ОЛИВЕР БАКРЕСКИ
ТАЊА МИЛОШЕВСКА
ЃОРЃИ АЛЧЕСКИ

ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА









д-р ОЛИВЕР БАКРЕСКИ
д-р ТАЊА МИЛОШЕВСКА
д-р Ѓ ОРЃ И АЛЧЕСКИ

ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА

ОЛИВЕР БАКРЕСКИ
ТАЊА МИЛОШЕВСКА
ЃОРЃИ АЛЧЕСКИ

ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА

Скопје, 2017

ЗАШТИТА НА КРИТИЧНА ИНФРАСТРУКТУРА

Рецензенти:
Проф. д-р Денис ЧАЛЕТА,
Институт за корпоративни безбедносни студии – Љубљана
Проф. д-р Драган ТРИВАН,
Факултет за бизнис студии и право – Белград

Издавач Комора на Република Македонија за приватно обезбедување

За издавачот: Верица МИЛЕСКА СТЕФАНОВСКА

Лектор м-р Лилјана ПАНДЕВА
Корица Андријана КИРОСКИ
Графички уредник Билјана ИВАНОВА

Печати Стеда графика – Скопје
Тираж 500

CIP – Каталогизација во публикација
Национална и универзитетска библиотека „Св. Климент Охридски“, Скопје

355.45

БАКРЕСКИ, Оливер
Заштита на критична инфраструктура / Оливер Бакрески, Тања Милошевска, Ѓорѓи Алчески. - Скопје : Комора на Република Македонија за приватно обезбедување, 2017. - 223 стр. : граф. прикази ; 21 см

Фусноти кон текстот. - Библиографија: стр. 213-223

ISBN 978-608-65990-4-1

а) Државна безбедност - Критична инфраструктура

COBISS.MK-ID 102853898

СОДРЖИНА

ПРЕДГОВОР

Критичната инфраструктура како витална, комплексна и меѓусебно структурно поврзана целина е од исклучителна важност и значење за непреченото функционирање на државата. Таа е јасна дијалектика и синергија што ги поврзува индустрискиот сектор, комуникациските системи, енергетскиот сектор и другите сектори, системи и мрежи што се од големо значење за државата бидејќи со неа се обезбедува потребната стабилност. Оттука нарушувањето или прекинот на работата на одредени сектори/системи може да доведе до сериозни последици што може да имаат и ослабувачки ефект на безбедноста на државата, на националната економија, на економскиот развој и просперитет, на стабилниот енергетски сектор, односно нарушувањето или прекинот на работата на само еден од наведените сектори може да доведе до сериозни последици врз другите критични сектори.

Заштитата на критичната инфраструктура е особено апострофирана во оваа книга бидејќи се знае дека овој сегмент е есенцијален, односно суштински дел на националната безбедност на секоја држава, па оттука нејзината заштита е врвна цел и приоритет на секоја земја, особено ако се знае фактот дека општествените девијации (на пример: кражби, измами, индустриски шпиунажи, саботажи, диверзии, злонамерни оштетувања и сл.), природните катастрофи, техничко-технолошките несреќи, човечките пропусти итн., сите може да предизвикаат големи човечки загуби и материјални штети. Ако на овие елементи се надоврзат и одредени специфични облици на загрозување, во чии рамки спаѓа и употребата на современите оружја и напредни технологии, вклучувајќи го и нуклеарниот материјал, хемиските и биолошките оружја и слично, сето тоа е јасен сигнал дека имаме сериозен безбедносен ризик кој надополнет со веројатноста таквото оружје да биде употребено во акти на незаконско постапување и врз критичната инфраструктура, ја на-

метнува потребата од создавање соодветни механизми за заштита на критичната инфраструктура.

Истражувањето спроведено во оваа монографија имаше за цел да го анализира сегментот на прашања поврзан со критичната инфраструктура која во суштина бара избалансираност, заеднички напор и висок степен на соработка на клучните субјекти. Тоа ја нагласува потребата за прифаќање на напредните безбедносни системи и процедури во развојот на обезбедувањето, како и постапките што треба да се преземат во случај на опасност, од страна на стручниот персонал, а сè со цел создавање услови за нормално функционирање на државата. Оттука, нашата намера е да се придонесе во креирањето на соодветни решенија за обликување на идните развојни стратегии во заштита на критичната инфраструктура како врвен приоритет и интерес на нашата држава. Со ваквиот пристап се изразува определбата на авторите критичната инфраструктура да се доближи до сите оние што посредно или непосредно се занимаваат со изучување на вакви прашања, но книгата според опфатот на содржината ја прави привлечна и интересна и за сите оние што имаат изразена љубопитност во образовниот сектор, но и надвор од образовната сфера, како што се вработените во безбедносниот сектор, во приватниот безбедносен сектор, како и во другите области во општествениот живот.

На крај, ние како автори изразуваме голема благодарност на почитуваните рецензенти проф. д-р Денис Чалета и на проф. д-р Драган Триван за исклучително добрите оценки за книгата, како и на сите оние што дадоа свои сугестии во текот на изработката на овој труд, а особено му се заблагодаруваме на д-р Николчо Спасов и на м-р Лета Барциева Миовска за нивниот конкретен ангажман во одредени делови во пишаното дело. Изразуваме голема благодарност на нашите семејства за разбирањето додека ја пишувавме книгата, а најголемата благодарност и ја изразуваме на Комората на Република Македонија за приватно обезбедување која овозможи критичната инфраструктура да биде целосно проучувана и објаснувана.

Скопје, јануари 2017 година Авторите

I глава

КРИТИЧНА ИНФРАСТРУКТУРА – ТЕОРИЈА И КОНЦЕПТ

1. ОПШТО ЗА КРИТИЧНА ИНФРАСТРУКТУРА

Развојот на технологијата го наметна трендот на подобрување на условите за живеење преку создавање современи системи и услуги коишто тие ги обезбедуваат. Ефектите од нивното дејствување за краток период ги надминаа капацитетите на националните граници. Денес овие системи и услугите се меѓусебно поврзани, испреплетени и во голема мера зависат едни од други, односно евидентна е нивната меѓузависност. Ваквата поврзаност овозможи брз проток на информации, на стоки, на луѓе, на услуги и на капитал. Тоа, пак, повеќе или помалку, ги редефинираше условите за остварување профит и благосостојба. Набргу стана јасно дека сите овие процеси најдобро функционираат во услови на либерална демократија. Меѓутоа, напорите да се воспостави демократското уредување на глобално ниво не се прифаќаат подеднакво или барем во регионите што се сметаат за проблематични, а најчесто имаат богати ресурси неопходни за функционирање на современите системи што го обезбедуваат благодетот на современото живеење.[1] Отпорот кон ваквите процеси започна да претставува сериозен безбедносен предизвик за инфраструктурата и за системите што го обезбедуваат сервисот за модерно живеење. Напаѓајќи ги т.н. „меки цели“, олицетворени преку критичната инфраструктура, овие актери директно му се заканија на западниот начин на живеење.[2] За ваквиот развој на настаните, сепак, делумно придонесе и различниот интерес на сопствениците на овие сервиси и услуги.[3] Имено, во трката по профит прашањата за заштита

[1] Graham E. Fuller, “Airstrakes Aren’t Endgame”, *Los Angeles Times*, August 24, 1998.

[2] Lawrence Freeman, “Out of Nowhere – Bin Laden’s Grievances”, *BBC Online*, 20 October 2011, достапно на: http:// www.bbc.co.uk/history/war/sept_11/build_up_05.shtml

[3] Benjamin R. Barber, “Jihad vs. McWorld”, *The Atlantic*, March 1992, стр. 24.

на овие инфраструктури се секогаш на маргините. Ефективноста, профитот, малите загуби и проширувањето на пазарот на кој се нуди продуктот во речиси ниту еден случај не ја земаат безбедноста на системите како примарна цел во превентивна смисла.[4] Таму каде безбедноста се зема предвид тоа се прави или врз основа на постфестум дејствување или, пак, врз основа на изолиран напор, а не на мрежен и координиран пристап.[5] Во овој контекст се и забелешките што се даваат на големите корпорации за несовесното однесување кон заштита на природата. Глобалните промени во животната средина во последните неколку години и елементарните катастрофи укажаа на итноста од потребата за сериозно преиспитување на заштитата на критичната инфраструктура во контекст на опасноста од елементарни непогоди.[6] Процесот на демократизација и потребата од поголем профит кај странските и кај домашните корпорации дополнително ја доведе во прашање заштитата на инфраструктурата што треба да ги поддржи системите и сервисот или услугите што тие и го даваат. Сепак, природата на критичната инфраструктура ги прави разумно аргументирани овие небалансирани појави кои треба да бидат земени предвид. Најсериозниот дисбаланс е ситуацијата во која капацитетите не се во можност да одговорат на побарувачката. Ова може да биде претставено со ситуација во која одреден дел од популацијата не го добива очекуваното ниво на критично добро или услуга, како, на пример, прекин на довод на електрична енергија. Втората сериозна состојба настанува кога системот ја надминува побарувачката и води до редукција на капацитетите, што потоа ре-

[4] Stephen Flynn, "*America the Vulnerable*", New York: Harper Collins, 2004, стр. x

[5] Milan Vrsec, Managing Corporate Security in the Energy Sector: Energy as Vital (Critical) Infrastructure for the Functioning of a State, Economy and Civil Society, во Denis Caleta and Paul Semella, "*Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection*", Center for Civil – Military Relations, Monterey, USA, 2011, стр.107-130.

[6] Venceslav Kostadinov, "*Vulnerability Assessment: New Nuclear Power Plants Universal Methodology for Terrorism Threats and Natural Disasters Analyses and Predictions*", in Denis Caleta, Paul Shemella, Iztok Podbregar, Branko Lobnikar, Ljubljana: Institute for Corporative Studies-ICS, Monterey: Center for Civil-Military Relations, 2011, стр. 145-158.

зултира со ранливост при сериозно зголемување на побарувачката. Оваа појава може да се разгледува во ситуации во кои приватниот сектор е првенствено ангажиран во доставувањето на доброто/услугата, но поради вишокот набавки, бизнисите го напуштаат пазарот затоа што стануваат непрофитабилни.

Во основа, процесот на транзиција во посткомунистичките земји не ја заобиколи постојната критична инфраструктура, но и напорите за изградба на нова и модерна инфраструктура. Трката за што побрза приватизација и побрзо остварување профит не можеше да се совпадне со безбедносните побарувања. Со други зборови, приватниот домашен или странски капитал прашањата за безбедноста ги стави на маргините. Тоа значи дека секогаш за да се задоволи минимум безбедност би се најмила фирма што ќе понуди услуга за најмалку средства. Од друга страна, ако фирмата што ја нуди услугата вложила во едукација на персоналот за да задоволи соодветни стандарди, нормално е дека ќе биде поскапа во понудата на безбедносни услуги. Тоа, пак, значи дека државата е таа што мора да стапи на сцена. За да може да се оствари сето тоа се наметнува потребата од ефективна стратегија за заштита на критичната инфраструктура. Ваквата стратегија ќе биде од корист и во случај на природни непогоди и катастрофи. Истата ќе овозможи подобра и поефективна координација за намалување на последиците од можните ефекти.

2. ПОИМ ЗА КРИТИЧНА ИНФРАСТРУКТУРА

Поимот „инфраструктура“ за првпат е воведен во XIX век од швајцарскиот воен теоретичар Антоан-Хенри Жомини, кој го истакнува стратегиското и оперативно значење за раководењето на воените дејства. Значи, до средината на XX век терминот „инфраструктура“ е воен термин со кој се означува територијалната организација на системот за одржување и функционирање на армијата. Подоцна терминот „инфраструктура“ почнува да се користи во економската теорија и во теоријата на управувањето[7], а постепено овој термин

[7] Idzorek, T., *Infrastructure and Strategic Asset Allocation: Is Infrastructure an Asset Class*?, Ibbotson a Morningstor Company, 2009, стр. 17.

навлегува во терминологијата на економијата, информатиката, како и во анализите за безбедноста. Со тоа постепено објектите на критичната инфраструктура претставуваат „крвоток“ за непречено функционирање на базичните елементи на општествата, така што нивната заштита претставува приоритет за секое општество.

Поимот критична инфраструктура е клучен за правилно разбирање на заштита на критичната инфраструктура. Придавката критичен доаѓа од старогрчкиот јазик, а во современиот македонски јазик е преземена од англискиот јазик. Од повеќето значења на придавката критичен, за поимот критична инфраструктура од значење се две поимања, и тоа: првото значење на критичен означува нешто што е суштинско, неопходно и животно важно (витално), а второто значење се однесува на нешто решавачко, судбинско и пресвртно.[8] И двете значења може да се разгледуваат одвоено, но и заедно, надополнувачки, па така, критичната инфраструктура поимно би можеле да ја определиме како инфраструктура што е суштествено, животно неопходна, а нарушувањето на нејзиното нормално функционирање може да доведе до загрозување на најзначајните вредности и добра врз коишто почива државата, општеството, економијата, благосостојбата и воспоставениот начин на живот. Оттука, јасно е дека всушност, заштитата на критичната инфраструктура е предуслов, претпоставка за заштитата на други пошироки општествени вредности, а самата критична инфраструктура може да се смета за инструментална, средствена вредност. Тоа подразбира дека критичната инфраструктура би можеле да ја одредиме поимно како вредност или збир вредности и добра што се од суштествено значење за економијата, државата и општеството, најчесто идентификувани како сложени материјални и нематеријални системи, чие нарушување во функционирањето или уништувањето би можело да создаде долгорочни штетни последици врз основните вредности на економијата, на државата и на општеството во целина.[9]

[8] http://www.merriam-webster.com/dictionary/critical, посетена на 20/11/2015, во Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр.9-29.

[9] Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр. 9-10.

Значи критичната инфраструктура како поим означува елемент, систем или дел од систем, лоциран во одредена држава, чии основни функции и значење се поддршка на виталните општествени функции, здравјето, безбедноста, економската и социјалната благосостојба, а чие нарушување или деструкција би имало огромни последици во самата држава, заради неможноста да се одржат тие функции. Со оглед на фактот дека инфраструктурните мрежи се меѓусебно зависни, заемно влијаат една на друга и имаат комплексни врски, нарушувањето на нивното функционирање може да доведе до огромни материјални и човечки загуби во општествата, дури и да доведе до крах на системите.

3. ДЕФИНИРАЊЕ НА КОНЦЕПТОТ КРИТИЧНА ИНФРАСТРУКТУРА

Дефинирањето, употребата и одржувањето на критичната инфраструктура е комбинација од процеси. Од аспект на тоа што треба да биде дефинирано како критична инфраструктура, треба да се излезе од рамките на класичната дефиниција и пред сè треба да се одговори најнапред на прашањата: „Дали инфраструктурата е неопходна за одржување и континуитет на одредено општество?“ и „Дали инфраструктурата функционира во ограничен контекст или во поширокото опкружување?“ (во смисла дали конкретниот одреден инфраструктурен систем е инсталиран само во локалната заедница, или е поврзан со други единици, што го прави повеќе ранлив). Ова влијае на тоа дали некој инфраструктурен систем се смета за критична инфраструктура во национален контекст или е витална вредност на локално ниво.

Во основа, концептот за заштита на критичната инфраструктура стана актуелен и за ова прашање се разви тема за анализа и за дискусија во академската и во експертската заедница; беа понудени разновидни материјали на конференции, во статии, трудови и други публикации, но сепак, ниту државите со високоразвиена технологија во транспортот, енергетиката, телекомуникациите, медицината и др., не успеа да развијат мултидисциплинарен и интегрален метод на организациско и технолошко ниво што ќе управува со овој витален

систем што треба да биде дизајниран подеднакво за да се фокусира на физичката и на дигиталната сајбер-безбедност.[10]

Во основа, не постои глобално прифатена дефиниција за тоа што претставува критичната инфраструктура. Различни држави и организации развија своја дефиниција за тој концепт, меѓу нив и OECD (2008) според која критичната инфраструктура претставува „меѓусебно поврзани информатички системи и мрежи, а прекинот или уништувањето може да предизвика сериозни последици врз здравјето, безбедноста, економската благосостојба на граѓаните, или пак на ефикасното функционирање на владата и економијата.“[11]

Според Дависон и Омар, во критична инфраструктура припаѓаат сите физички или виртуелни системи и средства што се од витално значење за нацијата, а со нивното онеспособување или уништување би се нанеле големи штети на националната и на економската сигурност, јавното здравство и безбедност,[12] односно критичната инфраструктура ги вбројува сите објекти, системи, мрежи и функции – физички или виртуелни, кои се витални за опстанокот на државата, чија инкапацитација или уништување би имало ослабувачко влијание врз безбедноста, националната економска безбедност, јавното здравје и сигурност, или која било комбинација од овие појави.[13]

Во аргументацијата на Мотеф и Парфомак, стои дека „инфраструктурата претставува основна физичка и организациска структура што му е потребна на едно општество, животна средина, организација или институција непречено да функционира во сопствени рамки.“ Тие исто посочуваат дека инфраструктурата е

[10] Homeland Security. Critical Infrastructure Security: http://www.dhs.gov/topic/critical-infrastructure-security, посетена на 4/11/2015.

[11] Lopez, J., Setola, R., Wolthusen, S., *Critical Infrastructure Protection: Information Infrastructure Models, Analysis and Defense, Springer*, 2012, стр. 39.

[12] Critical Infrastructure Protection - Multiple Efforts to Secure Control, Systems Are Under Way, but Challenges Remain – Report to Congressional Requesters – September 2007, www.gao.gov/assets/270/268137.pdf

[13] Dawson, M., Omar, M., *New Threats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference*, 2015, стр. 97.

множество на меѓусебно структурно поврзани елементи што обезбедуваат поддршка за целокупното функционирање на една средина.[14] Оттука, овие автори сметаат дека критичната инфраструктура треба да се прошири од она што е витално за националната одбрана и економската сигурност и континуитет на власта, до она што е витално за јавното здравје и безбедност како и она што е значајно за националниот морал.[15]

Сличен пристап во дефинирањето има Ларсон кој смета дека критичната инфраструктура значи систем од објекти, услуги и информациски системи, чие запирање, дефекти или уништување би имало сериозно негативно влијание врз здравјето и безбедноста на населението, животната средина, националното стопанство или врз ефикасното функционирање на државното управување.

Во елаборацијата на Денис Чалета стои дека критичната инфраструктура се однесува на сите физички и логични системи што се суштински за минимална оперативност на економијата и на владата.[16]

Покрај согледувањата на авторите, важно е да се потенцира дека и државите имаат свој дефиниционски пристап за критичната инфраструктура. Така, во САД „критичната инфраструктура" претставува термин што се однесува на широк спектар на различни фондови и средства потребни за секојдневно функционирањето на социјалните, на економските, на политичките и на културни системи. Каков било прекин на некои елементи на критичната инфраструктура претставува сериозна закана за правилно функционирање на овие системи и може да доведе до оштетување на материјалните до-

[14] Moteff J., Parfomak P., *Critical Infrastructure and Key Assets:Definition and Identification, Congresional Research Service* - The Library of Congress, 2004, стр. 5.

[15] Moteff, J., Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification, Congressional Research Service*, the Library of Congress, 2004.

[16] Radvanovsky, R. and McDougall, A, 2013, *Critical infrastructure: Homeland Security and Emergency Preparedness,* CRC Press, во Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр.5-30.

бра и приватната сопственост, човечките жртви, како и економски загуби.“[17] Исто така „критични инфраструктури се оние физички и сајбер-базирани системи, кои се од суштинско значење за минимално функционирање на економијата и на Владата на САД.[18]

Во Австралија „критичната инфраструктура ги претставува оние физички капацитети, систем на снабдување, информациски технологии и комуникациски мрежи, кои, ако се уништени или на долго време онеспособени, може значително да влијаат на социјалната или на економската благосостојба на народот, или да влијаат врз способноста на Австралија да се одржи националната одбрана и националната безбедност.

Во принцип, дефинирањето на рамката на критична инфраструктура во многу земји е направена врз основа на прецизна спецификација на критичните инфраструктури. За некои држави илустративно оваа листа е прикажана на Табела број 1.

[17] Škero M., и Ateljević V., Zastita kriticne infrastrukture i osnovne elemente usoglasivanja sa direktivom Evropske unija, *Vojno delo* 3/2015, стр. 193. http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-14-Skero.pdf , посетена на 21/05/2016.

[18] Moteff, J., Parfomak, P, *Critical Infrastructure and Key Assets: Definition and Identification*, 2004, стр.5.

Табела број 1.
Критична инфраструктура во различни земји во светот

КАНАДА	ВЕЛИКА БРИТАНИЈА	САД	ГЕРМАНИЈА	НОРВЕШКА	ШВАЈЦАРИЈА
Енергија (објекти со електричен и нуклеарен потенцијал, природен гас, нафта, производни и транспортни системи)	Енергија	Енергија	Енергија (електрична, нафта и плин)	Енергија и објекти	Објекти и служби
Комуникации	Телекомуникации	Информации и телекомуникации	Телекомуникации и информациска инфраструктура	Снабдување со нафта и гас	Телекомуникации
Сервиси (финансии, дистрибуција на храна, јавно здраство)	Здравствени служби	Јавно здравство	Јавно здравство	Телекомуникации	Дистрибуција на информации
Транспорт (воздушен, поморски, копнен)	Финансии	Храна	Банкарство, финансирање и осигурување	Јавно здравство	Јавно здравство
Безбедност (нуклерана безбедност, служби за спасување, итни служби)	Транспорт	Земјоделство	Транспортни системи	Банкарство и финансии	Храна
Влада (важни владини објекти, служби за информациски системи и мрежи)	Итна служба	Банкарство и финансии	Итни и спасувачки служби	Транспорт	Финансии
	Централна власт	Итни служби	Установи на јавни служби (полиција, војска, царина итн.)	Спасувачки служби	Транспорт
	Вода и одводнување	Влада		Одбрана	Цивилна одбрана
		Основна одбранбена индустрија		Полиција	Администрација
		Вода		Општествена безбедност	Воена одбрана
		Хемиска индустрија и опасни материи			Снабдување со вода

Извор: Škero M. Zastita kriticne infrastrukture, стр. 193-194.

Наведените дефиниции за критична инфраструктура ја потврдуваат суштината на значењето на овој поим, што подразбира ресурси и добра неопходни за непречено функционирање на економијата и на општеството.[19] Оттука, инфраструктурата се смета за логистичка функција со која се обезбедуваат поволни услови за квалитетно вршење на другите функции за логистичка поддршка. Инфраструктурата се дефинира и како системи направени од човек, процеси што функционираат во согласност и во синергија за да создадат и да распространат непречена алокација на стоките и услугите.

Значи целокупните анализи околу дефиницискиот пристап за критичната инфраструктура се однесуваат на тоа дека таа е столбот на државата. Оттука, ако направиме обид да ја дефинираме критичната инфраструктура ќе наведеме дека таа е сеприсутен феномен што е олицетворен во многу сектори кои директно или индиректно придонесуваат за нормалното функционирање на државата, а чие оневозможување или онеспособување ќе придонесе да има сериозни последици врз националната економија, здравјето на луѓето и државата во целост.

4. ПОТРЕБА ОД ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Поимот заштита на критичната инфраструктура (Critical Infrastructure Protection) во публикациите за прв пат се јавува во 1997 година, но концептот за заштита на критична инфраструктура започнува да се развива од 1962 година. Во времето на Кубанската ракетна криза, претседателот на САД, Кенеди и претседателот на СССР, Хрушчов имале проблеми во меѓусебната комуникација токму поради неадекватната телекомуникациска технологија.[20] Поради

[19] Škero M., и Ateljević V., Zastita kriticne infrastrukture i osnovne elemente usoglasivanja sa direktivom Evropske unija, *Vojno delo 3*/2015, стр. 193. http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_3-2015/67-2015-3-14-Skero.pdf, посетена на 21/05/2016.

[20] Lewis, T. G, *Critical Infrastructure Protection in Homeland Security: defining a networked nation,* 2006.

тоа телекомуникациите се првиот сектор што се смета за критичен. Иако е неоспорно значењето на телекомуникациите како критична инфраструктура, сепак, како што апострофираат Чалета и Радовиќ во однос на критичната инфраструктура треба да се примени сеопфатен пристап–*Sine Qua Non.*[21] Во таа смисла, критичната инфраструктура нема да се сведе само на телекомуникацискиот сектор. Напротив, поимот критична инфраструктура ќе се однесува на сите физички и логични системи што се суштествени за соодветна оперативност на економијата и на владата.[22] Оттука оние инфраструктури што се од таква важност за општеството, каде што, нивното нефункционирање или ограничено функционирање, може да создаде сериозни последици и проблеми ги дефинираме како „критични инфраструктури" и потребно е да бидат третирани како на национално така и на меѓународно ниво.[23] За граѓаните во основа тоа е електричната енергија што ја користат во своите домови, водата што ја пијат, транспортот со кој се превезуваат, комуникациските системи на кои се потпираат итн. За државите критичната инфраструктура се средствата, системите и мрежите, било да се физички или виртуелни, што се од витално значење за државата и нивното онеспособување и уништување, ќе предизвика ослабувачки ефект на безбедноста на државата, националната економска сигурност, јавното здравје, јавната безбедноста сл.[24]

Оттука не е доволно да се заштити една специфична област на инфраструктура, туку клучно е да се заштити нивната опслужувачка технологија. Затоа од клучно значење е секоја држава да има систематски пристап кон постојната инфраструктура, како и идентификација и приоритизација на критичната инфраструктура.

---

[21] Caleta, D. and Radovic, V, *Comprehensive approach as "Sine Qua Non" for critical infrastructure protection, IOS Press BV,* 2015.

[22] Radvanovsky, R. and McDougall, A, *Critical infrastructure: Homeland Security and Emergency Preparedness,* CRC Press, 2013, во Правна рамка за обезбедување на критичната инфраструктура, Комора на РМ за приватно обезбедување, Скопје, 2016, стр.9-29.

[23] http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html, посетена на 14/03/2014.

[24] Славески С. *Предизвик на современите општества*, 2015.

Безбедноста на критичната инфраструктура е под закана од два фактора. Првиот е природниот фактор и тука спаѓаат опасностите од земјотреси, пожари, поплави, епидемии и сл., и вториот фактор што се однесува на намерното предизвикување штети (кражби, вандализам, тероризам итн).[25] Значи, што се однесува до заканите за критичната инфраструктура, тие може да бидат вештачки, како резултат на тероризам или други криминални активности, но може да бидат и природни, предизвикани од временските услови, како што се бури, вулкански ерупции, поплави или други еколошки катастрофи. Исто така, критичната инфраструктура може да биде загрозена и од болести, пандемии и да влијае врз голем број критичен персонал.[26]

Во основа, државите се одговорни за заштита на населението и обезбедување на одредено ниво на социјална функционалност и безбедност, но фактот дека дел од критичната инфраструктура е во државна сопственост, а дел е во приватна сопственост (домашни или странски компании) и дека постојат сопственици кои не поседуваат исти вредности и ставови на обезбедување на системот на критичната инфраструктура се наметнува потреба од еден мултиваријантен пристап на државата и на операторите. Многу западни земји го имаат поголемиот дел од критичните инфраструктури во приватна сопственост, а државата со цел да обезбеди непречено работење и функционирање на критичните инфраструктури[27] – вложува големи напори за да обезбеди соработка на државните структури и приватните лица.[28]

---

[25] Flammini, F., *Critical Infrastructure Security: Assessment, Prevention, Detection, Response,* 2012, стр.9.

[26] Critical Infrastructure Security and Protection: The Public-Private Opportunity White Paper by CoESS – Confederation of European Security Services © December 2010.

[27] National critical infrastructure protection – regional perspective-Belgrade, December 2013 UDC726.9:75.041.5, ID176374796, Mihaljević B., Toth I., Stranjik A., Impact of Critical Infrastructure Ownership on the National Security of the Republic of Croatia.

[28] Во Германија 4/5 на критичната инфраструктура се во приватни раце. Во САД околу 85% од критичните инфраструктури се во приватна сопственост, но реалноста е дека пазарните сили сами за себе не се доволни да ја предизвикаат потребната инвестиција во заштитата во P. Auerswald,

Со оглед на фактот дека системите на критична инфраструктура ги преминуваат националните граници, нивната заштита и отпорност се грижа на владите, како и на регионалните и на меѓународните организации. Меѓузависноста на системите на критичната инфраструктура подразбира дека е неопходен заеднички напор и соодветни механизми што ќе ја осигурат безбедноста и отпорноста на системите на критична инфраструктура.

Со цел да се обезбеди целосна слика за трендовите и за методите за ефикасна заштита на критичната инфраструктура, акцентот е потребно да биде ставен на следните аспекти:

– Процена, земање предвид на ризиците и ранливоста, како и очекуваните резултати од можните последици. Ова се постигнува со методите на анализа, моделирање и симулација.
– Превенција, односно редукција на ризикот со прогнозирање на ефектите од заканите. Оваа димензија се постигнува по пат на заплашување, како и со други „пасивни“ противмерки (дизајнирана безбедност).
– Детекција – тоа е способноста за навремено препознавање на абнормалните состојби и однесување. Овој аспект се реализира со активни сензори и други технолошки апарати.
– Одговор – поточно, брза реакција на заканите. Овој аспект се реализира со методот на рано предупредување, следење на ситуацијата и системи за поддршка во донесувањето одлуки.[29]

Можни методологии што помагаат во идентификација на неопходните капацитети потребни за соочување со посебните закани вклучуваат:

– идентификација на основната инфраструктура, што е од клучно значење за непречено функционирање на општеството;
– евалуација на закани: проактивна идентификација на елементите на критичната инфраструктура, кои предвид ги земаат идните трендови;

L.M. Branscomb, T.M. La Porte, E.Michel – Kerjan – *The Chalenge of Protecting Critical Infrastructure – issues in science and tehnology,* 2005, стр. 77.

[29] Flammini, F., *Critical Infrastructure Security: Assessment, Prevention, Detection, Response*, 2012, стр.9.

– во оваа фаза е потребно да се изврши анализа на соодветните разузнавачки информации;
– евалуација на загрозувањето: утврдување на ефектите од инцидентот врз критичната инфраструктура, земајќи ја предвид ранливоста на постојните објекти.
– процена на ризикот: потребно е да се создаде листа на постојни веродостојни ризици, во зависност од потенцијалните ризици во однос на нивната природа, потенцијални цели, како и оцена на влијание.[30]

Според американските искуства заштитата на критичната инфраструктура, подразбира сите добра, имот и физички и логички системи, неопходни за минимум изведба на економијата и на владата. Колку овие системи стануваат сè поповрзани, се појавуваат два големи тренда. Првиот тренд се однесува на темпото со кое еволуира технологијата. Ова не е константа во целиот свет, и како што ќе изминува времето, ќе се сведочи или за општества што заостануваат, за општества што се трудат да го одржат темпото на развој, за општества со тенденција да одржуваат контрола врз нивото на развој, како и за општества што прават револуционерни скокови во напредокот. Вториот тренд го релативизира значењето на критичната инфраструктура. Конкретно, тоа што е критична инфраструктура од витално значење и приоритет за заштита на една заедница, може да нема исто значење во некоја друга заедница. Земајќи ги предвид изворите за загревање на домовите, како пример, во некои северни делови во светот огревот има огромно значење, а во географски потопли места тоа е релативно занемарлив проблем. Оттука важно е при проценатa за ранливоста и заштитата на критичната инфраструктура да се има предвид контекстуалниот аспект, т.е. (економското, политичкото, културното, еколошкото опкружување).[31] Со

[30] National Critical Infrastructure Protection – Regional Perspective-Belgrade, December, 2013, UDC726.9:75.041.5, ID176374796, Marjanović M., and Nađ I: Assesment of Threats to Critical Infrastructure Facilities from Serious and Organized Crime, стр. 78.

[31] Radvanovski, R., McDougall, A: *Critical Infrastructure: Homeland Security and Emergency Preparedness,* Third Edition. CRC Press, Taylor and Francis Group, 2013, стр. 23-77. https://books.google.mk/books?id=aVInAA

тоа заштитата на критичната инфраструктура е многу важен процес од повеќе аспекти – економски, политички, безбедносен, но и социетален и еколошки.[32] Ова се должи на фактот од анализите дека ако дојде до попречување или до уништување на дел од системот за критична инфраструктура, ќе има каскаден ефект што ќе се прелее од еден елемент на друг, без разлика дали потекнува од природен или од антропоген извор.

Во основа, ако ја разгледаме потребата од заштита на критичната инфраструктура низ призмата на примерот во САД, преку управувањето со ризици ќе видиме дека таа е многу широка и составена е од партнерства помеѓу сопствениците и операторите; федерални, државни, локални и територијални влади; регионалните ентитети; непрофитни организации; академијата и др. Управувањето со ризици од сериозни закани и опасностите поврзани со физички и со сајбер закани врз критичната инфраструктура бара интегриран пристап во поглед на:

– идентификување, спречување, откривање и подготовка за справување со закани и опасности на критичната инфраструктура;
– намалување на ранливоста на критичните системи и мрежи и
– ублажување на можните последици од инциденти или негативни настани што се случуваат врз критичните инфраструктури.[33]

Успехот на овој интегриран пристап зависи од целиот спектар на способности, експертизи и искуства во инфраструктурите и секако од засегнатите страни.[34]

За разлика од САД процесот на идентификација на критичните инфраструктури во ЕУ се темели на три фактора, а тоа се:

AAQBAJ&printsec=frontcover&dq=critical+infrastructure&hl=en&sa=X&redir_esc=y#v=onepage&q=critical%20infrastructure&f=false

[32] Vasilellis, E., Stergiopoulos, G.: Critical Infrastructure Protection Tools: A Survey. https://www.cis.aueb.gr/Publications/2016-%20Poster%20CIP%20Tools.pdf, посетена 24/06/.2016.

[33] Partnering for Critical Infrastructure Security and Resilience homeland security - USA, NIPP 2013.

[34] Исто., стр. 7.

1. човечки загуби, во кој се проценува потенцијалниот број на човечки загуби или повреди;
2. економскиот ефект, преку кој се проценува значењето и големината на економските загуби и/или деградација на производите или сервисите вклучувајќи ги и негативните ефекти врз човековата околина;
3. општествениот ефект, преку кој се проценуваат ефектите на јавната самодоверба, физичката загриженост и нарушувања во секојдневното живеење, вклучувајќи ги и основните сервиси.[35]

Со оглед на големиот број критични инфраструктури, се појавуваат значителни предизвици и тешкотии во остварувањето на заштитата, а тука како покарактеристични би ги издвоиле:

– Сложеноста на критичните инфраструктурни сектори. Невозможно е да се заштити целата критичната инфраструктура и сродните компоненти. На пример, во секторот транспорт, речиси е невозможно да се заштитат голем број километри долги комуникациски линии, голем број аеродроми, морски пристаништа, голем број мостови и слични структури.
– Недостаток на надлежност и одговорност во секторите каде што се ангажирани повеќе државни и приватни субјекти.
– Недоволна размена на информации меѓу институциите, што доведува до нова ранливост и влијае на ефикасноста на одговорите за заштита на критичната инфраструктура.
– Сложеност на знаење во поглед на посебни вештини што треба да се познаваат и пред политиките и пред стратегиите во областа на заштита на критичната инфраструктура.
– Меѓузависност на одделните сектори на критичната инфраструктура. Овој проблем дополнително влијае на комплексноста на заштита на критичната инфраструктура.

[35] Metodologija izbora kriticne informaticke infrastructure, Ministarstvo za informaciono društvo Itelekomunikacije Crne Gore – Oktobar, 2014, стр. 8.

– Несовршеноста на алатките за анализа на критичната инфраструктура и неговата ранливост. Науката обично се фокусира на општите пристапи, алатки и решенија.
– Асиметрични конфликти и сл.[36]

Нема дилема дека крајната цел на заштита на критичната инфраструктура е постигнување на соодветни безбедносни и заштитни потребни нивоа создавајќи континуитет на функционалноста на критичната инфраструктура. Со оваа фундаментална цел, важно е да се обезбеди процесот на опоравување во случај на деградација/катастрофа на функционалноста на системот. Идентификуваните и поставените компоненти на инсталираниот систем мора да го издржат влијанието на сите закани и ризици. Имајќи го предвид претходно наведеното, можеме да констатираме дека оптималното ниво на заштита на критичната инфраструктура претставува комбинација од: систем на физичка заштита; информатичка безбедност; планирање/управување со бизнис-сектор; административни процедури за безбедност и безбедносни мерки за вработените.[37]

[36] Prezelj, I., *Konceptualna opredelitev kritične infrastrukture*, FDV, Ljubljana, 2008, стр. 13. - National critical infrastructure protection – regional perspective- Belgrade, December 2013, UDC726.9:75.041.5, ID176374796, Mihaljević B., Toth I., Stranjik A., Impact of Critical Infrastructure Ownership on the National Security of the Republic of Croatia.

[37] Марија Мичовић, *Специфичности заштите критичне инфраструктуре*, Криминалистичко-полицијска академија, Београд, 2015, стр. 166-167.

II глава

ИНДИКАТИВНА ЛИСТА НА СЕКТОРИ НА КРИТИЧНА ИНФРАСТРУКТУРА

1. ИНДИКАТИВНА ЛИСТА НА СЕКТОРИ

Голем број држави имаат направено прецизна спецификација на критичните инфраструктури и генерално земено тоа се исти или слични сектори, што се повторуваат во повеќе земји со надополнување на одделни специфични сектори, карактеристични „условно“ за „посилните“ држави.

Примерите во САД, во Германија, во Шведска, во Холандија итн., говорат дека нема некои поголеми сигнификантни разлики во листата на сектори. Така, во *САД* листата вклучува: енергија, информации и телекомуникации, јавно здравство, храна, земјоделство, банкарство и финансии, службите за итна помош, Владата, основна одбранбената индустрија, вода, хемиска индустрија и опасни материи, пошти, а во *Германија* листата се однесува на: енергија (електрична, нафта и гас), телекомуникации и информатичка инфраструктура, јавно здравство (вклучувајќи и снабдување со вода и со храна), банкарство, финансии и осигурување, транспортни системи, итни и спасувачки служби, владата и јавните служби (вклучувајќи: полиција, царина и вооружените сили), додека во *Шведска* идентично како Германија се потенцирани: енергија, телекомуникации, електронски информациски служби, јавно здравство, храна, банкарство и финансии, транспорт, вода, општествени вредности.[38]

Во *Канада* индикативната листа на сектори вклучува: енергија (објектите на електрична и нуклеарна енергија, природен гас и нафта, производни и транспортни системи), комуникации, сервиси (финансии, дистрибуција на храна, јавно здравство, транспорт – воздушен, морски и копнен, безбедност – сигурност (нуклеарна сигур-

[38] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од виталeн интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016.

ност, служби за спасување, итни служби), влада (важни владини објекти, служби и информатички системи и мрежи).[39]

Во *Велика Британија* листата на сектори се однесува на: енергија, телекомуникации, здравствени служби, финансии, транспорт, итни служби, Владата, вода и одводни системи, додека во Австралија спаѓаат: енергија (гас, нафта и производи од нафта, производство и дистрибуција на електрична енергија), комуникации (телекомуникации: телефони, интернет, кабловски ТВ, сателити, масовни електронски медиуми), здравство (болници, јавно здравство, лаборатории за истражување и развој), снабдување со храна (земјоделско производство, складирање и дистрибуција), финансии (банки, осигурување, берзи), транспорт (воздушен, патен, морски и стоковно дистрибутивни центри), владини служби (објектите на одбраната и безбедносни служби), Парламент, важни министерства, странски дипломатски претставништва и резиденции, итни служби (полиција, противпожарни, медицински и други служби), услуги (вода, одводнување и прочистување на отпадните води), производство (воена, тешка и хемиска индустрија), национални вредности (градежни, културни, спортски и туристички вредности).[40]

Во *Норвешка* листата на сектори вклучува: енергија и објекти, снабдување со нафта и гас, телекомуникации, јавно здравство, банкарство и финансии, транспорт, спасувачки служби, одбрана, полиција, јавна безбедност, а во *Холандија* се посочуваат: енергијата и енергетските објекти, телекомуникации, јавно здравство, храна, банкарство и финансии, транспорт, јавен ред и безбедност, влада, одбрана, судство, вода за пиење, управување со води, објекти со висок ризик во вонредни ситуации, додека во *Швајцарија* листата се однесува на: објекти и служби, телекомуникции, дистрибуција на информациите, јавно здравство, храна, финансии, транспорт, цивилна одбрана, администрација, воена одбрана, снабдување со вода, социјална безбедност, индустрија, истражување и образование.[41]

[39] Исто., стр. 12-98.

