље 1
- Скела, Шабачки пут бб,
- Звечка, Д. Вуковића Корчагина бб,
- Забрежје, Радничка 1,
- Мала Моштаница.

Здравствене установе у Лазаревцу:

- Дом здравља „Др Ђорђе Ковачевић“ у Лазаревцу

Здравствене станице:

- Велики Црљени
- Рудовци
- Вреоци
- Јунковац
- Степојевац
- Дудовица
- Здравствени центар
- Антитуберкулозни диспанзер у Лазаревцу
- Породилиште у Лазаревцу

Здравствене установе у Лазаревцу:

- Дом Здравља Свилајнац

Здравствена заштита запсолених се врши у редовном здравственом збрињавању у здравственим установама или у амбулантама у оквиру организационих целина.

Прва медицинска помоћ је организована преко амбуланата и домова

здравља. Амбуланте су добро технички, материјално (санитетски материјал и лекови) и кадровски опремљени и могу удовољити потребама радника. Сви пацијенти који се не могу амбулантно санирати, упућују се за Београд на даље лечење у болничке центре.

Интерна путна мрежа

Путна инфраструктура ПД ТЕНТ има интерну путну инфраструктуру која се односи јавну мрежу путева и посебно развијену интерну мрежу путева и железничке мреже. Основна делатност се обавља уз интензивно коришћење путне мреже.

Железнички транспорт је веома развијен и користи се за снабдевање ТЕНТ „А“, ТЕНТ „Б“ и ТЕ „КОЛУБАРА“ угљем са површинских копова рударског, колубарског угљеног басена, док се ТЕ „МОРАВА“ снабдева угљем из површинских копова рударског, колубарског угљеног басена и подземне експлоатације ресавског угљеног басена.

Максимални годишњи превоз угља за ТЕНТ „А“ и ТЕНТ „Б“ је 27.331125 t угља, односно 17.851 воз. Максимални дневни довоз је 62 воза, односно 95.538 t угља, док је месечни максимални довоз 2.693199 t угља, односно 1.760 возова. Просечан дневни довоз износи 49 возова, односно 74.800 t угља.

За ТЕ „КОЛУБАРА“ просечно се годишње превезе 1.354008 t угља, односно 2.764 воза. Просечан дневни довоз износи 3.709 t угља, односно више од 7 возова (7,57 возова). Дневни максимум је 19 возова, односно 9.318 t угља.

Привредно друштво Тент, као критичну инфраструктуру, одређује следеће:

Објекти и постројења за снабдевање електричном енергијом

1. Мрежа за снабдевање електричном енергијом

Интерна путна мрежа

2. Материјална добра
3. Здравствена заштита

4. Снабдевање водом и
5. Објекти за складиштење и манипулацију опасним материјама

Критична инфраструктура са становишта угрожености од елементарних непогода и других несрећа, у погледу важности за функционисање ПД ТЕНТ се односи на следеће елементе приказане у табели 22.

Табела 22. Садржај критичне инфраструктуре у погледу угрожености од елементарних непогода и других несрећа

Р.бр.	**Садржај критичне инфраструктуре**	**Важност за функционисање**
1.	Објекти и постројења за снабдевање електричном енергијом	Одвијање функционисања основне делатности
2.	Мрежа за снабдевање електричном енергијом	
3.	Интерна путна мрежа, екстерна путна мрежа	Обезбеђен приступ свим електроенергетски објектима ради снабдевања, интервенције и отклањања кварова
4.	Материјална добра	Потпуни престанак или озбиљно нарушавање извршења основне делатности
5.	Здравствена заштита	Одржавање здравствене виталности запослених, нарочито на критичним местима система
6.	Снабдевање водом	Обезбеђење питке и техничке воде, заштита од пожара
7.	Објекти за складиштење и манипулацију опасним материјама	Заштита од хемијских удеса и терористичких напада

ИДЕНТИФИКАЦИЈА ПОТЕНЦИЈАЛНИХ РИЗИКА ЗА СВА ПРИВРЕДНА ДРУШТВА ЕПС

Идентификацијом опасности и проценом ризика разрађује се: приказ могућег развоја догађаја - сценарио, анализа последица од елементарних непогода и других несрећа и процена ризика.

Приказ могућег развоја догађаја-сценарија обрађује се по врстама опасности и обухвата сагледавање и евидентирање могућих извора опасности, обима и насталих последица по живот и здравље људи, животиња, животне средине,

материјалних и културних добара.

Анализом последица несреће обухватају се анализа повредивости и одређивање могућег нивоа несреће.

Процена ризика је свеукупан процес идентификације, анализе и оцене ризика према следећем процесу:

1. Прелиминарна анализа потенцијалних опасности.
2. Анализа ризика за одређивање нивоа ризика:
   - Вероватноћа (учесталост, рањивост-повредивост),
   - Последице (штета, критичност).

   где је:

- Вероватноћа (В) представља комбинацију учесталости одређеног штетног догађаја и повредивости (рањивости) у односу на потенцијалну опасност.
- Учесталост (У) се односи на понављање одређеног штетног догађаја у временском периоду или на изложеност штићене вредности одређеној потенцијалној опасности у одређеној временској јединици.
- Рањивост (повредивост) (Р) представља постојеће стање заштите субјекта, односно осетљивост субјекта на потенцијалне опасности.
- Последице (П) представљају ефекат штетног догађаја по штићене вредности, а манифестују се кроз величину губитка (штету) у односу на критичност штићене вредности.
- Штета (Ш) је мера оштећења штићених вредности.
- Критичност (К) је мера вредности односно важности штићене вредности односно осетљивости, на ефекте деловања штетног догађаја на штићене вредности.
- Ниво ризика је производ степена вероватноће и степена последица и може износити од минимално 1 до максимално 25.

3. Оцена ризика:

Ради оцене ризика потребно је извршити класификацију ризика у категорије а потом одреди који су ризици прихватљиви а који нису.

Ризици се класификују у категорије од најниже (прва) до највише (пета).

Нивои ризика од 1 до 9 су прихватљиви, а нивои ризика од 10 до 25 се неприхватљиви.

4. Третирање ризика:
- опције за ублажавање,
- опције за изводљивост,
- cost-benefit анализу.

5. Преиспитивање.

Могуће опасности и процена ризика од елементарних непогода и других несрећа разврставају се, у зависности од узрока настанка, на: сеизмичке, хидросферске, атмосферско метеоролошке, биосферске и техничко-технолошке.

Сеизмичке опасности се односе на потенцијалне опасности од:

ПН-1 Земљотреса;

ПН-2 Одрона, клизишта и ерозија.

Хидросферске опасности се односе на потенцијалне опасности од:

ПН-3 Поплава.

Биосферске опасности се односе на потенцијалне опасности од:

ПН-7 Суша;

ПН-8 Епидемије;

ПН-9 Епизоотија.

Атмосферско метеоролошке опасности се односе на потенцијалне опасности од:

ПН-4 Олујних ветрова;

ПН-5 Града;

ПН-6 Снежне мећаве, наноса и поледице.

Техничко-технолошке опасности се односе на потенцијалне опасности од:

ТТН-1 Пожара и експлозија,

ТТН-2 Техничко-технолошких удеса и терористичких напада,

ТТН-3 Нуклеарних или радијационих акцидента.

ПРОЦЕНА РИЗИКА

Процена ризика од елементарних непогода и других несрећа

Евидентирање карактеристика потенцијалних опасности врши се за сваку потенцијалну опасност посебно, а према могућим величинама, према следећем:

- Величина 1 - минимална опасност,
- Величина 2 - мала опасност,
- Величина 3 - средња опасност,
- Величина 4 - велика опасност и
- Величина 5 - максимална опасност.

Након завршетка прелиминарне анализе потенцијалних опасности од елементарних непогода и других несрећа, врши се анализа ризика, која резултује детерминисањем нивоа ризика.

Ниво ризика, који може бити у границама од минимално 1 до максимално 25, добија се као производ степена вероватноће и степена последица.

Степеновање величине вероватноће које одговара степену вероватноће, врши се према следећем:

1 - немогуће, 2 - невероватно, 3 - вероватно, 4 - скоро извесно, 5 - сигурно.

Степеновање последица које одговара величини последица, врши се према следећем:

1 - минималне, 2 - мале, 3 - Умерене, 4 - Озбиљне, 5 - Катастрофалне.

На основу одређеног **нивоа ризика** врши се класификација ризика у категорије од најниже (прва) до највише (пета) а потом одређује који су ризици прихватљиви, а који нису. Прихватљиви ризици су ризици прве, друге и треће категорије док су ризици четврте и пете категорије неприхватљиви. На основу листе прихватљивих и неприхватљивих ризика дефинише се листа приоритета за третирање.

Третман ризика, критеријуми за одређивање преосталог ризика, развој догађаја-сценарио најгорег могућег случаја, могуће последице по штићене вредности, анализа повредивости и могући ниво несреће, разматрају се за сваку врсту потенцијалне опасности од елементарних непогода и других несрећа, према одредбама које су дефинисане у Методологији.

Могући ниво несреће одређује се на основу предвиђеног сценарија и анализе повредивости, а изражава се као I, II, III, IV, V или VI ниво несреће.

Земљотрес

На основу квалитета градње, степена оронулости и карактеристика земљишта на којем су објекти изграђени, типа објеката, којима располажу привредна друштва ЕПС, одређује се величина потенцијалне опасности од земљотреса.

Идентификација и величина потенцијалних опасности од земљотреса врши се на основупостојећег „Критеријума за идентификацију потенцијалних опасности од земљотреса“ који су дефинисани у складу са „Методологијом“.

Критеријуми за идентификацију потенцијални опасности од земљотреса су дефинисани према следећем:

- Постојање докумената планског мониторинга,
- Постојање система за идентификацију, рану најаву и обавештавање,
- Постојање система мониторинга и евиденције,
- Густина насељености,

- Могућност генерисања других опасности.