[40] Исто., стр. 12-98.

[41] Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama, Zdenko Kljaic, dipl.ing. Member, IEEE, Sadko Mandžuka, dr.sc.

Генерално, наведените идентификувани листи на сектори се во корелација со Директивата на Европската унија за критични сектори, а тоа се: енергијата, информациските и комуникациските технологии, водата, храната, финансиите, јавната администрација, транспортот, хемиската индустрија, истражувачките дејности,[42] со сите нивни капацитети и дејности, производи или услуги.

2. СПЕЦИФИЧНИ СЕКТОРИ

Често е само една инфраструктура (во еднина), но често погрешно се става во множина, што се должи на погрешното верување дека штом има многу елементи, тогаш има и многу инфраструктури. Критичната инфраструктура составена од бројни сектори претставува систем од елементи што се наоѓаат најчесто на територијата на една држава, што се од суштинско значење за одржување на виталните јавни функции, здравје, безбедност, сигурност, економска или социјална благосостојба на населението, и чие нарушување или уништување би имало значителни последици во дадената држава како резултат на неможноста да ги задржи овие функции.

Во продолжение ќе бидат објаснети клучните специфични сектори што најчесто се сретнуваат во индикативните листи на национално ниво. Клучната дискусија ќе се води околу секторите: енергетика, информатички и комуникациски технологии, сообраќај и транспорт, водни системи, храната како критичен енергенс, хемиски сектор, финансиски и банкарски сектор, здравствена заштита и јавно здравство.

2.1. Енергетика

Историски гледано, борбата за превласт на енергетските извори била постојан предизвик за голем број држави. Дополнително,

Member, IEEE, Pero Škorput, mr.sc. Member, IEEE 18. Telekomunikacioni forum Telefor.

[42] Green paper on a European Programme for critical infrastructure protection Brussels, 17.11.2005, COM, (2005), 576 final, Annex II.

ако се знае дека тој што ги има на располагање критичните енергенси (нафта, гас и други природни извори ќе доминира во светски рамки. Тоа е јасен сигнал дека овие енергенси ги детерминираат вкупните односи во светски рамки. Оттука со сигурност може да се каже дека недостатокот на енергија, несигурноста во набавката на електрична енергија итн., може директно да влијаат во намалувањето на способноста на државата.

Значи, енергетската инфраструктура е основа на сите фундаментални процеси за функционирање на современото општество. Долгорочното, односно долготрајното нарушување на овој сектор би довело до огромни последици, така што многу од активностите за нормално функционирање на државата би биле невозможни.

Енергетската инфраструктура е поделена на три меѓусебно поврзани сегменти, вклучувајќи: електрична енергија, нафта и природен гас.[43] Секој од овие извори бара единствен сет на активности. Енергетската критична инфраструктура може да биде во сопственост на државни, федерални, локални и приватни субјекти како и на некои други корисници, како што се, на пример, големите индустриски и финансиски институции.[44] Оттука е значајно да се напомени дека општествениот контекст за заштита на критичната енергетска инфраструктура добива поголема тежина и станува потранспарентен од развојни и институционални причини, бидејќи националната критична инфраструктура сè повеќе е под притисок на меѓународен план и е во корелација и меѓузависност со најголемите производители и потрошувачи на енергија во интегрирана Европа.

Во услови на либерализација на производството и дистрибуцијата на енергија, безбедноста на приватизираните енергетски производни погони не може да биде осигурена само преку јавниот сектор, односно исклучиво на товар на државата. Оттука произлегуваат проблемите со интерното осигурување што правните лица го имаат при производство и дистрибуција на енергијата, како и проблемот со осигурувањето на преносните делови на енергетските постројки, со што се отвораат и дополнителни проблеми во односите помеѓу приватниот и јавниот сектор. Истото важи и за управувањето

[43] http://www.dhs.gov/energy-sector, посетена на 3/3/2016.
[44] http://www.dhs.gov/energy-sector, посетена на 3/3/2016.

со резервите со енергија и во делот на регулација на односите помеѓу објектите на критичната енергетска инфраструктура и локалните заедници. Ризикот е иманентен на начинот на кој е изградена критичната енергетска инфраструктура, а комплексноста на инфраструктурата дополнително го зголемува интензитетот на ризикот. Поради тоа неопходни се дополнителни напори за обезбедување на системите на критична енергетска инфраструктура.[45]

Во следната табела, претставени се трите клучни енергетски извори дефинирани во стратегиските документи во САД:

ЕЛЕКТРИЧНА ЕНЕРГИЈА	НАФТА	ГАС
Производство • Фосилни горива - Јаглен - Природен гас - Нафта • Нуклеарни горива • Хидроелектрични • Обновлива енергија **Пренос** • Базни станици • Мрежи • Контролни центри **Дистрибуција** • Базни станици • Мрежи • Контролни центри **Контролни системи** **Пазари на електрична енергија**	**Сирова нафта** • Внатрешни нафтени полиња • Надворешни нафтени полиња • Терминали • Транспорт (нафтоводи) • Складирање **Објекти за преработка на нафта** • Рафинерии • Терминали • Транспорт • Нафтоводи • Складирање • Контролни системи • Пазари на нафта	**Производство** • Внатрешни полиња • Надворешни полиња **Процесуирање** **Транспорт (гасоводи)** **Дистрибуција (гасоводи)** **Складирање** **Објекти за течен природен гас** **Контролни системи** **Пазари на гас**

Табела бр.2. **Клучни сегменти на енергетскиот сектор**

[45] http://www.pilar.hr/kritina-infrastruktura-u-hrvatskoj#sadržaj, посетена на 23/09/2016.

Треба да се нагласи дека важен аспект на заштита на критичната инфраструктура е разбирањето на концептот за енергетска безбедност, што произлегува од влијанието на енергијата на целокупниот економски живот во модерните општества. Ефективната заштита на енергетската критична инфраструктура е една од основните, ако не и клучна идеја за енергетска безбедност. Фактот што енергетската безбедност е комплексен концепт, обично Европската унија го дели на долгорочна безбедност (стабилна енергетска политика во ЕУ како и помеѓу ЕУ и земјите снабдувачи) и краткорочна безбедност (градење способност да се избегнат нарушувања во снабдувањето со енергија во вонредни ситуации).[46]

Од ова произлегува дека енергетскиот сектор претставува глобален проблем што ги надминува националните граници (мрежата на енергетската инфраструктура, на пример, во Европската унија ги надминува границите на ЕУ така што во комплексноста на синџирот на снабдување треба да се нагласи и меѓусебната зависност). Оттука заштитата на енергетскиот сектор бара заеднички одговор од сите субјекти кои имаат значајна улога во безбедноста на енергетскиот сектор почнувајќи од државата и секако одговорна улога имаат и сопствениците на енергетската инфраструктура, без разлика на локацијата. Значи, заштитата и подобрувањето на отпорноста од закани предизвикани од вештачки или од природни катастрофи бара континуирана будност, планови и обуки во комбинација со сеопфатни мерки за подготвеност, како од физички така и од сајбер-заканите.

Генерално, ако ги анализираме САД како водечка сила во поглед на заштита на критичната инфраструктура во делот на енергетиката, ќе видиме дека таму преку Министерството за енергетика и другите субјекти, покрај другото се залагаат и за стабилна и еластична енергетска инфраструктура што се базира на соодветен план што треба да обезбеди континуитет на бизнисот и на услугите. Во таа смисла, безбеден и сигурен систем опфаќа споделување на информациите, ефективни програми за управување со ризици,

[46] Klemen Groselj, *Critical Infrastructure Protection and the Energy Sector Counter – Terrorism Challenges regarding the Processes of Critical Infrastructure,* Ljubljana, Seprember, 2011, стр.136.

координирани активности за одговор и доверлив однос помеѓу јавниот и приватниот сектор на сите нивоа. Во овој контекст, САД во својот план апострофираат:

- воспоставување свесност за енергетскиот сектор преку навремено информирање и соодветна размена на информаци помеѓу јавниот и приватниот сектор;
- примена на соодветни принципи за справување со ризици со имплементација на физички и информатички мерки, заради подобрување на подготвеноста, обезбедувањето, еластичноста (флексибилноста);
- спроведување ефикасно планирање при вонредни ситуации и катастрофи, вклучувајќи обуки и вежби за да се подобри реагирањето во такви ситуации;
- јасно дефинирање на улогата и одговорностите на федералните, на локалните, на државните и на приватните сектори во насока на подобрување на координацијата помеѓу партнерите;
- разбирање на важноста на меѓузависноста и соработката со други сектори и имплементирање на знаењето во планирањето и во операциите;
- зајакнување на јавната доверба и довербата помеѓу партнерите, заради зајакнување на способноста на секторите за да се справат со ризици и имлементирање на ефективни мерки за обезбедување и посткризно опоравување.[47]

Нема дилема дека енергетскиот сектор има потреба да биде уреден со соодветна безбедносна политика и стандарди. Затоа, во контекст на обезбедување на енергетскиот сектор како дел од критичната инфраструктура, потребно е да се воспостави еден поширок опсег на заштита, не само во делот на физичката и на техничката заштита, туку и со контрибуција на сите засегнати страни со адекватна безбедносна политика во сите области.[48]

---

[47] Energy Sector-Specific PlanAn Annex to the National Infrastructure Protection Plan2010, Homeland Security – United States Department of Energy.

[48] Vrsec M., *Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) Infrastructure for the Functioning of State, Economy and Civil Society*. Counter – terrorism Challenges regarding the Processes of critical infrastructure : Ljubljana : Seprember 2011, стр.125.

2.1.1. Процена на заканите за енергетските компании

Проценатa на заканите на енергетските компании бара размислување за специфични карактеристики на енергенсите (електрична енергија, нафта и гас); потоа постоење соодветни закони поврзани со енергетиката, соодветни системи за обезбедување; специфични карактеристики на мрежи, локации, објекти, процеси, опрема и логистика, број и структура на вработените, бизнис-партнери, градежни компании и др. Базата на податоци за процена на заканите во енергетската компанија опфаќа:

- општи дескриптори за енергетската компанија;
- вредност на имотот;
- анкети и интервјуа;
- преглед на документацијата поврзана со безбедноста;
- испитување на бизнис-процесите;
- оперативно испитување на објектите и опремата;
- испитување на мрежите и логистиката;
- анализа на собраните податоци;
- поставување матрица на закана;
- идентификација на потребите за обезбедување.[49]

Гледано од просторен аспект, целосен пристап на заштита на енергетските компании се остварува преку:

- заштита на мобилни и на дистрибутивни мрежи, складишта, транспорт на енергија и целосна логистика (одржување на инсталациите за нафта и за гас, сигурносни аларми за заштита на критичките точки во инсталациите, хеликоптерска контрола на инсталациите, употреба на сателитска навигација и др.);
- заштита на периметар и локации на енергетските компании (огради, врати, контрола на влез и излез, видеонадзор и контрола на паркинг, итен пристап и сл.);
- заштита на енергетски објекти, згради, опрема и процеси (контрола на пристап и видео надзор);

[49] Vrsec M., *Managing Corporate Security in the Energy Sector: Energetics as a Vital (Critical) infrastructure for the Functioning of State, Economy and Civil Society*. Counter – terrorism Challenges regarding the Processes of critical infrastructure: Ljubljana: Seprember, 2011, стр.119.

– заштита на влезовите на објектите (заштита од провала, контрола на пристап и видеонадзор во однос на заканата);
– заштита во објектите – просториите (физичка и електронска заштита на компјутерската опрема, класифицирана документација, податоци, информации, архиви и електронски комуникации).[50]

2.1.2. Воспоставување интегрален систем за обезбедување на енергетскиот сектор во ЕУ

Европската енергетска политика ги поттикнува членките на ЕУ да ги подобрат системите за обезбедување во областа на енергетиката. Во таа насока ЕУ ја зголемува безбедносната политика во областа на енергетиката за што постои Директива на Европскиот совет што претставува конкретен европски документ за идентификација и одредување на европската критична инфраструктура, но и потребата да се унапреди заштитата. Главните насоки на оваа директива се:

– приоритетна задача за секој што менаџира со критичните инфраструктури е заштита од терористички закани;
– заштита од сите опасности што доаѓаат од човечки или од технолошки закани како и заканите што доаѓаат од природни катастрофи;
– примарната и конечната одговорност за заштита на критичната инфраструктура е дадена на државите членки на ЕУ и на сопствениците и операторите со овие инфраструктури;
– операторите на критичните инфраструктури треба врз основа на проценатa на заканите и безбедносните ризици да направат сигурносни планови што би биле во согласност со Директивите на ЕУ;
– да се забрза подобрувањето на безбедноста на критичната инфраструктура и развој на општите методологии за категоризација на опасностите, ризиците и ранливоста на критичната инфраструктура;

[50] Исто., стр.126.

- потребно е да се заштитат класифицираните податоци во согласност со актите на Унијата;
- сопствениците и операторите на критичната инфраструктура треба да ги следат докажаните практики при воспоставување на сигурносните механизми во енергетиката и транспортот, а кои што се дефинирани од членките на ЕУ;
- секоја членка на ЕУ треба да определи офицер за безбедност што е овластен за координација со другите земји членки;
- општата безбедност во енергетиката се подразбира како физичка, техничка и електронска заштита на енергетското производство, мрежа, транспорт, објекти и опрема и персоналот вработен во енергетските компании.[51]

Владите на земјите членки на Европската унија вложуваат огромни напори со цел да се спречи злоупотребата на енергетскиот сектор и да се воспостави функционална законската регулатива бидејќи многу од развиените држави во нивните безбедносни и воени тела го имаат препознаено проблемот на комплексноста и сложеноста на проблематиката. Оттука за адекватна безбедност на енергетскиот сектор се предлагаат мерки за обезбедување и заштита токму поради непосредната зависност на државата од енергетскиот сектор.

Сепак, за да се подобри обезбедувањето на критичната инфраструктура, потребно е да се развијат едноставни методологии за воспоставување и категоризирање на опасностите (безбедносни закани, ризици и ранливост во рамките на критичните инфраструктури). Поради тоа сопствениците и операторите на критичните инфраструктури вклучувајќи го и енергетскиот сектор, потребно е да ја следат добрата практика за воспоставување безбедносни системи регулирани во согласност со актите на ЕУ преку воспоставување на офицер за соработка што ќе биде главен за координација со другите држави, но ќе обезбедува и совети за државните оператори на критичните инфраструктури.[52]

[51] Исто., стр.124-125.

[52] Исто., стр.124-130.

2.2. Информатички и комуникациски технологии

Електронската комуникациска мрежа е преносен систем и таму каде што е применливо овие комуникациски или насочувачки опреми но и други средства овозможуваат пренос на сигнали преку жичени, радиобранови, оптички или други електромагнетни средства, вклучувајќи сателитски мрежи, фиксни (со комутација на кола или комутација на пакети, вклучувајќи и интернет) и мобилни земски мрежи, електроенергетски кабелски системи ако се користат за пренос на комуникациски сигнали, радиодифузни мрежи и кабелски телевизиски мрежи, независно од видот на информациите што се пренесуваат.[53]

Секторот за информатичка технологија е од централно значење за безбедноста, економијата, јавното здравство и безбедност на нацијата. Бизнисот, стопанството, владата, академските институции и граѓаните се сè повеќе зависни од информатичката технологија. Од тие причини, безбедноста на овој сектор потребно е да се темели на заштита: на информациските системи и мрежи, на инструментализација, автоматизација и контролни системи, на интернетот, на обезбедување на фиксната телекомуникација, на обезбедување на мобилната телекомуникација, на радиокомуникацијата и навигацијата, на сателитска комуникација, на емитувањето и др. Комплексноста и динамичниот развој на секторот го прави сложен од аспект на идентификување на заканите и слабостите што бара огромна компаниска соработка и креативен начин на заштита. Иако инфраструктурата што се однесува на информатичката технологија има одредено ниво на својствена еластичност поради големите меѓузависности, сепак претставува предизвик, како и можност за координирање на активностите помеѓу јавните и приватните сектори. Фактот дека потенцијалот на терористичките организации и поединци и во иднина постојано ќе се зголемува заедно со промените во информатичко–комуникациските технологии, справувањето со ваков вид закани е многу

[53] http://mio.gov.mk/files/pdf/dokumenti/zakoni/ посетена на 15/10/2016.

комплицирана задача на сите критични инфраструктури, што ги обединува оваа област.[54] Исто така, глобалното вмрежување во системот на комуникациската и на информатичката технологија стана основа на организираниот криминал, додека пак тероризмот доби уште една алатка во своите раце. Од аспект на употреба на интернетот во функција на организираниот криминал и тероризмот би ги издвоиле планирањето на противправните дејства, крадење податоци или хакирање, предизвикување насилства, регрутација и радикализација на корисниците на овие мрежи и др. Во овој контекст, нападот на информатичките системи, може да се дефинира како директна акција против мрежата или информатичкиот систем, со цел неовластено да се пресретне или да се прекине некоја операција, да се преземе контрола или да се уништи, да се промени или да се корумпира податокот (со меморирање или обработка).[55]

Улогата на државата во поглед на заштита на критичната инфраструктура од областа на ИТ безбедноста е клучна, но исто така секако дека е важна и улогата на операторите, односно компаниите што стопанисуваат со овие критични инфраструктури. Оттука заштитата претставува примарна дејност каде што најчесто опфаќа политика, односно стратегија за ИТ безбедност поткрепена со регулативи и нормативно правни акти во насока на:

- Управување со физичкиот пристап – обезбедување физички пристап до клучните компоненти само за ИТ персоналот, вклучувајќи ја и можноста за надзор. Оваа област е испреплетена со физичката заштита.
- Одделни услуги, автентикација и авторизација – централната база на податоци на корисници, овозможува управување со нивните податоци за идентификација и пристап, вклучувајќи логирање и следење на пристап.

[54] https://www.dhs.gov/information-technology-sector посетена на 24/10/2015.

[55] Stallings William, Network and Internetwork Security – Principles and Practices, Prentice Hall, Englewood Cllifs, New Jersey 1995., стр.29–30, преземено од *Корпорациски безбедносен систем*, Комора на РМ за обезбедување на лица и имот, Скопје, 2012, стр.165-243.

Потенцијалната експанзија може да претставуваат системи за управување со идентитетот, одделно најавување, или системи за мултифакторска проверка.

- Безбедносен надзор и управување со системот – важен елемент на сигурноста што овозможува собирање информации за настани од разни системи, обединети на едно место и потоа нивно оценување.
- Проверка на сите оперативни активности или мерки што ќе подразбира дека мора да се проверат од аспект на водење на утврдената политика за безбедност или од појава на ранливост – следење на придржувањето, скенирање за ранливост и тестови.
- Антивирусна заштита – често ја сочинува основата на ИТ безбедноста. Важно е да се изгради една или повеќе бариери на потенцијалната траса на заштита, односно повеќеслојна антивирусна заштита. Суштински елемент е централно управување и следење на антивирусните решенија и понатаму заштита од нови видови напади.
- Заштита на веб-периметарот се користи за одделување на интернетот од други мрежи на други субјекти и јавни мрежи. Често е составена од заштитен ѕид (firewall), IDS/ IPS сензор, филтри за содржина, антиспам и антивирусна заштита.
- Проверка на содржината – филтрирање на содржините на интернет со цел да се елиминираат несаканите содржини кога се трансферираат во мрежата на организацијата или во друга насока.
- Енкрипција на податоците – систем за да се спречи упад во податоците, нивна можна кражба или модификација. Се користи за да се заштитат податоците зачувани на диск, отстранливи медиуми и комуникација преку недоверливи мрежи. Особено тоа се системи за онлајн диск енкрипција, системи на датотеки, делови, електронска пошта, симетрична и асиметрична енкрипција на низа податоци – VPN.
- Заштита на мобилни уреди – користењето преносна опрема бара посебен акцент да се стави на безбедноста, бидејќи

овие уреди се надвор од стандардното разбирање за перимetарска заштита на компјутерските мрежи.[56]

Според некои автори, може да се разликуваат три вида напади на информатичкиот систем, и тоа:

- физички напад, насочен кон расположливоста на нападнатиот систем (употреба на конвенционални оружја против инфраструктурата каде се наоѓаат информатичките системи или против линијата на преносот на информацијата).[57]
- електронски напад (користење електронско оружје што е во можност да емитува електромагнетна енергија концентрирана во снопови со автоматски или субавтоматски честички или оружје, кое испушта електромагнетни импулси со цел да се преоптоварат или да се онеспособат електричните споеви на системот.[58]
- сајбер-напад (примена на т.н. злонамерни информатички програми чија задача е да го загрозат информатичкиот систем на противникот, со цел негово оштетување или крадење на различни доверливи или чувствителни податоци).[59]

Од изнесеното се наметнува заклучок дека ИТ безбедноста претставува општ интерес и потребно е имплементација на посебни методи и средства за заштита на информатичката безбедност. Во таа насока, изнаоѓањето законски решенија и регулативи за справување со сајбер-заканите, предвидување и спречување на нападите врз сајбер-просторот, соработка со приватниот сектор и безбедносните експерти, обука на државните безбедносни кадри, изнаоѓање соодветен одговор на нападите и брзо враќање во

[56] International Journal of Mathematical Models and Methods in Applied Sciences - Measures for Critical infrastructure Protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

[57] Marlin S. Darvey M. ,,Disaster – Recovery Spending on the Rise" Information Week, Manhasset NY, Avgust 2004., p.26, во Бакрески О. Триван Д. Митевски С., Корпорациски безбедносен систем, Скопје, 2012, стр.243.

[58] Бакрески О., Триван Д. и Митевски С. *Корпорациски безбедносен систем,* Комора на РМ за обезбедување на лица и имот, Скопје, 2012, стр. 243.

[59] Петковиќ Тодор оп.цит.стр.293, во *Корпорациски безбедносен систем,* Комора на РМ за обезбедување на лица и имот, Скопје, 2012, стр. 243.

функција на нападнатите системи и мрежи се приоритетни задачи за националните влади.[60]

2.3. Сообраќај и транспорт

Сообраќајот е значаен услов за стопанскиот развој на секоја земја и особено на одделни региони. Сообраќајната инфраструктура (патишта, пруги, реки и канали) со основните инфраструктурни објекти го овозможува процесот на сообраќајните услуги, истовремено и како просторно поврзување на различните фактори на производство, како услов за развојот на стопанството. Оваа функција го предодредува и одредениот третман на сообраќајната инфраструктура, а особено од аспект на економските ефекти и оцена на ефикасноста на инвестицијата и развојот и модернизацијата на сообраќајниот систем на една држава.[61]

Значи влијанието на сообраќајот во стопанскиот живот на секоја земја е повеќекратно и многу значајно. Постои цврста заемна зависност помеѓу степенот на развој на сообраќајот во една држава со развојот на економијата. Сообраќајот е резултанта на одредено ниво на развој на стопанството од една страна и од друга страна сам врши влијание на стопанскиот развој на секоја земја. Оттука, сообраќајот во секоја држава, има првостепено политичко, економско и општествено значење. Со самото тоа што поврзува одделни краеви во една целина, сообраќајот овозможува формирање на државна интегралност. Исто така, сообраќајот е важен иницијален фактор на економскиот развој на неразвиените подрачја во рамките на една држава. Новите сообраќајници иницираат развој на стопанството, претставуваат одлучувачки фактор за развој на туризмот во регионите и придонесуваат во претворање на туризмот од индивидуален во масовен феномен. Изградбата и модернизацијата на градскиот сообраќаен систем ја условува општествената поделба на работата и влијае на развојот на нови индустриски гранки. Историскиот развој на многу земји покажува дека сообраќајот игра

[60] Славески С., Предизвик на современите општества, 2015.

[61] Jusufranić, I., *Osnove drumskog saobracaja, Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje,* Травник, 2007.

значајна улога во формирање на начините на живеење, изградбата на сообраќајниците и сообраќајните превозни средства влијаеле отсекогаш на формирање на големината на населените места и на процесот на урбанизација.[62] Затоа безбедноста на овие системи отсекогаш била важна, но акцентот на нивната поголема заштита дојде до израз по терористичките напади од 2001 година во САД и тие што се случија во 2004 и во 2005 година (Лондон и Мадрид) и во Брисел 2015 година, каде што цели на напади беа транспортните системи.

Во основа, сообраќајот може да се врши на повеќе начини. Како критериум на поделбата, може да ни послужат некои технички карактеристики, начинот на превоз, како и некои економски функции на одделни сообраќајни дејности. Транспортниот систем според начинот на превоз и превозните средства може да се подели на:

1. копнен сообраќај, што се дели на патен, железнички, цевководен и сообраќај со преносни траки;
2. воден сообраќај, што го делиме на поморски, речен, езерски и канален;
3. воздушен сообраќај;
4. поштенски сообраќај;
5. телекомуникациски сообраќај.[63]

Според легислативата на САД, критичниот сектор за сообраќај и транспорт го сочинуваат седум потсектори, и тоа:

- воздухопловна инфраструктура, која што вклучува воздухоплови, системи за контрола на летање, хелиодроми, аеродроми вклучувајќи ги и воените аеродроми и воздухопловните бази;
- патна сообраќајна инфраструктура, која што ја сочинуваат патишта, мостови, тунели и превозните средства;
- инфраструктура на водениот сообраќај, која што ја сочинуваат брегот, пристаништа, водни патишта, конекциите со другите сообраќајни и сите пловни објекти;

[62] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 30-72.

[63] Jusufranić,I., *Osnove drumskog saobracaja, Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje*, Травник, 2007.

- инфраструктура за масовен транспорт и патнички железници, која што ја сочинуваат автобуси, патнички возови, метроа, лесни пруги, тролејбуси и трамваи, долги пруги како и самата мрежа на пруги;
- систем на цевоводи, што го сочинуваат голема мрежа на цевоводи што се протега низ целата држава што ја пренесува целокупната количина на природен гас што проаѓа низ државата како и голем број опасни течности и разни хемикалии;
- инфраструктура на товарната железница, која што ја сочинуваат системот на пруги, теретни вагони, превозници на стоки, локомотиви; и
- инфраструктурата на поштенските служби за достава на пакети која се нагласува заедно со поштенските служби, а не во рамките на превозот на стоки – карго превози (товарни железници и сл.), затоа што ова се однесува на достава на поштенски пратки, публикации, но и на мали и на средни пакети.[64]

Националната безбедност на САД ги идентификува следните цели кога е во прашање транспортниот сектор:

- управување со безбедносните ризици од физички, човечки и сајбер-елементи;
- подготвеност на вработените за одговор, обновување, координација и еластичност, односно флексибилност;
- ефективна соработка и споделување на информации со различни сектори;
- управување со сите опасности што произлегуваат од глобалниот транспортен систем за да се заштитат националните интереси.[65]

[64] https://www.dhs.gov/transportation-systems-sector 17.11.2012 - докторска дисертација Марко М. Ракиќ – кризни менаџмент у функции заштите критичних инфраструктура у земљама у транзиции - Универзитет у Београду – Факултет безбедности Београд, 2015.

[65] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

Од изнесеното произлегува дека приоритетите на транспортниот систем се насочени кон превенирање и детектирање на сите штетни противправни акти од тероризам насочен кон сите видови транспорт. Секој супсектор има единствени заштитни предизвици и специфични безбедносни стратегии за намалување на ризикот. На пример, контролата на влез на аеродромите е многу поригорозна отколку кај масовниот транспорт.[66]

Транспортната политика на ЕУ што го третира транспортот ги покрива секторите на патниот, железничкиот, внатрешните пловни патишта, интермодалниот, воздушниот и водениот транспорт вклучувајќи низа прашања заеднички за сите видови транспорт, како што се државната помош и правилата на конкуренција. Со правните текови пред сè се уредуваат техничките и безбедносните стандарди, социјалните стандарди, контролата на државната помош и либерализацијата на пазарот во согласност со внатрешниот пазар на транспорт.[67] Оттука, може да се каже дека транспортната стратегија на ЕУ2050, усвоена во 2011 година, има за цел креирање на заеднички европски транспортен простор (Single European Transport Area) со цел понатамошни интеграции на сите видови транспорт и пред сè намалување на штетните гасови. Доколку Европа сака да го оствари својот економски и социјален потенцијал, неопходно е да се развива сообраќајната инфраструктура и да се осигура идната одржливост на транспортниот систем земајќи ги предвид енергетската ефикасност и заштитата на животната средина.[68]

Според македонската легислатива, транспортниот сектор е составен од железничка инфраструктура што се состои од железнички пруги, објекти и инсталации на железничкиот систем, како и железнички возила од сите категории и потекла што се движат по таа инфраструктура.[69] Мрежата на јавните патишта ја сочинуваат државните патишта (автопатишта, експресните патишта, маги-

[66] Security An Introduction/ Philip P Purpura, CPP 2011, стр. 530.

[67] www.europeanpolicy.org/politike/14-transportna-politika.html, посетена на 25/09/2016.

[68] http://www.europeanpolicy.org/politike/14-transportna-politika.html

[69] http://mtc.gov.mk/media/files/Zakon_za_Sigurnost_vo_zeleznichkiot_sistem_47_09042010, Член, 3.

стралните и регионалните патишта од прва и од втора категорија) и општинските патишта и улиците во градовите и во другите населени места.[70] Внатрешни води се сите водени површини погодни за пловидба (езера, канали и реки); додека внатрешна пловидба е пловидба по внатрешните води.[71] Воздушен сообраќај е летање на воздухоплови или движење на воздухоплови по површините за маневрирање и платформите на аеродромите.[72]

За потребите на овој труд како најрегулиран сегмент во кој се применуваат најдобрите стандарди и практики во работењето ќе биде објаснет воздушниот сообраќај.

2.3.1. Воздушниот сообраќај како дел од транспортниот систем

Воздушниот сообраќај, набљудуван како глобален транспортен систем, од аспект на функционалната поставеност, условно може да се подели на три потсистеми: аеродроми (воздухопловни пристаништа), воздушни превозници (воздухопловни превозни средства) и контрола на летање (управување и контрола на воздушниот сообраќај). Секој од овие потсистеми се состои од повеќе функционални елементи: корисник на системот, инфраструктура, управувачки елементи, технолошки процедури, технички и кадровски ресурси, законска регулатива, меѓународна легислатива итн.[73] Фигуративно претставено, воздушниот сообраќај се реализира во воздух (воздухоплови) и на земја (аеродроми), со меѓусебна интерактивна поврзаност преку системите за негово управување и контрола. Воздухопловот е направа што може да се движи или да се одржува во атмосферата[74] без разлика на неговите конструктивни и технички карактеристики, перформанси или неговата намена

[70] http://mtc.gov.mk/media/files/javni_patista_84_11072008.pdf

[71] http://www.mtc.gov.mk/media/files/Vnatresna_plovidba_55_04052007.pdf

[72] http://www.mtc.gov.mk/media/files/vozduhoplovstvo.pdf

[73] Тунтев Т., *Аеродромски прирачник за прифат и отпрема на воздухоплови, патници и предмети,* Охрид, 2004, стр.13.

[74] Закон за воздухопловство („Службен весник на РМ“, бр.155 од 2012 година).

и за секој воздухоплов е пропишан начин за утврдување на неговата способност за безбедна воздушна пловидба. Во основа, воздушен сообраќај претставува летање на воздухопловот или негово движење по маневарските површини на аеродромот.[75] Значи поимот воздушен сообраќај не го опфаќа само летањето на воздухопловот во воздух, туку и неговото движење (маневрирање) и престој на земја. Тој дел од воздушната пловидба се одвива на аеродромот и ги опфаќа следните активности: полетување, слетување, возење по маневарските површини (таксирање, рулање), паркирање, застанување на позициите за чекање, водење итн.[76]

Гледано од страна на аеродромската проблематика од потсистемот на инфраструктура може да се издвои аеродромскиот потсистем. Делот на аеродромскиот потсистем, што се однесува на движење и паркирање на воздухопловите во процесот на одвивање на воздушниот сообраќај на еден аеродром се нарекува воздушна страна (airside). Вака разгледуваниот систем би опфаќал: простор, инсталации, објекти, опрема, активности на службите, почнувајќи од делот на терминалниот простор (простор и организација на чекање и завршен приод што често го одредуваат капацитетот на полетно слетната патека и секако самиот аеродром), па сè до пристанишната платформа.[77] Делот на системите каде што не се појавуваат воздухопловите, т.е делот од плаформата и пристанишната зграда до градскиот терминал се нарекува земна или градска страна (landside).[78]

Во современата воздухопловна терминологија, во согласност со меѓународно прифатената дефиниција, поимот „аеродром“ се користи за дефинирање на копнената или на воденатa површина на која се изведува полетување, слетување или возење на воздухопловите. Меѓутоа, во повеќе говорни подрачја во светот, меѓу кои и во македонското, поимот „аеродром“ се користи наместо

[75] Закон за воздухопловство („Службен весник на РМ“, бр.155 од 2012 година), Член 4.

[76] Тунтев Т., *Аеродроми*, Технички факултет, Битола, 2005.

[77] Мирковиќ Б., и Тошиќ В, *Воздухопловна пристаништа II*, Универзитет у Београду, Сообраќаен факултет – Београд, 2012, стр.13-72.

[78] Исто., 2012, стр.13-72.

поимот „воздухопловно пристаниште“.[79] По дефиниција, воздухопловно пристаниште претставува аеродром или дел од аеродром, оспособен и отворен првенствено за јавен воздушен превоз, додека под поимот „јавен воздушен превоз“ во воздушниот сообраќај се подразбира лет или серија летови за превоз на патници, карго и/или пошта за надомест или закупнина.[80] Тоа значи дека воздухопловното пристаниште е аеродром или дел од аеродром, што се користи за прифаќање и отпрема на воздухоплови со кои се превезуваат патници, багаж, стока и пошта, а аеродромот, освен за таа намена, може да биде и воен, спортски, школски или за сопствени потреби на одредени правни субјекти. Оттука, произлегува поширокото терминолошко значење на поимот „аеродром“ во однос на поимот „воздухопловно пристаниште“, меѓу кои, освен формална, постои и суштинска разлика.[81] Суштинската разлика меѓу поимите „аеродром“ и „воздухопловно пристаниште“ се состои во законски регулираната обврска за организирање и за функционирање на неопходните аеродромски служби на аеродромот, односно на воздухопловното пристаниште. Според позитивните законски прописи од областа на воздушната пловидба, на секој аеродром мора да постои служба за противпожарна заштита и служба за прва медицинска помош, додека на воздухопловното пристаниште, покрај овие две служби, мора да бидат организирани и следните служби: служба за прифаќање и отпрема на воздухоплови, патници и предмети; служба за контрола на летањето, служба за снабдување на воздухопловите со гориво, служба за обезбедување и служба за одржување објекти, уреди и инсталации што се од значење за безбедноста на воздушната пловидба.[82]

Воздухопловните пристаништа може да се користат и за меѓународен воздушен сообраќај (во тој случај мора да биде организирана пасошка и царинска контрола), што не е случај со други-

[79] Тунтев Т., *Аеродроми*, Технички факултет, Битола, 2005.

[80] Закон за воздухопловство („Службен весник на РМ“, бр.155 од 2012 година), Член 4.

[81] Тунтев Т., *Аеродромски прирачник за прифат и отпрема на воздухоплови, патници и предмети,* Охрид, 2004, стр.13.

[82] Тунтев Т., *Аеродроми*, Технички факултет, Битола, 2005.

те аеродроми. Аеродромите на вода, што се користат за оперирање на хидроавиони, се нарекуваат хидродроми, а аеродромите наменети за оперирање на хеликоптери се нарекуваат хелиодроми.

Примената на актите на незаконско постапување во цивилниот воздушен сообраќај покажува дека воздухопловството претставува честа мета на разни видови насилство или на терористички акти.[83] Последиците, односно штетите нанесени на цивилниот воздушен сообраќај обично се многу тешки со губење човечки животи и големи материјални загуби. Пропустите кои што се направени од страна на безбедносните служби и подготвеноста на саботерите да манипулираат со безбедносните системи сами по себе ја зголемува опасноста, особено од тероризам што претставува најекспониран причинител на загрозување, и датира уште од самите почетоци на воздушниот транспорт. Низ историјата на цивилното воздухопловство се забележани голем број терористички напади и закани. Тие се разликувале по тоа какви цели се сакани да се постигнат и по тоа какво средство се користело при извршувањето на нападите или за преземањето на цивилниот лет.[84]

Настаните што ја следат денешницата во поглед на загрозувањето на цивилното воздухопловство, вклучувајќи ги и случувањата од 11 Септември 2001 година, имаат директно влијание врз создавањето на одредени регулативи, практики и процедури, заради заштита од незаконски дејства со водење сметка за безбедноста, уредноста и ефикасноста на летовите, а сè со цел: да ја заштити сигурноста на патниците, екипажите, воздухопловите, земниот персонал и општата јавност во целост во однос на работите поврзани со обезбедувањето од незаконски дејства и секако подготвеност за брз одговор на зголемените закани врз безбедноста.[85]

Брзиот подем на воздухопловството и цивилниот воздушен сообраќај говори за сè поголемата потреба од безбедност, така што,

[83] Група автори, Аеродромска тренинг програма за заштита на цивилното воздухопловство, Скопје, 2008.

[84] http://www.airserbia.com/magazin/vuk/terorizam_u_vazduhu/terorizam.htm, посетена на 15/04/2010.

[85] ICAO – Анекс 17 International Standards and Recommended practices Marth, 2011.

заедничкиот именител на сите преземени активности и мерки претставува создавање претпоставки и услови за највисоко можно ниво на безбедност на воздушната пловидба, низ облик на обезбедување на цивилното воздухопловство или AVSEC (Aviation Security), што подразбира комбинација на мерки, човечки и материјални ресурси, со цел заштита на цивилното воздухопловство од дејства од незаконско постапување во остварување на основните принципи и филозофија на обезбедувањето, а тоа се:

- цивилното воздухопловство оперира од безбедна и обезбедена средина ослободена од незаконско постапување;
- државите развиваат и имплементираат законодавство и процедури какви што се неопходни за осигурување безбедна и обезбедена средина;
- Мерките за обезбедување, имплементирани од страна на државите, со цел заштита на цивилното воздухопловство од дејства од незаконско постапување се во согласност со Стандардите и препорачаните практики содржани во Анекс 17 од Конвенцијата на меѓународното цивилно воздухопловство, донесени од страна на ICAO и
- во согласност со националните закони државите ќе го гонат секое лице што ќе се обиде или ќе изврши дејство од незаконско постапување и / или ќе го/ги екстрадира/ат лицето/лицата во држави коишто се подготвени да гонат такви прекршители.[86]

Имајќи го предвид изнесеното како и потребата за што посигурна заштита на цивилното воздухопловство, Република Македонија е обврзана да ги почитува и да ги имплементира меѓународните стандарди што се однесуваат на безбедноста на цивилната воздушна пловидба. За да се постигне стандардизирано ниво за безбедност на воздушната пловидба, Република Македонија ја гради својата платформа за безбедност на воздушниот сообраќај преку градење сеопфатна политика, поддржана со законски прописи, што ќе ги спроведуваат сите субјекти, вклучени во која било безбедносна структура во цивилното воздухопловство.

[86] ICAO - Aviation Security Training Package Instructors - Trainee Reference Book, 2012.

За регулирање на работите од областа на воздухопловството утврдени со законот за воздухопловство во Р. Македонија надлежни се Министерството за транспорт и врски и Агенцијата за цивилно воздухопловство (АЦВ).[87]

Главни организации кои се вклучени во безбедноста на цивилниот воздушен сообраќај на национално ниво се: Агенцијата на цивилното воздухопловство. Министерството за внатрешни работи, аеродромските оператори и авиопревозниците.[88]

Ефикасна сигурност на цивилната авијација може да се постигне низ развојот, примена и одржување на сеопфатни и ефикасни законски прописи, програми, мерки и процедури на национално ниво. Насоките за развојот на националните легислативи за безбедност на цивилното воздухопловсво, треба да бидат во согласност со меѓународната регулатива, односно со ЕУ, ICAO, ECAC, EUROCONTROL, JAA/EASA и др., вклучувајќи ги и конвенциите и протоколите што ја регулираат оваа област.

2.4. Водни системи

Недостигот од квалитетна вода за пиење е проблем за голем број држави и може со сигурност да се каже дека денес сè повеќе се наметнува како сериозен безбедносен проблем во светот.

Постојат големи тензии и отворени судири помеѓу одредени држави во поглед на искористувањето на природните извори на водата за пиење, особено во сливните подрачја на реките Нил, Тигар и Еуфрат. По завршувањето на Втората светска војна, па сè до денес, изворите на водата за пиење, како и пропратната инфраструктура, многу често, особено во регионот на Блискиот Исток претставувала стратегиска цел во вооружените судири. Според податоците од Годишниот извештај на Светската банка, Блискиот Исток и Северна Африка забрзано чекорат кон водна криза.[89] Според одредени по-

[87] Закон за воздухопловство („Сл. весник на РМ“, бр.63 од 13.05.2013), Член 5.

[88] Закон за воздухопловство („Сл. весник на РМ“, бр.63/13“).

[89] Џејмс Р. Крег, Дејвид Вогели и Брајан Слеинер, *Ресурси на Земјата – Потекло, употреба и влијание врз животната средина*, стр.434.

датоци се посочува дека од недостиг на чиста вода секоја година умираат околу 1,8 милион деца. Од дијареа, која исто така најчесто се јавува поради загадената вода, умираат околу 2,2 милиона луѓе годишно. Голем дел од отпадот доаѓа од земјите во развој кои 90 проценти од отпадните води ги исфрлаат непрочистени. Се препорачува да се користат системи за прочистување на водата.[90] Оттука нема дилема дека националната инфраструктура на вода за пиење е од витално значење за заштита на јавното здравје и безбедноста, но исто така, ги поддржува бизнисот, индустријата и националната економија.[91]

Во основа, снабдувањето со вода е исклучително важна задача на секоја нација и снабдувањето со вода директно или индиректно влијае и на другите системи и средства што влегуваат во критичната инфраструктура (енергија, транспорт, служби за итна помош, критичните индустрии и слично). Земајќи ја предвид важноста на воденатa инфраструктура во сите домени на живеењето, таа со илјадници години наназад била цел на напади.[92]

Во основа, секторот вода и општо водните системи се подложни на различни видови акти на незаконско постапување, вклучително и контаминација со смртоносни агенси, физички и сајбер-напади. Во случај на вакви акти резултатот може да биде мерен со голем број жртви, заболени и материјални загуби. Откажувањето на снабдување со вода, исто така, ќе влијае на јавното здравје и економската виталност на државата. Голем број услуги вклучувајќи ги здравството, енергетиката, земјоделството, прехранбениот сектор, транспортните системи, службите за итни ситуации и други ќе трпат негативни последици од нарушениот систем.[93]

Ако го разгледаме секторот води низ системот на заштита што е утврден од страна на САД преку специфичниот План за сек-

[90] Исто., стр. 434.

[91] Critical Infrastructure Protection - Multiple Efforts to Secure Control, Systems Are Under Way, but Challenges Remain - Report to Congressional Requesters – September 2007, www.gao.gov/assets/270/268137, pdf.

[92] Dan Kroll, Aqua ut a Telum "Water as a Weapon", 2010, http://hachhst.com/technical-library

[93] http://www.dhs.gov/water-and-wastewater-systems-sector, посетена на 14/07/2015.

торот води, што ги опишува процесите и активностите за заштита и оправување на секторската инфраструктура ќе видиме дека главниот акцент се става на:

1. Профилирање на секторот и на целите преку:
- профили (вода за пиење, отпадни води, клучни авторитети);
- субјекти: агенции, сопственици и оператори, државната безбедност и други федерални оддели, регионални субјекти и меѓународни организации и странски држави;
- цели (елементи и карактеристики) и
- визија (обезбедување и подобрување на водата за пиење и отпадните води, заштита на таа инфраструктура преку ефективни програми за подготвеност, безбедносни практики и мерки).

2. Идентификување објекти, системи и мрежи. Ова претставува сет од системи на вода за пиење и отпадни води. Ажурирање на податоците поврзани со системот се прави преку периодични истражувања и контроли од страна на надлежните институции.

3. Ризици. Секторските објекти се ранливи при одделни и комбинирани напади или природни катастрофи и ова вклучува: напади со експлозивни направи, загадување на питката вода, саботажа на системите, пуштање на опасни материи, информатички напади на контролните системи итн., но исто така, и природните катастрофи како што се: земјотресите, пандемиите и ветровите, преставуваат закани за секторот вода.

4. Приоритетни делови на инфраструктурата. Сопствениците и операторите при проценатa на ризиците ги идентификуваат компонентите како што се пумпите, генераторите и сл., кои при евентуален инцидент би предизвикале големи последици. Постојат неколку критериуми за определување на сензитивноста на инфраструктурата, и тоа: колку се опслужува популација, количината на складиран хлор, економскиот импакт, критичната маса на потрошувачи и др.

5. Развој и имплементација на иницијативи, стратегии за заштита и оправување. Пристапи при изработка и имлементирање на стратегии за заштита и оправување вклучуваат: обуки, вежби, техничка асистенција, меѓусебна регионална помош, заштита на информатичките системи и подготовки при пандемии.

6. Развојни мерки.

7. Истражување и развој на мерките за заштита.

8. Менаџирање и координација на секторските одговорности.[94]

2.5. Храната како критичен енергенс

Општо, низ историјата, храната често пати била средство што се користело за постигнување цели во војна или терористички напади насочени кон војските или цивилите. Заканите на терористичките организации со посредство на храната можеби не доаѓаат во преден план во однос на нападите кои се реализираат со експлозивни материи и заземаат главен медиумски простор и што за жал, се многу чести во последно време,[95] но сепак, како

[94] Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan, 2010, United States Environmental Protection Agency – Homeland Security.

[95] Една од потенцијалните мети на терористичките организации претставува и храната, поради можноста од насочување на акциите кон широката популација и лесно предизвикување паника. Во последно време, ваквите инциденти не се реткост и сценариото за можен терористички напад на некој од синџирите на исхрана веќе не се сведува само на теорија. Светската здравствена организација (WHO) го дефинира тероризмот во однос на храната како активност или закана за намерна контаминација на храната со биолошки, со хемиски, со физички или со радиоактивни материи во насока на предизвикување на ранување или смрт на цивилното население или загрозување на социјалната, на економската или на политичката стабилност. Притоа, како биолошки агенси се подразбираат: вируси, бактерии и паразити. Хемиските агенси може да бидат вештачки или природни токсини, додека физичките агенси можат да вклучат широк спектар на различни делови како што се стакло, игли и парчиња метали. Радионуклидните материјали се дефинирани во контекст на радиоактивни хемикалии, способни да предизвикаат повреди, кога се присутни во неприфатливи количини. Освен храната за луѓето и храната за животните се смета за погодно подрачје за извршување терористички активности ако е наменета кон економски искористувани животни што служат за човековата исхрана. Оттука било да се работи за биотероризам, каде што се нанесува материјална штета, со цел да се сврти вниманието кон некој еколошки проблем, или загадување на големи количини на храна со опасни агенси за да се нанесат големи човечки загуби,

покарактеристични би ги издвоиле примерите од 1984 година кога членови на религиска секта имаат заразено со бактеријата *Salmonella typhimurium*, повеќе ресторани во САД, со што се предизвикани 751 случај на заболувања од салмонелоза, што воедно бил како пробен напад пред поинтензивниот напад, чија цел била спречување на одржување на локалните избори. Друг пример е тој во 1996 година кога незадоволен работник намерно ја заразил храната со бактеријата *Shigella dysenteriae* тип 2, предизвикувајќи заболување кај 12 лица. Во 2003 година во Кина, училишниот појадок е затруен со отров за штетници. Последен познат пример со намерна контаминација е тој во САД во 2011 година, кога поради конкуренција сопственик на пицерија поставил торби со штетници во соседните пицерии.[96] Ова се само некои примери за труење со храна, гледано во светски размери. Намерното труење со агенси не изгледа големо, но тоа не значи дека не треба да се преземат адекватни мерки на заштита. Бројните примери на труење со храна говорат за потенцијалот што го поседува храната како терористичко оружје. Тука треба да се спомене ширењето на хепатитисот А на 300.000 луѓе во Шангај – Кина, по конзуминирањето контаминирани ракови, што воедно се смета за најголем инцидент во историјата на инциденти со храна.[97]

Значи храната претставува многу лесно подрачје за контаминација во функција на биотероризмот, за што постојат голем број сомнителни контаминации, било тоа да се од економски или од други побуди, но сепак прехранбената индустрија претставува висок ризик кога станува збор за актите на незаконско постапување.[98]

целта е иста, а тоа е предизвикување неред. Во таа насока, во последните години се придава големо значење, а особено со воведување стандарди и воведување превентивен систем на заштита. Види кај Antunovic B., Varga I, Kralik G, Baban M, Poljak V, Njari B, Pavlovic Z, Mackic S: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – Krmiva 53 (2011), Zagreb 1: стр.31-46.

[96] Antunovic B., Varga I, Kralik G, Baban M, Poljak V, Njari B, Pavlovic Z, Mackic S: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – Krmiva 53 (2011), Zagreb 1: стр.31-46.

[97] Исто., стр.31-46.

[98] Исто., стр.31-46.

Од тие причини, потребно е адекватен приод кон проценитe на ризици, со цел спречување на контаминацијата на храната во сите облици на користење. Во тој контекст, проценатa на ризик од терористички напади по пат на храна ги содржи следните компоненти: идентификација на опасноста, карактеризација на опасноста, процена на изложеност и карактеризација на ризикот. Оваа постапка е разиена во Агенцијата за храна и лекови во САД (FDA, 2003). Мерките на превенција, заедно со зголемениот надзор и средствата за адекватен одговор во случај на намерен или случаен инцидент, подоброто следење на храната и можноста од брзо повлекување, двонасочната комуникација на државните служби и прехранбената индустрија, однапред предвидените сценарија што ќе ги распределат ресурсите и поедноставување на приоритетите во случај на инциденти, како и координацијата помеѓу владата и индустријата и јавноста, треба да биде минимумот што треба да го реализира секоја влада.[99]

Генерално, секторот за храна претставува еден од покомплексните сектори за заштита. Комплексноста доаѓа од неговата обемност, отвореност, разновидност, подложност од аспект на загрозување, како и огромната зависност од другите сектори. Прехранбените производи се движат брзо во трговијата до потрошувачите и времето што е потребно за откривање и идентификација на опасноста и еколошката штета, како што се опасностите од животинско или од растително потекло од аспект на болести или контаминација на храната, може да биде долго и комплексно. Загрозувањата може да резултираат со огромни последици и од тие причини заштитата вклучува широк спектар активности со голем број инволвирани субјекти.[100] Исто така, заштитата подразбира постоење и на соодветна законска регулатива.

Суштинските правни основи на законодавството за храна се Регулативата бр.178/2002 (ЕС) и Регулативата бр.882/2004(ЕС) кои

[99] Antunovic B., Varga I, Kralik G, Baban M, Poljak V, Njari B, Pavlovic Z, Mackic S: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – Krmiva 53 (2011), Zagreb 1: стр.31-46.

[100] http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf, посетена на 11/01/2016.

директно се применети во сите земји членки на ЕУ. Со Регулативата бр.178/2002 (ЕС) дадени се генералните принципи и барања на законодавството за храна на Унијата. Регулативата ги опфаќа сите фази на производство и обработка на храна во синџирот на храна врз принципот „од фарма до трпеза". *Со Регулативата бр. 882/2004(ЕС)* се дадени генералните принципи за спроведување контрола, деталите за изготвување на повеќегодишни национални контролни планови од страна на земјите членки и кореспондентни извештаи во рамките на Унијата. Проценета на ризикот е институционално одвоена од управувањето со ризикот. Комуникацијата со ризик, третата компонента на анализата на ризикот, е поделена помеѓу проценителите и управувачите со ризик. Проценете на ризик се објавуваат на интернет.

Во однос на поставеноста на правната рамка во Република Македонија во делот на безбедност на храната, може да се каже дека основата е дадена во Законот за безбедност на храна донесен во 2010 година. Примарната цел на овој закон е да се обезбеди висок степен на заштита на здравјето на луѓето, како и да ги заштити интересите на потрошувачите во односот на храната. Исто така, цел на овој закон е да обезбеди и ефикасно функционирање на внатрешниот пазар на храна и на храната за животни, но и да воспостави систем на контрола за безбедноста на храната и за храната за животни. Исто така, овој закон ги уредува обврските на операторите со храна и храна на животни што се вклучени во повеќе фази, почнувајќи од производство, преработка, складирање, дистрибуција, увоз и извоз. Законот ги пропишува основните барања што мора да бидат задоволени од аспект на безбедноста на храна и на храната за животни, а се пропишани и општите и посебните одредби за хигиена на храната, начинот и постапката на регистрација и одобрување на операторите со храна, процедурите засновани на ХАСАП принципите и упатствата за добра хигиенска пракса. Во законот се уредени и прашањата на службените контроли, со кои треба да се гарантира дека храната е со соодветен квалитет, односно е соодветно безбедна за користење од страна на потрошувачите.[101]

[101] *Закон за безбедност на храна,* („Службен весник на РМ", бр.157 од 7 декември 2010 година).

Со донесувањето на Законот за безбедност на храната беше предвидено и донесување повеќе подзаконски акти (во форма на правилници, одлуки и упатства) со кои ќе се доуредат некои прашања што со законот се само таксативно набројани или пак попрецизно во детали ќе се опише одредена процедура или постапка. Досега се донесени и во сила се повеќе од 50 подзаконски акти, што ги пропишуваат посебните барања за пластични материјали што доаѓаат во допир со храната, правилата за генетски модифицирана храна и одредени барања во врска со неа, правила за адитивите и други додатоци што се користат во производството на храна, критериуми за микробиолошките стандарди за храната, правила за посебна нутритивна вредност и додатоците во исхраната, потоа правилата, односно правилник за начинот и постапката за рекламирање на храната што има посебно нутритивно и здравствено значење. Со подзаконски акт се уредени и правилата за квалитетот на меленото месо и производите од месо, квалитетот на пивото и безалкохолните пијалаци, зачините, екстрактите од зачините и смесите на зачините.[102]

Покрај Законот за безбедност на храната, што претставува општ закон што ја регулира областа на заштита на здравјето на луѓето од аспект на безбедноста на храната, постојат и уште неколку други закони што првенствено регулираат материја што не е во оваа област, но сепак постои поврзаност, бидејќи со тие закони во еден дел се регулираат процеси и појави што директно или индиректно влијаат на безбедноста на потрошувачите и храната што се дистрибуира и што се конзумира.

2.6. Хемиски сектор

Хемиската индустрија претставува гранка во индустријата што по хемиски пат преработува растителни, животински и минерални суровини, како и разни отпадоци. Таа има исклучително голем спектар на дејствување и обединува повеќе гранки на индустријата користејќи ги нивните суровини.[103]

[102] http://www.fva.gov.mk/index.php?option=com_content&view=article&id=54&Itemid=49&lang=en

[103] https://sh.org/Hemijska_industrija, посетена на 12/11/2015.

Врз основа на крајниот производ овој сектор може да се подели во пет главни сегменти, а тоа се:

- основни хемикалии;
- специјални хемикалии;
- земјоделски хемикалии;
- фармацевски производи;
- производи за широка потрошувачка.[104]

Секој од овие сегменти има различни карактеристики, специфики, динамика на раст, пазари, развој на настаните и др., но исто така треба да се истакне дека овој сектор е многу разновиден, поседува голема географска дисперзија и зависност од суровини, транспортни системи, истражувачки капацитети, енергенси и слично.

Значи хемискиот сектор претставува составен дел на економијата на сите современи држави, но исто така потпирајќи се на широката лепеза на дејности што спаѓаат во неговите рамки ја прави круцијална зависноста помеѓу хемискиот сектор и другите сектори што се дел на критичната инфраструктура. Ако повлечеме паралела на меѓузависност помеѓу хемискиот сектор и другите сектори ќе видиме дека голем број критичните сектори се потпираат на хемиската индустрија што во основа бара големи количини на енергенси што се добиваат од другите сектори.

Според официјалните податоци, овој сектор на ниво на ЕУ опфаќа 60.000 компании што вработуваат околу три милиони работници.[105] Во САД хемискиот сектор преработува суровини во повеќе од 70.000 различни производи и е главна компонента на американската економија, што учествува со околу 25 проценти од бруто-домашниот производ. Исто така, 96 проценти од производите во САД во 2013 година се произведени со поврзаност на хемискиот сектор. Од тие причини овој сектор е од суштинско значење за националната и за економската сигурност на САД.[106]

[104] https://www.dhs.gov/chemical-sector, посетена на 7/07/2016.

[105] file:///C:/Users/win7/Downloads/SA_kemijska-industrija_ozujak-15%20(2).pdf, посетена на 7/08/2016.

[106] Chemical Sector Specific Plan An Annex to the NIPP 2013 2015 Homeland Security https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf, посетена на 7/07/2016.

Употребата на големи количини на опасни хемикалии е неизбежно во некои индустриски сектори што се од витално значење за современите индустрии на напредните општества. Од тие причини сите држави во светот уште во 1992 година, низ прифаќањето на Агендата 21 и главата 19 од Конференцијата на ООН за животна средина и развој (UNCED), се обврзаа за зголемување на националните способности и за сигурно управување со хемикалиите, коишто вклучуваат: соодветно законодавство, собирање и следење на податоците, воспоставување сигурно управување со хемикалиите, создавање административни способности за управување со хемикалиите вклучувајќи и образование, воспоставување соодветен надзор, екипирање, приправност и интервенирање.[107] Со тоа преку разни меѓународни организации државите презеле обврски за спроведување голем број европски и конвенции на ООН со кои е уредено безбедното управување со хемикалиите.[108]

Во Европа катастрофалната несреќа во италијанскиот град Севесо во 1976 поттикна донесување законска регулатива за спречување и контрола на ваквите несреќи. Севесо Директивата (Директива 82/501 / ЕЕС) подоцна беше изменета во поглед на научените лекции од подоцнежните несреќи како што се Бопал, Тулуз или Енхеде и резултираше со Директивата Севесо II (Директива 96/82 / ЕС), за во 2012 година да се донесе Директивата Севесо III (Директива 2012 / 18). Директивата сега се однесува на повеќе од 10.000 индустриски претпријатија во Европската унија каде постојат, се користат или се чуваат опасни супстанции во големи количини. Со оглед на многу високата стапка на индустријализација, Европската унија со Директивата Севесо придонесе за постигнување заштитеност од хаварии. Директивата се смета како репер за политика при индустриска несреќа и е пример за законодавството во многу земји низ светот.[109]

[107] http://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_143_3961.html, посетена на 17/08/2016.

[108] http://narodne-novine.nn.hr/clanci/sluzbeni/2008_12_143_3961.html, посетена на 17/08/2016.

[109] http://ec.europa.eu/environment/seveso/, посетена на 17/08/2016.

Директивата Севесо вклучува:

- класификација, означување и пакување на хемикалиите;
- механизам за цивилна заштита на Унијата;
- заштита на критичната инфраструктура;
- политика за одговорност за животната средина и за заштита на животната средина преку кривичното право;
- операции поврзани со безбедноста на нафта и гас на копно.[110]

Одделот за национална безбедност на САД идентификува три безбедносни прашања поврзани со хемикалиите:

- *ослободување – испуштање* токсични, запаливи или експлозивни хемикалии или материјалите што имаат потенцијал за значителни негативни последици врз животот или здравјето на луѓето;
- *кражба или пренасочување* на хемикалиите или на материјалите што имаат потенцијал да бидат злоупотребени како оружје или лесно да се конвертираат во оружје со користење едноставна хемија, опрема или техника, со цел да се создадат значителни негативни последици врз животот или врз здравјето на луѓето;
- *саботажа* врз хемикалиите или материјалите коишто, ако се мешаат со лесно достапни материјали, имаат потенцијал да предизвикаат значителни негативни последици врз животот или врз здравјето на луѓето.[111]

Од аспект на ризиците и опасностите потребно е да се спомене дека како и голем број критични инфраструктури, поголем дел од хемиските капацитети (производство, складирање, транспорт) спаѓаат во приватна сопственост. Оттука сопствениците, односно операторите на ваквите компании треба да бидат свесни особено во делот на потенцијалните здравствени и безбедносни ризици што ги носи хемиската индустрија и да се воспостави систем на безбедност со кој ќе се гарантира дека нивните производи и ресурси се адекватно заштитени и безбедни од евентуални напади со ставање врвни при-

[110] http://ec.europa.eu/environment/seveso/, посетена на 17/08/2016.

[111] https://www.dhs.gov/appendix-a-chemicals-interest-list, посетена на 7/07/2016.

оритети на адекватни безбедносни мерки. Потребно е операторите да воспостават тесна соработка со државниот безбедносен апарат и да се фокусираат на реализација на Планот за заштита на овој секор со цел постигнување адекватна безбедност, размена на информации и практики низ партнерство што ќе гарантира безбедност.

Во таа смисла потребно е да се спомене и колку е важна меѓусекторската соработка и градење партнерство низ контакти, тренинзи, научни конференции и слично, со цел да се развие безбедноста и да се обезбеди континуитет и развивање на бизнисот. Соработката на приватниот сектор и националните капацитети на државата се реализира за: да се постават цели и задачи, да се идентификуваат средства, да се направи процена на ризиците, да се дадат приоритети и да се спроведат заштитни програми.[112]

Во Република Македонија со закон се уредени класификацијата, пакувањето и означувањето на хемикалиите; условите за производство на хемикалиите; правата и обврските на правните лица што произведуваат, ги стават во промет хемикалиите или ги употребуваат хемикалиите; водењето регистар на хемикалии; ограничувањето и забраната на производството; ставањето во промет и употребата на хемикалиите; увозот и извозот на одредени опасни хемикалии; ставањето во промет на биоцидните производи и детергентите; надзорот, како и други прашања што се однесуваат на хемикалиите.[113]

Во основа, Законот обезбедува високо ниво на заштита на здравјето на луѓето и животната средина, вклучително и претставување алтернативни методи за оцена на опасностите што произлегуваат од супстанциите, како и обезбедување на унапредувањето на конкурентноста и иновативноста. Одредбите од овој закон се применуваат и на:

- производство и промет на хемиско оружје и хемикалии за добивање хемиско оружје, ако со овој закон поинаку не е уредено;
- производство и промет на прекурзори, ако со друг закон поинаку не е уредено и
- предмети за општа употреба.

[112] https://www.dhs.gov/chemical-sector, посетена на 7/07/2016.

[113] http://zdravstvo.gov.mk/wp-content/uploads/2015/10/1-Zzakon, Zakon-za-hemikalii-145.10.pdf

Нема дилеми дека хемикалиите се од исклучителна важност за секојдневното живеење, но истовремено претставуваат и сериозна закана во случај на неправилно ракување, складирање, транспортирање и употреба или несреќа што може да се случи поради терористички или воени дејства.[114] Во таа смисла во хемиските несреќи во кои учествуваат опасните материи доаѓа до палење, до експлозии, до неконтролирано истекување и до разлевање на опасните материи, до деформирање на складиштата или композициите што може да предизвика до силни експлозии, пожари, труења, изгореници, заболувања и загадување на животната средина.[115] Исто така, некои хемикалии, во нивната основна форма или во комбинација со други хемикалии, може да предизвикаат значителни повреди и оштетувања и од тие причини овој сектор може да биде привлечен како цел за напад пред се поради потенцијалните токсични последици, но и како суровина за производство на оружје за масовно уништување или импровизирани експлозивни направи, или пак да се користи за саботажа или за контаминација.[116] Сепак, секоја хемиска несреќа има посебни специфики, така што секоја од нив е потребно да се разгледува одделно, во зависност од видот, од силината, од просторниот опсег, од последиците и од времетраењето.[117] Опсегот на опасност при несреќи во хемиските компании и транспортот на опасни материи се определува и врз основа на токсичноста на опасната материја и на просторниот зафат на загадувањето.

2.7. Финансиски и банкарски сектор

Структурата на финансискиот сектор ја сочинуваат: пазар на пари, пазар на капитал, девизниот пазар, депозитни институции (комерцијални банки, штедилници, кредитните унии) и недепозит-

[114] Philip P Purpura, *Security An Introduction*, CPP 2011, стр.534.

[115] Инђић Д., *Место јединица АБХ службе у обезбеђењу од хемиских удеса*, Универзитет одбране у Београду, Војна академија стр. 290.

[116] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.

[117] Инђић Д., *Место јединица АБХ службе у обезбеђењу од хемиских удеса*, Универзитет одбране у Београду, Војна академија, стр. 290.

ни институции (осигурителни компании, пензиски и инвестициски фондови).[118]

Политика за финансиски услуги треба да осигура стабилен, безбеден и ефикасен финансиски пазар и да обезбеди кохерентност и конзистентност помеѓу различни области, како што е банкарството, осигурувањето, хартиите од вредност и инвестициските фондови, инфраструктурата на финансиските пазари, финансиските услуги на мало и платните системи.[119]

Развојот на финансиските системи, финансиските услуги и отпорноста на финансиските шокови, се важни за севкупниот економски развој и стабилност. Оттука, развиените модели за финансиските системи имаат важна улога во креирањето на политиките, како и во делот на давање соодветни препораки за имплементација и за надградба на домашните и на светските регулаторни барања.[120]

Со цел да се подобри и да се унапреди безбедноста и отпорноста потребно е секторот да работи на унапредување на четирите основни цели, и тоа:

1. Имплементирање и одржување на структурирана рутина за размена на навремени и точни информации поврзани со сајбер и физички закани и слабости помеѓу компаниите, во рамките на секторите на индустријата и помеѓу приватниот сектор и владата.
2. Подобрување на капацитетите за управување со ризик и одржување на безбедноста на компаниите во целиот финансиски и услужен сектор, преку поттикнување на развојот и употреба на заеднички пристапи и најдобри практики.
3. Соработка со националната безбедност со цел спроведување на законот, соработка со разузнавачките служби; со финансиски регулаторни органи; како и со другите сектори на индустријата; но и со меѓународните партнери за одговор и опоравување од покомплексни и поголеми инциденти.

[118] http://www.financethink.mk/mk/istrazuvacki-programi/finansiski-sistemi/

[119] http://ec.europa.eu/finance/general-policy/index_en.htm посетена на 23/09/2016.

[120] http://www.financethink.mk/mk/istrazuvacki-programi/finansiski-sistemi/

4. Комуникациска политика и регулаторни иницијативи што ќе ги унапреди безбедноста на инфраструктурата и еластичноста - флексибилноста преку силна координација помеѓу владата и индустријата.[121]

Во основа, е потребно финансискиот сектор да биде соодветно заштитен со цел да се овозможи непречено банкарското работење, фукционирање на финансиските пазари и на регулаторните институции и складиштата за документи и финансиски средства.[122] И покрај тоа што денес голем број финансиски активности се извршуваат електронски, сепак сè уште постои и физички пренос на средства. Инфраструктурата на финансиските услуги вклучува електронски уреди како што се компјутери, уреди за складирање и телекомуникациски системи. Покрај клучните физички компоненти, овој сектор вклучува и високо специјализирани вештини за работа што се сметаат како основни елементи на критичната инфраструктура.[123]

Генерално, како и другите критични сектори и банкарскиот и секторот на финансиски услуги се потпира на неколку други сектори што обезбедуваат континуитетот на работењето вклучувајќи електрична енергија, транспорт, јавни служби за безбедност и секако ИТ и телекомуникациските системи. Нарушувањето на функционалноста на овие системи дава директна рефлексија на финансискиот сектор на секоја држава. Како пример на ваквата зависност може да се споменат пазарите на сопственичките хартии од вредност што останаа затворени четири работни дена по нападите од 11 септември 2001 година во САД, затоа што телекомуникациските линии што се наоѓале на долниот дел на Менхетен биле многу оштетени.[124] По овие случувања, во финансискиот сектор се направени голем број корективни мерки за подобрување на безбедноста и програми за одговор и за обновување, како и форум за размена на најдобрите практики вклучувајќи голем број на здруженија и други интердисциплинарни групи како на национално, така и на меѓународно ниво.

[121] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.

[122] The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, the White House Washington February 2003, стр.75.

[123] Исто., стр.75.

[124] Исто., 76.

Треба да се спомене дека утврдувањето на приоритетните закани за финансиските системи со користење анализа на разузнавачки информации и навремено известување на финансискиот сектор е една од методологиите на заштита што функционира во современите држави.

Што се однесува до банкарските ризици во Република Македонија во согласност со важечките прописи што ја регулираат оваа област предвидени се следните видови ризици: кредитниот ризик, ликвидносниот, валутниот, пазарниот, ризикот од промена на каматните стапки, ризикот од концентрација на изложеноста на банката и оперативниот ризик.[125]

Како најекспониран ризик од аспект на обезбедувањето тука ќе го споменеме оперативниот ризик.

Овој ризик настанува како последица на:

- измама (погрешно известување, кражба од страна на вработените и др.);
- работните навики и сигурноста на работното место (право на оштета на вработениот, повреда на здравствените права, општата одговорност);
- постапки поврзани со клиентите, производите и деловните активности (злоупотреба на доверливите информации, перење пари, продажба на неавторизирани производи);
- штети на материјалните добра (тероризам, протести, пожари, поплави);
- прекин на работата поради грешки во информацискиот систем (хардвер, софтвер или телекумуникациски проблеми);
- погрешно управување со процесите (погрешни влезни информации, погрешна процена на инструментите за осигурување на податоците, нецелосна документација, неовластено пристапување до важни информации и др.).[126]

[125] http://www.nbrm.mk/WBStorage/Files/Regulativa_Odluka_upravuvanje_so_rizicite_2011.

[126] BIS, Sound Practices for the Management and Supervision of Operational Risk, *BSBS*, 2003, во Кузманоска С., *Анализа, мерење и управување на банкарските ризици*, докторска дисертација одбранета на Економски Факултет, Прилеп, 2014, стр.33.

Во согласност со наведените причини оперативниот ризик се појавува во различни категории, и тоа:

- ризик од неадекватна или недоволна инфраструктура (застарени мерки и капацитети, нејасно дефинирани системски одговорности, недостаток на практично искуство на вработените и др.);
- технолошки ризик (ризици од информациска поддршка);
- ризик од извршените операции или деловни процеси (неадекватни или застарени процедури, постоење критични процесни делови поради техничко-технолошките проблеми);
- ризик од човечкиот фактор (недоволна култура во однос изложеноста на банката на ризици, недоволен број вработени, ризик од управување, интерни криминални активности и сл.) и
- ризик од економските случувања (екстерни криминални активности, природни катастрофи, војни и друго).[127]

Негативните последици од оперативниот ризик може да се манифестираат како: целосна финансиска загуба, нарушување на угледот на банката и/или односот со клиентите, неспособност за извршување одделни банкарски трансакции и др.[128]

Извори на оперативниот ризик се:

- човечки фактор – се однесува на загуби што се поврзани со недоволна култура кон ризиците, а особено кон оперативниот ризик, ненамерно кршење на интерните политики од страна на актуелните или од поранешните вработени, недоволен број вработени и др.
- процеси – ризик од неадекватни или недоволни процедури, критични делови од процесите кои настануваат поради техничко-технолошки проблеми. Загубите во оваа категорија може да бидат последици од човечки грешки или од направени пропусти поради непочитување на ва-

[127] Кузманоска С., *Анализа, мерење и управување на банкарските ризици*, доктрска дисертација одбранета на Економски Факултет, Прилеп, 2014, стр.33.

[128] Исто., стр.33.

жечките процедури и најчесто ваквите загуби предизвикани од процеси се третираат како ненамерни загуби;
- системи – предизвикуваат загуби што настануваат поради пад на постојните информациски системи и технологии. Загубите од оваа категорија ако се поврзани со одредена намера се класифицираат во категоријата во кои причини се човечките фактори или екстерните случувања;
- екстерни случувања – предизвикуваат загуби што настануваат како последица на виша сила и природни катастрофи, екстерни дејства или активности предизвикани од страна на трети лица.[129]

Управувањето со оперативниот ризик е ист како и кај кредитниот ризик, ликвидносниот ризик (ризик на ликвидност) и пазарниот ризик, а тоа е насочено кон:
- заштита од потенцијални случувања што се манифестираат како оперативен ризик;
- ублажување на ефектите што ги предизвикува оперативниот ризик;
- идентификување на внатрешните и на надворешните активности што може да помогнат во предвидување на оперативниот ризик;
- одредување и алоцирање на капиталот потребен за покривање на загубите настанати како последица на оперативниот ризик и
- спроведување адекватна контрола на штетите при евентуално настанување на оперативниот ризик.[130]

За сите непредвидени ситуации во делот на финансиското работење потребно е да се изработи план за непрекинатост во работењето и план за вонредни ситуации што вклучува: дефинирање на настаните коишто се сметаат како вонредни услови или сериозно нарушени услови за работа; поделба на надлежностите и определување лица со посебни права и одговорности и/или вработени во банката што ќе бидат одговорни за преземање соодветни активности при појава на вонредни услови или сериозно нарушени

[129] Исто., стр.200.
[130] Исто., стр.203.

услови за работа; создавање услови за продолжување на непреченото функционирање на најзначајните системи и процеси на банката; временски рокови во кои треба да се обезбеди продолжување на непреченото функционирање на најзначајните системи и процеси; детални процедури за обезбедување непрекинато функционирање на најзначајните системи и процеси; начин на информирање во случај на сериозно нарушени услови за работа.[131]

2.8. Здравствена заштита и јавно здравство

Здравствениот сектор има клучна улога во зачувувањето и во унапредувањето на здравјето на луѓето, но исто така неговата примарна цел е и спречување, рано откривање и сузбивање болести, повреди и други нарушувања на здравјето предизвикани од влијанието на работната и животната средина, навремено и ефикасно лекување и здравствена нега и рехабилитација.[132]

Значи здравствениот сектор е многу важна карика и исклучително важна компонента и треба да биде предмет на заштита од државата за да се намали ранливоста на овој сектор од потенцијални влијанија и ризици. Оттука денес болници, клиники итн., се слободно достапни капацитети поради природата на работењето и од тој аспект идентификацијата на потенцијалните закани и пристап до одредени ресурси го прави овој сектор многу комплексен кога станува збор за обезбедувањето. Како сериозен проблем во анализата на опасностите и загрозувањата што го следат овој сектор претставува и потребата од преземање мерки во однос на спречување на ширење епидемии, изолираност па се до дистрибуција на залихи, лекови, енергенси и слично. Од безбедносна перспектива предизвиците со кои се соочува овој сектор се бројни. Така, здравствените установи имаат контрола за ограничен пристап на посетители на кои често им се издава дозвола за влез. Сепак тие, но и постериите за итна помош често се предмет на

[131] http://www.nbrm.mk/WBStorage/Files/Regulativa_Odluka_upravuvanje_so_rizicite_2011.pdf

[132] http://zdravstvo.gov.mk/wp-content/uploads/2015/10/1-Zakon za zdravstvena zastita-43.12.pdf, член 2.

насилство и закани од страна на агресивни пациенти, членови на семејства или насилни групи.[133]

Во ситуација на кризни или вонредни состојби овој сектор ќе биде доминантен и ќе има значајна улога заради карактерот на состојбите и евентуалните повреди и човечките загуби. Затоа предизвиците што ги носи овој сектор стануваат врвен приоритет на секоја современа држава и особено ако се знае фактот дека јавното здравство и медицинските установи ја носат главната улога кога се во прашање човечките животи. Кај конвенционалните терористички напади, институциите како што се полицијата, противпожарните единици, итната помош ја претставуваат првата линија на отпор. Додека од аспект на биотерористичките напади, јавните здравствени установи и медицинските институции се директно на првата линија на одбраната. Во случај на добиени сознанија дека постои закана со биолошки оружја и информацијата дека смртоносните патогени супстанци и може да бидат пуштени на јавно место, лекарската фела е таа што треба да ги препознае и соодветно да реагира. Во ваквите случаи соработката на владата, локалните и национални здравствени организации, јавната безбедност, разузнавачките служби е неминовна.[134] Во ситуации на предизвикување големи медицински загрозувања, односно наплив на зголемени медицински потреби предизвикани, на пример, од биолошки тероризам или друг вид пандемии, овој сектор доаѓа до примарно значење и има врвна улога кога станува збор за справување со настаната ситуација. Медицински наплив е „способност да се обезбеди адекватна медицинска потреба или грижа за време на настани што ги преминуваат границите на нормалната медицинска инфраструктура“. Ваквиот концепт е есенцијален во претпланирањето на поголеми настани што бараат медицинска грижа.[135]

Националната безбедност денес се потпира на подготвеноста и на способноста на државните институции брзо да реагираат во

[133] Philip P. Purpura, *Security An Introduction*, CPP, 2011, стр. 522.

[134] Милиќ Д., Биотероризам и употреба биолошког оружја – Центар за безбедносне студије, Београд ISSN 1452-9777 број 2, 2010, *Ревија за безбедност - стручни часопис о корупции и организованом криминалу*, стр. 113.

[135] Philip P Purpura, *Security An Introduction*, CPP 2011, стр. 520.

услови на извршен биолошки напад. Потенцијалните штети предизвикани од евентуалните биотерористички напади, пред сè, зависат од времето потребно за дистрибуција на антибиотици, лекови или вакцини за загрозените подрачја. Бројноста на потенцијалните агенси, условува здравствената инфраструктура да биде опремена така што кризните ситуации треба брзо да се решаваат. Превентивните мерки, пред сè подразбираат подготовка на граѓаните за препознавање напади од хемиски и од биолошки оружја.[136]

[136] Милиќ Д., Биотероризам и употреба биолошког оружја – Центар за безбедносне студије, Београд ISSN 1452-9777 број 2, 2010, *Ревија за безбедност - стручни часопис о корупции и организованом криминалу*, стр. 112.

III глава

КРИТИЧНА ИНФРАСТРУКТУРА – ЗАКАНИ, РАНЛИВОСТ И ЗАШТИТА

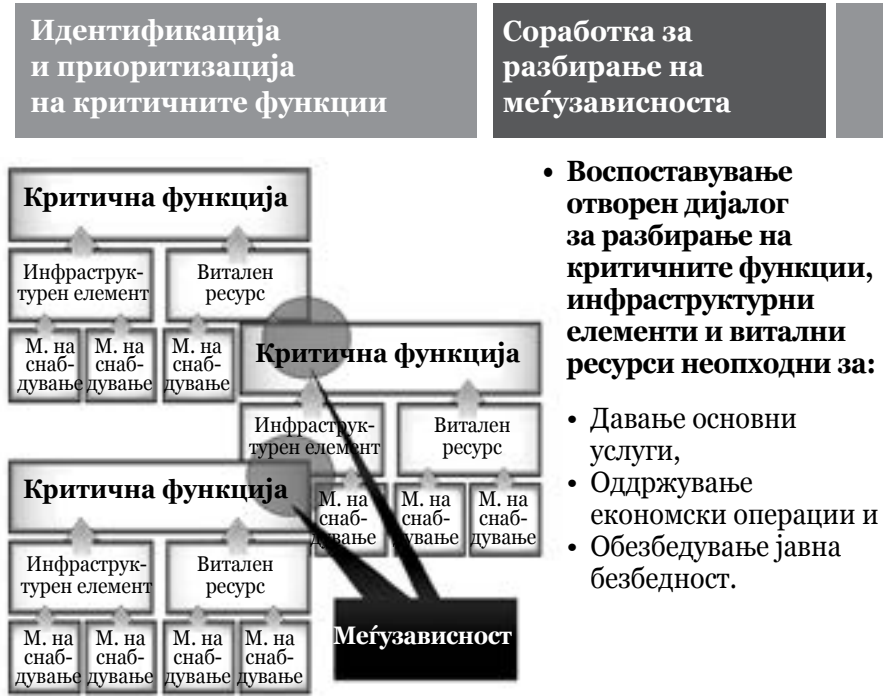
1. КРИТИЧНАТА ИНФРАСТРУКТУРА КАКО ТРАНСНАЦИОНАЛЕН ИНТЕРЕС

Нападите насочени кон критичната инфраструктура, без разлика дали зад нив стојат политички, верски, сепаратистички или други видови организации или станува збор за тероризам, индустриска шпиунажа, хакерски напади, претставуваат едни од најопасните глобални закани што ја следат денешницата. Новите облици на загрозување што произлегуваат од се посложените меѓународни односи и новите облици на невоените закани, што се во согласност со променетиот концепт на безбедност, ги менуваат и концептите на меѓународната, а особено и националната безбедност. Комплексноста и сложеноста на проблематиката што ја третира безбедноста на критичната инфраструктура, директно се врзува со стратегиите на националната безбедност на голем број држави каде што се добива поширока витална димензија, вклучувајќи економски, стопански, политички и еколошки прашања. Националната безбедност повеќе не подразбира исклучиво воени стратегии, туку сè почесто се настојува да се елиминираат невоените загрозувања со воочување на реалната опасност и ефикасна елиминација на истата. Често тоа претставува создавање стратегии на национална безбедност, низ еден деликатен и сеопфатен процес вклучувајќи ја и безбедноста на критичната инфраструктура како составен дел на безбедносниот концепт на секоја држава.