На основу карте сеизмичког зонирања Србије и броја објеката подложних оштећењима услед земљотреса, изведен је закључак о величини потенцијалне опасности од земљотреса за територију сваког привредног друштва ЕПС. Ова величина служи као основа за вршење процене угрожености од земљотреса за сва привредна друштва ЕПС.

За сваки од претходно наведених критеријума, а на основу свих прикупљених података и сагледавања стања у свим привредним друштвима ЕПС, одређена је средња величина опасности за свако привредно друштво, у складу са **Методологијом,** према следећем:

Табела 23. Величина потенцијалне опасности од земљотреса

Р.бр.	**Привредно друштво**	**Величина потенцијалне опасности од земљотреса**
1.	ЕПС ДИРЕКЦИЈА	4
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	4
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	4
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4
11.	ЕЛЕКТРОСРБИЈА	4
12.	ЈУГОИСТОК	3
13.	ЦЕНТАР	4
14.	ЕПС СНАБДЕВАЊЕ	4

АНАЛИЗА РИЗИКА

Анализом ризика се одређује могућност настанка и величина потенцијалних последица за свако разматрано привредно друштво. Обзиром да се земљотрес не може предвидети, могућност настанка се анализира са аспекта степена примене савремених решења заштите од земљотреса.

Анализа ризика од потенцијалне опасности резултује детерминисањем **нивоа ризика,** који представља производ **вероватноће настанка и могућих последица**, који су дефинисани у складу са **Методологијом**.

На основу величине опасности од земљотреса, као и анализом свих прикупљених података и сагледавања стања у свим привредним друштвима ЕПС, одређене су све вредности које су неопходне за утврђивање **нивоа ризика.**

На основу утврђене вредности за **ниво ризика** одређује се категорија ризика и утврђује прихватљивост или неприхватљивост ризика.

Анализа ризика од земљотреса, за сва привредна друштва ЕПС, приказана је према табели 24.

Табела 24. Анализа ризика од земљотреса

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ЕПС ДИРЕКЦИЈА	4	3	3	3	2	2	3	9	3	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3	3	3	3	3	3	3	10	4	Неприхватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3	3	3	3	3	3	3	10	4	Неприхватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	4	3	3	3	2	2	3	9	3	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4	4	2	3	4	3	3	10	4	Неприхватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4	4	2	3	4	3	3	10	4	Неприхватљив
ПАНОНСКЕ ТЕ-ТО	2	2	3	2	3	3	3	6	3	Прихватљив
РУДАРСКИ БАСЕН КОЛУБАРА	4	4	2	3	4	3	3	10	4	Неприхватљив
ЕЛЕКТРОВОЈВОДИНА	2	2	3	2	3	3	3	6	3	Прихватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4	3	3	3	4	3	4	10	4	Неприхватљив
ЕЛЕКТРОСРБИЈА	4	4	2	4	4	2	4	16	4	Неприхватљив
ЈУГОИСТОК	3	4	3	3	3	3	3	9	3	Прихватљив
ЦЕНТАР	4	4	2	4	4	2	4	16	4	Неприхватљив
ЕПС СНАБДЕВАЊЕ	4	3	3	3	2	2	3	9	4	Прихватљив

Одрони, клизишта и ерозије

Табела 25. Величина потенцијалне опасности од одрона, клизишта и ерозија

Р. бр.	Привредно друштво	Величина потенцијалне опасности од одрона, клизишта и ерозија
1.	ЕСП ДИРЕКЦИЈА	1
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	1
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3
11.	ЕЛЕКТРОСРБИЈА	3
12.	ЈУГОИСТОК	3
13.	ЦЕНТАР	3
14.	ЕПС СНАБДЕВАЊЕ	1

Табела 26. Анализа ризика од одрона, клизишта и ерозија

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ЕПС ДИРЕКЦИЈА	1	1	5	1	1	2	2	2	1	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	4	4	3	2	2	3	10	4	Неприхватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	3	2	4	2	2	3	10	4	Неприхватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	1	1	2	2	1	3	1	2	1	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3	2	2	3	3	3	3	10	4	Неприхватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3	2	2	3	3	3	3	10	4	Неприхватљив
ПАНОНСКЕ ТЕ-ТО	2	2	4	2	2	3	2	4	1	Прихватљив
РУДАРСКИ БАСЕН КОЛУБАРА	3	2	2	3	2	2	3	10	4	Неприхватљив
ЕЛЕКТРОВОЈВОДИНА	2	2	4	2	2	3	2	4	1	Прихватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3	3	2	4	2	2	3	12	4	Неприхватљив
ЕЛЕКТРОСРБИЈА	3	3	2	4	2	2	3	12	4	Неприхватљив
ЈУГОИСТОК	3	2	2	3	2	2	3	10	4	Неприхватљив
ЦЕНТАР	3	3	2	4	2	2	3	12	4	Неприхватљив
ЕПС СНАБДЕВАЊЕ	1	1	2	2	1	3	1	2	1	Прихватљив