Безбедност на инфраструктурата подразбира заштита на оние инфраструктури што се перцепираат како критични, како што се аеродромите, автопатишта, болници, мостови, транспортни јазли, мрежни комуникации, медиуми, мрежи за снабдување со електрична енергија, брани, нуклеарни електрани, пристаништа, рафинерии за нафта, водни системи итн. Главна цел на заштита на критичната инфраструктура е ограничување на ранливоста на конкретната инфраструктура, спречување на саботажи, тероризам и контаминација, како и спречување на ширење на негативни ефекти на одредено поголемо подрачје и на поголем број сектори, во случај на одреден на-

стан со што би се прекинало нормалното функционирање на инфраструктурата.

Критичните инфраструктури во својот развој сè повеќе користат информациони технологии, со оглед на тоа дека тие стануваат достапни на пошироката јавност. Како резултат на интензивното користење информатички технологии од страна на разни сектори, доаѓа до формирање голема меѓузависност меѓу различните инфраструктурни сектори. Во тој контекст, особено е забележителна и значајната зависност на речиси сите инфраструктурни сектори од информационите технологии (што прераснаа во еден критичен, а најверојатно и најкритичен инфраструктурен сектор). Оттука постоењето голема меѓуповрзаност на инфраструктурата е еден од најголемите проблеми во управување со инфраструктурата.[137]



Слика број 1. Идентификација и приоритизација на критичните функции

[137] Li, H., et al, *Strategic Power Infrastructure Defense*, Proceedings of the IEEE, 2005.

Критичната инфраструктура е од витално значење за правилно функционирање на општеството и на државата. Инциденти, несреќи или намерно попречување на нормалното функционирање на инфраструктурата може да остави сериозни последици врз економијата и да ја спречи на подолг или на пократок период работата на инфраструктурата, што може да се одрази на поголем број човекови активности.

Намерното узурпирање на функционирањето на мрежите за снабдување со електрична енергија може да има големо негативно влијание врз националната безбедност, националната економија и на животот на секој човек. Бидејќи дистрибутивната мрежа за електрична енергија е многу разгранета, голем предизвик е да се зачува нормалното функционирање на оваа инфраструктура.[138] Саботажите како што се сајбер-нападите во голема мера може да го оштетат производството и дистрибуцијата на електрична енергија и да се спречи нормална комуникација и функционирање на информациските системи и не само на национално, туку и на транснационално ниво.

Оваа тенденција, последиците од нарушување на нормалното функционирање на инфраструктурата на земјата да се чувствуваат и надвор од границите на одредена држава, доведе до воведување нов термин – транснационална инфраструктура, што ги означува оние инфраструктури што ги поврзуваат државите.[139]

Денес, може да се зборува за сè поголем број инфраструктурни сектори што се трансформираат во транснационални – секторот за информатичка и комуникациска технологија одамна ги надмина националните граници на државите (а од ден на ден станува сè повлијателен), а исто така, транснационални се секторите за транспорт (патен, железнички, воздушен, воден), телекомуникациската, хемиската индустрија, како и нуклеарната индустрија. Особено значаен е и финансискиот сектор, кој дефинитивно во голема мера е транснационален, за што постојат многу очигледни докази. Гло-

[138] Massoud, A., "Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)". *Computer* (IEEE computer society), 2002.

[139] Schot, J., *Transnational Infrastructures and the Rise of Contemporary Europe*, working Doc No.1, 2003.

балната економска криза, што започна во 2007 година во САД многу брзо од национално се пренесе на меѓународно ниво, доведе до глобална рецесија и ги потресе темелите на националните пазарни економии и ја доведе во прашање досега неприкосновената ефикасност на слободниот пазар.[140]

Увидот во сите релевантни и на меѓународно ниво значајни транснационални инфраструктури во Европа беше постигнат со формирање листа на критична инфраструктура на Европската унија. Всушност, еден од предусловите одредена инфраструктура да е од клучно значење на ниво на ЕУ е да биде транснационална, односно последиците од нејзино откажување да се почувствуваат не само во земја каде што има прекин на функционирањето, туку барем и во друга земја. Слични правила и прописи постојат на ниво на сите организации што имаат транснационален карактер, а се занимаваат со прашањата за поефикасно користење и заштита на инфраструктурата.

Новите размислувања одат во насока дека комплексните инфраструктурни системи е потребно да се разгледуваат како отворени, ранливи системи со многу внатрешни проблеми.[141]

Денес експертите во областа на заштитата на критичната инфраструктура повеќе ја практикуваат оваа концепција на критична инфраструктура, а со оглед на фактот дека заштитата на критичната инфраструктура не се гледа само како на заштита од надворешни напади, туку под овој концепт се подразбира и планирање на обновувањето, кој е важен индикатор на успешната политика на заштита на критичната инфраструктура за да може системот да функционира во сите услови и да може брзо да закрепне во случај на оштетување на одреден сегмент на критичната инфраструктура.

[140] *Global Economic Crisis*, A Publication of Yale Center for the Study of Globalization, Yale Global Online, достапно на: http://yaleglobal.yale.edu/content/global-economic-crisis, посетена на 17/11/2012.

[141] Lundborg, T., Vaughan-Williams, N., Resilience, Critical Infrastructure and Molecular Security: the Excess of Life in Biopolitics, *International Journal Political Sociology*, vol. 5, no. 4, 2011, стр. 369.

Слика број 2.
Приоритети на иницијативата на Европската комисија за заштита на критичната инфраструктура од 2013 година

Инаку, критичната инфраструктура претходно се сметаше за нешто стабилно и конректно, било да се работи за физички или за информациони и комуникациски системи, но денес е актуелна холистичката перцепција на критичната инфраструктура што претставува збир на мрежи и системи што се од витално значење за општеството како целина.[142] Разликите во концептуализацијата и во дефинирањето на критичната инфраструктура во различни земји се резултат на различната перцепција на заканите и безбедносните ризици и разлики во географските и во историските услови, но влијаат и социополитичките фактори.

[142] Pursiainen, C., *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6, 2009, стр. 723.

2. ЖИВОТЕН ЦИКЛУС НА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Постојаните и брзите промени во меѓународните односи, зголемувањето на безбедносните предизвици, ризици и закани како и состојбата на безбедносен дефицит условуваат глобалната безбедносна слика да станува комплексна, а критичната инфраструктура добива нова димензија и зголемена важност на национално и на меѓународно ниво. Како што критичната инфраструктура стана важен сегмент на националната безбедност, така и заштитата на критичната инфраструктура почна да се развива и денес таа претставува еден од главните приоритети на секоја држава.

Непреченото функционирање на системите на критичната инфраструктура претставува приоритет на заедницата на локалната самоуправа, на секоја држава, како и на наднационалните творби.

Заштитата на критичната инфраструктура во контекст на современите глобални безбедносни закани, претставува приоритетно прашање за националната безбедност на секоја држава.

Постапката на заштита на критичната инфраструктура не е ограничена само на непосредно обезбедување и на ефикасен одговор во случај на прекин. Напротив, евидентно е постоење одредени фази во циклусот на заштита на критичната инфраструктура, што ги комбинира постапките на превенција и соодветен третман.[143]

Досегашната практика во САД ги идентификувала главните фази во циклусот на заштита на критичната инфраструктура, што се случуваат пред, за време и по некој настан што може да ја загрози или да ја деградира инфраструктурата. Овие фази претставуваат рамка за сеопфатно решение за квалитетот на инфраструктурата. Тие се структуирани на следниот начин:

- *Фаза 1 (анализа и процена).* Анализата и проценатa претставуваат темелна активност и е најважна фаза во животниот циклус во заштита на критичната инфраструктура.
- *Фаза 2 (санација). Фазата на санација (ремедијација)* подразбира превентивни мерки и активности што се преземаат пред да дојде до несакани случувања.

[143] Perrow, C., *Normal Accidents: Living with High Risk Technologies*, Princeton University Press, 1984.

– *Фаза 3 (индикации и предупредување).* Фазата на индикација и предупредување (пред или за време на настанот) подразбира следење на процената на способностите на осигурување на имотот на критичната инфраструктура и утврдување на постоење одредени индикации на настанот.[144]

3. РИЗИЦИ И ЗАКАНИ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА

Идентификацијата и проценатa на ризиците по критичната инфраструктура е најважниот чекор во креирањето успешна стратегија за подобрување на безбедноста и нивна заштита.

Идентификацијата на ризик е процес на наоѓање, пропишување и карактеризирање на ризичните елементи во согласност со целите на управување, или процена на ризикот. Неопходно е да се идентификуваат изворите на ризик, настаните или збир на околности, како и нивните потенцијални последици.

Сеопфатната идентификација и регистрирање ризици е од суштинска важност, бидејќи одреден ризик, што во оваа фаза не е идентификуван, се исклучува од понатамошна анализа. Идентификацијата треба да ги содржи сите ризици без разлика на тоа дали тие се контролирани или не се под контрола.[145]

Методологијата на процесот на заштита на критичната инфраструктура може да ги содржи следните елементи:

– прецизна идентификација на критичните инфраструктури и нивна дефиниција;
– утврдување на опасностите што се закануваат на идентификуваната критична инфраструктура;
– анализа на ранливост/чувствителност на оние инфраструктури на кои им се заканува ризик и оние што придо-

[144] National Guidelines for Protecting Critical Infrastructure from Terrorism, 2011; National Communications Systems, Office of the Manager, 2000.

[145] Кековиќ, З., Савиќ, С., Комазец, Н., Милошевиќ, М., Јовановиќ, Д., *Процена ризика у заштити лица, имовине и пословања,* Центар за анализу ризика и управљање кризама, Београд, 2011.

несуваат за прекин во случај на намерен напад и во случај на природни или случајни настани;
- процена на ризик од деградација или губење на критичната инфраструктура и приоритет на оние што се ризични и се ранливи;
- примена на контрамерки каде што не постои прифатлив ризик, со цел да се заштитат инфраструктурните капацитети за ефикасно извршување на активностите во итни ситуации.[146]

При изработка на методологија за процена на заканата, подобро е да се користи систематски и мерлив пристап за да се оцени што се тие специфични закани за одредена држава и критична инфраструктура. Структурата на овој методолошки пристап има три основни принципи на безбедност: идентификација, имплементација и одржливост. Кога се прави процена за закана, аналитичарите главно го користат првиот принцип, идентификација, а другите два принципа имаат значајна улога во процесот на управување со ризиците.[147] Првиот чекор е да се идентификува заканата или заканите врз критичната инфраструктура, а следната задача е да се спроведе соодветна безбедносна реакција пропорционална со таквата закана.

При преземање на задачата на оценување закана, постојат неколку извори на емпириски докази и статистички податоци од областа на разузнавањето и безбедноста на критичната инфраструктура, од кои се формира една анализа на минатите трендови на дејства на незаконско постапување. За да се обезбеди, носителите на одлуки да направат веродостојна процена на заканата, сепак, треба да се истражат повеќе извори на информации. Имено, многу тешко се доаѓа до сигурни информации во врска со заканите, така што, аналитичарите мора да ги оптимизираат споредните и

[146] 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, Nov 2005, достапно на: http://www.cpqd.com.br, http://www.cpqdusa.com

[147] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionAppendix 2Thret Assessment Methodology, посетена на 12/11/2014.

нејасни информации што се достапни. Аналитичарите на овој вид информации, без разлика дали тие се од обучени разузнавачки специјалисти, полициски службеници или професионалци за безбедноста, треба редовно да ги оценуваат вклучувајќи ја и тековната безбедност на историските податоци и нејзиното влијание на безбедноста. Аналитичарите треба да се обидат да не се ограничени од страна на традиционалните методи и процеси, но треба да ги вклопуваат традиционалните размислувања со иновативните техники за евалуација.[148]

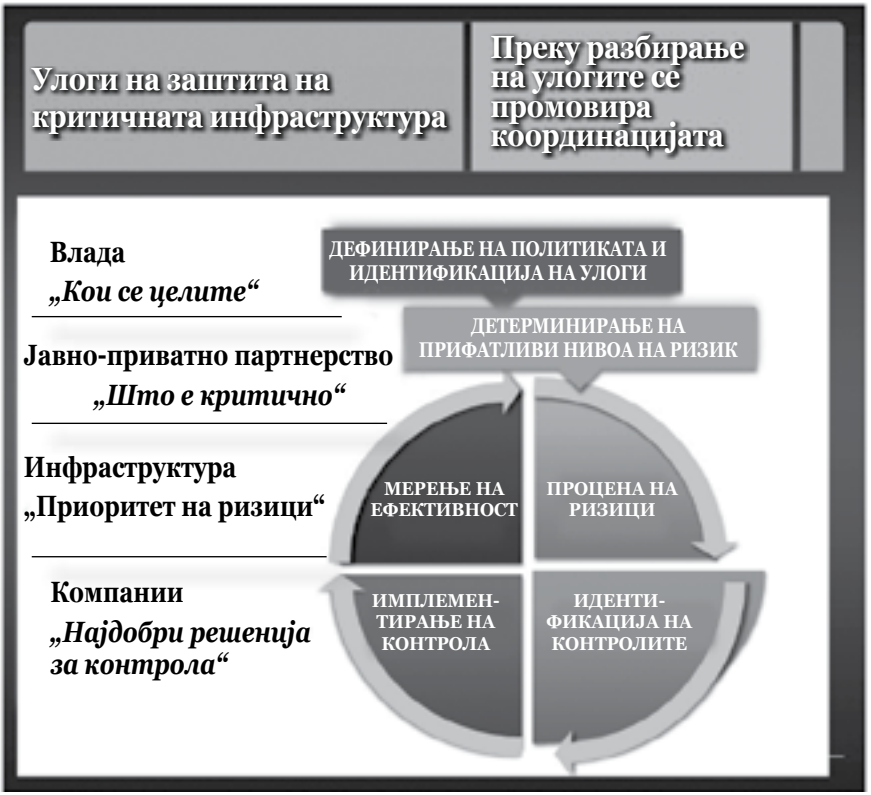
Во современата литература не постои единствена дефиниција за тоа што е ризик. Одредени автори сметаат дека ризик претставува ситуација во која постои можност од отстапување во однос на посакуваниот резултат,[149] за други тоа е мерка на веројатност дека последиците штетни за животот, здравјето, сопственоста, и/или животната средина може да се појават како резултат на некои одредени опасности,[150] додека трети сметаат дека ризик е комплексната особина со која се опишува веројатност од настанување штетни настани и очекувана големина на последици од тие настани за сиот систем и за време на утврдената должина на временскиот интервал или за време на одредена мисија.[151] Исто така, според некои дефиниции ризикот претставува неможност да се предвиди резултатот од идните случувања со целосна сигурност.

[148] Исто.

[149] Vaughan J. Emmett, *Risk Management*, John Wiley & Ins Inc, New York, 1996, стр.23.

[150] Sage P. Andrew, *Systems Engineering for Risk Management*, Norwel MA, 1995, стр.4

[151] Бакрески О., Триван Д. и Митевски С., *Корпорациски безбедносен систем*, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012.



Слика број 3. Улогата на субјектите во заштита на критичната инфраструктура

Можните опасности и процена на ризиците од природни непогоди и други несреќи се класифицираат во зависност од причините на: сеизмички, хидросферски, атмосферски-метеоролошки, биосферски и техничко-технолошки. Евидентирање на карактеристиките на потенцијалните опасности се обработуваат одделно за секоја потенцијална опасност според можните големини, како што се следните:

- Големина 1 – минимална опасност,
- Големина 2 – мала опасност
- Големина 3 – средна опасност
- Големина 4 – голема опасност
- Големина 5 – максимална опасност.

По завршувањето на прелиминарната анализа на потенцијалните опасности од природни непогоди и други несреќи, се извршува анализа на ризик, што резултира со детерминирање на нивото на ризик.

Нивото на ризик кој може да биде во опсег од најмалку 1 до максимум 2,5, а се добива како производ на степенот на веројатноста и степенот на последица.

Степенувањето на големината на веројатноста што одговара на степенот на веројатност, се реализира на следниов начин:

1 – невозможно, 2 – неверојатно, 3 – веројатно,
4 –речиси сигурно, 5 – сигурно

Степенување на последиците што одговараат на големината на последиците, ќе се врши на следниот начин:

1 – минимални; 2 – мали, 3 – умерени, 4 – сериозни и
5 – катастрофални.

Врз основа на одредено ниво на ризик се изработува класификација на ризик за категорија од најниска (прва) до највисока (петта), а потоа се одредува кои ризици се прифатливи, а кои не се.

Прифатливи ризици се ризиците од првата, од втората и од третата категорија, додека ризиците од четврта и од петта категорија се неприфатливи. Врз основа на листата на прифатливи и на неприфатливи ризици се дефинира листа на приоритети за третирање.

Класификацијата на безбедносните закани и ризици за критичната инфраструктура може да се направи на неколку начини. Така, на пример, тие можат врз основа на потеклото да бидат поделени на три изолирани категории:

1. природни катастрофи/елементарни непогоди;
2. грешки во внатрешноста на инфраструктурата на системот, што последователно според потеклото на причините може да се поделат на: грешки од човечки фактор – погрешно планирани активности во рамките на секторот, невнимание на операторите кон критичната инфраструктура, несоодветната соработка и координација на активностите и грешки од техничко-технолошки причини – откажување на машини, дефектни драјвери или грешки во софтверот

што се користи во контекст на одреден инфраструктурен сектор.[152]

3. напади на системите на критичната инфраструктура, каде може да се направи дистинкција помеѓу физички (терористички напади, саботажи) и виртуелни (сајбер-напади).[153]

3.1. Утврдување критериуми за закана и ранливост

Аналитичарите треба да утврдат критериуми за заканата и ранливоста пред спроведувањето на проценатa, преку одредување фокусни точки или центри, што може да се дефинираат како фактори или критериуми кои се проценуваат дека имаат најмногу тежина или вредност во одреден процес, на пример, оператор на воздухоплов, аеродром, или група луѓе.[154]

Повеќето инфраструктури од причини што имаат ограничени човечки и технолошки ресурси, применуваат квантитативен аналитички пристап што бара помалку информации за формирање заклучок. Таквата анализа го насочува аналитичарот да ги смета релевантните податоци објективно, наместо со субјективни шпекулации. Процесот користи два аспекта на анализа што заедно формираат веродостојни средства за оценување на опасноста и утврдување безбедносен одговор преку примена на мерки за управување со ризик. Смислено дело на незаконско постапување против критичната инфраструктура мора, по дефиниција, да биде со предумисла и спроведено од страна на сторителите, што значи дека некој има причина да спроведе противправно дело и продолжува со планирањето до негово извршување. Затоа, пред оценувањето, како акт на незаконско постапување, аналитичарите прво треба да ги разгледаат причините поради кои би било извршено незаконско

[152] Оневозможеното функционирање или уништувањето на еден или повеќе елементи од критичната инфраструктура, може да предизвика техничко-технолошки акциденти, односно да предизвика одредени кризи.

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

[154] ICAO - Aviation Security Manual https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio, посетена на 12/11/2014.

дело и веројатноста тоа да биде сторено. Ова премиса ја елиминира можноста за користење на оваа методологија за анализа на закана за каков било инцидент каде што функционалноста на критичната инфраструктура може да биде нарушена од страна на непослушни лица или ментално нестабилен поединец, чии акции не може да се предвидат, а кои што се спонтани.[155]

Следниот чекор е да се создадат алатки за работа за помош во процесот на оценување. Алатката за работа за оваа методологија се нарекува матрица на ранливост. Може да се комбинираат повеќе матрици за да ја формираат крајната анализа на продолжението на процесот за управување со ризиците или може да се користи одделно од секоја друга во зависност од потребите на аналитичарот. Треба да се напомене дека со цел да се проценат ранливостите на некоја критична инфраструктура, треба да се користи матрицата на категории на закана за безбедноста во бараната област, односно критичната инфраструктура.[156]

Во однос на матрицата на ранливост за профилирање на некоја група, може да се претпостави дека повеќето системи базирани врз човечки фактор може да се организираат во согласност со пет основни атрибути, при што секоја група може да се дефинира со следните компоненти: лидерство, систем од суштинско значење, инфраструктура, бројност и механизам на борбата. Овие атрибути се централни точки за оценување на една група што има потенцијал да изврши дејство на незаконско постапување, без разлика дали профилот се однесува на терористичка група, бунтовничка фракција или организиран криминал. Функциите се опишани на следниот начин:

- лидерство, вклучува хиерархија на групата, присуството на легитимна политичка застапеност и употреба на харизматични личности итн;

[155] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 33-133.

[156] ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio, посетена на 12/11/2014.

- систем од суштинско значење, може да се опише како волја и средства на една група да ги претвори теоретските цели, како политички агенди или религиозните причини во практична примена преку операции на надзор, стекнување оружје и развој на изворите на финансирање и обука на оперативците;
- инфраструктура што комбинира неколку елементи, како што се големина и број на ќелии на групата или поединци (една основана комуникациска мрежа и ефективна употреба на линии за транспорт и снабдување);
- бројноста се однесува на постоење голема мрежа за поддршка, составена од локалните симпатизери или други што може да обезбедат засолниште, храна и пари за групата, без разлика дали е тоа во согласност со целите на групата, или е од страв и од принуда;
- механизам на борбата се членови што вршат активности со цел остварување на целите на групата. На пример, членови-киднапери може да бидат сметани за воини, а креаторите на бомби може да бидат наведени како техничари.[157]

Во рамките на наведените пет атрибути, може да се додадат функционални поткатегории, според длабинската анализа од страна на аналитичарите. Таквите подкатегории може да вклучуваат индикатори, како што се: способност на групата да спроведе насилна акција, локација и историја на познати претходни активности и ниво на посветеност кон своите идеолошки цели и др. Откако ќе се доделат вредности на поените за секое клучно тежиште, вкупниот број им го дава на аналитичарите профилот на групата и релевантната процена на веројатноста за способноста на таа група да изврши дејство на незаконско постапување.

Втората матрица на ранливост е базирана на шесте категории на закани и може да се прошири и на други фактори за кои ќе се процени дека се важни за аналитичарот. За целите на овој модел, бројот на категории беше ограничена на оние што најчесто влијаат на безбедноста. Категориите вклучуваат присуство на група што би

[157] ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio, Table A2-1. Vulnerability Matrix No. 1, посетена на 12/11/2014.

можела да изврши незаконско дело, историја на напади, постоење внатрешни немири, услови на економска криза, ризични сегменти во работењето на инфраструктурата и сл. Овие области на фокус претставуваат различни тежишта од оние во профилот на групата затоа што овие тежишта се подобро приспособени за проценатa на заканата од страна на државата и на операторите. Откако ќе се соберат сите податоци, аналитичарот ќе примени мерлив метод на предвидување на нивото на закана за целта што се оценува. Ако збирот се комбинира со збирот за профилот на групата, резултатот може да биде директно поврзан со примена на контрамерки за безбедност пропорционално на проценетата закана.[158]

За завршната анализа и комплетирање на матриците аналитичарите треба: да ги наведат критериумите што треба да се оценуваат; да се пополнат колоните според клучните вредности од матриците и да се соберат сите поени во секој ред или колона, како што е соодветно; да се одредат приоритетите за контрамерки според бројот на поени со поголем број поени еднаков на повисоко ниво на закана и ранливост.[159] Исто така, треба да се претпостави дека темелното објаснување со опфаќање на причината за одредени заклучоци треба да ја следи проценатa на закана. Добро темелно објаснување ја оправдува програмата за управувањето со ризикот, што ќе се осмисли за да им се спротивстави на проценетите закани. Придобивките од таквиот процес се важечки само ако процесот се преземе рутински. Пропишаните периодични прегледи на тековните податоци се од суштинско значење кога се оценува секоја промена на проценетите закани. Така, со соодветна контрола и управување, методолошкиот пристап за процена на заканата треба да продолжи да обезбедува средства за ефикасно управување со ризик и безбедносен одговор за професионалците од областа на безбедноста и другите носители на одлуки.[160]

---

[158] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 50-83.

[159] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionAppendix 2Thret Assessment Methodology, посетена на 12/11/2014.

[160] ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio, посетена на 12/11/2014.

3.2. Модел на управување со ризици

Двата елемента (процена на заканата и управување со ризик) што заедно ја формираат основата на одржлив и ефективен безбедносен одговор на закани врз критичните инфраструктури од аспект на моделот за управување со ризици, безбедносните професионалци одамна препознаа дека спроведувањето на зголемени превентивни мерки, пропорционално со повисоко ниво на закана е поврзано со трошоци што може да резултираат со големи финансиски оптоварувања на ресурсите на државата или на компанијата. Затоа се смета дека е поефикасно да се употреби заштитната компонента само во ситуации кога за тоа е најмногу потребно, наместо тоа да се применува универзално.[161]

Стандардите што се дадени низ законските регулативи се состојат од основниот сет на низа превентивни мерки за безбедност за кои се очекува да бидат еднакво применети во критичните инфраструктури, без разлика на типот на заканите што влијаат врз работењето, со намера да се обезбеди минимум унифицирани стандарди на безбедност. Доколку државата воведува дополнителни безбедносни мерки за да одговори на повисокото ниво на закана, спроведувањето може да биде тешко одржливо, особено ако дополнителните мерки не се приспособени кон секоја специфична закана. Затоа, откако една држава правилно ја оценила природата и степенот на загрозеност на својата територија, тогаш треба да применува соодветни засилени мерки на критичните инфраструктури. Со цел да се поттикне конзистентен пристап во сите договорни држави во нивната реакција на зголемени услови на закана, потребно е да се развие модел за управување со ризиците што би можел да се користи и да се приспособи според потребите.[162]

Ако се претпостави дека потенцијалните сторители на заканата може да го изместат безбедносниот систем, ако им се дадат

[161] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 50-83.

[162] ICAO – Aviation Security https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Edition, посетена на 12/11/2014.

доволно информации, време и можност, тогаш логична цел е како најдобро да се одвратат сторителите од реализирање на успешно дејство на незаконско постапување. Затоа е важна имплементација на погодни мерки за превентивна заштита.

Оперативна интервенција доведува до третиот принцип, одржливост, што може да се опише дека државата има политичка волја и придружни способности да се одржуваат соодветни и сигурни безбедносни практики. Без обврска за одржување ефективни мерки за безбедност, ефикасноста на другите принципи е намалена.

3.3. Потреба од воведување матрица за управување со ризик

Постојат три нивоа на услови за закана, за кои се поставени соодветни комплети на контрамерки во корелација со матрицата за управување со ризик на следните нивоа:

1. основно – покажува ниски услови на закана каде што во отсуство на сигурни разузнавачки информации што укажуваат дека критичната инфраструктура е цел на напад, има можност за незаконско постапување од страна на поединци или групи, како што се: граѓански немири, работни спорови и активно присуство на антивладини фракции;
2. средно – разузнавачките информации укажуваат дека постои веројатност еден или повеќе објекти да се посочени за напад и
3. високо – разузнавачките информации укажуваат дека еден или повеќе оператори се специјално одредени за напад.[163]

Сепак, пред да се преземат одредени противмерки, треба да се разгледаат следните постапки што се во насока да се согледа:

- природата и степенот на загрозеност на операторот во согласност со валидна процена на заканата;
- да се утврди времетраењето на зголемените услови на закана;

[163] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Edition, посетена на 12/11/2014.

- запознавање со изгледот и со работата на погодените објекти;
- да се спроведе попис на расположливиот персонал и безбедносната опрема;
- да се разгледаат тековните безбедносни мерки; и
- да се оцени бројот на објекти што би биле предмет на подобрени безбедносни процедури.[164]

Управувањето со ризици претставува исклучително важен дел во целокупното управување на корпорациите и нејзините активности. Практично, не постои компанија што не користи некој облик на процена на ризик, иако често не е свесна за тоа.[165] Современите корпорации сериозно пристапуваат кон инвестирање во процесот на управување со ризици, а во тој поглед се истакнуваат финансиските институции, кои се регулирани со регулаторни притисоци.[166]

4. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ОД ПРИРОДНИ КАТАСТРОФИ

4.1. Елементарни непогоди и катастрофи

Заштитата на критичната инфраструктура од природни непогоди и катастрофи е исклучително сложена задача. Во такви сложени услови главната цел на заштита на критичната инфраструктура е насочена кон одржување континуитет во нејзиното функционирање.

Една од мерките за заштита на критичната инфраструктура при елементарни непогоди и катастрофи е изработка на плановите на заштита и спасување во вонредни ситуации.

Како *природни непогоди* ги вбројуваме оние непогоди чија разорна моќ на природните сили и нивната појава се надвор од

[164] ICAO – Aviation Security https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Edition, посетена на 12/11/2014.

[165] Даничиќ М, Сајиќ Љ, оп. цит.стр.113, во Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012, стр.67.

[166] Според: lackovic M., „Upravljanje rizikom-kojiko treba ga se bojati u poslovanju?", Empirija Magna d.o.o Zagreb, 2009, во Корпорациски безбедносен систем, Скопје, 2012, стр.67., и во Даничиќ М, Сајиќ Љ, оп. цит.стр.116.

човечкото влијание. Природните непогоди во зависност од нивниот интензитет и силина и од временскиот интервал може да предизвикаат помали или поголеми материјални загуби и човечки жртви. Под *елементарни непогоди* се подразбираат вонредни ситуациии кои настанале поради природни појави, како што се: земјотреси, поплави, лизгање на теренот, ерозивни процеси, силни ветрови, снежни наноси, како и разни видови технички катастрофи. Освен природни елементарни непогоди можат да настанат и појави со катастрофални последици каде што фактор е човекот со својата активност, како што се: техничко-технолошките катастрофи, потоа епидемии и други вонредни ситуации. Проценатa на загрозеноста од природните непогоди всушност претставува анализата на видот, на обемот, на степенот и на веројатноста на појава на опасноста на зафатениот простор. Исто така, проценатa служи како основа за преземање мерки за одбрана и заштита, односно сведување на опасностите на најниско ниво, а сето тоа овозможено преку развојот на науката, на техниката и на технологијата што овозможува следење и процена на загрозеноста.[167]

Во спектарот на закани се вклучени и последиците од природни непогоди, бидејќи тие, исто така, може да доведат до несакани последици. Четирите природни непогоди кои генерално се користат за оценување ги вклучуваат: ураганот, земјотресот, торнадото и поплавите.[168] Претпоставка е дека историските податоци се валидни за предвидување на идното постоење/појавување природни непогоди. Ако местото се наоѓа во еден регион што бил погоден од природни непогоди во минатото, треба да се спроведе анализа за да се процени нивото на потенцијална штета на местото и опремата. Ако локацијата не се наоѓа во област под влијание на природни опасности, се претпоставува дека ризикот ќе биде низок и не е потребна анализа.[169]

---

[167] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 30-113.

[168] Sandia National Laboratories, *Security Risk Assessment Methodologies,* 2001–2010, http://www.sandia.gov/ram, accessed April 13, 2012.

[169] Betty E. Biringer, Eric D. Vugrin, Drake E. Warren, *Critical Infrastructure System Security and Resiliency*, CRC Press, 2013.

Разгледувајќи ги елементарните непогоди како природни појави, пожарот и поплавите ги ставаме во категорија на појави што можат да се контролираат и превентивно да се дејствува, додека земјотресот како елементарна непогода е појава што се јавува брзо и ненадејно, при што човекот не е во состојба да ја предвиди однапред и да преземе мерки за нејзино превентивно дејствување.

Проценатa на опасностите во случај на природни непогоди и други несреќи се заснова на реалните процени и врз искуствата од минатото.

Анализата на заканите од природни непогоди утврдува дали некој од природните непогоди како – ураган, земјотрес, торнадо, поплави претставува потенцијална закана за специфични објекти или инфраструктура.[170]

Регионот на Југоисточна Европа (ЈИЕ) има прилично безбедна географска положба во однос на опасноста од цунами, од урагани или од торнада. Иако во последните неколку години климатските промени се евидентни, умерено-континенталната и континенталната клима се доминантни. Климатските промени, меѓутоа, започнаа да претставуваат сериозна закана по биодиверзитетот во регионот на ЈИЕ.[171] Тоа што од овој аспект е интересно за нашата расправа нé запира кај опасноста од поплави и земјотреси. Регионот е исклучиво богат со вода (голем број реки), а одредени делови спаѓаат и во групата на високо трусни подрачја.[172] Климатските промени во значителна мерка се одразуваат на бројот на поплави и, секако, преку тоа врз појавата на земјотреси. Појавата на земјотресите и поплавите сериозно може да и се закани на критичната инфраструктура и на тој начин каскадно да предизвика ефекти на загрозување на безбедноста, меѓу другото и во доменот на енергетската безбедност. Многу е

[170] National Oceanic and Atmospheric Administration (NOAA)—*Flooding*: NOAA Watch: NOAA's All-Hazard Monitor: National Oceanic and Atmospheric Administration, http://www.noaawatch.gov/themes/flooding.php, accessed May 7, 2016.

[171] Констатација на над 60 експерти кои се собраа на конференцијата под наслов "Changing Climate, Changing Biodiversity in South-East Europe", одржана во Белград од 18 до 19 јуни 2008 година, достапно на: http:// www.eurosite.org/en-UK/content/south-east-europe-combat-climate-change-impacts-biodiversity

[172] European Spatial Planning Observation Network (ESPON), "*The Spatial Effects and Management of Natural and Technological Hazards in Europe*", Luxembourg, 2006.

извесно дека поплавите и земјотресите може негативно да се одразат врз инфраструктурата што е поврзана со искористувањето или производството на енергија, но и врз инфраструктурата што обезбедува каков било сервис или е поврзана со енергетската безбедност.[173]

4.1.1. Загрозеност од земјотреси

Земјотресите претставуваат природна појава што предизвикува страв, паника, големи човечки жртви и материјални загуби. Оваа појава го следи човекот во текот на сета негова историја. Заради успешна заштита и отстранување на последиците човештвото, се занимава со проучување на оваа појава векови наназад. Какви опасности предизвикува земјотресот може да се види од многубројните примери и податоци, како што се: земјотресот што го опфатил Лисабон во 1755 година, во кој загинале 50.000 луѓе, потоа земјотресот во заливот Сагали кај Токио, во кој настрадале околу 150.000 луѓе. Земјотресот во Скопје во 1963 година уништи 80% од националното богатство на градот, загинале преку 1000 луѓе и имало 10.000 повредени. Заради подобра заштита и отстранување на настанатите последици неопходно е да се изработат планови за заштита и спасување и асанација на последиците предизвикани од земјотресите. За таа цел неопходно е да се изврши процена на загрозеност и повредливоста од земјотреси.

Проценатa од закана на земјотресот се применува на оние локации што се наоѓаат во сеизмички активни области. Проценатa за фреквенцијата поврзани со различни нивоа на сеизмички настан треба да биде направена за секоја локација одделно. Информации што е потребно да се разгледаат за време на сеизмичка анализа вклучуваат големина/јачина на сеизмички настан и оддалеченоста од епицентарот на земјотресот.[174]

---

[173] Patrick Sawer, "Japan Earthquake: Nuclear Disaster Feared After Power Plant 'Explosion'", *The Telegraph*, 12 Mar 2011, достапно на: http://www.telegraph.co.uk/news/worldnews/asia/japan/8377506/Japan-earthquake-nuclear-disaster-feared-after-power-plant-explosion.html.

[174] National Oceanic and Atmospheric Administration (NOAA)—*Earthquakes*: NOAA Watch: NOAA's All-Hazard Monitor: National Oceanic and Atmospheric Administration, http://www.noaawatch.gov/themes/quake.php, accessed May 7, 2016.

4.1.2. Загрозеност од поплави и уривање високи брани

Под поимот поплава се подразбира постепено поплавување на теренот со излевање на водите од природните и од вештачките водотеци како последица на високи водостои, пробивање или рушење насипи, вештачки акумулации, како и поплавување на теренот од последиците на абнормални хидролошки ситуации, големи количества на паднат дожд при што доаѓа до прелевање на реките и на езерата. Поплавените води може да ги покријат површините изложени на поплави за неколку часа, како што е случајот со ненадејните поплави или да се задржи неколку недели, како што е случај со есенскиот и со пролетниот период.[175]

Во основа, надворешните поплави може да бидат предизвикани од временските услови или поврзани со времето. Информациите што може да се користат за да се идентификува и да се анализира потенцијалот за надворешни поплави во една област вклучува топење снег, големи невремиња со грмотевици, извори на вода и тропски циклони. За внатрешни поплави изворите на вода мора да бидат идентификувани, вклучувајќи ја и фреквенцијата за појавување на секој извор.[176]

Поплавите се природни непогоди што често пати ја зафаќаат територијата на Република Македонија. Тие настануваат како резултат на специфичностите на теренот (релјефот, топографските, геоморфолошките) и климатските услови на нашето подрачје. Од досегашните направени согледувања и добиените податоци може да се заклучи дека скоро сите реки и водотеци, вклучувајќи ја и реката Вардар имаат пороен карактер со што заштитата и спасувањето од поплави ја прават сложена, специфична и комплексна самата ситуација.[177] Исто така, во Република Македонија не постои цело-

[175] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од виталeн интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 30-133.

[176] Исто., стр. 33-133.

[177] Донева К., Втор национален извештај на Република Македонија кон рамковната конвенција на Обединетите нации за климатски промени-Дел: процена на ранливоста и адаптација за секторот водни ресурси, Министерство за животна средина и просторно планирање, декември 2006.

сно изграден систем за заштита и спасување од поплави (целосна регулација на водотеците и на реките, изграденост на одбранбените насипи, целосно уредени порои, планови за заштита и спасување од поплави во сите подрачја и региони).[178] Како потврда на изнесениот став е и поплавата што се случи во август 2016 година во Скопскиот регион, што однесе голем број човечки животи и нанесе големи материјални штети.

4.1.3. Загрозеност од ветрови

Загрозеноста од ветрови е често присутен феномен. Најкарактеристични од ветровите се сепак ураганите и торнадата. Закана на ураганот се применува на оние објекти лоцирани во регионите што може да бидат подложни на ураган. Временските информации може да се користат за да се идентификуваат оние региони што може да бидат под влијание на ваква циклонска активност. Историски податоци може да се користат за процена на фреквенцијата на вакви настани. Ураганите ја оштетуваат инфраструктура, како што се: цевководи, водоводна мрежа и слично (како на пр. ураганот Ајк или ураганот Катрина). Параметрите на интерес што се поврзани со урагани вклучуваат: брзина на ветерот (на пример, категорија), бура, акумулација на дожд (длабочина и стапка), времетраењето и големината (земја-покриена површина).[179] За разлика од ураганот, заканата за торнадо се применува за оние области каде што постои потенцијалот за торнада или екстремни ветрови. Историските податоци можат да се користат за да се утврди можноста за нивна појава. Анализите треба да ја проценат веројатноста за торнада и екстремни ветрови и поврзаноста со брзината на ветерот како и времетраењето.

[178] Национална стратегија за води (2012-2042), Проектни тимови, Влада на Република Македонија во партнерство со Влада на Р. Словенија, мај, 2012.

[179] Holland, G., *Assessing Hurricane Impacts,* Willis Research Network and National Center for Atmospheric Research, достапно на: http://www.willisresearchnetwork.com/lists/publications/Attachments/55/WRN_Princeton_March%2009_Holland.pdf, accessed May 20, 2016.

4.1.4. Загрозеност од акциденти предизвикани од опасни материи и од радиолошка, од хемиска и од биолошка контаминација

Опасните материи претставуваат хемиски соединенија, односно смеси на хемиски соединенија или хемиски елементи што поседуваат опасна (штетна) особина, како што се: експлозивност, запаливост, радиоактивност, токсичност или некоја друга особина. Практично земено, голем број од опасните материи се употребуваат во секојдневното живеење (стопанството, медицината, хемиската индустрија и др). Исто така, опасните својства што ги поседуваат некои материи се контролираат и се употребуваат во дејности каде што постои целосна сигурност. Ваквите опасни материи многу лесно може да се најдат во рацете на одредени криминални или терористички структури, па оттука е реално да се очекува да има нивна злоупотреба. Влијанието понатаму може да биде повеќекратно како врз живите организми, така и врз материјалните добра, односно тоа може да биде директно, индиректно или комбинирано. Опасното дејство зависи од видот на опасната материја и намената. И покрај тоа што постојат голем број материи каде што не се во голема мера познати нивните карактеристики, во одредени услови и тие може да се трансформираат во опасни. Сепак, во овој дел поделбата на опасните материи е направена во четири групи: експлозивни, запаливи, радиоактивни, токсични (отровни) материи.[180]

Во рамките на сите поделби на опасните материи примарно место заземаат *експлозивните материи*, што претставува и показател дека се работи за најопасната материја. Нивното опасно дејство е засновано на особината на овие материи, така што под влијание на некое надворешно дејство (средство за иницирање), многу брзо се разлагаат со ослободување на голема енергија и на продукти од разлагањето. Експлозивите тоа едноставно и многу ефикасно го извршуваат, без посебни механизми за трансформација на својата хемиска енергија во механичка смисла на зборот. Трансформацијата се извршува многу брзо, што има за последица способност на

[180] Група автори: *Основи противдиверзионе заштите*, Министерство за унутрашњих послова Република Србије - Институт Безбедности, Београд, 1998.