Поплаве

Табела 27. Величина потенцијалне опасности од поплава

Р. бр.	Привредно друштво	Величина потенцијалне опасности од поплава
1.	ЕПС ДИРЕКЦИЈА	3
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	3
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4
7.	ПАНОНСКЕ ТЕ-ТО	3
8.	РУДАРСКИ БАСЕН КОЛУБАРА	4
9.	ЕЛЕКТРОВОЈВОДИНА	4
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3
11.	ЕЛЕКТРОСРБИЈА	4
12.	ЈУГОИСТОК	4
13.	ЦЕНТАР	4
14.	ЕПС СНАБДЕВАЊЕ	3

Табела 28. Анализа ризика од поплава

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ЕПС ДИРЕКЦИЈА	3	3	2	4	1	5	1	4	2	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4	5	3	4	4	2	4	16	4	Неприхватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4	5	3	4	4	2	4	16	4	Неприхватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	3	3	2	4	1	5	1	4	2	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4	4	2	4	5	2	5	20	5	Неприхватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4	5	2	5	4	2	4	20	5	Неприхватљив
ПАНОНСКЕ ТЕ-ТО	3	4	3	4	2	2	3	12	4	Неприхватљив
РУДАРСКИ БАСЕН КОЛУБАРА	4	5	3	4	4	2	4	16	4	Неприхватљив
ЕЛЕКТРОВОЈВОДИНА	4	5	4	3	3	3	3	10	4	Неприхватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3	4	3	4	2	3	2	9	3	Прихватљив
ЕЛЕКТРОСРБИЈА	4	4	3	3	3	3	3	10	4	Неприхватљив
ЈУГОИСТОК	4	5	3	4	3	3	3	12	4	Неприхватљив
ЦЕНТАР	4	5	2	5	2	3	2	10	4	Неприхватљив
ЕПС СНАБДЕВАЊЕ	3	3	2	4	1	5	1	4	2	Прихватљив

Олујни ветрови

Табела 29. Величина потенцијалне опасности од олујних ветрова

Р.бр.	**Привредно друштво**	**Величина потенцијалне опасности од олујних ветрова**
1.	ЕПС ДИРЕКЦИЈА	1
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	4
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3
7.	ПАНОНСКЕ ТЕ-ТО	3
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	4
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4
11.	ЕЛЕКТРОСРБИЈА	4
12.	ЈУГОИСТОК	4
13.	ЦЕНТАР	3
14.	ЕПС СНАБДЕВАЊЕ	1

Табела 30. Анализа ризика од олујних ветрова

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ЕПС ДИРЕКЦИЈА	4	4	2	4	1	4	1	5	2	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4	4	3	3	3	3	3	10	4	Неприхватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4	4	3	4	2	4	2	8	3	Прихватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	4	4	2	4	1	4	1	5	2	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3	4	2	4	2	3	2	8	3	Прихватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3	4	2	4	3	3	3	12	4	Неприхватљив
ПАНОНСКЕ ТЕ-ТО	3	4	2	4	2	3	3	12	4	Неприхватљив
РУДАРСКИ БАСЕН КОЛУБАРА	3	4	2	1	2	3	2	10	4	Неприхватљив
ЕЛЕКТРОВОЈВОДИНА	4	4	2	4	2	3	3	12	4	Неприхватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4	4	2	4	3	3	3	12	4	Неприхватљив
ЕЛЕКТРОСРБИЈА	4	4	3	3	3	3	3	10	4	Неприхватљив
ЈУГОИСТОК	4	4	3	4	2	4	2	8	3	Прихватљив
ЦЕНТАР	3	4	2	4	2	3	3	10	4	Неприхватљив
ЕПС СНАБДЕВАЊЕ	4	4	2	4	1	4	1	5	2	Прихватљив

Табела 31. Величина потенцијалне опасности од града

Р. бр.	Привредно друштво	Величина потенцијалне опасности од града
1.	ДИРЕКЦИЈА	2
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	2
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4
11.	ЕЛЕКТРОСРБИЈА	3
12.	ЈУГОИСТОК	3
13.	ЦЕНТАР	3
14.	ЕПС СНАБДЕВАЊЕ	2

Табела 32. Анализа ризикаод града

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈА	2	1	4	1	2	3	2	2	1	ПР
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	1	4	1	2	3	2	2	1	ПР
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4	4	4	3	4	2	4	16	4	ПР
ЕПС ОБНОВЉИВИ ИЗВОРИ	2	1	4	1	2	3	2	2	1	ПР
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4	4	4	3	3	3	3	12	4	НЕПР
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3	4	3	3	4	3	3	12	4	НЕПР
ПАНОНСКЕ ТЕ-ТО	2	1	5	1	2	3	2	2	1	ПР
РУДАРСКИ БАСЕН КОЛУБАРА	3	4	2	4	2	3	2	8	3	ПР
ЕЛЕКТРОВОЈВОДИНА	2	1	5	1	2	3	2	2	1	ПР
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	4	3	3	3	3	2	4	12	4	НЕПР
ЕЛЕКТРОСРБИЈА	3	3	3	3	3	2	4	12	4	НЕПР
ЈУГОИСТОК	3	1	5	1	2	3	2	2	1	ПР
ЦЕНТАР	3	5	3	4	4	3	3	12	4	НЕПР
ЕПС СНАБДЕВАЊЕ	2	1	4	1	2	3	2	2	1	ПР

Снежне мећаве, наноси и поледице

Табела 33. Величина потенцијалне опасности од снежних мећава, наноса и поледица

Р. бр.	Привредно друштво	Величина потенцијалне опасности од снежних мећава, наноса и поледица
1.	ДИРЕКЦИЈА	2
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	2
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3
11.	ЕЛЕКТРОСРБИЈА	3
12.	ЈУГОИСТОК	3
13.	ЦЕНТАР	3
14.	ЕПС СНАБДЕВАЊЕ	2

Табела 34. Анализа ризика од снежних мећава, наноса и поледица

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈА	2	1	4	1	2	3	2	2	4	ПР
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	4	4	1	5	3	3	3	15		НЕПР
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	4	4	2	4	2	1	4	16	1	НЕПР
ЕПС ОБНОВЉИВИ ИЗВОРИ	2	4	1	5	1	3	1	5	1	ПР
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3	1	4	1	2	3	2	12	4	НЕПР
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3	5	3	4	4	3	3	12	4	НЕПР
ПАНОНСКЕ ТЕ-ТО	2	3	5	2	2	3	2	4	1	ПР
РУДАРСКИ БАСЕН КОЛУБАРА	3	1	4	1	2	3	2	12	4	НЕПР
ЕЛЕКТРОВОЈВОДИНА	2	3	5	1	2	3	2	10	1	НЕПР
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3	3	3	3	3	2	4	12	4	НЕПР
ЕЛЕКТРОСРБИЈА	3	3	3	3	3	2	4	12	4	НЕПР
ЈУГОИСТОК	3	3	5	2	2	1	4	8	1	ПР
ЦЕНТАР	3	5	3	4	4	3	3	12	4	НЕПР
ЕПС СНАБДЕВАЊЕ	2	1	4	1	2	3	2	2	4	ПР

Табела 35. Величина потенцијалне опасности од суша

Р. бр.	Привредно друштво	Величина потенцијалне опасности од суша
1.	ДИРЕКЦИЈА	2
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	2
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3
11.	ЕЛЕКТРОСРБИЈА	3
12.	ЈУГОИСТОК	3
13.	ЦЕНТАР	3
14.	ЕПС СНАБДЕВАЊЕ	2

Табела 36. Анализа ризика од суша

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈА	2	1	4	1	2	3	2	2	1	ПР
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	1	4	1	2	3	2	2	1	ПР
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	1	4	1	2	3	2	2	1	ПР
ЕПС ОБНОВЉИВИ ИЗВОРИ	2	1	4	1	2	3	2	2	1	ПР
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2	1	4	1	2	3	2	2	1	ПР
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	3	5	3	4	4	3	3	12	4	НЕПР
ПАНОНСКЕ ТЕ-ТО	2	1	5	1	2	3	2	2	1	ПР
РУДАРСКИ БАСЕН КОЛУБАРА	3	1	4	1	2	3	2	2	1	ПР
ЕЛЕКТРОВОЈВОДИНА	2	1	5	1	2	3	2	2	1	ПР
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	3	3	3	3	3	2	4	12	4	НЕПР
ЕЛЕКТРОСРБИЈА	3	3	3	3	3	2	4	12	4	НЕПР
ЈУГОИСТОК	3	1	5	1	2	3	2	2	1	ПР
ЦЕНТАР	3	5	3	4	4	3	3	12	4	НЕПР
ЕПС СНАБДЕВАЊЕ	2	1	4	1	2	3	2	2	1	ПР

Епидемије

Табела 37. Величина потенцијалне опасности од епидемија

Р. бр.	Привредно друштво	Величина потенцијалне опасности од епидемија
1.	ДИРЕКЦИЈЕ	2
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	1
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2
7.	ПАНОНСКЕ ТЕ-ТО	3
8.	РУДАРСКИ БАСЕН КОЛУБАРА	3
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	2
11.	ЕЛЕКТРОСРБИЈА	2
12.	ЈУГОИСТОК	2
13.	ЦЕНТАР	2
14.	ЕПС СНАБДЕВАЊЕ	2