извршување огромно дејство во краток временски интервал. Тоа дејство предизвикува разорување, рушење и уништување со што се прикажува опасната особина на експлозивните материи.[181]

Запаливите материи опасното дејство го манифестираат при согорувањето, при што доаѓа до трансформација на хемиската во топлотна енергија. Температурата во зоната на согорување расте, со што се манифестира како опасно дејство во смисла на палење, односно предизвикување пожари.

Токсичните материи спаѓаат, исто така, во многу опасни материи. Токсичноста е многу значајна карактеристика на хемиските материи, а особено ако се знае дека може да се манифестира на различни начини. Хемиските материи, меѓусебно се разликуваат по својата отровност. Одреден број хемикалии воопшто не е токсичен, а одреден број се токсични, додека некои се токсични во таа мера што ракувањето со нив претставува голема опасност.[182]

Радиоактивните материи се посебен вид опасни материи, чие опасно дејство се манифестира по пат на јонизирачко зрачење на опасните (штетни) невидливи зраци. Овие зраци поседуваат огромна енергија, го јонизираат воздухот, предизвикуваат разни хемиски реакции, а на живите организми предизвикуваат разорно дејство со што доведуваат до тешки и неизлечиви рани или смртни последици.[183]

Современите услови за живеење и работа, како и сè поизразениот технолошки развој, во голема мера придонесува за зголемување на степенот на загрозеност на државите од радиолошка, од хемиска и од биолошка контаминација и акциденти предизви-

[181] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 55-103.

[182] Група автори*: Основи противдиверзионе заштите*, Министерство за унутрашњих послова Република Србије - Институт Безбедности, Београд, 1998.

[183] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 20-143.

кани од опасните материи. Значи во процесот на производство се користат најразлични опасни материи (отрови) што се гасовити, лесно испарливи, синтетски и според нивните карактеристики се отровни, експлозивни, запаливи и емитуваат разни видови зрачења со што предизвикуваат опасност за населението и материјалните добра, особено во услови на природни непогоди и други несреќи, како и во услови на војна. Широкиот спектар на опасни материи што се користат во процесот на производство и за други намени, може за многу краток временски период да предизвика контаминација – загадување на воздухот, водата, почвата и објектите. Големото влијание врз концентрацијата на контаминацијата, нејзиното проширување, интензитет и слично имаат релјефот, климатските услови, температурата и влажноста на воздухот, атмосферските врнежи, брзината на ветерот, правецот и стабилноста на ветровите, густината на изграденост и населеност, како и локацијата на производствените капацитети што лористат опасни материи во процесот на производството или ги произведуваат.

Во рамките на спроведувањето на мерките за заштита при складирање, транспорт, депонирање и уништување на радиоактивниот отпад, од големо значење е преземање на сите пропишани оперативни постапки од страна на субјекти што се вклучени во таа проблематика.

5. ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА ОД АСИМЕТРИЧНИ ЗАКАНИ

5.1. Заштита на критичната инфраструктура од тероризам

Остварување поголеми приходи беше врвен приоритет на компаниите наспроти грижата за поголема безбедност, односно беше маргинализирано прашањето за заштитата на критичната инфраструктура. Па така, критичната инфраструктура стана недоволно заштитена и ранлива. Терористичките организации, како „Ал Каеда“ или Исламската држава – ИСИС, анализирајќи ја ранливоста на противникот, ги сменија дотогашниот modus operandi и

го префрлија бојното поле на домашна почва на нивните противници. Очигледно е дека заканите врз критичната инфраструктура се дел од агендата на терористичките организации. Промената на modus operandi на „Ал Каеда“ и присуството на „спиечки ќелии“ на европска почва ја зголемува можноста за терористички напади врз европската критична инфраструктура. Затоа перцепцијата за закани надвор од постојните граници треба да се дополни и со анализа на ризици од внатрешноста.

Новиот тероризам се одликува со воен карактер, екстремна бруталност, односно нов стил на дејствување, што ќе биде поразорен и поубиствен во споредба со традиционалниот тероризам. Новите терористички организации постојано го усогласуваат своето дејствување со современите процеси, достигнување во науката и со техниката, особено со примената на комуникациските технологии и употреба на интернет за потребите на пропаганда, регрутирање, индоктринација, собирање средства и водење психолошка војна. Во економски зависен систем, новиот тероризам ги менува целите и стратегијата на сопственото дејствување. Неговата цел сè повеќе се поместува од едноставен психолошки ефект за креирање страв и несигурност кон цели за масовно разорување делови од светските економски, финансиски или технолошки мрежи.[184]

Нападите врз критичните системи на инфраструктура може да се поделат на физички (директни терористички напади и саботажи) и виртуелни (сајбер напади). Исто така, во рамките на оваа категорија може како закана да се сметаат и евентуалните воени конфликти.

Бројни се причините поради кои инфраструктурата мора да биде добро обезбедена и заштитена. Некои од причините се терористички напади (ситуации кога се напаѓа инфраструктурата од политички или од идеолошки причини, како нападите на Светскиот трговски центар во САД (2001 година), нападот на железничката инфраструктура во Мадрид (2004 година), бомбашките напади во лондонското метро (2005 година), бомбашките напади на главната

[184] Милошевска Т., Модели на поврзаност на тероризмот и на транснационалниот организиран криминал, Универзитет „Св. Кирил и Методиј“, Филозофски факултет, МАР-САЖ Скопје, 2016, стр. 38-39.

железничка станица во Мумбаи (2008 година), бомбашкиот напад на аеродромот Домодедово во Русија (2011 година) итн. Овие терористички напади се илустрација колку е комплицирано да се заштити критичната инфраструктура во едно отворено општество.[185]

Директни инфраструктурни ефекти	Каскадни нарушувања или заплена на функциите на критичната инфраструктура или клучните средства преку директни напади на критичен модул, систем или функција.
Индиректни инфраструктурни ефекти	Каскадни нарушувања и финансиски последици за едно претпријатие/организација преку реакции за нападот од јавно-приватниот сектор.
Експлоатација на инфраструктурата	Експлоатација на елементите на одредена инфраструктура за да се наруши или да се уништи друга цел.

Табела број 3. Долготрајни стратегиски цели на терористичките организации.[186]

Терористичките организации таргетирајќи ја критичната инфраструктура и извршувајќи ги нападите на САД, Лондон, Мадрид, Париз и Брисел му ја презентираа на светот својата нова агенда со глобален и апокалиптичен акцент, со што го сменија и текот и размерите на глобалната борба против тероризмот. Обидите за напад што делумно беа успешни, како и големиот број напади што беа спречени

[185] Brian T. Bennett, *Understanding, assessing, and responding to terrorism, Protecting critical infrastructure and personnel*, John Wiley & Sons, Inc, 2007.

[186] John Sullivant, *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, John Wiley & Sons, Inc., 2007.

како оние во Германија,[187] САД,[188] како и оние што беа „успешно" изведени во Ница и во Берлин во 2016 година, но и на други места во светот, се најдобар доказ за потенцијалната опасност. Од друга страна, проблемите со недостатоците од соодветна стратегија за заштита на критичната инфраструктура кај поголем број од земјите во ЈИЕ се дополнителен проблем во присуство од потенцијална закана за критичната инфраструктура од современиот тероризам.

Глобалната борба против тероризмот и менаџирањето кризи предизвикани од терористичките напади добија нови димензии, што директно ја вклучија критичната инфраструктура како предмет на интерес.

Сериозноста на заканите од современиот тероризам за критичната инфраструктура во ЈИЕ е вклештена помеѓу три причини. Прво, заканите од современиот тероризам се глобални. Второ, во согласност со досегашниот modus operandi на современиот тероризам заради активното учество во глобалната војна против тероризмот, оправдано е регионот да се перципира како потенцијална цел. Трето, како и во сиот свет така и во ЈИЕ, во услови на глобализација, критичната инфраструктура егзистира со истите безбедносни недостатоци.

Современите терористички организации напаѓаат „меки" и „незаштитени" или слабо заштитени цели, т.е. инфраструктурата и сервисот што тие го даваат и од кој сите ние зависиме, за разлика од националистичкиот тероризам чија цел беа безбедносните сили.[189] Преку обидите за напад и успесите во нападот врз критичната инфраструктура современиот тероризам успеа во значителна мера да го предизвика современиот начин на живеење. Кај дел од државите тоа се одрази врз промена на политичките одлуки. Кај други, пак, предизвика сериозни дебати околу методите и неопходноста од

[187] "Frankfurt Shooting, The Kosovo Connection", *Economis*t, March 03, 2011, достапно на: http://www.economist.com/blogs/ newsbook/2011/03/ frankfurt_shootings.

[188] United States Senate Committee on Homeland Security and Governmental Affairs, "Violent Islamist Extremism, The Internet, and the Home Grown Terrorist Threat", Majority & Minority Staff Report, 8 May 2008, стр. 11.

[189] John Spyer, "The Al–Qa'ida Network and weapons of mass-destruction", *Meadel East Review of International Affairs*, Vol. 8, No 3, September 2004, стр. 33.

мерките преземени во насока на сузбивањето на современиот тероризам.[190] Дилемите што се наметнаа во оваа насока во значителна мера ја ставија на тест функционалноста на демократијата.[191] На една страна се стави потребата за обезбедување заедничко добро преку што поефективна одбрана. На друга страна, пак, се исправи потребата од ефективното гарантирање и почитување на основните слободи и права. Со други зборови, државите се најдоа заглавени во потребата од менаџирање на точката на балансот помеѓу безбедноста на државата (заедничко добро) и слободата (заштита на индивидуалните слободи и права). Решението на оваа дилема, која извесен период претставуваше енигма, се надмина со воведување параметри, процедури и до одредена мера, стандарди за заштита на критична инфраструктура.[192]

Годишната финансиска програма за превенција, подготовка и последици од спречување на тероризмот, Европскиот совет ја започна во 2007 година како финансиска програма под наслов: „Превенција, подготовка и санација од последиците на терористички напади и безбедносни инциденти“, со цел да се обезбеди финансирање на мерки што се однесуваат на заштита на критична инфраструктура.[193]

Европската унија за справување со тероризмот како глобална закана што го загрозува степенот на заштита на слободата и безбедноста на земјите-членки, им наложува на земјите членки да располагаат со ефикасни кривични закони за борба против тероризмот.

Оваа програма се спроведува во рамките на една поширока европска програма за заштита на критичната инфраструктура и ги поддржува (преку финансирање на спроведување на соодветни мерки за заштита на критичната инфраструктура) заложбите на

[190] Louis Richardson, “Counterterrorism and Democracy”, *Harvard Magazine*, 2009.

[191] A. Hehir and N. Robinson, (eds) “*State Building: Theory and Practice*. London: Routledge”, 2007.

[192] Center for Security Studies, “*Crisis and Risk Network Critical Infrastructure Protection*”, Center for Security Studies (CSS), ETH Zürich, 2009.

[193] Одлука на Советот на ЕУ број 2007/124/EC - Council Decision 2007/124/EC of 12 February 2007, Programme ‘’Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks”.

земјите-членки да се спречат терористички напади, воспоставување и одржување адекватно ниво на подготвеност во случај на напад и заштита на луѓето и на критичната инфраструктура од терористички напади и други безбедносни инциденти.

Следејќи го примерот на ЕУ, тоа што дескриптивната анализа на горенаведената законска легислатива го покажа е дека Република Македонија, за постигнување на полноправно членство во ЕУ, а во рамките на глобалната борба против тероризмот, неопходно е да функционира во насока на зајакнување на европската превенција, подготвеност и одговор на терористички напади врз критичната инфраструктура. Во таа насока, а со цел стандардизирање на постапките на субјектите од системот за управување со кризи по прогласена кризна состојба, од страна на Владата на Република Македонија во февруари 2012 година усвоени се „Стандардни оперативни процедури за комуникација, координација и соработка помеѓу субјектите од системот за управување со кризи во прогласена кризна состојба“, каде што е опфатена и криза предизвикана од терористички напад. Врз основа на член 24 став 1 од Законот за управување со кризи[194] Главниот штаб на Системот за управување со кризи донесува одлука за ангажирање на соодветни ресурси, како и начинот на нивно ангажирање, односно, со одлуката се дефинираат ангажираните ресурси (човечки, материјално-технички и финансиски), како и начинот на нивно ставање во функција, и тоа според времето и намената, а според следново:

- оперативни активности, веднаш по настанокот на кризата (по случувањето на терористичкиот напад);
- укажување помош на непосредно загрозени лица;
- справување со последиците предизвикани од терористичкиот напад;
- помош на посредно загрозени лица од терористичкиот напад и
- логистичка подршка.

Во моментот на случување на терористички напад, во улога на оперативно стручно тело, со активности за превенција и справување

[194] Законот за управување со кризи „Сл. весник“ на Република Македонија, бр. 29/05.

со кризната ситуација, раководи Главниот штаб, што би бил формиран во Центарот за управување со кризи од претставници на субјектите од системот за управување со кризи. Стандардните оперативни процедури за комуникација, координација и соработка помеѓу субјектите од системот за управување со кризи во прогласена кризна состојба", се единствен документ во кој се опфатени активностите на субјектите од системот за управување со кризи за справување (реакција и поддршка) со терористички активности.

5.1.1. Опасните материи во функција на терористички дејства

Опасните материи и терористичките дејства се тесно поврзани, затоа што за извршување на диверзантско-терористичките дејства во голема мера се користат опасните материи. Кога опасното дејство на опасната метерија ќе се насочи кон намерно рушење или палење на виталните објекти, за труење или уништување на луѓето, животинскиот и растителниот свет, тогаш се работи за свесно изведена опасна активност што спаѓа во диверзантско-терористичко дејство. За оваа цел може да се употребат сите четири видови опасни материи, и тоа:

1. Експлозивните материи претставуваат едни од најекспонираните опасни материи што се применуваат за извршување на терористичките активности. Според Адам Долник, скоро една половина од сите досегашни терористички напади се реализирани со бомбашки напади.[195] Од тие причини експлозивите претставуваат најважен сегмент во терористичките напади. Како тактика за употреба на експлозивите може да споменеме:

- подметнувања експлозиви на земја (такви примери се употребата на молотови коктели, импровизираните експлозивни направи, минирањата и сл.);
- подметнувања експлозиви во воздушен (употреба на мали количини на експлозив за предизвикување големи загуби), морски, патен и железнички сообраќај;

[195] Adam Dolnik, *Understanding Terrorist Innovation - Technology, Tactics and Global Trends*, 2007. стр. 13-157.

- исфрлање бомби од мали авиони врз дадени цели или пак употребата на воздухопловите како средство за масовно уништување (пример 11 септември 2001 година во САД).[196]

Експлозивните материии се хемиски соединенија и хомогени, односно хетерогени смеси на повеќе компоненти соединенија што под влијание на одреден енергетски импулс, во многу кратко време со своето хемиско разлагање ослободуваат голема количина топлина и загреани гасови. Продуктите на разлагање, кои во голема мера се гасови, а многу ретко честички на металните оксиди, се стабилни и понатаму не подлежат на реакција. Во разликата на притисоци помеѓу продуктите на реакција и околината доаѓа до ширење на гасови, при што еден дел од енергијата се претвора во работа. Експлозивните материи во принцип имаат стабилна хемиска структура и без доведување на одреден енергетски импулс не доаѓа до разградување на нивната внатрешна градба, меѓутоа има и такви експлозивни материи што практично може спонтано да детонираат без какво било побудување, но поради нивната нестабилност и преголемата опасност не се користат во чист облик. Експлозивните материи постојат во сите три агрегатни состојби, но како разорни експлозиви се користат цврстите и течните експлозиви во облик на цврсти и на течни супстанции, соединенија и смеси.[197]

Најчесто применувани се експлозивите што се користат за воени цели, како што се:

- тринитротолуен (TNT);
- хексоген и неговите смеси, како што е циклотол – B (смеса хексоген и TNT) и некои од пластичните експлозиви со ознаки C – 2, C – 3, C – 4, H – 6, и P – 4;
- пентрит и неговите смеси, како што е пентолит (смеса на пентритот со TNT) и пластичниот експлозив деташит – C и
- октоген и неговата смеса октол (октоген и TNT).[198]

[196] Исто., стр.13-157.

[197] Група автори, *Основи противдиверзионе заштите,* Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд, 1998, стр. 34-121.

[198] Исто., стр. 34-121.

Во некои случаи за изведување на терористички цели се користат и стопанските експлозиви што се карактеризираат со помала разорна моќ во однос на другите. Фактот дека ваквите експлозиви се лесно достапни стануваат многу значајни за анализа кога се во прашање терористичките акции и употребата на импровизирани експлозивни направи. Прашестите стопански експлозиви врз основа на амониум нитрат што го носат трговскиот назив „амонекс“ би ги издвоиле од причина што нивната употреба е присутна во градежништвото, рударството и сл.

Експлозивните материи се карактеризираат со своите физичко-хемиски особини, хемискиот состав и експлозивните својства. Врз основа на овие карактеристики може да се направи и соодветна поделба на: цврсти, течни и гасовити. Концентрациската енергија е најмала кај гасовитите експлозиви, додека течните експлозиви се многу опасни за ракување, па затоа во практика најмногу се користат експлозивите во цврста агрегатна состојба, коишто, покрај другото, содржат и најголема концентрација на енергија.

Според начинот на иницирање и нивната намена, експлозивните материи се делат на четири групи, и тоа:

- примарни експлозивни материи (иницијални експлозиви);
- секундарни експлозивни материи (бризантни експлозиви);
- погонски експлозивни материи (барути)
- пиротехнички смеси.[199]

2. Запаливите материи во својство на употреба при терористички напади, пред сè се користат за предизвикување пожари во сите чуствителни делови на критичната инфраструктура. Предноста на запаливите материи во однос на другите опасни материи се: лесна достапност, едноставна изработка на импровизирани запаливи материи, големи ефекти на страв и паника итн. За намерно предизвикување пожари најчесто се користат запаливи смеси со оксиданс (термит) или без оксиданс (напалм, легура „електрон“ или бел фосфор), користени како темпирани или моментални дејства.

[199] Исто., стр. 6.

3. Радиоактивните материи спаѓаат во посебна група на опасни материи, каде што опасното дејство се манифестира преку јонизирачко зрачење. Тоа својство го имаат некои природни или вештачки елементи или изотопи, како што се кобалт 60, стронциум – 90, цезиум – 137 и др. Јонизирачкото зрачење има голема енергија, што се гледа по нивното дејство. Тоа го јонизира воздухот, предизвикува разни хемиски реакции, а врз живите организми предизвикува тешки радијациони заболувања (опасни и неизлечиви рани). Различните облици на радијација се разликуваат според енергијата и продорната моќ, па врз основа на тоа и различното дејствување врз живите организми.[200]

4. Токсични/отровните материи претставуваат специфична безбедносна закана којашто се карактеризира со спојот од висок степен на смртност, релативно едноставен начин на производство и прикриена употреба. Од аспект на терористичките организации и групи, употребата на биолошките оружја има големи предности во однос на конвенционалните експлозивни средства, и тоа:

- биолошкото оружје произведува поголем степен на смртност кај луѓето, животните и растенијата;
- со мала количина на патогени може да се постигне голем степен на деструкција;
- патогените многу лесно и брзо се активираат (ослободуваат);
- биолошкото оружје дава можност за трајно активирање;
- неопходната опрема е евтина и лесно достапна;
- активните живи микроби што се користат во биолошкото оружје се наоѓаат во природното опкружување или може лесно да се нарачаат од биолошките складови.[201]

Отровите и токсичните материи во функција на терористичките активности може да се претстават од аспект на нивната особи-

[200] Група автори, *Основи противдиверзионе заштите*, Министерство за унутрашњих послова Република Србије - Институт Безбедности, Београд, 1998, стр.8.

[201] Далијела Милиќ, Биотероризам и употреба биолошког оружја, *Ревија за безбедност* 2/10 Центар за безбедносне студије.

на на труење, која може да резултира со здравствени заболувања и смрт. Како основна мерка за токсичност се смета минимална смртна доза која вообичаено се нарекува латентна доза ЛД. Токсичните материи може да се слабо, умерено, јако и екстремно токсични материи. Токсичните материи при терористичките активности во врска со труење на личностите може да се внесат во организмот на следните начини: преку органите за варење, преку органите за дишење, кожно и директно во крвта. Токсичните материи се делат и на гасовити, лесно испарливи, минерални, растителни, синтетички и други поделби. Продирање отров во организмот го нарекуваме труење или интоксикација. Тоа има за последица нарушување на функциите на организмот под влијание на отровите, со што може да се наруши здравјето или да се предизвика смрт. Отровните супстанции генерално можеме да ги поделиме во две основни групи: отрови од природно потекло и отрови од вештачко потекло (синтетички).[202]

5.2. Националната критична инфраструктура како цел на сајбер-нападите

Критичните информациони инфраструктури може да бидат особено ранливи на напади од страна на хакери, криминалци и терористи. Главните алатки што се користат за напад на критичните системи се малициозен софтвер (вируси, црви, тројански коњи), што ги менуваат и ги уништуваат податоците или ги блокираат системите, кражба на идентитет (phishing) напади на веб-апликации (SQL напади), напади со откажување на услуги (DOS, DDoS), внатрешни напади (социјален инженеринг) и слично. Различни автоматски алатки овозможуваат напади од далечински систем, во рок и од неколку секунди. Ова претставува важна основа за поголем обем на активности поврзани со националната безбедност и подготвеност на комуникациите во време на кризни ситуации.

[202] Група автори, *Основи противдиверзионе заштите*, Министерство за унутрашњих послова Република Србије - Институт Безбедности, Београд, 1998, стр.8.

Информационото војување (приватни корисници-хакери или пак одредени држави може од различни причини да ги нападнат информациските системи во различни земји и да доведат до големи проблеми не само во функционирање на информатичката инфраструктура, туку и во многу други сектори, со оглед на фактот дека многу се потпираат на информациските системи, на пр. сајбер-нападите за време на 2008 година – војната во Јужна Осетија).

Голем дел од оваа инфраструктура е контролирана од индустриски контролни системи – ИКС, кои, исто така, се познати како „Надзорна контрола и стекнување со податоци“ (Supervisory Control and Data Acquisition – SCADA[203]), програми кои се ранливи на хакирање или DDoS-напади. Ако заканата не може да предизвика хакирање во системот, тогаш секогаш е можно да се пробие заштитата поради човечки фактор, т.е. корисничка грешка. Многу е полесно да се напаѓаат корисниците (се мисли персоналот) отколку самата опрема. Кога нападот е успешен, опциите за извршување на посакуваниот удар се многубројни. Важно е да се напомене дека повеќето инфраструктурни системи имаат слични проблеми: исти оперативни системи, недостаток на средина во која би можело да се тестира моменталната сајбер-безбедносна состојба, локален менаџмент и нема присуство на надзор. Програмите се направени за специфични системи што оригинално се поставени во затворени мрежи, па се направени со земање предвид на можноста за високи побарувања, но без заштита на доверливоста или интегрирани заштити.[204] Сопствениците на овие системи веруваат дека тие ќе бидат заштитени со тоа што се непознати за јавноста и никој нема да хакира во нивните системи. Исто така, тие се чувствуваат недопирливи, тргнувајќи од тоа дека нивните програми во кои целиот систем работи се специјално напишани само за нив, односно се уникатни со конкретни исполнувања што ги бара специфичниот дизајн на хардверот. Повеќето од овие системи користат исти протоколи што се развиени/напишани во истите програмски јазици како и сите другите програми на пазарот денес, што пак е релативно лесно да

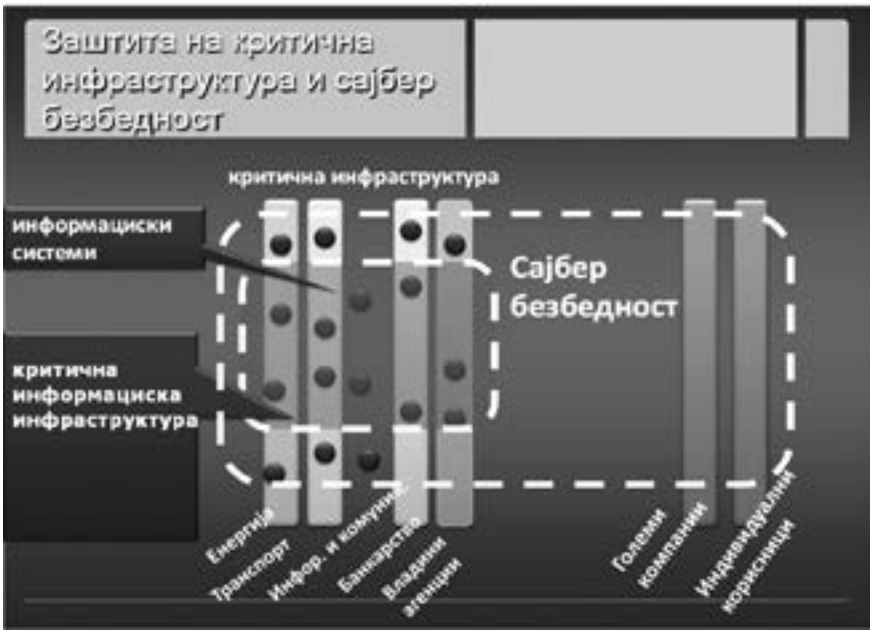
[203] George Loukas, *Cyber-Physical Attaks- A Growing Invisible Threat*, Elsevier Inc, USA, 2015.

[204] Edward G. Amoroso, *Cyber Attacks Protecting National Infrastructure*, Elsevier Inc, USA, 2011.

се најдат ранливости во нив. Нападите против SCADA системите се дуплираа во 2014 година на повеќе од 160.000 напади.[205]

Ако погледнеме во критичната инфраструктура во полето на водоснабдувачкиот систем, на пример, потенцијалните терористи може да навлезат во системите и да ги отворат вентилите/портите на браната и да предизвикаат поплави или да внесат хемикалии за пречистување до степен водата да стане отровна. Реалноста е дека сајбер-проблемите се исто толку важни како и други проблеми со кои се соочуваат овие системи.

Оваа еволуција, или подобро речено револуција на сајбер-нападите, може да биде видена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа и критична воена инфраструктура, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер-просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.



Слика број 4. Заштита на критична инфраструктура и сајбер-безбедност

[205] Dell's, 2015 Annual Security Report, достапно на: http://www.huffingtonpost.com/daniel-wagner/the-growing-threat-of-cyb_b_10114374.html.

Во однос на Република Македонија, до денес критичната инфраструктура не била цел на сајбер-напади. Со оглед на примерот за стакснет-вирусот и фактите дека во Република Македонија не постојат нуклеарни електроцентрали, не треба да се исклучи можноста од ваков тип напади. Постојат други делови од критичната инфраструктура на државата, како што се: електроенергетскиот систем, водоснабдувачките системи, телекомуникацискиот и информацискиот систем што можат да бидат цел на евентуален сајбер-напад. Оттука, државата треба да има соодветна политика и капацитети за справување со сајбер-заканите.[206]

Терминот сајбер-криминал, најчесто е мошне широко толкуван и во теоријата не постои една широко прифатена и унифицирана дефиниција за него. Она што како елемент се јавува во речиси сите дефиниции е тоа дека сајбер-криминалот е криминал што е овозможен од или е насочен против компјутери. Сајбер-криминалот може да опфати кражба на интелектуална сопственост, злоупотреба на патент, трговска тајна и сл., но исто така вклучува и напади против компјутери со цел намерно нарушување на нивното функционирање или недозволено копирање на класифицирани информации складирани во компјутерските системи.[207]

Одредени автори укажуваат на постоење на четири основни класи на меѓузависност, кои меѓусебно не се исклучуваат:

- физички, како резултат на физички врски помеѓу инфраструктурите; Output на една инфраструктура е input за другите и обратно;
- сајбер, како зависност на податоци разменети преку информацискаата инфраструктура;[208]
- географски, настанати како резултат на просторната близина за кои нерегуларни настани може да создадат корелација и промени во соседните инфраструктури;

[206] Стојан Славески, Сајбер-заканите, предизвик за современите општества, Министерство за одбрана на Република Македонија, достапно на: http://morm.gov.mk/?shtit

[207] Wilson, C., Botnets, *Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, January, 2008, стр. 7

[208] Во голем степен функционирањето на современите инфраструктури зависи од компјутерските контролни системи.

– логичка, кога зависноста не се изразува преку физички, сајбер и географски механизми.[209]

Терористите секако дека ги искористуваат придобивките на информатичката технологија, и токму од поврзаноста на тероризмот и интернетот произлегува и една нова форма на тероризам – сајбер тероризмот.

Сајбер-тероризмот е конвергенцијата помеѓу сајбер-просторот и терористичките активности, на пример, политички мотивирано хакирање, кое има за цел да предизвика сериозна штета како загуба на човечки животи и/или сериозни економски последици.

Основните карактеристики на хакирањето се:

- насилен планиран пристап, бидејќи станува збор за пробивање на заштитата на системот;
- неовластеното навлегување („упад“) во системот, кое се базира на високо професионално знаење;
- местото на „упадот“ е по правило оддалечено од местото каде што се наоѓа напаѓачот;
- при самото хакирање, напаѓачот истовремено врши и други дела: измами, кражба на идентитет, саботажа, дистрибуција на вируси и сл.;
- неовластени навлегувања може да вршат поединци или групи, физички или правни лица.[210]

Кога се зборува конкретно за сајбер-терористички напади, веднаш се знае дека тие се насочени кон информациско-комуникациските системи, односно нападот е извршен со помош на нив, а се насочени кон критичните инфраструктури. Сајбер-терористот како цели за напад може да ги земе информационите системи и мрежи на болници, банки, влада, авиокомпании, поединци, и сл., при што ќе се бараат слабости и ранливости во тие системи, со цел да ги нападнат и уништат.

[209] Rinaldi, S., Peerenboom, J., Kelly, T., „Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies“, *IEEE Control Systems Magazine*, Vol. 21, No. 6, Dec 2001, стр. 11-25.

[210] Петровић, Р., С., *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007, стр.111

Генерален заклучок, кога се работи за компјутерски/сајбер-тероризам е дека со текот на времето кое доаѓа, терористите сè повеќе ќе користат висока технологија како за шпионажа и за саботажа така и за пропагирање на своите идеи. Веројатни терористички цели можат да бидат:

- банки на податоци;
- компјутерски системи;
- владини комуникациски системи;
- автоматизирани електроцентрали со кои управуваат компјутери;
- рафинерии за нафта;
- аеродромска инфраструктура и др.[211]

Првиот, добро познат сајбер-напад врз инфраструктурата на НАТО беше за време на интеревенцијата на НАТО на Косово во март 1999 година. Тогаш бројни просрпски хакерски групи реагираа на оваа интервенција на Алијансата, напаѓајќи ја интернет-инфраструктурата на НАТО. По бомбардирањето на кинеската амбасада во Белград од страна на САД и кинеските хакери се вклучија во конфликтот. Бројните хакерски напади создадоа море од испратени „мејлови“ кои ја парализираа секојдневната комуникација на НАТО. Неколку денови беше оневозможено користењето на официјалната веб-страница на НАТО. Во исто време неколку официјални веб-страници на земјите-членки на НАТО, помеѓу кои и на владините сајтови на САД, беа нападнати и беа поставени анти НАТО пораки со повик за прекинување на операцијата на НАТО. Целта што си ја постави хакерите (прекин на воената операција) не беше постигната, меѓутоа, им се даде до знаење на воените авторитети дека не се безбедни и за првпат темата за сајбер-безбедноста се стави на политичката агенда на НАТО. Меѓутоа, сајбер-прашањето се третираше како техничко, со лимитиран потенцијал за нанесување сериозна штета.

Во април 2007 година се извршени напади врз информацисko-комуникациските системи на Естонскиот парламент, во банките, во Владата, во медиумите, всушност, во сите значајни државни

[211] Според Американска комисија за заштита на критичната инфраструктура, достапно на: http://searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html

институции, при што предизвикале дестабилизација на државната безбедност, што од страна на мноштво експерти беа карактеризирани како класичен пример за сајбер-тероризам. Ваквиот вид на напад сепак не претставува напад со огромни последици и загуби, голема материјална штета или човечки жртви, но тоа беше првиот напад од такви размери за да се блокираат сите витални институции на државата, со што целиот систем и државата одат во насока на колапс. Многу пострашен исход би имал нападот што би се состоел од навлегување во естонските компјутери и бази на податоци на здравствени или криминални евиденции, исчезнување на банкарски сметки и сл.[212]

Како прв комбиниран напад на сајбер-напад и воена офанзива се бележи нападот врз Грузија. DDoS - напади[213] од мали размери (напади со дистрибуиран прекин на услугите) врз грузиската интернет инфраструктура, биле регистрирани во јуни, скоро два месеци пред петодневната војна помеѓу Русија и Грузија, по прашањето за Јужна Осетија. На 20 јули 2008 година, фондацијата Shadowserver регистрирала група чувари на интернет кои приметиле повеќе DDoS напади насочени кон официјалната веб-страница на Грузијскиот претседател Михаил Сакашвили, што резултирале со пад на веб-страницата повеќе од 24 часа. Утврдено било дека нападот бил координиран преку Американски сервери, факт кој ја нагласува транснационалната природа на оваа закана. Според „Њујорк тајмс“ нападите врз грузиската комуникациска мрежа кулминирале на 8 август 2008 година, првиот ден од војувањето, кога биле регистрирани напади на веб-страниците на владата и медиумите. Како што се заоструваl конфликтот, така ескалирале и on-line нападите што руските хактивисти ги вршеле над веб-страниците на претседателот, парламентот, министерството за одбрана и надворешни работи, грузиската народна банка и новински агенции. Грузија од сајбер-нападите претрпела мала штета бидејќи грузиската економија и виталната

[212] Lewis, J., Cyber Attacks Explained, June 15, 2007, преземено од http://www.csis.org/tech/070615 cyber attacks.pdf.

[213] Повеќе за ваквите напади во “Explaining Distributed Denial of Service Attacks to Campus Leaders,” May 3, 2005, http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.pdf.

инфраструктура сè уште не биле интегрирани во е-општество. Сеедно, кампањата водена од страна на националистичките хактивисти, поттикнати на акција со помош на рускиот on-line хакерски форум, ефикасно ја нарушила дистрибуцијата на информации на Владата на Грузија, во клучните моменти на нападот.

Овие сајбер-напади имаа три целни групи:

1. серверите задолжени за интернет-инфраструктурата на државата;
2. веб-страниците на владините институции и важни политичари во земјата и
3. провајдерите на приватниот сектор во земјата (банките, медиумите итн).

Оваа еволуција, или подобро речено револуција на сајбер-нападите, може да биде видена како модерна алатка за индиректна интервенција за тајно уништување на противничката мрежа и критична воена инфраструктура, покажувајќи ја стратегиската важност на технолошката еволуција во сајбер-просторот и на тој начин навестувајќи го полето на развој на идната сајбер-војна.

Според истражувањето на компанијата Symantec, повеќе од половина (53%) од критичните информациски инфраструктури имале проблеми во 2010 година од сајбер напади. Просечната цена на нападот бил 850.000 американски долари.[214]

Сајбер-безбедноста се разгледува како дел од заедничката безбедносна политика на ЕУ и предлага државите од ЕУ да одредат национален орган за сајбер безбедност, како и создавање меѓународен систем за рано предупредување при ризици и инциденти. Се предлага операторите на критични инфраструктури во некои сектори (финансиски услуги, транспорт, енергетика и здравство), даватели на услуги за информатичко општество и јавната администрација да известуваат за значителни инциденти, поврзани со безбедноста на нивните услуги. Според статистиката, секојдневно се присутни околу 150.000 вируси, а 148.000 компјутери се засегнати. Според Светскиот економски форум, има 10-процентна веројатност од значаен пад на критичната информа-

[214] Critical Information Protection (CIP) Survey, 2010, достапно на: www.symantec.com

тичка инфраструктура во наредната деценија што и би можело да нанесе штети од 250 милијарди долари.

Од овие причини, во последните години големо внимание се посветува на овој елемент од критичната инфраструктура преку создавање нови политики и воведување нови безбедносни мерки.

Сајбер-безбедноста обезбедува заштита на лица и средства што ги вклучуваат податоците, компјутерите, серверите, зградите/објектите. Целта на сајбер-безбедноста е заштита на податоците додека се пренесуваат и додека се стационирани. На пример, земјотресите, поплавите, падот на електричната мрежа може да предизвикаат инциденти или може да го оштетат системот или организацијата на државата, но само намерните закани може да се третираат како сајбер-закани. Ова важи за физичката инфраструктура на територијата на една држава но, исто така, важи и за критичната информатичка и компјутерска инфраструктура на државата.

Во Табела број 3 е даден приказ на најпознатите сајбер-напади зад кои како напаѓачи се јавуваат држави или непознати групи, а чија цел се важни државни јавни и приватни институции. Најчести последици од овие напади се одбивање услуга, шпионажа, саботажа[215] и крадење информации.[216]

[215] Саботажи се ситуации кога една личност или организирана група, на пример, поранешни вработени во некоја инфраструктура, политички противници на владата или групи за заштита на животната средина извршуваат напад со кој ја преземаат контролата над функционирање на критичната инфраструктура. Саботажата е прикриена, спонтана или организирана дејност со која, на подмолен и перфиден начин за пократко или подолго време се оневозможува или попречува нормалното функционирање на производствените, управните и другите дејности на општеството и посредно или непосредно се предизвикуваат определени материјални и морално политички последици.

[216] "Investigating Cyber Security Threats: Exploring National Security and Law Enforcement Perspectives", Frederic Lemieux, Report GW-CSPRI-2011-2, 7 April 2011, достапно на: http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-2%20Investigating%20Cyber%20Security%20Threats%20Lemieux.pdf.

Табела број 4. Познати напади врз националната/ глобалната безбедност и критичната инфраструктура

Година	Напаѓач	Цел	Последици
1982	САД-ЦИА	Логичка бомба насочена кон гасоводот на СССР во Сибир	Деструкција
1999 и 2000	Русија	Пентагон, NASA, Национална Лабораторија	Шпионажа
2004	Кина	Sandia Национална Лабораторија, Lockheed Martin и NASA	Шпионажа
2007	Кина	Компјутерска мрежа на САД (750,000 компјутери)	Одбивање услуга
2007	Русија	веб страни на владата и на други важни институции/банки на Естонија	Одбивање услуга
2008	Непознато	Воена мрежа на САД	Злонамерен код
2008	Кина и/или Русија	Претседателски избори на САД	Упад во email системите
2008	Русија	веб страници на Владата и други важни институции/банки на Грузија	Одбивање услуга
2010	Непознато (неофицијално Израел)	Иранско објект за збогатување на ураниум	Саботажа
2010, 2011, 2012	Anonymous “Operation Avenge Assange”	Повеќе цели во западните земји (јавни и приватни)	Одбивање услуга
2015	Неофицијално Русија	Контролен енергетски центар во Украина	Одбивање услуга-прекин на електрична енергија (до 230.000 лица)

Извор: Bogdanovski M., Risteski A., *Industrial cyber attacks*, Pdf.

Ако може да се каже дека компјутерските мрежи станаа нешто налик на „нервен систем“ на инфраструктурите на цивилниот и на воениот сектор, онеспособувањето на овој „нервен систем“ ќе значи и парализа на целокупниот систем, на целата земја. Сајбер нападите може лесно да бидат извршени од страна на криминалци, но може да бидат подготвени од терористички ќелии и меѓународно распространети групации. Ако еден насилен напад над државните инфраструктури го сметаме за акт на војна, тогаш зголемениот број релевантни актери значи и дека војната не е повеќе базирана единствено на политичката рационалност. Цел на нападите може да бидат мали или големи системи и може да се мотивирани од обичен вандализам, финансиски и политички придобивки, па сè до начин на докажување и заработување, но и престиж во очите на другите „сајбер војници“. Географската оддалеченост и границите се, исто така, неважни, бидејќи една цел може да биде погодена од спротивната страна на светот за само неколку секунди.[217]

Во листата што следува, нападите се распоредени според нивното влијание и тоа од наједноставни, до најдеструктивни:

- сајбер-шпионажа претставува акт или практика на здобивање тајни (чуствителни, сопствени или класифицирани информации) од индивидуалци, конкуренти, ривали, влади и непријатели за стекнување воена, политичка или економска предност, користејќи нелегални методи за искористување на интернетот, мрежите, софтверот и/или компјутерите.
- веб вандализам-напади што ги обезличуваат веб страниците или напади со одбивање на услуга.
- пропаганда. При овој вид напад можно е да се испраќаат политички пораки кон секој што има пристап до интернет.
- собирање информации. Овој напад се користи со цел информациите кои не се чуваат безбедно да се пресретнуваат, па дури и да се модифицираат, овозможувајќи вршење шпионажа од кој било дел од светот.

[217] Thomas A. Johnson (ed), *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.

- напади со дистрибуирано одбивање услуга. Овој напад се карактеризира со можност за искористување голем број компјутери во една или повеќе држави за лансирање на напад врз системите на државата од каде воопшто и не се лансира нападот.
- Нарушување на функционирањето на опремата. Жртви на овој напад се воените активности во кои за координација се искористени компјутери и сателити. Користејќи го овој напад, злонамерниците може да ги пресретнат или да ги изменат наредбите и комуникациите, со што војниците би се ставиле во ризична ситуација.
- Напаѓање на критичната инфраструктура. Со помош на овој напад, злонамерниците може да навлезат во системите за контрола на електрична енергија, водата, горивото, комуникациите, транспортот и слични клучни инфраструктурни елементи и да се обезбеди контрола врз нив со основна цел уценување, кражби, изнудувања, измама и слично.
- Компромитиран фалсификуван хардвер. Овој напад се однесува на заедничкиот хардвер искористен во компјутерите и мрежите што имаат злонамерен софтвер скриен во софтверот, firmware-от или дури и во микропроцесорите.[218]

За превенција на вакви и слични напади на националната критична инфраструктура, било тоа да е физички или сајбер-напад, секоја држава треба да има стратегиски план за превенција, брз одговор и брзо отстранување на последиците и враќање во нормален работен тек на нападнатата критична инфраструктура, што опфаќа: процена на слабостите што би довеле до физички или сајбер-напад; план за отстранување на значајните слабости; развивање системи за идентификување и спречување на обидите за напад; сигнализација за евентуален напад и отпор на нападот и обновување на работните способности на нападнатиот систем од критичната инфраструктура. Физичките системи се ранливи на надгледување, вандализам, саботажа и напад.

[218] E. Nickolov, "Modern Trends In The CyberAttacks Against The Critical Information Infrastructure", ITU, Regional Cybersecurity Forum, 7-9 October 2008, Sofia, Bulgaria, достапно на: http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/nickolovmodern-trends-sofia-oct-08.pdf.

5.3. Електроенергетска инфраструктура, транспорт на нафта и природен гас – потенцијални ранливи сегменти на критичната инфраструктура

Електроенергетската инфраструктура, транспортот на нафта и природен гас, како и нуклеарните централи се најранливи сегменти од енергетската инфраструктура и претставуваат најверојатни терористички и субверзивни цели. Стотиците илјади километри гасоводи, нафтоводи, далноводи и други енергетски капацитети, кои буквално ја испреплетуваат планетата Земја, претставуваат лесно воочливи и делумно заштитени цели. Клучните електроенергетски јазли, преку кои се менаџира протокот на електричната енергија, претставуваат критични точки и потенцијални терористички цели, чие целосно уништување или саботирање повлекува дополнителни финансиски средства за нивна обнова, или може да предизвика целосен прекин на дистрибуцијата на електрична енергија, т.н. „блекаут".[219] Дополнително, временските промени и природните катастрофи што го потресоа светот во изминатите неколку години ја направија ранлива безбедноста на овие системи и сервисот што тие го даваат. Оттука, станува јасно дека воспоставувањето ефективна стратегија за енергетска безбедност мора да ја земе предвид ефективната заштита на критичната инфраструктура преку која оваа енергија се обезбедува, произведува или на кој и да било друг начин е поврзана со неа.

По нападите на 11 септември 2001 година во САД, тероризмот, како потенцијална закана за безбедноста на нуклеарната енергетска инфраструктура во рамките на ЕУ, предизвика огромно внимание и неодложна потреба од итни мерки за нејзина заштита. Нуклеарниот тероризам има потенцијал да предизвика огромни човечки загуби, последици врз животната средина и дестабилизација на економската и безбедносната состојба.

[219] Танески Н. и Чаминski Б., Геополитичкото значење и заштитата на енергетската инфраструктура на Европската унија од асиметрични закани, *Современа македонска одбрана*, година 14, бр.27, декември 2014.

Околу потребата од дефинирање на т.н. критична инфраструктура и нејзината заштита може да се види во систематизираниот пристап на Центарот за безбедносни прашања од Швајцарија или пак на Homeland Security на САД, кои имаат изработено студии околу ова прашање. Според ваквиот безбедносен пристап, најдобро е кога секоја држава би имала систематизиран пристап кон постојната инфраструктура дефинирајќи ја како критична – потенцијална цел или инфраструктура што може да предизвика значителна штета во случај на елементарни непогоди или човечка грешка. Со цел справување со проблемите и заканите врз неа треба да се развие соодветна стратегија за превентивно дејствување или пост-фестум намалување на ризикот. Преку тоа, според овој пристап се намалуваат ризиците од загрозување на безбедноста, меѓу другото и на енергетската безбедност. Штитејќи ја т.н. критична инфраструктура се штити производството на енергија, снабдувањето со енергија (што е особено изразено во пристапот на ЕУ кон енергетската безбедност).[220]

Потенцијалните економски импликации предизвикани од терористички акт врз енергетската инфраструктура се огромни и претставуваат сериозна закана за глобалната економија. Во таа насока, на 14 февруари 2007 година, со цел да ја разниша економијата на САД, крилото на „Ал-Каеда“ во Саудиска Арабија, ги повика милитантните исламисти во светот, да ги нападнат сите извори на нафта и природен гас.[221] Од даденият пример може да се заклучи дека не само САД, туку и другите држави директно се изложени на ризикот наметнат од фокусот на тероризмот кон енергетската инфраструктура, како најслаба точка на современите економии.

[220] Директивите на ЕУ, на пример, 2005/89 и 2004/67 – Security of Supply for Electricity and Natural gas, 2006/32 – on Energy Efficiency and ESCO, 2003/30 – Biofuels or other Renewable Fuels for Transport, 2010/31 – Energy Performance of Buildings 2010/30 – Labelling of Energy-related Products, како и регулативите: R1228/2003 и R1775/200 – Cross-Border Exchange of Electricity and Natural gas) како и сите други услуги кои овозможуваат остварување на овој процес индиректно. Пошироко да се види во: Center for Security Studies, “Crisis and Risk Network Critical Infrastructure Protection”, Center for Security Studies (CSS), ETH Zürich, 2009.

[221] “Al Qaeda Calls For Attacks on U.S. Oil Sources.” Xinhuanet, 15 February 2007.

Свесни за политичкото и за економското значење на енергетските ресурси за современите демократски општества, терористичките организации ја напаѓаат енергетската инфраструктура за да ги постигнат следните цели:

- преку нападите на енергетската инфраструктура може да предизвикаат сериозни економски последици и да ја нарушат стабилноста на владите против кои се борат, притоа олеснувајќи го начинот да дојдат до посакуваната цел – преземање на власта;
- нападите на енергетската инфраструктура во повеќе случаи се перцепираат како значаен чекор во борбата против странските сили кои во дадениот регион имаат стратегиски интерес, кои ја поддржуваат официјалната влада, како и против меѓународните компании кои се инволвирани во развојот на енергетската инфраструктура и експлоатацијата на енергетските ресурси;[222]
- да ја искористат можноста да обезбедат финансиски средства или да се заканат со прекин на доставата, со цел набавка на оружје или зголемување на економското и на социјалното влијание помеѓу популацијата што сакаат да ја контролираат.[223]

Терористичките напади и проблемите со електро-мрежата покажаа дека штета или целосно губење на инфраструктурата во една од државите на ЕУ може да има негативно влијание на поголем број од земјите, како и на европската економија во целина. Затоа, Европскиот совет побара од Европската комисија да подготви стратегија и акционен план за подобрување на заштитата на Европската критична инфраструктура (ECI). Веќе од 20 октомври 2004 година, Европската комисија го усвои документот со наслов „Заштита на критичната инфраструктура во борбата против

[222] Ely Karmon. "*The Risk of Terrorism against Oil and Gas Pipelines in Central Asia.*" International Institute for Counter-Terrorism, 6 January 2002, достапно на: http://212.150.54.123/articles/articledet. cfm?articleid=426

[223] Ely Karmon. "The Risk of Terrorism against Oil and Gas Pipelines in Central Asia." International Institute for Counter-Terrorism, 6 January 2002, достапно на: http://212.150.54.123/articles/articledet. cfm?articleid=426

тероризмот“, кој укажува на јасни сугестии за подобрување на превенцијата, подготвеност и одговор на терористички напади што влијаат на критичната инфраструктура.

Со централизираниот начин на донесување одлуки сите актери применуваат ист пакет на мерки и стандарди. Стандардите, пак, овозможуваат да се намали индиректната ранливост на критичната инфраструктура поврзана со енергетската безбедност. Така, на пример, независно што во доменот на државно управуваната инфраструктура ќе се усвојат стандардизирани процедури и мерки за заштита, ако приватниот сектор не ги следи овие стандарди заради поврзаноста и испреплетеноста на одделните дејности, негативните последици врз критичната инфраструктура можат и тоа многу да ја загрозат целата критичната инфраструктура и негативно да се одразат врз енергетската безбедност. За таа цел е потребно да е соодветно обучен и информиран (што ќе се постигне преку централизираниот начин на координација и донесување одлуки). Тоа дополнително ќе придонесе кон намалување на потенцијалните човечки грешки што може да ја загрозат енергетската безбедност директно или индиректно.[224]

Оттука, градењето ефективна стратегија на заштита на критичната инфраструктура е еден од клучните елементи што ќе придонесат во создавањето ефективната стратегија за енергетска безбедност. За да го разбереме тоа, пак, потребно е да ја разбереме сериозноста на заканите на критичната инфраструктура.

[224] Metodi Hadži-Janev,Critical infrastructure protection as one of the key elements in the search for an effective strategy for regional energy security, *Political thought*, Instite for democracy, Konrad Adenauer Stiftung, vol.9, December 2011.

IV глава

КРИТИЧНАТА ИНФРАСТРУКТУРА ВО НЕКОИ ОД СОВРЕМЕНИТЕ ДРЖАВИ

1. ПРИСТАПОТ НА САД СПРЕМА КРИТИЧНАТА ИНФРАСТРУКТУРА

Критичната инфраструктура во САД за прв пат особено е нагласена во документот насловен како: „Критични основи за заштита на американската инфраструктура“ објавен во САД во 1997 година. Извештајот содржи главно клучни дефиниции, анализи и насоки за заштита на критичната инфраструктура. Веднаш потоа, Претседателот на САД донесе Директива поврзана со критичната инфраструктура (код NSC – 63). Оваа директива е проследена до сите служби што се поврзани со критичната инфраструктура или со националната безбедност. Во неа се внесени националните интереси, листа на критични инфраструктури, чекори кои треба да бидат преземени за заштита и насоки за координација на службите.[225] Следен чекор во заштита на критичната инфраструктура е направен по трагичниот настан од 11 септември 2001 година што беше реална основа да се обедини американската власт, приватниот сектор и граѓаните во партнерство и заложбите за заштита на критичната инфраструктура и клучните објекти. Претседателот Буш во 2003 година потпиша „Национална стратегија за физичка заштита на критичната инфраструктура и клучните објекти“ (National Strategy for the Physical Protectionof Critical Infrastructuresand Key Assets). Новиот документ е креиран во согласност со Националната стратегија на САД за внатрешна безбедност (National Strategy for Homeland Security) и идентификува јасни цели и принципи што ќе ги поткрепат напорите за заштита на инфраструктурата и на виталните објекти од значење за здравјето, за националната безбедност, за економијата, за водењето на државата и за довербата на граѓаните. Стратегијата

[225] Алчески Ѓ., *Имплементација на современите безбедносни системи и процедури во развојот на обезбедувањето на објектите од витален интерес за Република Македонија,* докторска дисертација одбранета на Филозофски факултет, октомври, 2016, стр. 55-103.

обезбедува унифицирана структура, дефинирани улоги и одговорности и суштински иницијативи што ќе ги водат приоритетите за заштита, но најважно е што обезбедува основа за градење услови за соработка меѓу државните институции, индустријата и граѓаните.[226]

Како резултат на проактивните и координирани активностите во САД на полето на уредување на состојбите во сферата на критичната инфраструктура во 2006 година е усвоен Национален план за заштита на критичната инфраструктура (National Infrastructure Protection Plan) што утврдува унифициран државен став за координирани дејствувања на полето на заштита на критичната инфраструктура. Тој е ревидиран во 2009 година. Дополнително на 12 февруари 2013 година претседателот Обама усвојува Директива за отпорност и заштита на критичната инфраструктура (Presidential Policy Directive – Critical Infrastructure Security and Resilience). Директивата упатува на заедничка, споделена одговорност меѓу федералните, државните, локалните, територијалните ентитети и јавните, односно приватните сопственици и оператори на критичната инфраструктура. Истовремено, се наметнува и потребата од повторна ревизија на Националниот план за заштита на критичната инфраструктура, како резултат на значителната еволуција на состојбите во кои функционира критичната инфраструктура, како што се: степенот на ризик, политиките, оперативноста и сл., и секако врз основа на стекнатите искуства и научени лекции од последните формализирани акти.[227]

Во основа, претседателската директива 21 (ППД-21) од 2013 година идентификува 16 критични сектори, и тоа:

- хемиска индустрија/Секторот, специфична агенција/Одделот за национална безбедност;
- комерцијални објекти/Секторот, специфични агенција/Одделот за национална безбедност;
- комуникации/Секторот/специфични агенција/Одделот за национална безбедност;

[226] *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр.21-22.

[227] Исто., стр.21-22.

- критично производство/на конкретен сектор агенција/Одделот за национална безбедност;
- брани/Секторот, специфична агенција/Одделот за национална безбедност;
- индустриска база за одбрана/Специфични сектори/агенција/Министерство за одбрана;
- службите за итни случаи/Секторот, специфична агенција/ Одделот за национална безбедност;
- енергија/Специфични сектори/агенција/Министерство за енергетика;
- финансиски услуги/Специфични сектори/агенција/Министерство за финансии;
- храна и земјоделство/Коспецифични секторски агенции во САД на Министерството за земјоделство и Министерството за здравство и социјални услуги;
- владини капацитети/Ко-секторот, специфични Агенции/ Одделот за национална безбедност и Генералниот за администрација;
- здравството и јавно здравство/Секторот/специфична агенција/ Одделот за здравство и социјалните услуги;
- информациска технологија/Секторот/специфична агенција/Одделот за национална безбедност;
- нуклеарни реактори, материјали и отпад/Секторот, специфични агенција/Одделот за национална безбедност;
- транспортни системи/Ко-секторот/специфични агенции/ Одделот за национална безбедност и Министерството за транспорт;
- вода и отпадни води системи/Секторот/специфична агенција: агенција за заштита на животната средина.[228]

Примарна цел на основната политика на САД е да се зајакне безбедноста и издржливоста на критичните инфраструктури против физичките и сајбер-заканите. Сојузната влада работи со сопствениците на критичните инфраструктури и територијалните субјекти со цел да се преземат проактивни чекори за управување со ризик и да се зајакне безбедноста и издржливоста на критичната инфраструктура

[228] Presidential Policy Directive-Critical Infrastructure Security and Resilience, February 12, 2013.

во државата, со оглед на сите опасности што би можеле да имаат влијание врз националната безбедност, економската стабилност, јавното здравје и сигурноста, или која било комбинација.[229]

2. ПРИСТАПОТ НА АВСТРАЛИЈА СПРЕМА КРИТИЧНАТА ИНФРАСТРУКТУРА

Концептот на заштита на критичната инфраструктура разгледуван низ призмата на документот насловен како: „Национални насоки за заштита на критичната инфраструктура од тероризам", донесен од страна на Комитетот за борба против тероризмот, наменет за Австралија и за Нов Зеланд, обезбедува рамка за национален конзистентен пристап на заштита на критичната инфраструктура, државата, владата и бизнисот. Стратегијата е дизајнирана да им помогне на сопствениците и на операторите на критичните инфраструктури во нивните дискусии со надлежните органи (вклучувајќи ја и Владата) при заштита на критичната инфраструктура од тероризам. Во неа, исто така, е дефинирано дека третирањето на индивидуалните критични инфраструктурни капацитети ќе зависат од одредување на критичноста на објектот, природата на безбедносното опкружување, односно, видовите ризик за објектот или релевантниот сектор. Како што се наведува во документот, заканата од тероризам бара постојани напори за заштита, вклучувајќи ги и разузнавачките информации заради развој на соодветни нивоа на заштита на критичните инфраструктури во Австралија. Иако владите имаат значителна улога во заштита на критичните инфраструктури, сепак одговорноста паѓа на сопствениците или на операторите. Операторите треба да го разберат тероризмот како опасност во рамките на менаџментот на ризици. На национално ниво критичната инфраструктура е дефинирана како „оние капацитети, ланци на снабдување, информациски технологии и комуникациски мрежи со чие уништување или оштетување би имале значително влијание на социјалната и економската благосостојба или би

[229] https://www.dhs.gov/topic/critical-infrastructure-security, посетена на 16/02/2015.

ја нарушила способноста на Австралија да ја обезбеди национална одбрана и безбедност".[230]

На национално ниво, терминот заштита на критична инфраструктура (Critical Infrastructure Protection – CIP) се користи за да се опишат активностите и мерките за справување со одредена закана од тероризам. Еластичност/ флексибилност на критичната инфраструктура е термин што се користи во стратегијата за да се опише пристапот кон „сите ризици" и опфаќа активности како што се превенција, подготовка, одговор и опоравување од опасности вклучувајќи природни катастрофи пандемии, негрижа, несреќи, криминални активности, напади на компјутерски мрежи како и тероризам. Австралиската Влада ја подржува флексибилност на критичната инфраструктура преку TISN (Trusted Information Sharing Network) мрежата за споделување доверливи информации и преку CIAC (Critical Infrastructure Advisory Council) – Советодавен совет на критичната инфраструктура.

Националните насоки за заштита на критичната инфраструктура од тероризам ги поддржуваат и ги препознаваат следните активности:

- клучна одговорност на операторите во заштита на критичната инфраструктура;
- рамка за менаџмент со ризици при заштита во однос на идентификација и приоритизација на критичните инфраструктури;
- национален антитерористички план;
- национален прирачник за заштита на критичните инфраструктури;
- владина стратегија за еластичност на критичните инфраструктури;
- релевантни австралиски стандарди;
- релевантна легислатива и меѓународни обврски што се применуваат во специфични индустрии како што се транспортот или производство на нафта и гас надвор од државата.[231]

[230] https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf, посетена на 1/11/2015.

[231] https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf, посетена на 1/11/2015.

Од аспект на секторирање на критичните инфраструктури, односно, идентификување на критичните инфраструктури по области во Австралија, застапени се следните сектори: економија, транспорт, енергија, води, здравје, храната и комуникациите, но исто така, и клучните владини сервиси, производството и синџирите на снабдување. Нагласена е потребата од обезбедување на нејзин континуитет како есенцијална важност за економскиот развој на нацијата, националната безбедност и социјалната благосостојба.

Австралиската држава и влада соработува со бизнисот при идинтификација на критичните инфраструктури вклучувајќи ги зависностите помеѓу различните елементи на критичните инфраструктури заедно со одредените надлежности. Државата и владата ја идентификуваат критичната инфраструктура во рамките на нивните надлежности кои се критични или важни за нивната улога. Австралиската Влада има направено рамка за менаџмент со ризици при заштитата на критичните инфраструктури, со идентификација и приоритизација на критичните инфраструктури. Нивоата на критичност дефинирани со Националните насоки за заштита на критичната инфраструктура од тероризам се:

- витално ниво – одредени услуги или капацитети не може да бидат обезбедени на национално или на регионално ниво;
- Главно ниво – ако услугите или капацитетите се потешко оштетени би се применеле рестрикции, па така службите или капацитетите би зависеле од националната асистенција;
- Значително ниво – услугите или капацитетите се достапни, но со одредени рестрикции споредено со нормалните услови;
- Ниско ниво – услугите и капацитетите се функционални на целата територија;
- Непознато ниво – незначителна штета на процесите.[232]

Во однос на пристапот кон контратерористичките мерки врз основа на информации и разузнавање, Австралија се потпира на силна разузнавачка активност, при превенција и подготвеност во антитерористичките подготовки. Овој пристап вклучува мерки за-

[232] https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf, посетена на 11/11/2015.

сновани на принципите на менаџментот со ризици и обезбедување на капацитети за справување со различни видови терористички напади и справување со нивните последици. Овие разузнавачки и криминални истраги се изведуваат од страна на Австралиска служба за разузнавање (Australian Security Intelligence organization – ASIO) и слични агенции со цел спречување и истражување на заканите од клучните елементи при процена на ризик, а тоа се:

- идентификација на клучните елементи во критичните инфраструктурни капацитети;
- земање предвид дали критичните инфраструктури се производител на продукти што може да се искористат од терористите;
- идентификација на можни закани;
- определување ризици што бараат или не бараат третирање;
- средства со кои би се извршил нападот;
- процена на ранливост;
- последици;
- надворешни меѓузависности.[233]

Важен елемент во оваа насока секако претставува функционирањето на Национален советодавен систем при терористички закани. Исто така, превенцијата и подготвеноста како и одговор, опоравување и менаџирање со јавни информации и медиуми се од исклучителна важност, а се дефинирани во стратегијата. Како составен дел на стратегијата, секако претставуваат и прилозите во поглед на одговорностите, безбедносните мерки и сите корисни информации.

3. ПРИСТАПОТ НА ЕВРОПСКАТА УНИЈА СПРЕМА КРИТИЧНАТА ИНФРАСТРУКТУРА

Активностите на Европската комисија во однос на утврдување на регулатива за критичната инфраструктура се во форма на неколку иницијативи, директива и повеќе комуникации во правец на подобрување на безбедноста на критичната инфраструктура. По

[233] Исто., посетена на 11/11/2015.

бомбашките напади на „Ал-Каеда“ во Мадрид, во јуни 2004 година, Европскиот совет ја интензивира работата и ја истакнува важноста на уредување на заштитата на критичната инфраструктура и иницира изработка на глобална стратегија за заштита на критична инфраструктура. На 20 октомври 2004 година, Европската комисија ја поттикна комуникацијата за заштита на критичната инфраструктура во борба против тероризмот што опфаќа пред сè инциденти на критичните инфраструктури предизвикани од терористички напади. Дополнително, во декември 2004 година, Советот на Европа иницира потреба од дефинирање на Европска програма за заштита на критичната инфраструктура (European Programme for Critical Infrastructure Protection-EPCIP), како и Мрежата на информации за предупредување за критичната инфраструктура (Critical Infrastructure Warning Information Network-CIWIN). Во ноември 2005 година по интензивна експертска работа, Европската комисија усвојува (Green Paper on a European Program for Critical Infrastructure Protection – Green Paper on EPCIP)[234] сет на подготвителни активности за пилот-проекти од областа на критичната инфраструктура.[235] Во овој документ се дефинира заштитата на критичната информациона инфраструктура: „сите програми и активности на сопственици, оператори, производители и корисници на инфраструктурата како и регулаторни органи, кои за цел имаат обезбедување на квалитетно функционирање, минимизирање на штетата и брзо обновување на критичната информационата инфраструктура во случај на дефект или напади врз критичната информациона инфраструктура, ја претставуваат програмата за заштита на критичната информациона инфраструктура“.[236]

[234] Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, p. 19, документот е достапен на: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.

[235] *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр.23-24.

[236] Commission of the European Communities, Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM (2004) 702 final, p. 3, документот е достапен на: http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf

Документот на Европската програма за заштита на критичната инфраструктура дава и преглед на критичните инфраструктурни сектори. Во критичната инфраструктура според овој документ се набројуваат 11 сектори прикажани на Табела број 5:

Табела 5. Категоризација на критичната инфраструктура по сектори

Сектор	Производ или услуги
Енергетика	√ производство на нафта и гас, рафинирање, преработка и складирање, вклучувајќи гасоводи и нафтоводи; √ производство на електрична енергија; √ пренос на електрична енергија, нафта и гас; √ дистрибуција на струја, нафта и гас.
Информациони и комуникациски технологии - ИКТ	√ информациони системи и мрежна заштита; √ интернет; √ обезбедување услуги од областа на фиксната телефонија; √ обезбедување услуги во областа на мобилната телефонија; √ радиокомуникација и навигација; √ сателитски комуникации.
Вода	√ обезбедување и дистрибуција на вода за пиење: √ контрола на квалитетот на водата; √ контрола на расположливоста на вода за пиење.
Храна	√ снабдување со храна и заштита на безбедноста и квалитетот на храната.
Здравство	√ медицински и болничка здравствена заштита; √ лекови, серуми, вакцини; √ биолаборатории и биоагенси.
Финансиски системи	√ платежни услуги: √ владини финансиски услуги.
Јавен ред и мир, јавна безбедност и правосудство	√ зачувување на јавниот ред, мир и безбедност; √ судска администрација.
Цивилна администрација	√ владини тела, вооружени сили, службите на цивилна администрација; √ служба за итна интервенција во вонредни ситуации; √ поштенски и курирски услуги.

Сообраќај и транспорт	√ патен сообраќај; √ железнички сообраќај; √ воздушен сообраќај; √ речен сообраќај; √ морски и океански сообраќај и транспорт.
Хемиска и нуклеарна индустрија	√ производство, складирање и преработка на хемиски и нуклеарни материјали; √ цевководи за транспорт на опасни супстанции.
Истражување на вселената	√ вселена; √ истражување.

Извор: Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final, стр. 19.

Заштитата на критичната инфраструктура е во голема мера децентрализирана во рамките на земјите-членки на ЕУ. Во секоја од државите, значителен дел од инфраструктурата е во приватна сопственост и затоа мора да постои соработка со државните институции. Нивото и степенот на учество на приватниот сектор во заштита на критичната инфраструктура е различно. Во одделни земји, претставниците на приватниот сектор активно или систематски се вклучени во развојот на политиката, додека во други, приватниот сектор се вклучува ако е потребно и тоа најмногу поради спроведување на минималните стандарди за заштита воспоставени од страна на државниот сектор.

Директивата на Европскиот совет за идентификација на Европската критична инфраструктура, како и потребата за заштита на критичната инфраструктура од 2008 година,[237] ја пропишува процедурата што секоја земја-членка мора да ја исполнува со цел успешно да ја идентификува и да ја заштити критичнатата инфраструктура. Во рамките на ЕУ постојат голем број напори заштитата на критичната инфраструктура да се разгледува одделно во секој посебен сектор.[238] Како резултат на тоа, експертите ја опишуваат работата на ЕУ за заштита на критичната инфраструктура како асистирање

[237] Council Directive 2008/114/EC of 8 December 2008.

[238] Eriksson, P., Barck-Holst S., *Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis,* FOI, Stockholm, 2005.

на државите во рамките на јасно дефинирани сектори, при што помеѓу секторите постои соодветна координација.[239] Проблемот на соработка помеѓу ЕУ и земјите-членки во процесот на заштита на критичната инфраструктура може да биде став на државите дека некои податоци мора да бидат зачувани во национални рамки.[240] Според процедурата, секоја земја-членка мора да ја идентификува потенцијалната критична инфраструктура во секторот на енергетика и сообраќај според дефинирани критериуми за критичност на инфраструктура од членот 2 (а) и член 2 (б) од Директивата.[241] Како поддршка на државите-членки е усвоено и необврзувачко упатство што ќе им помогне во спроведувањето на Директивата.

Комисијата на ЕУ предложила три фактори што треба да бидат земени предвид при идентификување на потенцијални критични инфраструктури во рамките на секоја земја-членка и тоа:

1. Опсег/обем. Губењето на одредени елементи на критичната инфраструктура предизвикува негативни последици, но тоа не предизвикува загуба на секој елемент, ниту загуба на секоја инфраструктура во иста мера. Исто така, овој негативен ефект може да се одрази на поголема или на помала географска област. Според големината на географската област во која загубата или оштетувањето на некоја инфраструктура може да има влијание, може да варираат и да се разликува инфраструктурите, кои имаат меѓународен, национален и локален карактер.

2. Интензитет. Во зависност од степенот на откажување или уништување на одредена инфраструктура која може да има влијание врз целото општество, може да се формираат неколку категории: инфраструктура чие уништување нема никаков или има занемарлив ефект, инфраструктура чие откажување или уништување има минимален ефект, инфраструктура чие уништување или откажување има умерен ефект, и инфраструктурата чие уништување има голем ефект

[239] Larsson, R., *Tackling Dependency: The EU and its Security Chalenges*, Swedish Defense Research Agency, 2007, стр. 9-24.

[240] Jarlsvik, H., Castenfors, K., *Security and Preparedness in the EU*, Stockholm, 2004, стр.64.

[241] Процедурата на идентификација е опишана во член 3 и Анекс III од Директивата на Советот на ЕУ (2008/114/ЕС).

врз функционирањето на целото општество. Со цел да се процени степенот во кој откажувањето или уништување на инфраструктурата има влијание, постојат неколку критериуми кои всушност, претставуваат влијанија врз различни сегменти на општеството, и тоа: влијанието врз јавноста (број на граѓани што ги чувствуваат негативните ефекти поради губење на инфраструктура, бројот на загубени животи, број на пациенти, бројот на сериозно повредени лица, бројот на евакуирани луѓе); економски ефект (влијание врз БДП, значење на економската загуба и/или деградација на производството или услугите); влијанието врз животната средина (загадување или уништување на животната средина); меѓусебна поврзаност и меѓузависност со други инфраструктури (ова вклучува утврдување на степенот до кој одредена инфраструктура е поврзана со друга инфраструктура, и во која мера функционирањето на другите инфраструктури зависи од правилното функционирање чие влијание се разгледува) и политичко влијание (во зависност од можностите и ефикасноста на владата на една земја во намерата да се справи со проблемот на откажување или губење одреден инфраструктурен сегмент).

3. *Временски ефект*. Овој критериум всушност се однесува на податоци во кој момент губењето или откажувањето на одредена инфраструктура ќе има сериозно влијание (на пример, инфраструктурното откажување може моментално да покаже негативни ефекти, потоа за период од 24 до 48 часа од моментот кога се случило откажување или една недела по откажувањето на инфраструктурата). Во повеќето случаи, се предлага и испитување психолошки ефекти од откажувањето или прекинот на фукционирање на одредена инфраструктура.[242]

Во насока на подобрување на заштитата на критичната инфраструктура, Европската комисија во јуни 2012 година утврди работен документ за ревизија на Европската програма за заштита на критичната инфраструктура[243] којшто утврдува глобален план насочен кон подобрување на заштитата на критичната инфраструктура во сите членки на ЕУ и во сите релевантни сектори на економска

[242] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, стр.3-5.

[243] Commision Staff Working Document on the Rewiew of the European Programme for Critical Infrastructure Protection (EPCIP).

активност. Програмата е резултат на редовна размена на информации помеѓу сите членки на ЕУ во рамките на клучните средби и таа повеќе не е ограничена само на тероризам, туку, исто така, вклучува и криминални активности, природни катастрофи и други причини за незгоди, т.е. таа има за цел да ги утврди сите видови опасности во сите сектори.[244]

Во август 2013 година Европската комисија формулира дополнителен документ со нов пристап кон европската програма за заштита на критичната инфраструктура со тенденција европската критична инфраструктура да биде уште побезбедна (Commision Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure). Документот е базиран на практичната примена на активности од типот на превенција, подготвеност и реакција. Дополнително, во значителен сегмент од документот се обработува меѓусебната поврзаност на критичните инфраструктури со матичната индустрија, но и со другите сектори и секако со државните институции, истакнувајќи ги во овој случај последиците што поради напад/инцидент врз критичната инфраструктура може да настанат кај поширок спектар на субјекти во различни инфраструктури. Исто така, треба да се нагласи дека во истата година Европската комисија го развива порталот: „Мрежа на информации за предупредување за критичната инфраструктура“ (CIWIN), каде е обезбеден систем за интернет/размена на идеи, студии и добри практики за заштита на критичната инфраструктура. Оваа иницијатива има за цел да ја подигне свеста и да се придонесе за заштита на критичната инфраструктура во Европа.[245]

И покрај сеопфатната, темелна правна нормативa што Европската унија ја креира во согласност со надлежностите во својот домен, останува фактот дека на меѓународната сцена ЕУ сè уште е во процес на дефинирање на својата улога во однос на критичната инфраструктура.

---

[244] *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр.24-25.

[245] Исто., стр.25.

За потребите на оваа студија анализата на критичната инфраструктура кај одделни земји членки на Европската унија е сведена на следните држави: Германија, Шпанија, Холандија, Швајцарија, Норвешка, Австрија, Франција, Романија, Чешка, Словенија и Хрватска, кои преку своите искуства претставуваат релевантен извор на насоки за постапување во случајот со Република Македонија.

3.1. Пристапот на Германија спрема критичната инфраструктура

Својот концепт на заштита на критичната инфраструктура германската држава го темели на „Националната стратегија за заштита на критична инфраструктура“ донесена од страна на Сојузното министерството за внатрешни работи во 2009 година. Во овој документ заштитата на критичната инфраструктура е претставена како централно прашање на безбедносната политика на земјата и се раководи според принципот на заедничка акција од страна на државата, општеството, бизнисот и индустријата. Тука државата соработува на партнерска основа со други јавни и приватни субјекти во изготвувањето анализи и заштитни концепти, односно, оние што ги дефинирала како критичност и области на одговорност.[246]

Националната стратегија на Германија за заштита на критична инфраструктура врз основа на технички, структурални и функционални карактеристики може да биде класифицирана во две главни групи: витална техничка основна инфраструктура и витална инфраструктура за социоекономски услуги, во која се издвојуваат девет сектори, и тоа: снабдување со енергија; информациска и комуникациска технологија; транспорт; снабдување со вода за пиење и канализација; јавно здравство, храна; услуги за итни случаи и спасување, контрола и менаџмент на катастрофи; Парламент, Влада, јавна администрација; финансии, осигурување; медиуми и објекти од културно наследство.[247]

[246] National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Republic of Germany Federal Ministry of the Interior, Berlin, 17th June, 2009.

[247] *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр.29-30.

Во Националната стратегија за заштита на критичната инфраструктура снабдувањето со електрична енергија е рангирано на врвот во споредба со другите земји. Ова се должи на фактот дека приватните компании се под законска обврска да работат со безбедна и со сигурна мрежа за снабдување. Слична е состојбата и со телекомуникациските услуги, што исто така, се предмет на законски прописи и мора да се заштитат релевантните телекомуникациски и информативни системи за обработка, со помош на техничките заштитни мерки и други мерки, против неовластен пристап.

Стратегијата посочува дека Сојузното министерство за внатрешни работи е задолжено да обезбедува секторски координации. Нема дилема дека координацијата како процесна функција придонесува за поинтензивна соработка и размена на информации помеѓу релевантните партнери и актери, вклучувајќи ги особено: сојузната администрација; сојузните министерства и нивните специјализирани агенции; сојузните држави (Länder) и нивните органи; административните области; општините и локалната власт; инфраструктурните оператори; различните организации за помош и итни случаи; релевантните индустриски асоцијации и секторски/професионални здруженија; научната и истражувачката заедница; безбедносната индустрија; јавноста воопшто (популација, медиуми); меѓународни и наднационалните институции и други институции по потреба.[248]

Во име на Сојузното министерството за внатрешни работи, властите во рамките на нивната надлежност, како на пример Сојузната канцеларија за цивилна заштита и помош при катастрофи (Bundesamt für Bevölkerungsschutz Katastrophenhilfe - BBK), Сојузниот завод за информациска сигурност (Bundesamt für Sicherheit Informationstechnik - BSI), Сојузната кривична полициска служба (Bundeskriminalamt - BKA) и Федералниот институт Сервис за техничка поддршка“ (Bundesanstalt Technisches Hilfswerk, THB), развиваат процена на заканите, анализи и заштита.[249]

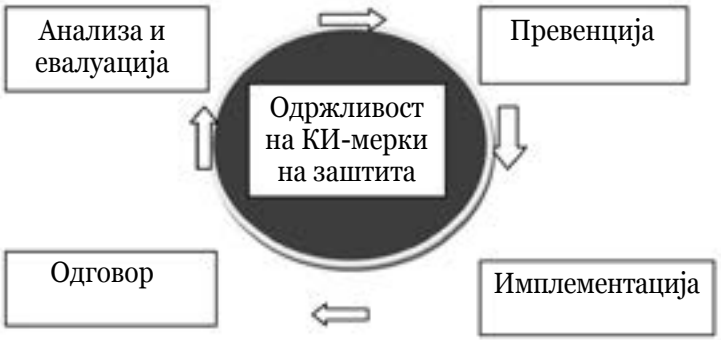
Значи сојузните и локалните власти во Сојузна Република Германија се обврзани заеднички да работат на подобрување

[248] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of Germany Federal Ministry of the Interior Berlin, 17th June, 2009.

[249] Исто., стр. 5.

и спроведување на заштитата на критичната инфраструктура во нивните области на одговорност. Оваа цел се сервира како структурирана имплементација. Постапката се состои од работни пакети, што се спроведуваат паралелно, и врз основа на кооперативен пристап усвоен од страна на Сојузната администрација со вклучување други големи „играчи“, односно оператори и соодветни здруженија во контекст на: дефинирање на општите цели на заштита; анализа на закани, слабости и менаџмент; процена на заканите; спецификација на цели, земајќи ги предвид постојните заштитни мерки; анализа на постојните прописи, применливоста, идентификација на дополнителни мерки што придонесуваат за постигнување на целта и потребите.

Овие работни пакети, првично беа имплементирани од јавниот сектор во соработка со компаниите и операторот. Одговорноста за координација на сојузно ниво е на Министерството за внатрешни работи. Имплементација на мерките за постигнување на целите се врши според: специфични решенија и внатрешна регулатива, договори за поддршка на бизнисот и индустријата, развој на заштитните концепти од страна на компаните, постојан процес на комуникација за ризиците (дијалог за наодите од анализите, проценте, заштитни цели и акциони планови).[250]



Слика број 5. Принципи на заштита претставена преку Германската стратегија

[250] National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Republic of Germany Federal Ministry of the Interior Berlin, 17th June, 2009, стр.16.

3.2. Пристапот на Шпанија спрема критичната инфраструктура

Со одобрувањето на Европската програма за заштита на критичната инфраструктура (EPCIP) од страна на Европскиот совет во 2004 година, како и имплементацијата на Мрежата за известување за критична инфраструктура (CIWIN), Владата на Шпанија објави Национален план за заштита на критична инфраструктура.[251] Следствено на тоа, беше формиран Националниот центар за заштита на критична инфраструктура – тело чија функција е менаџирање, координација и надзор над заштитата на критичната инфраструктура, а е зависно од Бирото за безбедност во рамки на Министерството за внатрешни работи на Шпанија.[252]

Националниот центар за заштита на критичната инфраструктура е тело што е одговорно за усвојувањето на секторските стратегиски планови. Првиот стратегиски секторски план (електрична енергија, гас, нафта, нуклеарна енергија и финансии) е усвоен во мај 2013 година. Со тоа се прецизира регулацијата со која се уредува заштитата на критичната инфраструктура и реализацијата на утврдените насоки.[253] Законот 8/2011 ги уредува и ги пропишува мерките за заштита на критичната инфраструктура и претставува солидна основа врз која се развиваат секторските стратегиски планови.

Надлежностите на Националниот центар за заштита на критичната инфраструктура, меѓу другите се следните:

- поддршка на Државниот секретар за безбедност, во исполнувањето на неговите/нејзините функции во работите поврзани со заштита на критичната инфраструктура, делувајќи како точка за контакт и координатор за агентите на системот;

[251] Plan Nacional De Protección de Infraestructuras Criticas [SES07].