Табела 38. Анализа ризика од епидемија

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈЕ	2	1	2	2	1	4	1	2	1	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	2	3	2	1	4	1	2	1	Прихватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	1	2	2	1	4	1	2	1	Прихватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	1	1	3	1	1	3	1	1	1	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3	2	3	2	1	4	1	2	1	Прихватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2	1	3	1	1	4	1	1	1	Прихватљив
ПАНОНСКЕ ТЕ-ТО	3	2	3	2	1	4	1	2	1	Прихватљив
РУДАРСКИ БАСЕН КОЛУБАРА	3	1	2	2	1	4	1	2	1	Прихватљив
ЕЛЕКТРОВОЈВОДИНА	2	2	3	2	1	4	1	2	1	Прихватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	2	1	2	2	1	4	1	2	1	Прихватљив
ЕЛЕКТРОСРБИЈА	2	2	3	2	1	4	1	2	1	Прихватљив
ЈУГОИСТОК	2	1	3	1	1	3	1	1	1	Прихватљив
ЦЕНТАР	2	1	3	1	1	4	1	1	1	Прихватљив
ЕПС СНАБДЕВАЊЕ	2	2	3	2	1	4	1	2	1	Прихватљив

Епизоотије

Табела 39. Величина потенцијалне опасности од епизоотија

Р. бр.	Привредно друштво	Величина потенцијалне опасности од епизоотија
1.	ДИРЕКЦИЈЕ	1
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	1
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	1
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	1
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	2
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	1
11.	ЕЛЕКТРОСРБИЈА	1
12.	ЈУГОИСТОК	2
13.	ЦЕНТАР	2
14.	ЕПС СНАБДЕВАЊЕ	1

Табела 40. Анализа ризика од епизоотија

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈЕ	1	1	4	1	2	5	1	1	1	Прихват.
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	1	2	5	1	3	4	2	2	1	Прихват.
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	1	1	3	1	5	1	3	2	Прихват.
ЕПС ОБНОВЉИВИ ИЗВОРИ	1	1	5	1	3	5	2	2	1	Прихват.
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2	1	5	1	1	5	1	1	1	Прихват.
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2	1	4	1	2	5	1	1	1	Прихват.
ПАНОНСКЕ ТЕ-ТО	2	2	5	1	3	4	2	2	1	Прихват.
РУДАРСКИ БАСЕН КОЛУБАРА	2	1	1	3	1	5	1	3	2	Прихват.
ЕЛЕКТРОВОЈВОДИНА	2	1	1	3	1	5	1	3	2	Прихват.
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	1	2	5	1	3	4	2	2	1	Прихват.
ЕЛЕКТРОСРБИЈА	1	2	5	1	3	4	2	2	1	Прихват.
ЈУГОИСТОК	2	1	5	1	3	5	2	2	1	Прихват.
ЦЕНТАР	2	1	5	1	1	5	1	1	1	Прихват.
ЕПС СНАБДЕВАЊЕ	1	2	5	1	3	4	2	2	1	Прихват.

Пожари и експлозије

Табела 41. Величина потенцијалне опасности од пожара и експлозија

Р. бр.	Привредно друштво	Величина потенцијалне опасности од пожара и експлозија
1.	ДИРЕКЦИЈА	3
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	2
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4
7.	ПАНОНСКЕ ТЕ-ТО	4
8.	РУДАРСКИ БАСЕН КОЛУБАРА	4
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	2
11.	ЕЛЕКТРОСРБИЈА	2
12.	ЈУГОИСТОК	2
13.	ЦЕНТАР	2
14.	ЕПС СНАБДЕВАЊЕ	2

Табела 42. Анализа ризика од пожара и експлозија

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈЕ	3	2	4	2	2	2	3	6	3	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3	3	3	3	3	1	5	15	4	Неприхватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3	3	3	3	3	1	5	15	4	Неприхватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	2	2	5	1	2	2	3	3	2	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	4	3	2	4	3	2	4	16	4	Неприхватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	4	3	3	3	3	1	5	15	4	Неприхватљив
ПАНОНСКЕ ТЕ-ТО	4	3	3	3	3	1	5	15	4	Неприхватљив
РУДАРСКИ БАСЕН КОЛУБАРА	4	3	3	3	3	1	5	15	4	Неприхватљив
ЕЛЕКТРОВОЈВОДИНА	2	2	4	2	2	2	3	6	3	Прихватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	2	2	4	2	2	2	3	6	3	Прихватљив
ЕЛЕКТРОСРБИЈА	2	2	5	1	2	2	3	3	2	Прихватљив
ЈУГОИСТОК	2	2	4	2	2	2	3	6	3	Прихватљив
ЦЕНТАР	2	2	4	2	2	2	3	6	3	Прихватљив
ЕПС СНАБДЕВАЊЕ	2	2	4	2	2	2	3	6	3	Прихватљив

Техничко-технолошки удеси и терористички напади

Табела 43. Величина потенцијалне опасности од техничко-технолошких удеса и терористичких напада

Р. бр.	Привредно друштво	Величина потенцијалне опасности од техничко-технолошких удеса и терористичких напада
1.	ДИРЕКЦИЈА	1
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	1
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	2
9.	ЕЛЕКТРОВОЈВОДИНА	2
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	2
11.	ЕЛЕКТРОСРБИЈА	2
12.	ЈУГОИСТОК	2
13.	ЦЕНТАР	1
14.	ЕПС СНАБДЕВАЊЕ	1

Табела 44. Анализа ризика од техничко-технол. удеса и терористичких напада

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈЕ	1	1	4	1	2	3	2	2	1	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	3	2	1	4	3	2	4	16	4	Непихватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	3	2	1	4	3	2	4	16	4	Непихватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	1	1	4	1	2	3	2	2	1	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	3	2	1	4	3	2	4	16	4	Непихватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	2	1	2	2	2	2	3	6	3	Прихватљив
ПАНОНСКЕ ТЕ-ТО	2	1	2	2	2	2	3	6	3	Прихватљив
РУДАРСКИ БАСЕН КОЛУБАРА	2	1	2	2	2	2	3	6	3	Прихватљив
ЕЛЕКТРОВОЈВОДИНА	2	1	1	3	3	2	4	12	4	Непихватљив
ЕДБ БЕОГРАД	2	1	1	3	3	2	4	12	4	Непихватљив
ЕЛЕКТРОСРБИЈА	2	1	1	3	3	2	4	12	4	Непихватљив
ЈУГОИСТОК	1	1	3	1	3	2	4	4	2	Прихватљив
ЦЕНТАР	1	1	3	1	3	2	4	4	2	Прихватљив
ЕПС СНАБДЕВАЊЕ	1	1	3	1	3	2	4	4	2	Прихватљив

Нуклеарни и радијациони акциденти

Табела 45. Величина потенцијалне опасности од нуклеарних и/или радијационих акцидената

Р. бр.	Привредно друштво	Величина потенцијалне опасности од нуклеарних и/или радијационих акцидената
1.	ДИРЕКЦИЈЕ	1
2.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
3.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2
4.	ЕПС ОБНОВЉИВИ ИЗВОРИ	1
5.	ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2
6.	ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	1
7.	ПАНОНСКЕ ТЕ-ТО	2
8.	РУДАРСКИ БАСЕН КОЛУБАРА	1
9.	ЕЛЕКТРОВОЈВОДИНА	1
10.	ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	1
11.	ЕЛЕКТРОСРБИЈА	1
12.	ЈУГОИСТОК	1
13.	ЦЕНТАР	1
14.	ЕПС СНАБДЕВАЊЕ	1

Табела 46. Анализа ризика од нуклеарних и/или радијационих акцидената

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ДИРЕКЦИЈЕ	1	1	2	2	2	3	2	4	2	Прихватљив
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	1	1	3	1	2	2	6	3	Прихватљив
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	1	2	2	2	3	2	4	2	Прихватљив
ЕПС ОБНОВЉИВИ ИЗВОРИ	1	1	2	2	2	3	2	4	2	Прихватљив
ТЕРМОЕЛЕКТРАНЕ НИКОЛА ТЕСЛА	2	1	1	3	1	2	2	6	3	Прихватљив
ТЕРМОЕЛЕКТРАНЕ И КОПОВИ КОСТОЛАЦ	1	1	2	2	2	3	2	4	2	Прихватљив
ПАНОНСКЕ ТЕ-ТО	2	1	2	2	2	3	2	4	2	Прихватљив
РУДАРСКИ БАСЕН КОЛУБАРА	1	1	2	2	2	3	2	4	2	Прихватљив
ЕЛЕКТРОВОЈВОДИНА	1	1	1	3	1	2	2	6	3	Прихватљив
ЕЛЕКТРОДИСТРИБУЦИЈА БЕОГРАД	1	1	2	2	2	3	2	4	2	Прихватљив
ЕЛЕКТРОСРБИЈА	1	1	2	2	2	3	2	4	2	Прихватљив
ЈУГОИСТОК	1	1	2	2	2	3	2	4	2	Прихватљив
ЦЕНТАР	1	1	2	2	2	3	2	4	2	Прихватљив
ЕПС СНАБДЕВАЊЕ	1	1	2	2	2	3	2	4	2	Прихватљив

Анализа последица по функционисање субјекта

Табела 47. Величина потенцијалне опасности од рушења хидроакумулационих брана

Р. бр.	Привредно друштво	Величина потенцијалне опасности од рушења хидроакумулационих брана
1.	ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2
2.	ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2

Табела 48. Анализа ризика од рушења хидроакумулационих брана

Привредно друштво	Величина опасности	Учесталост (У1 или У2)	Повредивост (рањивост)	Вероватноћа	Штета	Критичност	Последице	Ниво ризика	Категорија ризика	Прихватљивост
ХИДРОЕЛЕКТРАНЕ ЂЕРДАП	2	2	2	3	2	2	3	9	3	Прихватљиво
ДРИНСКО-ЛИМСКЕ ХИДРОЕЛЕКТРАНЕ	2	2	2	3	2	2	3	9	3	Прихватљиво

Прилог 3. Изјава о ауторству

Потписана Марија Д. Мићовић

Број индекса (уписа) 142

Изјављујем

да је докторска дисертација под насловом

БЕЗБЕДНОСНИ АСПЕКТИ ФУНКЦИОНИСАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршила ауторска права и користила интелектуалну својину других лица.