[252] Gómez, S., J., Fernando, Arranz, A., A., Miguel: The Need for the Protection of Critical National Infrastructures: http://link.springer.com/chapter/10.1007%2F978-3-8348-9283-6_33#page-1 посетена на 2/12/2016.

[253] Влада на Шпанија, Министерство за внатрешни работи: http://www.interior.gob.es/web/interior/prensa/noticias/-/asset_publisher/GHU8Ap6ztgsg/content/id/2174254 посетена на 1/12/2016.

- имплементација и ажурирање на Националниот план за заштита на критична инфраструктура;
- одредување на критичноста на инфраструктурата вклучена во Националниот стратешки инфраструктурен каталог, ажурирање и операционално негово одржување;
- насочување и координирање на анализите на ризик спроведени од страна на специјализирани јавни или приватни органи за секој стратегиски сектор, во рамките на секторските стратегиски планови;
- воспоставување минимум за операционални безбедносни планови и Планови за оперативна поддршка, како и надгледување на нивната елаборација;
- процена на плановите за операционална безбедност и нивно предлагање за одобрување на државниот секретар за безбедност;
- анализирање на специфични нацрт-планови за заштита од страна на сопствениците/операторите на националната и/или Европската критична инфраструктура и предложување за нивно одобрување од страна на државниот секретар за безбедност;
- валидација на плановите за оперативна поддршка за секоја критична инфраструктура во Шпанија во согласност со државниот закон, по известувањето на Владините делегации на соодветните автономни региони, или до автономните региони со статутарни надлежности за јавна безбедност и заштита на лица и добра;
- Известување на државниот секретар за безбедност, или органот што се делегира за предлозите за прогласување критични зони;
- имплементирање на постојан информатички, известувачки и комуникациски механизам, според општиот принцип на доверливост со согласност од секој посредник во системот;
- прибирање, процена и анализа на податоците за стратегиска инфраструктура обезбедени од страна на јавните институции, силите за спроведување на законот и инструментите за меѓународна соработка, како и нивно проследување до Националниот антитеристички центар при Министерството за внатрешни работи и други овластени органи;

- учество при организирање вежби и обуки во областа на заштитата на критична инфраструктура;
- координација на работата и учество на експерти во различни работни групи и средби за заштита на критичната инфраструктура на национално и на меѓународно ниво;
- улога на национална контакт точка за меѓународни тела и Европската комисија во областа на заштита на критичната инфраструктура, како и проследување на информациите и консултација со Националниот координативен антитеристички центар во врска со заканите, ранливоста и процените за ризик за секој потсектор во кој се дефинираат европските критични инфраструктури, во временски период и услови утврдени од страна на Директивата.[254]

3.3. Пристапот на Холандија спрема критичната инфраструктура

Во почетокот на 2002 година Холандската влада започна проект за заштита на критичната инфраструктура (Bescherming Vitale Infrastructuur) со цел развивање интегриран збир од мерки за заштита на критичната инфраструктура на владата и индустријата (вклучувајќи ја и информатичката и комуникациската технологија), што претходеше на барањето од 2001 година од страна на холандскиот индустриски сектор за интегриран секторски пристап при заштита на критичната инфраструктура.[255]

Настаните од 9/11 во САД ја забрзаа реакцијата во Холандија и беше донесен Акциониот план на холандската безбедност за борба против меѓународниот тероризам (ТК01) во чиј состав е и планот за заштита на критичната инфраструктура.[256]

---

[254] https://www.developmentaid.org/#!/organizations/view/43468, посетена на 2/12/2016.

[255] Critical Infrastructure Protection of the Netherlands: A Quick Scan. http://cip.management.dal.ca/publications/CIP%20Netherlands.pdf, посетена на 1/12/2016.

[256] http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf посетена на 2/12/2016.

Со цел да се одреди националната критична инфраструктура и од што таа се состои, потребно е првенствено да се утврди што е „критично“[257] за да се избегнат двосмислени и нејасни терминологии, имајќи предвид дека не постои една универзална дефиниција. Така, за да се истражи што ја сочинува холандската критична инфраструктура употребен е пристапот ориентиран на процесот.

За време на Студената војна во Холандија критичната инфраструктура беше утврдувана со планови за витални објекти (пристанишни кранови, мостови, енергетски капацитети), но овој пристап не е повеќе валиден, имајќи предвид дека во современи услови голем процент од системите на критичната инфраструктура се поврзани и се зависни од други системи на критична инфраструктура и нивните функционални процеси се мрежно поврзани.[258]

[257] Производот или услугата се критични кога или обезбедуваат есенцијален придонес кон општеството во одржувањето на дефинираниот минимум ниво на квалитет на националниот и на меѓународниот поредок, јавната безбедност, економијата, јавното здравје и еколошката средина, или пак кога загубата или прекинот влијае на граѓаните или на владината администрација на национално или на меѓународно ниво или пак го загрозува минимумот квалитет.

[258] http://subs.emis.de/LNI/Proceedings/Proceedings36/GI-Proceedings.36-1.pdf, посетена на 1/12/2016.

Табела број 6. Критични сектори на Холандија и нивни производи и услуги

Бр.	Сектор	Производ или услуга
1	Енергија	Струја, гас, нафта
2	Телекомуникации	Фиксни, мобилни, радио, сателитски и емитувачки услуги; пристап до интернет, поштенски услуги
3	Пивка вода	Залихи на питка вода
4	Храна	Резерви со храна и безбедност на храна
5	Здравство	Здравствена заштита
6	Финансии	Финансиски услуги и финансиска инфраструктура (приватна), финансиски трансакции (државна)
7	Зачувување и управување со површински води	Управување со квалитет на вода, одржување и управување со квантитет на вода
8	Јавен ред и безбедност	Одржување на јавниот ред и безбедност
9	Легален поредок	Владеење на правото, спроведување на законите
10	Јавна администрација	Дипломатија, пристап до информации од страна на владата, вооружени сили/ одбрана (поддршка во итни ситуации), јавна администрација
11	Транспорт	Патнички, железнички, воздушен сообраќај, внатрешен сообраќај, океански транспорт, цевководи

Ревизијата на критичната инфраструктура, секторите и услугите беше направена во мај 2015 година, со што се доби ажурирана и ревидирана листа на сектори, поделени во две категории. Категоријата А ја сочинуваат инфраструктурни системи што достигнуваат одреден праг на еден од четирите импакт критериуми: економски последици (оштетување или пад на БДП), физичко влијание (жртви), социетален импакт (преживување емоционални проблеми) или каскадни

ефекти. За категоријата Б пониските прагови се апликативни за првите три критериуми.[259]

Како што е наведено во заканите за индустриските процеси на Холандија, според Светскиот економски форум и Извештајот за глобални ризици од 2008 година, штетата од напад на дигиталната критична инфраструктура во просек изнесува 4,9 милиони евра дневно, а дури 7, 6 милиони евра на ден би изнесувале штетите од напад на енергетскиот сектор. Во истиот извештај постојат процени дека постојат 10 до 20% шанси на масивен дефект на критичната инфраструктура во следната деценија, што потенцијално би чинел 250 милијарди долари.[260]

3.4. Пристапот на Швајцарија спрема критичната инфраструктура

Швајцарската програма за заштита на критичната инфраструктура издвојува десет сектори што се сметаат критични на национално ниво. Дополнително тие се категоризирани во 28 потсектори. Според анализите, мерките за заштита се на напредно ниво за одделни потсектори, како што се инсталациите од кои се содржани, но сепак меѓусекторската координација и консолидираниот пристап се и понатаму недоволни.

Во јуни 2005 година, Федералниот совет на Швајцарија ја задолжи Федералната канцеларија за цивилна заштита координирано да се ангажира во областа на заштитата на критичната инфраструктура. Беше формирана работна група, односно Совет за заштита на критичната инфраструктура во кој беа вклучени сите релевантни актери на федерално и на локално ниво.[261] Овој совет изработи „Стратегија

[259] https://www.thehaguesecuritydelta.com/media/com_hsd/report/53/document/Securing-Critical-Infrastructures-in-the-Netherlands.pdf, посетена на 2/12/2016.

[260] World Economic Forum, Global Risk Report 11th Edition. http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf посетена на 6/12/2016.

[261] https://www.shareweb.ch/site/Disaster-Resilience/resilience-and-related-topics/Documents/FOCP_Critical-Infrastructure-Protection.pdf посетена на 5/12/2016.

за заштита на критичната инфраструктура на Швајцарија“ донесена во 2009 година. Следствено на тоа, Националната стратегија за заштита на критичната инфраструктура беше одобрена од страна на Федералниот совет во јуни 2012 година. Меѓу другото во стратегијата се истакнати стратегиските цели и релевантните принципи, но исто така, е направена дескрипцијата на соодветните мерки што ќе бидат преземени во доменот на заштита на критичната инфраструктура.

Целта на Националната стратегија за заштита на критичната инфраструктура е да се зајакне отпорноста на системите на критична инфраструктура на Швајцарија преку сеопфатен метод и координиран пристап помеѓу сите инволвирани страни. Отпорноста конкретно ја означува способноста да се издржат сите нарушувања и да се одржи функционалноста што е можно подолго, или доколку нема простор за тоа, веднаш да се постигне претходната состојба.

Отпорноста е составена од овие четири компоненти:

1. робустност на системите (критична инфраструктура, државна администрација, економија, општество);
2. расположливост на вишок;
3. способност за мобилизација на ефективни мерки за олеснување;
4. брзина и ефикасност на мерките за олеснување.

Според компонентите, целите на Националната стратегија за заштита на критичната инфраструктура се дополнително поделени на две области: а) зајакнување на робустноста и флексибилноста на заштитата на критичната инфраструктура и б) подобрување на соработката помеѓу потсекторите на критичната инфраструктура со цел зајакнување на робустноста и флексибилноста на општеството, економијата, како и државата (федерални, кантонални и општински агенции) и осигурување дека во случај на непредвиден и немил настан постојат соодветни ефективни и брзи олеснувачки мерки.[262]

[262] https://www.shareweb.ch/site/Disaster-Resilience/resilience-and-related-topics/Documents/FOCP_Critical-Infrastructure-Protection.pdf посетена на 2/12/2016.

Слика број 6. Принципи на заштита на критичната инфраструктура

3.5. Пристапот на Норвешка спрема критичната инфраструктура

Во Норвешка, концептот на „ранливо општество“ стана примарна тема на јавните и на политичките дебати, по што следуваше Извештајот од владината комисија предводена од поранешниот премиер Каре Вилох (Kåre Willoch).[263] Комисијата на Вилох, наброи неколку нови предизвици што се однесуваат на општествената ранливост и предложи сет мерки во својот извештај, што станаа и основа за Белата книга на Норвешка. Тука вклучително спаѓаат:

1. технолошки промени;
2. зголемена комплексност во општествата;

[263] Project description: Critical infrastructures, public sector reorganization and societal safety (CISS) https://www.sintef.no/globalassets/project/samrisk/ciss/critical-infrastructures-and-societal-safety.pdf посетена 03/12/2016.

3. зголемен притисок за ефективност на трошоците;
4. редукција на персонал во јавните сервиси и *аутсорсинг* на јавните услуги на комерцијални претпријатија.[264]

Овие предизвици, заедно со појавата на старо–новите закани како што се: тероризмот, организираниот криминал и климатските промени претставуваат фундаментално променет контекст за субјектите одговорни за одржувањето и заштита на критичната инфраструктура.

Критичната инфраструктура во Норвешка се дефинирана како „оние конструкции и системи што се есенцијални за одржување на општествените критични функции, што ги штитат основните потреби на општеството и придонесуваат за чувството на безбедност и сигурност во општото јавно мислење".

Критичната инфраструктура во Норвешка идентификува четири секторски функции што се сметаат за особено критични, и тоа: електрично напојување, телекомуникации, транспорт и информации и менаџмент.

Посебен аспект што е важен да се напомене е високото ниво на интегрираност и меѓузависност помеѓу различните секторски функции, така што сериозни пречки во една функција ќе резултираат со распространувачки ефект и на другите функции.

Според анализите, целото норвешко општество, вклучувајќи ги и норвешките одбранбени сили и субјектите за цивилно вонредно планирање се зависни од јавните телекомуникациски системи со тенденција за дополнително зголемување на зависноста, поради зголемената употреба на електронски услуги. Понатаму, комерцијалниот и технолошкиот развој ќе резултира со уште поголема ранливост, ако властите не почнат со имплементација на противмерки. Овие мерки се категоризирани на следниот начин: заштита на критичните делови на инфраструктурата против физички и електронски закани; зголемена мрежна флексибилност и елиминација на вишок; заштита на внатрешните информатички

[264] Report on Safety and Security of Society. Report no. 17 to the Storting (2001-2002). Government Norway: https://www.regjeringen.no/en/dokumenter/Statement-on-Safety-and-Security-of-Soci/id420173/ посетена на 6/12/2016.

инфраструктури за мрежен менаџмент и производство на услуги и зголемена ефикасност на услугите и на ресурсите во кризниот менаџмент.[265]

3.6. Пристапот на Австрија спрема критичната инфраструктура

Модерните општества какво што е австриското се многу зависни од континуираното работењето на клучните сектори на критичната инфраструктура што ќе овозможат понуда на клучни стоки и услуги. Тие вклучуваат, меѓу другото, снабдување со електрична енергија, снабдување со вода, информации и комуникации, технологии или отстранување на отпадот и слично.

На 4 ноември 2014 година, Советот на министри во Федералната влада на Австрија донесе нова програма за заштита на критичната инфраструктура позната како Мастер план (Austrian Program for Critical Infrastructure Protection – APCIP Masterplan 2014). Мастер планот е развиен од страна на Федералната канцеларија BKA и Федералното министерство за внатрешни работи. Оваа програма се базира на програма од 2008 година, во која не се вклучени одделни секции за сајбер-безбедност и заштита на критичната информатичка инфраструктура; особено ако се знае дека и двате се важни, релевантни и чуствителни сегменти.

Стартната точка на Мастер планот е идентификација на стратешки важни субјекти што оперираат со критичната инфраструктура и нивни ангажман во безбедносни партнерства. Целокупниот процес на имплементација на Мастер планот во Австрија е надгледуван од страна на Федералната канцеларија на Федералното министерство за внатрешни работи. Тој е поддржан од конзорциум што се состои од претставници од министерствата, Австриските административни единици, стратешки компании и различни интересни групи. Соработката се базира на доброволно самообврзување. Овој вид безбедносни партнерства се регулирани со правно необврзувачки договори

[265] Критична инфраструктура, реорганизација на јавен сектор во Норвешка. Документ: http://textlab.io/doc/580185/critical-infrastructures--public-sector-reorganization-and, посетена на 6/12/2016.

за соработка. Правните активности се преземаат единствено во случаи кога доброволните мерки, ќе се покажат како неефективни.

Концептот за заштита на критичната инфраструктура во Австрија има таканаречен пристап кон сите опасности со цел да се обезбеди непречен проток на различните инфраструктурни системи и нивна оперативност и заштита од природни несреќи, технички акциденти, човечка грешка, сајбер-хазарди, криминал и тероризам.[266] Одговорностите во вид на задачи и капацитети на јавните агенции се регулирани според федералниот Акт за безбедносни политики и вклучуваат: идентификација на критична инфраструктура, поддршка за организациите во креирањето безбедносна архитектура, осигурување физичка заштита и организирање вежби за сајбер-безбедност.[267]

Австриската национална критична инфраструктура се заснова на 13 критични сектори, и тоа: 1. енергија; 2. информатичко-комуникациски технологии; 3. вода; 4. храна; 5. здравство; 6. финансии; 7. транспорт; 8. хемиска индустрија; 9. истражување; 10. уставни институции; 11. социјален систем; 12. дистрибутивен систем; 13. потрага и спасување.

Во современо опкружување, Австрија се стреми да го одржи високото ниво на безбедност и доверба во однос на протокот и функционирањето на системите на критична инфраструктура на ниво на федерална влада, локално, преку стратешките компании и организации, преку изградба на механизми за соработка и комуникација со цел да се достигне и да се одржи отпорноста на системите на критичната инфраструктура.[268]

---

[266] Австриска програма за заштита на критична инфраструктура: https://www.onlinesicherheit.gv.at/nationale_sicherheitsinitiativen/schutz_strategischer_infrastrukturen/71359.html, посетена 06.12.2016.

[267] Europe Integration Foreign Affairs, Federal Ministry of the Republic of Austria Security Policy: https://www.bmeia.gv.at/en/european-foreign-policy/security-policy/ (посетена 05.12.2016).

[268] Austrian Security Strategy. Security in a New Decade – Shaping Security. Federal Chancellery of the Republic of Austria. Vienna 2013: http://www.bundesheer.at/pdf_pool/publikationen/sicherheitsstrategie_engl.pdf, посетена 06.12.2016.

3.7. Пристапот на Франција спрема критичната инфраструктура

Во Франција идентификацијата на критичната инфраструктура ја следи доктрината за одбрана и национална безбедност, а пристапот што се фокусира на „оператори со витално значење" значи оператор чија недостапност силно ќе го загрози економскиот или воениот потенцијал, безбедноста и отпорноста на нацијата. Секој оператор ја идентификува критичната компонента во својот продукциски систем и има обврска да ги предложи како точки со витален интерес и субјекти за кои е потребна специјална заштита.[269]

Со Декретот од 2 јуни 2006 година во Франција се идентификувани 12 области и активности. Овој декрет претрпе измени во јули 2008 година. Овој документ ги елаборира заканите, ги идентификува генеричките ранливости, ги дефинира потребите за заштита и ги одредува градираните мерки што треба да бидат имплементирани во зависност од интензитетот на заканата и во согласност со владиниот план Vigipirate.[270] Од страна на премиерот на Франција беа одобрени 21 насока, со кои се специфицираат заканите, прашања што се во корелација со ранливоста и безбедносните цели, во кои беа номинирани 150 оператори во седум сектори.

[269] Secrétariat Général de la Défense et de la Sécurité Nationale: http://www.sgdsn.gouv.fr/site_rubrique70.html, посетена 06.12.2016.

[270] Централна алатка по иницијатива на премиерот на Франција на Францускиот систем во борба против тероризмот http://www.eaubonne.fr/Services-en-ligne/Actualites/Plan-Vigipirate-Alerte-attentat, посетена 06.12.2016.

Табела број 7. Критични сектори на Франција

Критичен сектор	Надлежно министерство
1. Државни цивилни активности	Министерство за внатрешни работи
2. Правни активности	Министерство за правда
3. Државни воени активности	Министерство за одбрана
4. Производство	Министерство за земјоделство
5. Електронски комуникации, аудиовизуелни информации	Министерство за електронски комуникации
6. Енергија	Министерство за енергетика
7. Вселена и истражување	Министерство за истражувања
8. Финансии	Министерство за економија и финансии
9. Управување со вода	Министерство за екологија
10. Индустрија	Министерство за индустрија
11. Здравство	Министерство за здравство
12. Транспорт	Министерство за транспорт

3.8. Пристапот на Романија спрема критичната инфраструктура

Пристапот кон критичната инфраструктура во Романија започнува со потпишувањето на договорот за пристапување на Романија во Европската унија, на 25 април 2005 година, со потпишување во прилог на протоколи, обврски за транзитирање суровини на целата заедница.

Понатаму чекорите околу заштитата на критичната инфраструктура продолжуваат со вградувањето на критичната инфраструктура како поим во „Националниот развоен план 2007-2013 година“, донесен од страна на романската влада во 2005 година, каде што насоките се дадени кон реализирање на глобалната цел, а тоа е намалување на разликата на социоекономски развој меѓу Романија и другите ЕУ земји-членки. Еден од овие приоритетни правци, вклучени во „Националната стратегија за одржлив развој 2013-2020-2030“ се однесува на инфраструктурата и на нејзиниот развој, како и на заштитата на критичните елементи на инфраструктурата.

Од 2009 година постигнат е напредок во спроведувањето на законската регулатива и критериумите за идентификација и ознака на критичната инфраструктура, а во ноември 2010 година, беше одобрена Уредбата за воспоставување правна рамка за идентификација и означување на национално и на европско ниво искажано низ призмата на секторски основи и процена на потребата да се подобри нивната заштита.

Листата на сектори и потсектори што се однесуваат на Националната критичната инфраструктура (NCI) и на Европската критична инфраструктура (ECI) е дополнета со критериуми и критични прагови (дефиниран во зависност од сериозноста на влијанието на нарушување или уништување на одредена инфраструктура), како и примената на меѓусекторски критериуми што опфаќаат:

- критериуми во однос на жртвите: процена во зависност од можниот број смртни случаи или направени штети;
- критериуми за економските ефекти: процена во зависност од важноста на економска загуба и/или деградација на производи и услуги, вклучувајќи ги и штетите на животната средина;
- критериуми во однос на ефектите врз населението, процена во зависност од влијанието на довербата на јавноста, физичко страдање или нарушување на секојдневниот живот, вклучувајќи губење на основните услуги.[271]

3.9. Пристапот на Чешка спрема критичната инфраструктура

Република Чешка, како земја-членка на ЕУ, ја спроведува Директивата на Советот 2008/114/ЕС, во своето законодавство од декември 2010 година, преку креирање амандман 430/2010 на актот 240/2000 (Критички акт) со кој се одредуваат нови обврски кога се работи за заштита на критичната инфраструктура. Во смисла на овој амандман, во тек е постапката за идентификација и

[271] Augusta-D. Gheorghiu, Eugen Nour, Alexandru Ozunu, (2013), Critical infrastructure protection in Romania. Evolution of the concept, vulnerabilities, hazards and threats, http://www.aes.bioflux.com.ro/docs/2013.148-157.pdf

означување на критичната инфраструктура. Амандманот 430/2010 создава услови за справување со прашања за заштита на критичната инфраструктура на национално ниво. Дефинирање на критичната инфраструктура во Република Чешка претставува и предуслов за специфицирање на Европската критичната инфраструктура (ЕКИ) и со тоа дури и за исполнување на условите кои што произлегуваат од Директивата.[272]

Во правниот кодекс на Република Чешка, прашањата за критична инфраструктура не биле регулирани до декември 2010 година. Постапка за идентификација и означување на критичната инфраструктура е во процес. Постапката произлегува од законската регулатива, а се состои од четири чекори:

1. Избор на критична инфраструктура во рамките на одделни сектори. Овој чекор е во тек во Република Чешката и субјектите што го имплементираат овој чекор се администратори за одделните сектори (министерства и други централни органи на управата, во чија сфера спаѓа критичната инфраструктура) и субјектите (индивидуални сопственици или оператори на критичните инфраструктури). Селекцијата се врши врз основа на консензус помеѓу администраторите и субјектите на критична инфраструктура, според критериуми дефинирани од страна на законодавството.

2. Примена на дефиницијата на критична инфраструктура. Овој чекор е директно испреплетен со претходниот. Суштината на овој чекор е дека потенцијалната критична инфраструктура мора да е во согласност со дефиницијата за критична инфраструктура која е дадена од законодавството (директива). Овој чекор се врши од страна на истите лица како и во претходниот чекор.

3. Примена на дефиницијата за Европска критична инфраструктура (ЕКИ). Дефиницијата за Европска критична инфраструктура ќе се примени на критична инфраструктура како што е дефинирано со критериумите на секторот и во согласност со дефиницијата за критична инфраструктура. Критичните инфра-

[272] International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

структури што ја задоволуваат дефиницијата за трансграничен елемент ќе го следат следниот чекор од процедурата. Критичните инфраструктури што не го задоволуваат трансграничниот елемент на дефиницијата на Европска критична инфраструктура, можат да бидат назначени како национална критична инфраструктура на Република Чешка. Овој чекор се врши од страна на истите лица како и во претходните два чекори.

4. Примена на сеопфатни (вкрстени) критериуми. Секоја земја-членка ќе ги применува вкрстените критериуми со останатите потенцијални Европски критични инфраструктури. Вкрстените критериуми ќе ја земат предвид тежината на влијанието врз инфраструктурата која обезбедува основни услуги, понатаму достапноста на алтернативи и времетраењето на прекинот/закрепнувањето. Потенцијална Европска критична инфраструктура што не ги задоволува вкрстените критериуми нема да се смета за Европска критична инфраструктура. Овој чекор е покриен од страна на Министерството за внатрешни работи – Генерален директорат на Противпожарна служба како највисок администратор и субјект за контакт во Република Чешка, во смисла на Европска критична инфраструктура.[273]

Критичните инфраструктури што поминале низ сите чекори на оваа постапка се сметаат за потенцијална европска критична инфраструктура (ЕКИ). Овие потенцијални ЕКИ ќе бидат објавени од страна на Министерството за внатрешни работи до соодветната надлежна служба на ЕУ - Европската комисија и на оние земји-членки на кои што може да има силно влијание. Како што следува од постапката за идентификација на критична инфраструктура, елементи и активни субјекти на заштита на критична инфраструктура во Република Чешка, сега се Министерствата и другите централни органи на управата, во чија сфера спаѓаат некои сектори на критична инфраструктура и индивидуални сопственици на критична инфраструктура или операторите на критична инфраструктура.

[273] International journal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

Во Република Чешка постојат повеќе примарни субјекти кои влијаат на системот на заштитата на критичната инфраструктура. Овие субјекти се од Европско ниво, преку национално, па се до регионално. Како главни потенцијални субјекти на критична инфраструктура, индивидуални администратори и коадминистратори, што се вклучени во сегашната постапка на идентификација на елементи и означување на критична инфраструктура во Република Чешка се:

– *Министерствата и другите централни административни органи на Република Чешка*. Министерствата и другите централни административни власти се администратори или коадминистратори за одделни сектори за критична инфраструктура и нивната главна задача е координација и изнаоѓање консензус со субјектите на критична инфраструктура при спроведувањето на заштитата на критична инфраструктура. Овие Министерства се: Министерството за надворешни работи, Министерството за одбрана, Министерството за финансии, Министерството за труд и социјална политика, Министерството за внатрешни работи, Министерството за животна средина, Министерството за индустрија и трговија, Министерството за транспорт и врски, Министерството за земјоделство, Министерството за здравство и Министерството за правда. Министерството за внатрешни работи е контакт точка за работи за европска критична инфраструктура и ги извршува задачите во секторот на заштита на критична инфраструктура кои следуваат од членството на Република Чешка во Европската Унија (предлага вкрстени критериуми; ја процесира листата која е основа за определување на критична инфраструктура и ЕКИ елементите; комуницира и ја информира Европската комисија во врска со ЕКИ и др.). Централни административни канцеларии во својство на администратори и коадминистратори за одделни критични инфраструктурни сектори се: Регулаторната канцеларија за енергетика, Управата на државните материјални резерви, Чешката управа за телекомуникации, Чешката народна банка, Државниот завод за нуклеарна безбедност, Чешката управа за рударство, Националната безбедносна управа,

Заводот за статистика на Република Чешка, Безбедносно информативната служба. Денес се ангажирани главно администартори и коадминистратори од сектори во кои се врши постапката на идентификација и означување на критична инфраструктура (енергетика и транспорт).[274]

– *Субјекти на критична инфраструктура - сопственици/оператори на критична инфраструктура.* Според законската регулатива, субјекти на критична инфраструктура се поединечните сопственици или оператори на критична инфраструктура. Постапката за идентификација и означување на критична инфраструктура сè уште не е завршена, така што индивидуалните субјекти сè уште не се информирани за тоа дека се сопственици/оператори на ЕКИ и за правата и обврските што ги имаат во врска со оваа назнака. Сепак, во интерес на овие субјекти е да бидат дел од постапката на заштита на критична инфраструктура, бидејќи поголемиот број субјекти во постапката на идентификација и означување на критична инфраструктура учествуваат активно. Во согласност со законската регулатива, основната и крајна одговорност за заштита на европска критична инфраструктура зависи од земјите-членки и сопствениците/операторите на овие инфраструктури. Па, така ако, потенцијалните субјекти во оваа постапка земат учество во неа, тие може (меѓу другото), исто така, да влијаат на тоа кои и колку ЕКИ елементи се назначени, а подоцна и на финансиските побарувања (ефективност) на мерките што ќе се применат во однос на заштита на критична инфраструктура. Финансиската одговорност во врска со мерките за зголемување на безбедноста на елементите на Европска критична инфраструктура е на сопственикот/операторот на елементите на Европска критична инфраструктура.[275]

[274] Исто.

[275] International jpurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal – Issue 7, Volume 5, 2011.

– *Економски субјекти*. Под економски субјекти се подразбираат лица (физички, правни) или збирни категории на лица. Економските субјекти не спаѓаат во првите две опишани групи на субјекти, но тие се економски заинтересирани за потенцијалните сектори на критична инфраструктура. Со тоа се поврзани економските влијанија на овие субјекти од имплементацијата на заштитата на критична инфраструктура. Активното учество на економските субјекти во системот на заштита им овозможува да имаат влијание на економската страна на преземените чекори според системот на заштита. Со тоа, како главни барања за финансиска активност се подразбираат преземените чекори за спречување и за отстранување на дуплирањето во системот, правичност на мерките итн.
– *Јавност*. Претходната категорија може да се сфати и како јавен субјект. Исто така, јавните интереси се примарно претставени, пред сè, од централно административните органи на Чешка. Оттука, и јавните субјекти треба да се разгледуваат одделно. Начините на кои системот на заштита може да влијае врз јавноста се повеќекратни.
– *Други субјект*. Последна група на субјекти претставуваат институции и субјекти што се занимаваат со прашања на заштита на критична инфраструктура. Тоа вклучува платени услуги (контролни, консултантски или советодавни компании) или истражувачки (универзитети, истражувачки институти, итн.). Овие субјекти имаат висок потенцијал за влијание врз системот за заштита на критична инфраструктура, главно во однос на професионален аспект.[276]

[276] Исто.

3.10. Пристапот на Словенија спрема критичната инфраструктура

Словенските искуства од аспект на управување со критичните инфраструктури и нивната заштита, говорат дека, како и другите земји-членки од ЕУ и Република Словенија ги има идентификувано критичните инфраструктури и има усвоено темелна дефиниција околу поимот национална критична инфраструктура. Усвојувањето на дефиницијата не претставува најделикатен, најтежок и најважен процес, како што истакнуваат словенските научници, кои ја третираат оваа област, кога се работи за прашањата поврзани со заштитата на критичните инфраструктури, туку го истакнуваат утврдувањето на критериумите со кои ќе се дефинира тоа и кои објекти и процеси спаѓаат во рамките на критични инфраструктури.[277]

Имплементирањето на Директивата (ЕС) No. 114/2008 и обврските што произлегуваат од спроведување на Директивата, гледано преку Министерството за одбрана, Република Словенија ги има регулирано актите што се однесуваат за заштита на критичната инфраструктура. Така, Владата на Република Словенија на 12 мај 2011 година донесува Уредба за Европска критична инфраструктура, со која се утврдува: постапката за идентификување и определување европска критична инфраструктура во Република Словенија; содржината на Оперативниот план за безбедност; назначување офицер за безбедност, процедури и рокови за известување на Комисијата на Европската унија и задачите на контактот за заштита на критичната инфраструктура во Република Словенија. Покрај наведеното, во 2008 година, Република Словенија донесе и Одлука за определување задолжително обезбедување што ја надгради во 2012 година, а се однесува на обезбедувањето на критичната инфраструктура. Клучната улога во овие подзаконски акти ја имаат субјектите од областа на приватното обезбедување кои вршат заштита на критичната инфраструктура.[278] Исто така, низ билатерални средби со соседните

[277] http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html, посетена на 1/11/2016.

[278] Gerasimoski, S. & Sotlar, A,, *Private Security in Protection of Critical Infrastructures-Legal and Practical Aspects: Comparatie Study of Macedonia*

земји-членки Словенија соработува во процесот на идентификување на потенцијалните европски критични инфраструктури.

Како основни критериуми при утврдувањето на критичната инфраструктура во Република Словенија се земаат следните:

1. Критичната инфраструктура што поради недоволно или неуспешно функционирање може да предизвика смрт на повеќе од 50 лица;
2. Критичната инфраструктура што поради нефункционирањето може да резултира со значително влијание врз здравјето на населението до таква мера што ќе биде неопходно да се хоспитализираат повеќе од 100 луѓе за повеќе од една недела;
3. Оштетувањето или уништувањето на критичната инфраструктура и нејзиното нефункционирање може да предизвика оштетување и уништување објекти или подрачја со влијание врз националната безбедност на Република Словенија, до тој степен да биде отежнато спроведувањето на националната одбрана, внатрешната безбедност или заштитата од природни и други катастрофи;
4. Критичната инфраструктура што влијае во спроведувањето на економските или други активности претставена во рамките на штета или загуба на приходи од над 10 милиони евра на ден;
5. Критичната инфраструктура што поради нефункционалност влијае на прекин со снабдување со вода за пиење или храна за население во обем од околу 100.000 луѓе за повеќе од една недела;
6. Критичната инфраструктура што поради нефункционалност влијае на прекин со снабдување со електрична енергија за три дена или природен гас за повеќе од една недела за население во обем од околу 100.000 луѓе;

---

and Slovenia, Paper presented at International Scienticfic Conference held by Faculty of Security Skopje in Ohrid во *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр. 30.

7. Критичната инфраструктура што поради нефункционалност влијае на прекин во снабдувањето со нафтени производи за повеќе од една недела, за население од над 100.000 луѓе;
8. Критичната инфраструктура што предизвикува многу штета поради влијание на водата и загрозува живеалишта и почва во површина од над 100 хектари;
9. Критичната инфраструктура што поради нефункционалност резултира со губење на информации или комуникациска поддршка за работата на други критични инфраструктури до 24 часа;
10. Критичната инфраструктура што резултира во прекугранични последици и во други земји, во согласност со претходните критериуми.[279]

Уредбата за европска критична инфраструктура ја регулира европската критична инфраструктура во секторите: енергија со три потсектори и транспорт со пет потсектори.

[279] www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ Številka: 802-15/2011-67 Ljubljana, dne 28. 9. 2012 – Republika Slovenija Ministarstvo za obrambo - Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji - Точка 1.

Табела број 8: Листа на сектори на европска критична инфраструктура во Словенија

Сектор	**Потсектор**	
Енергија	Електрична	Инфраструктура и објекти за производство (со исклучок на нуклеарни централи) и пренос на електрична енергија заради обезбедување со електрична енергија
	Нафта	Производство, рафинирање, обработка, складирање и пренос на нафта преку цевки
	Гас	Производство, рафинирање, обработка, складирање и пренос на гас преку цевки Терминали за течен природен гас
Транспорт	1. Патен сообраќај 2. Железнички сообраќај 3. Воздушен сообраќај 4. Сообраќај по копнени водени патишта 5. Океански и поморски сообраќај и пристаништа	

Извор: *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр. 31.

3.11. Пристапот на Хрватска спрема критичната инфраструктура

Во однос на законската регулатива за заштита на критичната инфраструктура Република Хрватска е во напредна фаза за разлика од другите држави од поранешна Југославија што ја има регулирано заштитата на критичната инфраструктура, односно управувањето и заштитата на критичната инфраструктура е регулирано со Законот за критични инфраструктури во 2013 година,[280]

[280] Zakon o kritičnim infrastrukturama, (Narodne novine 56/2013).

што се заснова на Директивата 114 од 2008 година на ЕУ. Покрај донесувањето на соодветниот закон, Република Хрватска има донесено и уште два подзаконски акта, и тоа: Одлука за одредување на секторите од кои средишните тела на државната управа ги идентификуваат националните критични инфраструктури,[281] како и Листата на редоследот на секторите на критичната инфраструктура и Правилник за методологијата на изработка на анализа на ризикот во управувањето со критичните инфраструктури.[282]

Со Законот за критични инфраструктури Република Хрватска ги има уредено националните и европските критични инфраструктури, потоа секторите на националните критични инфраструктури, управувањето со критичните инфраструктури, изработката на анализата на ризик, безбедносниот план на сопствениците, безбедносниот координатор за критични инфраструктури, постапки со чуствителни и класифицирани податоци, како и надзорниот механизам над спроведување на законот.[283]

Во Законот за критични инфраструктури на Република Хрватска како сектори во националните критични инфраструктури се издвојуваат:

- енергетиката (производство, вклучувајќи ги и акумулациите и браните, пренос, складирање, транспорт на енергенсите, дистрибуцијата);
- комуникациската и информатичката технологија (електронските комуникации, преносот на податоци, информатичките состави, аудио и аудиовизуелните медиски услуги);
- транспортот (патнички, железнички, воздушен, поморски и внатрешна пловна инфраструктура);

[281] Odluku o određivanju sektora iz kojih središnja tijela državne uprave identificiraju nacionalne kritične infrastrukture te liste redoslijeda sektora kritičnih infrastruktura, *Narodne novine* 108/2013.

[282] Pravilnik o metodologiji za izradu analize rizika poslovanja kritičnih infrastruktura, *Narodne novine* 128/2013.

[283] Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

- здравството (здравствената заштита, производството, трговијата и надзорот над лековите);
- водата (регулација и заштита на снабдителните системи за вода и комуналните постројки);
- храната (производство и снабдување со храна и безбедноста на храната, залихите);
- финансиите (банкарство, берзи, инвестиции, осигурување);
- производство, складирање и превоз на опасни материи (хемиски, биолошки, радиолошки и нуклеарни материјали);
- јавните служби (обезбедување јавен ред и мир, заштита и спасување, итна медицинска помош);
- национални и културни вредности.[284]

Покрај овие сектори со Одлука на владата на Република Хрватска, можат да се одредат и критични инфраструктури од други области. Исто така, со овој закон Владата на Хрватска со посебна одлука одредува кои сектори на органите на централната власт се идентификуваат како критична инфраструктура, со цел да се обезбеди сеопфатна акција за заштита и намалување на негативните ефекти и го одредува редоследот на листата на секторите на критичната инфраструктура.

Државната управа надлежна за вршење на операции за заштита и спасување, годишно поднесува извештај до Владата на Република Хрватска и до Комитетот во Собранието одговорни за националната безбедност во врска со критичната инфраструктура по сектори, нивната критичност и спроведување на мерки за заштита на критичната инфраструктура.

Сопствениците, односно, менаџерите на критичната инфраструктура се директно одговорни за управување и заштита на критичната инфраструктура во сите услови.

Анализата на ризикот за идентификација на критичната инфраструктура на Република Хрватска се базира на утврдување на севкупните причинители по следниот редослед:

[284] Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

– човечки губитоци (се проценува бројот на можните човечки загуби или повреди при престанок на работа на определена критична инфраструктура);
– стопански губитоци (проценатa се врши врз основа на важноста на стопанските губитоци и/или можните влијанија на околината);
– влијанието врз јавноста (оваа процена се однесува на довербата на јавноста, загриженост и нарушување на секојдневното функционирање на животот, вклучувајќи и загуба на основните јавни услуги).[285]

За потребите на наведените елементи, хрватската држава има определено државни тела кои во соработка со регулаторните агенции и стручните здруженија за секој сектор изработуваат анализа на ризици и секторски планови за обезбедување на критичната инфраструктура врз основа на проценатa на секторската загрозеност. Со законот се задолжуваат сопствениците, односно стопанствениците на критичната инфраструктура да направат анализа на ризикот како и план за обезбедување.

Планот за обезбедување ги опфаќа мерките на заштита и обезбедување и продолжување со работа на критичната инфраструктура и испорака на услуги и роба. Планот за обезбедување на критичната инфраструктура треба да опфаќа најмалку:

– идентификација на важните делови и објекти на мрежата;
– анализа на ризикот втемелена на сценарија на големи закани, ранливоста на секој објект, состав, мрежа и функционалноста, можните последици во редовна работа и во случај на престанок со работа, вклучувајќи и ризик од напуштање на локацијата;
– идентификација, одбирање и одредување на сите потребни мерки и постапки за смалување на ранливоста и обезбедување на дејствување на сите утврдени критични делови или објекти, мрежи или состави со примена на:

[285] Закон о критичним инфраструктурама NN56 13 член 9http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

постојани сигурносни мерки и постапки (технички, организациски, комуникациски мерки и мерките и постапките за навремено предупредување и зголемување на свеста), како и степенување на безбедносните мерки што се активираат во зависност од јачината на заканата.

– преиспитување на безбедносните планови (временска рамка).[286]

[286] Закон о критичним инфраструктурама NN56 13 член 13 http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, посетена на 14/11/2016.