Потпис докторанда

У Београду, 23.02.2016

Марија Мићовић

Прилог 4. Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Марија Д. Мићовић

Број уписа 142

Студијски програм _____

Наслов рада Безбедносни аспекти функционисања критичне инфраструктуре у ванредним ситуацијама

Ментор проф. др Владимир Јаковљевић

Потписана мр Марија Мићовић

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предала за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 23.02.2016

Марија Мићовић

Прилог 5. Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

БЕЗБЕДНОСНИ АСПЕКТИ ФУНКЦИОНИСАЊА КРИТИЧНЕ ИНФРАСТРУКТУРЕ У ВАНРЕДНИМ СИТУАЦИЈАМА

која је моје ауторско дело.

Дисертацију са свим прилозима предала сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице *(Creative Commons)* за коју сам се одлучила.

1. Ауторство
2. Ауторство - некомерцијално
3. Ауторство - некомерцијално - без прераде
4. Ауторство - некомерцијално - делити под истим условима
5. Ауторство - без прераде
6. Ауторство - делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 23.02.2016 Матања Митровић

1. Ауторство - Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство - некомерцијално. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијалнобез прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство – некомерцијално- делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство - без прераде. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољавате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.

Прилог 6. Списак слика и табела

СЛИКЕ

ГРАФИКОНИ У ОКВИРУ АНКЕТНОГ УПИТНИКА

ТАБЕЛЕ

БИОГРАФСКИ ПОДАЦИ

Марија Д. Мићовић је рођена 20. септембра 1980. године у Бијелом Пољу, где је завршила основну школу и гимназију. Факултет цивилне одбране (сада Факултет безбедности) Универзитета у Београду уписала је 2000. године. Студирала је убрзано, а студије је завршила као најуспешнији студент у својој генерацији, са просечном оценом 9,24.

Академске 2004./2005. године уписала је магистарске студије на смеру *Заштита*. Од септембра 2005. до априла 2006. године радила је у Средњој техничкој школи „Јован Вукановић“ у Новом Саду, као професор на предмету *Безбедносна култура* и као менаџер за безбедност у школи. Реч је о учешћу у Пројекту „Учењем до безбедности“ чији је циљ био да се уведе нова наставна дисциплина у средњешколско образовање. Носиоци овог пројекта били су Министарство Просвете и спорта Републике Србије и Факултет безбедностиУниверзитета у Београду.

Од маја 2006. године запослена је у Криминалистичко-полицијској академији у Београду, прво у звању *истраживач-приправник*, потом, априла 2010. године изабрана је у *истраживача-сарадника*. Од септембра 2006. године обавља послове секретара Редакције часописа Криминалистичко-полицијске академије „*Наука-безбедност-полиција - Журнал за криминалистику и право*“.

Учествовала је на више међународних и домаћих саветовања из области безбедности и заштите и аутор је више радова из ових области.Говори енглески језик и познаје рад на рачунару.

Марија Д. Мићовић је учествовала у реализацији следећих пројекта:

1. *Учењем до безбедности*

Носиоци пројекта: Министарство просвете и спорта Републике Србије и Факултет безбедности Универзитета у Београду; место реализовања пројекта: Техничка школа „Јован Вукановић“ у Новом Саду; период: 2005-2006;

2. *Правни аспекти примене форензичких метода у криминалистици*

Носилац пројекта: КПА у Београду, период: 2009-2011.

3. *Развој институционалних капацитета, стандарда и процедура за супротстављање организованом криминалу и тероризму у условима међународних интеграција, (члан истраживачког тима)*

Пројекат финансира Министарство просвете и науке Републике Србије (бр. 179045), а реализује КПА у Београду, период 2011-2015.

4. *Иновирање форензичких медота и њихова примена* (члан истраживачког тима)

Пројекат финансира Министарство просвете и науке Републике Србије (бр. 34019), а реализује КПА у Београдупериод 2011-2015.

5. *Национална безбедност Републике Србије и безбедносне интеграције*, носилац Криминалистичко-полицијска академија у Београду

6. *Криминалитет у Србији и инструменти државне реакције*

Носилац: Криминалистичко-полицијска академија у Београду, период: 2015-2019;

Такође, похађала је три едукативна семинара који су реализовани у оквиру пројекта МУП Републике Аустрије и МУП Републике Србије. Назив пројекта је „Полицијска сарадња у циљу сузбијања трговине и кријумчарења људи и илегалних миграција“. Семинари су одржани у Криминалистичко-полицијској академији, и то:

- „Одузимање имовине стечене кривичним делом“, 25.-27.09.2007. године;
- „Управљање пројектом и планирање интервенције“, октобар 2007. године и
- „Заштита сведока“, 16.-19.09.2008. године.

Током новембра и децембра 2010. године похађала је два семинара у оквиру Пројекта „Подизање капацитета МУП-а у оквиру припреме пројеката“ у организацији Meritum International group у сарадњи са Министарством унутрашњих послова Републике Србије (Одељење за управљање пројектима финансираним из фондова Европске уније) и Амбасадом Велике Британије у Београду.