V глава

ЗАШТИТАТА НА КРИТИЧНА ИНФРАСТРУКТУРА ВО РЕПУБЛИКА МАКЕДОНИЈА – РЕЗУЛТАТИ ОД СПРОВЕДЕНОТО ИСТРАЖУВАЊЕ

1. ПРИСТАПОТ НА РЕПУБЛИКА МАКЕДОНИЈА КОН ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Темата на критичната инфраструктура станува неодминливо прашање, особено во последните години и во Република Македонија.

Критичната инфраструктура во Република Македонија е релативно нова област којашто сè уште е законски нерегулирана, односно сè уште не постои правна рамка за дефинирање, идентификација и заштита на критичната инфраструктура, а со тоа нема формална утврдена листа на критична инфраструктура. Сепак, треба да се нагласи дека идентификацијата на критичната инфраструктура нема да започне од почеток, затоа што е реално да се очекува таа да се заснова на некои постојни акти што ја препознаваат оваа област. Особено треба да се обрне внимание на Законот за приватно обезбедување, односно во регулативата на Република Македонија за приватно обезбедување, особено проблематиката на задолжително обезбедување кај правни лица е третирана уште со првиот Закон за обезбедување на лица и имот (Сл.весник на РМ“ бр 80/99, 66/07 и 51/11) каде во посебна глава IV во член 25 е пропишано „Владата на Република Македонија определува кои правни лица се должни да имаат обезбедување на лица и имот за свои потреби, ако вршењето на нивната дејност е поврзано со ракување: со радиоактивни материи или други опасни материи за луѓето и околината; со предмети и објекти од особено културно и историско значење како и во други случаи кога тоа е во интерес на безбедноста, односно одбраната на Република Македонија.“ Новиот Закон за приватно обезбедување во својата содржина ги следи суштинските определби на Законот за обезбедување лица и имот и издвојува посебна глава V, за уредување на темата „Задолжително приватно обезбедување“, која во Член 44, став 1 и натаму ја делегира обврската за определување на правните лица на Владата на Република Македонија и ги набројува веќе утврдените

дејности со претходното решение. Значајна интервенција Законот за приватно обезбедување врши со определувањето дека приватното обезбедување може да биде организирано или за сопствени потреби или може да се склучи договор за услуги.[287] Во однос на пропишаното значајни се две карактеристики. Прво, и одредбите на Законот за приватно обезбедување укажуваат на тоа дека има одреден континуитет во насока на препознавање на критичните сектори и вториот значаен елемент на севкупното третирање на оваа значајна проблематика е дека во периодот од 10 години од донесување на Законот не постоеше акт што ги пропиша конкретните правни лица. Во таа смисла, Владата на РМ донесе Одлука за определување правни лица што се должни да имаат обезбедување на лица и имот за свои потреби („Сл.весник на РМ“ бр. 166/10) врз основа на Законот дури во декември 2010 година.[288]

Одлуката на Владата на Република Македонија за определување правни лица кои се должни да имаат приватно обезбедување дефинира три групи правни лица. Двете групи правни лица се формулирани според дејноста на правните лица, па во таа смисла првата група правни лица врши „дејност која е поврзана со ракување со радиоактивни материи или други по луѓето и околината опасни материи“, а втората група правни лица врши „дејност која е поврзана со ракување со предмети и објекти од особено културно-историско значење“. Дополнително, Одлуката пропишува трета група правни лица што се должни да имаат приватно обезбедување врз основа на посебен критериум т.е. истите се од интерес за безбедноста и одбраната на Република Македонија.[289]

Покрај Законот за приватно обезбедување („Сл.весник на РМ“ бр. 166/2012, 164/2013, 148/2015, 193/2015, 55/2016) во некои законски решенија се препознаваат одредени елементи со кои се идентификува критичната инфраструктура. Така, Законот за одбрана, особено Глава 6 која ги дефинира субјектите од посебно

[287] Исто., стр. 44.

[288] *Правна рамка за обезбедување на критичната инфраструктура*, Комора на Република Македонија за приватно обезбедување, Скопје, 2016, стр. 43.

[289] Исто., стр. 44-45.

значење за одбраната, за какви што се сметаат јавните претпријатија и трговските друштва од областа на енергетиката, сообраќајот, врските, комуналните дејности и градежништвото итн.[290] Концептот на критична инфраструктура се препознава и во други законски акти и стратегиски документи. Ќе наведеме неколку од нив. Така, во Националната стратегија за развој на информатичкото општество што е донесена во 2005 година стои дека постојната инфраструктура во Република Македонија главно ја сочинуваат фиксните јавни телекомуникациски мрежи и јавните мобилни телекомуникациски мрежи, додека во Законот за национална инфраструктура на просторни податоци е наведено дека националната инфраструктура на просторни податоци значи полесен пристап, размена, употреба и дистрибуција на стандардизирани просторни податоци со цел да се исполнат потребите на приватниот и на јавниот сектор. Исто така, Законот за железници ја препознава оваа терминологија низ призмата на железничкиот сообраќај или како што е потенцирано во самиот закон управувањето, изградбата, реконструкцијата, заштитата на железничката инфраструктура итн., како дејности од јавен интерес ги врши јавно претпријатије за железничка инфраструктура или друго правно лице под услови утврдени со законот за железници.

Предусловите за квалитетен напредок и кохерентноста на сите сегменти на заштита на критичната инфраструктура треба во наредниот период да се засноваат на сегментарно парцијални решенија како што беше илустрирано во претходните примери, туку треба да се засноваат на специфични знаења и треба да се инвестираат значителни средства со цел превентивните механизми заеднички да дејствуваат во една стратегиска рамка за критична инфраструктура.

Со имплементација на законодавството на ЕУ во областа на заштита на критичната инфраструктура, усогласување на македонскиот правен систем со законодавството на ЕУ и со евентуално донесување на посебен Закон за заштита на критична инфраструктура и соодветни подзаконски акти ќе се овозможи да се создаде формална рамка за заштита на националната критична инфраструктура што за да обезбеди соодветна персонализирана сеопфатна заштита

[290] Закон за одбрана, „Службен весник на РМ“, бр. 185 од 30.12.2011 година (член 90-96).

потребно е претходно да се направи анализа на потенцијалните закани. Еден од главните предизвици во полето на безбедноста во Македонија денес е идентификација на сите безбедносни ризици и закани со кои може да се соочи државата, како и нивното влијание врз критичната национална инфраструктура.

Затоа при примена на заштитни активности за заштита на критичната инфраструктура од новите безбедносни закани, вклучувајќи го и меѓународниот тероризам, адекватна и ефективна заштита може да се постигне со изградба на систематски и целосен/ сеопфатен концепт на заштита на критичната инфраструктура, со силна превентивна компонента, но, исто така, и ефикасна /репресивна/ компонента за навремен и соодветен безбедносен одговор на актуелните закани. Компонентата за адекватен одговор е можна единствено во синергија на јавниот и приватниот сектор но, исто така, и со вклучување и развој на граѓанското општество за да се одговори на сите нови видови потенцијални безбедносни закани на адекватен начин.

2. КОНЦЕПТУАЛНА РАМКА И ОПФАТ НА ИСТРАЖУВАЊЕТО

Критичната инфраструктура е концепт што е широко прифатен во голем број земји кои се согласуваат дека овој концепт ја истакнува потребата од заеднички ангажман во неговата заштита и отпорност. Оттука, заштитата на критичната инфраструктура е примарна грижа на секое модерно општество.[291] Пред дваесет години терминот инфраструктура првенствено беше дефиниран во однос на адекватноста на функционирањето на јавниот сектор во дадено општество, но веќе во средината на 90-те години на минатиот век, зголемената закана од меѓународен тероризам ги наведе политичарите да го редефинираат поимот инфраструктура во контекст на безбедноста на национално ниво. Следуваа владини политики и закони, нови и редефинирани, а нивното толкување се базираше на проширениот број инфраструк-

[291] Moteff, J., Parfomak, P., *Critical Infrastructure and Key Assets: Definition and Identification*, 2004, https://www.fas.org/sgp/crs/RL32631.pdf

турни сектори и видовите добра и услуги што се сметаат за критични за целите на економската безбедност. [292]

Значи заштитата на критичната инфраструктура е релативно нов концепт, што ги заменува поранешните помалку сеопфатни програми како заштита на виталните објекти или објекти од посебно значење за државата што подразбира адаптација и градење соодветни механизми што ќе ја осигурат безбедноста и отпорноста на системите на критична инфраструктура.

Во овој контекст, во Република Македонија меѓу многуте други процеси, треба да се развива и еден специфичен процес што треба да се поврзе со критичната инфраструктура. Со тоа се очекува прашањата врзани со заштитата на критичната инфраструктура да станат клучен предизвик за бројни институции и воопшто за нашата држава. Тоа ќе значи дека заштитата на критичната инфраструктура ќе треба да се базира на широка платформа за реализација и за конкретизација на Директивата на ЕУ за заштита на критичната инфраструктура, но и преземање на одредени чекори и одредени задачи за подобрување на внатрешната структура на безбедносниот сектор. Тоа ќе значи фокусирање на новата реалност со соодветна трансформација за да се нагласат реалните способности за спроведување на сите предвидените мерки за заштита на критичната инфраструктура. Исто така, овој процес треба да биде фокусиран и насочен кон заедничко поврзување на задачите, односно синхронизирање на активностите на клучните субјекти што ќе бидат задолжени за заштита на критичната инфраструктура за да можат да функционираат како една заедничка хармонична целина во остварување на потребната заштита.

За да се согледа како се перципира концептот на заштита на критичната инфраструктура беше спроведено истражување, што имаше за цел да ги анализира безбедносните капацитети на компаниите што во основа се и дел на критичната инфраструктура. Истражувањето беше спроведено низ два елемента: прво, се направи согледување на критичната инфраструктура од аспект на нејзиното значење врз националната безбедност и второ, анализа-

[292] Република Македонија, Центар за управување со кризи, бр. 2 (2008). http://www.macefdrr.gov.mk/files/dokumenti/pzrdo/Godisnik2008.pdf

та е направена за да се согледа какви чекори се прават или треба да се направат за да се обезбеди нејзина соодветна заштита.

Во однос на сложеноста на истражувачкиот проблем, акцент беше ставен на детаљната процена на факторите што доведуваат до неефикасност на самото планирање на безбедноста, мерките за обезбедување, условите, како и имплементацијата на напредните системи и процедури, особено како и согледување, изнаоѓање и дефинирање на можностите и условите за применливоста на напредните процедури и системи во развојот на обезбедувањето.

За целосна имплементација на меѓународните стандарди и процедури во обезбедувањето, потребни се трансформации на безбедносните капацитети во делот на обезбедување на критичните инфраструктури. Ваквата комплексност на проблемот на истражување ја прави заштитата на критичната инфраструктура многу сложена во изучувањето. Во тој контекст, истражувањата за состојбите во делот на заштитата на критичната инфраструктура подразбираат дефиниран интерес и подготвеност да се согледаат сите аспекти (структурни, суштински па дури и прагматични), но и секако низ призмата на одредени решенија со кои се поедноставува работата во обезбедувањето на потребната заштита.

Во реализација на истражувањето што беше направено за потребите на оваа студија застанавме на нивото на научно емпириска елаборација на проблемот што е предмет на истражување. Периодот што се врзува со немањето на законската рамка во делот на заштитата на критичната инфраструктура е една временска рамка што беше репер во нашите настојувања на проблемот да му пријдеме во неговиот тоталитет за на крајот да се понудат одредени решенија што ќе се базираат на истражувањето со што би се помогнало да се заокружи овој сегмент што е од исклучителна важност не само во теориска смисла, туку што е уште поважно за конституирањето на практиката во сферата на заштитата на критичната инфраструктура.

Во основа, целта на ова истражување беше да се согледа како релевантните фактори ги перципираат и ги толкуваат прашањата коишто се поврзани со критичната инфраструктура, односно да се утврди каква е состојбата во овој сегмент; да се согледа како ги третираат прашањата поврзани со обезбедувањето на критичните инфраструктури во Република Македонија, потоа да се утврди каква е состојбата со обезбедувањето на критичните инфраструктури, да

се согледаат приоритетите во обезбедувањето, да се согледа основната перцепција за значењето на критичните објекти, да се утврди во какви услови функционираат безбедносните капацитети, да се утврди меѓузависноста и соработката со институциите задолжени за осигурување на потребната заштита итн. Основна цел на ова истражување беше да се соберат објективни, односно целосни, проверливи, системски и попрецизни искуствени податоци за појавата што ја истражувавме. Оттука собирањето на искуствените податоци беше насочено од самиот карактер на истражувачкиот проблем и сето тоа подлегнува на стандардизирана планска процедура.

Во истражувањето како техника за прибирање податоци беше користено интервју (нестандардизирано интервју). Нестандардизираното интервју имаше ограничена примена, што се однесува на статистичкиот примерок што беше интервјуиран. Во однос на изборот на примерокот во нашиот случај беше користен *примерокот на процена* како најтипичен за квалитативните истражувања. Овој примерок е условен од проценатa какви испитаници ќе бидат соодветни за истражувањето. Примерокот што беше опфатен со интервјуто беше намерен заради добивање податоци од конкретните носители на функции, особено од оние што директно или индиректно се ангажирани во фирмите и во компаниите и се грижат за безбедноста во компанијата. Вкупно, беа изведени 28 интервјуа. Теренската работа се одвиваше во временски период во 2015 и во 2016 година во голем број компании што се од витален интерес за Република Македонија од енергетскиот сектор, од собраќајниот и од транспортниот сектор, од секторот води и од стручната и експертската заедница. Најголем дел од прашањата беа идентични за сите компании, а разговорите се водеа слободно и се обработија квалитативно, односно оние прашања што имаа само општа индикативна вредност. За средување на податоците од интервјуто и на отворените прашања беше користена анализа на содржината (семантичка и фреквентна). Анализата во основа ја зачува автентичноста на податоците бидејќи беше системска и целовита, а исто така анализата на одговорите поради карактерот на доверливост беа анализирани внимателно, со цел да се запази дискретност и препознавање на слабостите што ги следат критичните инфраструктури во Република Македонија.

За успешно и објективно спроведување на интервјуто претходеше подготвителна фаза што опфати прелиминарни разговори.

Потоа се пристапи кон истражувањето. Откако беа добиени податоците од интервјуто се пристапи кон анализа и кон обработка на податоците. Преку анализата на исказите, што ќе биде ограничена на дескриптивно ниво и инференцијална статистичка обработка со експликација, по одредените прашања беше направена и нивна селекција и категоризација на податоците врз основа на издвојување на поуспешните, на специфичните и на репрезентативните податоци, а нецелосните и нејасните беа отфрлени. Значи врз основа на теренската опсервација на компаниите се пристапи кон обработка на податоците селектирани врз основа на нивната јасност, концизност и прецизност.

Во следната фаза на анализата следеше определување на тематската рамка за работа и преку процесот на апстракција и конкретизација се дојде до концептуализација, односно избор на неколку клучни теми околу кои се групирани податоците.

Откако беше поставена иницијалната рамка започна повторното препрочитување на податоците на секој транскрипт одделно и определување на темата во која ќе биде сместен. Сортирајќи ги исказите на испитаниците, компарирајќи ги сличностите и разликите меѓу нив, настојувавме да откриеме некои нови внатрешни димензии. За полесно групирање на исказите, испитаниците ги поделивме во четири категории, односно со истражувањето беа опфатени следните категории на испитаници, и тоа:

1. испитаници претставници на енергетскиот сектор;
2. испитаници претставници од собраќајниот и транспортниот сектор;
3. испитаници претставници од секторот води;
4. испитаници претставници од експертската заедница.

Што се однесува до постигнување на дефинираните цели и очекуваните резултати, тие делумно се остварени. Периодот додека се спроведуваше истражувањето (политичката состојба) предизвика непосредни импликации врз расположливоста на испитаниците и врз нивниот интерес да му се стават на располагање на истражувањето во пресрет на проектираните барања.

Мора да се истакне дека истражувањето покажа и одредени слабости. Кај некои од испитаниците се покажаа слабости поради ограничените познавања. Еден дел од испитаниците не покажаа подготвеност за соработка, додека кај дел од испитаниците

комуникацијата се одвиваше тешко. Исто така, евидентно беше дека дел од испитаниците се однесуваат порезервирано во изнесувањето ставови по одредени прашања, особено тие кои моментално се наоѓаат на раководни места.

3. ИНТЕРПРЕТАЦИЈА НА РЕЗУЛТАТИТЕ

Во излагањето што ќе следува ќе бидат изнесени општите констатации за ставовите на испитаниците во однос на потребата од регулирање на сферата на заштита на критичната инфраструктура, односно нормативната рамка; координацијата и соработката помеѓу релевантните субјекти; ризиците и заканите со кои се соочуваат компаниите; безбедносните процедури што се применуваат при заштита на критичната инфраструктура; планирањето како процесна функција и значењето на плановите како елемент или производ на процесот на планирање; системот на образование и обука неопходна за заштита на самата инфраструктура или како придонесува стручната подготовка во насока на правилно вршење на задачите во делот на заштитата итн.

3.1. Регулирање на критичната инфраструктура

Регулирањето на критичната инфраструктура во национални рамки е повеќе од потребна, а истовремено тоа е тешка и одговорна работа и задача, но сепак, нејзиното целосно ефектуирање пред сè зависи од антиципативниот пристап на инволвираните субјекти. Прописот може да се толкува како обичен формален документ што треба да обезбеди адекватна заштита на критичната инфраструктура и да овозможи универзална примена на законот. Во принцип, ние тврдиме дека поголема регулатива може да доведе до зголемена одговорност.[293]

[293] O'Connor Lippert, Greenfield & Boyle, 'After the "Quiet Revolution": The Self-Regulation of Ontario Contract Security Agencies', *Policing & Society*, Vol. 14, No. 2, June 2004, p. 153.

Критичната инфраструктура во Република Македонија како реалативно нова област сè уште не е законски регулирана. Оваа состојба во голема мера оневозможува да постои реална основа за дефинирање, идентификација и заштита на критичната инфраструктура. Значи критичната инфраструктура треба да биде предмет на законска регулатива со што ќе се создадат сите предуслови за формално утврдување на листата на критична инфраструктура, но правната рамка ќе значи и одредување на начинот на работа, условите за работа, начинот на заштита, санкционирање на можните злоупотреби на работата, начинот на соработка на клучните субјекти, безбедносните процедури и мерки итн.

Со цел да се согледа како размислуваат испитаниците во однос на нормативното уредување на критичната инфраструктура им беше поставено прашањето: „Дали има потреба за донесување соодветна правна рамка за заштита на критичната инфраструктура?“.

Податоците од нашето истражување покажаа дека најголем дел од испитаниците се согласија дека донесување соодветен закон е повеќе од потребно затоа што тој ќе претставува солидна основа за давање адекватен одговор на заштита. Во квалитативните одговори има атрибути што се слични според својата природа, сепак не ги вкрстуваме во квалитативни категории за да се согледаат сите варијации на одговорите на испитаниците. Квалитативните одговори што имаат атрибути слични според својата природа, а најчестите одговори беа во контекст:

- за да се обезбеди потребната функционалност на секторите што ќе бидат определени во индикативната листа на сектори;
- за да се обезбеди одреден степен на соработка и координација на клучните субјекти што ќе бидат инволвирани во заштитата;
- да се прецизира целосно овој сегмент за да не постои некохерентност во однос на парцијалниот приод даден со други законски решенија и особено да нема терминолошки дивергенции околу поимите објекти од посебно значење, објекти од посебен интерес, витални објекти и објекти на критичната инфраструктура;
- за да се подобри обезбедувањето на критичните инфраструктури во целост;

- за да се направи прецизна нормативо-правна рамка на обезбедувањето;
- да се зголемат надлежностите на обезбедувањето;
- да се подигне свеста кај целокупниот безбедносен и небезбедносен персонал.

Сепак, ако се направи попродлабочена анализа и конкретизација на одговорите, тие ќе нè упатат на фактот дека испитаниците претставници на енергетскиот сектор и на секторот води се согласуваат дека правната рамка ќе обезбеди системски пристап од сите инволвирани субјекти и ќе доведе до институционален одговор од државата, додека испитаниците претставници на сообраќајот и транспортниот сектор сметаат дека евентуалниот закон ќе придонесе да се зголеми мобилноста, ефикасноста и брзината на реакција при евентуални закани и ризици со кои би се соочила критичната инфраструктура, а испитаниците претставници на експертската заедница се на мислење дека со донесувањето на потребниот закон ќе се зајакне заштитната компонента и моќта на државата, но истакнаа дека мора да се води сметка при изработката на законот да се земат предвид компаративно најдобрите светски пракси од областа на заштита на критичната инфраструктура.

Во рамките на поставеното прашање беше поставено и потпрашање што требаше да даде одговор на правната поставеност на заштитната компонента на компаниите. Во делот на правната поставеност, главно сите компании обезбедувањето го темелат во согласност со правилници за работа на службата за обезбедување донесени од страна на управувачкиот одбор на компаниите, врз чијашто основа се изработени планови за обезбедување како и процедури за работа. Во сите акти, како што посочија речиси сите испитаници припадници на енегретскиот, на сообраќајот и транспортниот сектор и на секторот вода запазен е Законот за приватно обезбедување со кој се уредуваат условите за вршење приватно обезбедување. Покрај целосната примена на Законот, голем број компании имаат изработено и интерни планови, правилници, процедури за обезбедување во кои генерално е опишана заштитата на објектите, критичните места за обезбедување, обрските и правата на персоналот за обезбедување, техничките средства и опреми и др., заради давање насоки за имплементација на мерките

за обезбедување, како што е барано во согласност со домашните прописи, со исклучок на аеродромското обезбедување, каде што во целост се применуваат и меѓународните стандарди и препорачани практики, земајќи ја предвид безбедноста, уредноста и ефикасноста на летовите. Во воздухопловството, покрај законските прописи како што се: законот за воздухопловство и прописите донесени врз овој закон и другите законски и подзаконски прописи, со кои се регулираат правата и надлежностите на сите субјекти што се инволвирани во одвивањето на обезбедувањето на цивилното воздухопловство од дејства на незаконско постапување, дефинирана е и „Национална програма за обезбедување на цивилното воздухопловство" донесена од страна на Владата на Република Македонија. Со оваа програма се утврдени насоките за имлементација на стандардите и препорачаните практики како од меѓународен, така и од домашен карактер и воедно претставува збир на правила, постапки, активности и процедури што се применуваат за заштита на цивилниот воздушен сообраќај од акти на незаконско дејство, а сè со цел да се обезбедат неопходните безбедносни услови за непречено одвивање на воздушниот сообраќај, да се овозможи заштита на патниците, вработените, посетителите, воздухопловите, аеродромските објекти, радионавигационата опрема, објектите, уредите и инсталациите значајни за воздушниот сообраќај, минимизирање, отстранување и справување со уловите во зголемен ризик и закана, намалување на последиците предизвикани од вонредни состојби и др. Во програмата опишани се сите надлежни органи и институции во функција на обезбедувањето на цивилното воздухопловство од акти на незаконско постапување со нивните права, надлежности и одговорности. Додека пак, секој оператор на аеродром изготвува аеродромска програма за обезбедување, што е дефинирана во согласност со меѓународните и со домашните прописи.

Во овој контекст, најголем дел од испитаниците (95% од вкупниот број од сите категории) наведоа дека важна компонента во обезбедувањето на критичните инфраструктури претставува потребата од попрецизно регулирање на критичните инфраструктури по примерот на воздухопловната безбедност. Имено, потребно е доизградување на регулативите врз основа на референтниот објект. Во таа насока, процесот на дорегулирање на објектите од витален интерес е сложен процес, што подразбира најнапред

донесување документи неопходни за дефинирање на обезбедување критични инфраструктури, процес на спроведување, односно, имплементирање на спецификите и карактеристиките на дефинираната критична инфраструктура и на крај реализација на актите во пракса. Целата таа активност е потребно да биде поддржана од регулаторните тела и треба внимателно да биде планирана и адаптирана кон постојните законски и подзаконски акти. Овие акти бараат јасно разбирање на барањата што ги носи обезбедувањето на критичните инфраструктури, способност за детекција на заканите, ризиците и опасностите што ги следи секоја критична инфраструктура и изработка на адекватни планови и процедури во функција на севкупните безбедносни процени. Улогата на националните институции во насока на подобрување на обезбедувањето потребно е да се издигне на едно повисоко ниво по примерот со обезбедувањето на цивилното воздухопловство преку Агенцијата за цивилно воздухопловство како надлежен орган за координација и следење на заедничките основни стандарди утврдени со Законот за воздухопловство, преку изготвување правни документи за регулација на дејноста и претставува на некој начин национален координатор во делот на обезбедување на воздухопловството, воедно, претставува и тело што е одговорно за имплементирање на домашните и на меѓународните стандарди и давање насоки за нивно постапување.

Генерално, податоците од резултатите на испитаниците покажаа дека со цел да се разгледа подетално состојбата во Република Македонија и какво решение да се понуди потребно е да се формира тело или работна група составена од сите релевантни субјекти вклучувајќи ја и Комората на Република Македонија за приватно обезбедување за да се придонесе во регулирање на областа, која и тоа како, влијае на целокупната безбедност на Република Македонија.

Општиот заклучок од овој пакет на прашања и добиените одговори е дека, обезбедувањето во современите општества подлежи на постојани промени, како во насока на техничко технолошко осовременување, како во делот на најсовремените достигнувања од технички аспект, така и во организациска и процедурална надградба на прописите и упатствата со која се дефинира областа. Исто така, анализата на прашањата супституционално потврди

дека приватната безбедност е тесно поврзана со заштитата на критичната инфраструктура, бидејќи многу од овие инфраструктурни објекти се под заштита на приватниот безбедносен сектор. Успешното функционирање на приватниот безбедносен сектор во областа на заштитата на критичната инфратруктура во нашата држава е оневозможена поради недостаток на правна рамка. Анализата посочува дека е направен еден сублимат на синтеза на одговори за тоа како критичната инфраструктура треба да биде прифатена. Во таа насока, очекувањата се дека ќе следи имплементација на добиените сознанија во нашето позитивно право и секако изработка на соодветна законска рамка што ќе овозможи правното регулирање и примена на најдобрата пракса од областа на заштита на критичната инфраструктура кај нас.

3.2. Потреба од координација и соработка во заштита на критичната инфраструктура

Координацијата произлегува од потребата за соработка меѓу релевантните субјекти и таа е задолжена да ги поврзе одделните елементи што имаат префикс на заштитна компонента. Оттука проучувањето на внатрешниот механизам на приватниот безбедносен сектор првенствено треба да се заснова на негово целосно разбирање и разграничување за да се избегне каква било импровизација и парцијализам, особено ако знаеме дека високиот степен на соработка е од голема корист за работата на секторите којашто не е едноставна и којашто е непредвидлива.

Денес се смета дека одредена состојба може да се проблематизира поради лошите процени на состојбата, вклучувајќи ја и самата координација, но и од недостаток на навремени информации што укажуваат на постоење опасност, како и од неподготвеноста субјектите да се справат со безбедносните предизвици. Следствено на тоа, практичен момент за подготовките за справување со потенцијалната опасност е носење одлука на вистински начин и во вистинско време, како и постоење на потребната координација на релевантните субјекти, која не секогаш е навремена. Тоа значи дека не е сеедно кога ќе биде донесена одлуката, затоа што избрзана или задоцнета одлука може да биде опасна и пресудна во заштита на критичната инфраструктура. Оттука не е сеедно како се гледа

на конкретните закани по критичната инфраструктура и како и на кој начин се реагира на нив.

За да може да се понуди кохерентно објаснување што ќе биде приспособено за изучување на сложените структурни, институционални, социјални и други проблеми што го оптоваруваат работењето на критичните инфраструктурни објекти, нашето стојалиште е дека најдобрата основа за анализа е да се согледа каква е координацијата и соработката на релевантните субјекти во обезбедување на потребното ниво на заштита на овие сектори. Оттука во истражувањето особено не интересираа ставовите во однос на прашањето „Дали има потреба од координација и соработка на клучните субјекти во заштита на критичната инфраструктура"? Од вкупно анкетирани 28 лица, најголемиот дел од испитаниците 25 се изјасниле дека координацијата и соработката имаат големо значење за ефикасна заштита на критичната инфраструктура. Кординацијата, како во внатрешноста на инфраструктурите, така и со надворешните субјекти претставува значајна варијабла во безбедносниот систем на компаниите. Координираноста во поглед на обезбедување на критичните инфраструктури најнапред е потребна на национално ниво, па таа координираност да биде применета и на компаниско ниво.

Според исказите на испитаниците претставници на сообраќајниот и транспортниот сектор е наведено дека во областа на аеродромите, обезбедувањето претставува засебна целина која ги третира исклучиво актите на незаконско постапување – security аспектот, додека безбедноста, односно safety е предмет на посебен дел во рамките на компанијата. Со цел обезбедување поголема координација на активностите на сите субјекти во обезбедувањето што се инволвирани во одвивањето на воздушниот сообраќај беше посочено од оваа категорија испитаници дека е формирано тело – Национален комитет за обезбедување на цивилното воздухопловство со свој постојан состав дефиниран со Законот за воздухопловство. Во основа, овој комитет претставува советодавно и координативно тело, чија основна задача претставува усогласување на планирањето, спроведувањето и развојот на севкупните мерки и активности на сите инволвирани субјекти – чинители на безбедноста на цивилното воздухопловство. Покрај Национален комитет, формиран е и Аеродромски комитет за обезбедување во функција на спроведување на програмите за обезбедување на аеродромите.

Во однос на претходно наведеното прашање од исказот на најголем број испитаници претставници на енергетскиот сектор следи заклучокот дека започнатата форма на соработка и координација треба да се надогради и практично да се имплементира за да нема одредени отстапувања. Всушност, соработката треба да биде израз на реалната потреба што е во интерес на секој сектор за да може да се обезбеди потребната заштита на објектите од неговиот сектор. За разлика од оваа категорија испитаници, поголем број од испитаниците претставници на експертската заедница сметаат дека координацијата и соработката ќе зависат од волјата на инволвираните страни за правење практични чекори за имплементирање на најдобрите решенија во оваа сфера. Значи координацијата ќе биде иста како и во безбедносниот сектор стара болка и проблематичен сегмент и дека и понатаму треба да се бараат потребните начини како да се подобри координацијата. Интересно е да се нагласи дека и претставиците на секторот вода имаат речиси идентични ставови како и другите испитаници, односно се согласуваат дека координацијата е сè уште отворено прашање и дека го има приматот на едно од најчувствителните.

Од изнесените податоци може да се заклучи дека не постои голема разлика за суштинската димензија на координацијата. Следи дека со зајакнување на врските, односите, правната регулатива итн. дека ќе се направи голем исчекор на полето на координацијата и соработката. Исто така, од исказите на поголемиот број испитаници, следи заклучокот дека соработката и координацијата треба да се издигнат на повисоко ниво со посебно вклучување на претставници од критичните инфраструктури во сите тела што ја третираат безбедноста на државата. Потребни се што повеќе експертски дебати, обуки, вежби со цел да се зголеми комуникацијата помеѓу клучните ресори, а сето тоа да биде поткрепено со правна рамка.

3.3. Ризици и закани по критичната инфраструктура

Перцепцијата на ризикот се смета како значаен фактор во процесот на определување на значењето на ризикот. Во оваа смисла, во теоријата се развиваат два правца што се обидуваат да дадат одговор на прашањата за ризикот, тоа се психометричниот модел и теоријата

на културата. Според првиот модел, ризикот претставува субјективно доживување на поединецот, кој е под влијание на мноштво психолошки, социјални и институционални фактори (Slovic). Но, основниот проблем што доминира во овој модел е како да се измери влијанието на овие фактори врз перцепцијата на поединецот. Додека преку „теоријата на културата", се настојува да се разбере влијанието на културата, навиките, обичаите, односно одредени норми и вредности што се препознатливи за некоја група или заедница и влијанието на сето тоа врз поединечните/групните перцепции за ризикот.[294] Кога станува збор за тоа дека перцепцијата на ризикот влијае на начинот на неговото определување и конципирање, треба да се спомене и т.н. „јавна перцепција" и „реална перцепција". Јавната перцепција е поврзана со разбирањето и доживувањето на ризикот од страна на јавноста (поединци, групи и сл.) и поблиску е до лаичкото разбирање на ризикот. Реалната перцепција за ризиците доаѓа од страна на експертската заедница, која своите ставови ги поставува врз научни и методолошко поставени истражувања. Ризиците за кои зборуваат експертите се т.н. реални ризици и нивното објаснување се поткрепува преку принципите на објективност, аналитичност и сеопфатност. Вториот пристап е релевантен за системите за управување со ризици, што во различна организациска и институционална форма се воспоставени и функционираат во јавниот и во приватниот сектор во Република Македонија.[295]

Со вклучувањето на сите овие елементи, ризикот се поставува на широка основа, со што се проширува неговото основно значење што произлегува од чисто техничката основа, а концептот на ризик се настојува да се разбере покомплексно. Основната претпоставка што произлегува од комплесниот концепт на ризикот упатува на тоа дека ниту една активност во општеството не е имуна на ризик, ниту пак дека ризикот може во целост да се елиминира. Ризикот може само да се намали (редуцира) на некое прифатливо ниво,

[294] Slović P., *The Perception of Risk*, Earthscan, London, 2000, во Корпорациски безбедносен систем, Комора на РМ за обезбедување на лица и имот, Скопје, 2012, стр. 23-176.

[295] Бакрески О., Триван Д., и Митевски С., *Корпорациски безбедносен систем*, Комора на РМ за обезбедување на лица и имот, Скопје, 2012.

кое е дефинирано во безбедносната скала на поединецот, групата, општеството, државата итн.[296]

Ако се земе предвид значењето на критичната инфраструктура евидентно е дека справувањето со потенцијалните закани треба да се заснова на проценатa на секоја реална и потенцијална закана, што може да предизвика повреда или смрт на лица или уништување (губење на имотот на компанијата и или намалување на профитот, односно финансиски загуби без разлика на неговата големина). Се однесува на постепена или на системска анализа на работата и постапки што произлегуваат од процесот на работа на компанијата со цел идентификација на ризик или закана на компанијата и изработка на проактивни препораки, решенија и процедури за нивна елиминацијаи/или ублажување на последиците, во случај на остварување на заканата во текот на работата на компанијата.[297]

Од анализата на резултатите добиена од 28 испитаници може да се заклучи дека постои голема поделеност во мислењата поврзани со фактот дека безбедносните ситуации што владеат во земјата и во регионот, но и пошироко може да имаат силен импакт во функционирањето на критичните инфраструктури, поради лошите безбедносни процени од страна на релевантните субјекти. Исто така, ако лошата процена се надополни со лоша координација на сите инволвирани субјекти ангажирани во извршувањето на безбедносни задачи, или пак недостаток од навремени и точни информации за постоење опасност надополнета со неподготвеноста на безбедносните капацитети да се справат со современите ризици што ја следат денешницата, потенцијалната опасност што ја демне државата ќе биде и мошне опасна не само за критичната инфраструктура, туку и за целата држава па и пошироко.

Од одговорите евидентно беше дека проценитe на ризици и закани што ги прават компаниите, во основа се однесуваат на обврските што произлегувааат од Законот за управување со кризи

[296] Исто., стр. 23-176.

[297] Бакрески, О. Триван, Д. Митевски, С., *Корпорациски безбедносен систем*, Комора на РМ за обезбедување на лица и имот, Скопје, 2012, стр. 67, во Даничиќ М, Сајиќ Љ, оп. цит.стр.47.

во кој се третита и областа на тероризмот и другите акти на незаконско постапување. Во воздухопловството, особено испитаниците од сообраќајот и транспортниот сектор сметаат дека проценатa на заканата и соодветно преземење мерки ја прави Агенцијата за цивилно воздухопловство, Министерството за внатрешни работи и другите надлежни субјекти кои се подразбира дека треба да бидат на висина на задачата. Понатаму посочија дека во доменот на проценатa на нивото на закана се организираат зачестени контроли и воведување дополнителни мерки на заштита.

Сепак, размислувањата на експертската заедница во поглед на природата на заканите, ризиците и опасностите што ги следат критичните инфраструктури во Република Македонија, може да се каже дека нужно е да се изградат и да се развиваат модерни служби за обезбедување што ќе одговораат адекватно на современите закани. Интересно е да се потенцира дека прашањето поврзано со евентуалните закани, безбедносен ризик, како и настани кои влијаат на безбедноста и нормалното функционирање на компанијата, добиени се одговори од најголем број од испитаниците претставници на енергетскиот сектор дека се соочиле со одредени видови загрозувања, од незаконско отуѓување на имот, саботажи во работењето поради материјална корист на поединци, анонимни закани за подметнувања експлозивни направи, нарушувања на јавен ред и мир од поголеми размери, шверцување стоки и предмети што може да ја загрозат безбедноста итн.

3.4. Безбедносни процедури што се применуваат во секторите на критичната инфраструктура

Во основа, се констатира дека сите опсервирани компании опфатени со истражувањето имаат поставено систем на обезбедување воден од домашните прописи, со исклучок на аеродромската безбедност што во целост ги има имплементирано меѓународните стандарди регулирани во согласност со регулативата на ICAO, ECAC и EU.

Начелно корпорациската безбедност опфаќа:

– административна безбедност (Administrative Security) – процедури и политика во областа на информатичката заштита;

- физичка и техничка безбедност (Outsource/Proprietary) – машини, постројки и објекти;
- безбедност на имотот и на надворешни партнерства (Personnel Security)
- лична безбедност (Protective security), заштита на лица и заштита при работа;
- заштита од пожари (Fire Security);
- работа во вонредни ситуации (Contingency Planning);
- информатичка безбедност (Information Security);
- безбедност на менаџерот (Executive Security);
- безбедност на различни деловни случувања (Event Security);
- безбедност на договорени работи со државни структури;
- истраги (Investigations) програма за заштита од криминалитет и
- програма за едукација и развој на безбедносната култура на вработените (Security Education Awareness and Training Program).[298]

Од анализираните четири категории на испитаници интересни варијации во одговорите дадоа испитаниците на првата, на втората и на третата категорија опфатени со истражувањето кои укажаа дека делумно ги имаат воведено функциите на корпорациската безбедност, додека сетот прашања што беа поставени во поглед на физичката заштита се однесуваа на условите за планирање на безбедноста од самото почнување со градба на објектите или измени на постојните објекти, како и во поглед на дефинирање на зоната на заштита како еден од основните превентивни мерки на заштита. Генерално сите компании се оградени со периметарска ограда со ограничен број на влезно-излезни капии и прецизна контрола на возила и лица со постојан надзор поддржан со електронски системи и уреди. Висините на оградите се дефинирани со актите на компаниите, а постои и дополнително оградување на местата што се дефинирани како критични.

[298] Kovachic L. Gerald, Halibozek P. Edward, *The Managers Handbook for corporate security*: Establishing and Managing a Successful Assets Protection Program, Butterworth – Heinemann, Boston MA 2002., стр. 61-162, во Корпорациски безбедносен систем, Скопје, 2012, стр.117.

Од аспект на определување на зоните на движење, истражувањето посочи дека констатирани се дефинирани критичните делови на сите компании, но не се поставени јасни опишани граници на зоните на движење, освен на аеродромите каде што прецизно е дефинирана секоја зона и контролата на пристап до нив според важноста, функционалната улога и техничко-технолошката поставеност на одредени објекти, површини, инсталации, уреди, средства и опрема во аеродромскиот комплекс. Во согласност со зонската поставеност на јавна, на ограничена, на безбедносно ограничена и на критичните делови на безбедносно ограничените зони, поставени се и фукционираат местата за обезбедување со јасно дефинирана контрола на движење, пристап и надгледување на лицата и возилата. Границата помеѓу јавната зона и ограничената зона потребно е да биде јасно дефинирана и видлива, а воедно спречува неовластен пристап. Секое преминување во безбедносните зони на компаниите треба да овозможи адекватна проверка на лицата и предметите што се внесуваат. Додека пак, при движењето кон критичните делови на безбедносно ограничените зони, треба да подлежи на дополнителни безбедносни контроли и опсервации како и исполнување на дефинираните безбедносни услови. Пристапот кон овие зони потребно е да осигура дека не постои неовластен пристап. Пристапот до ваквите зони може да се одобри само под посебно утврдени услови и поседување на овластување издадено од надлежниот орган за обезбедување на критичната инфраструктура. Истото важи и за возилата и за возачите.

Во делот на идентификационите картички сондирањето на мислењата покажа дека испитаниците од трите категории се согласуваат дека освен на аеродромите, во сите други компании не постојат унифицирани идентификациони картички на кои се означени дозволените зони на движење. Исто така, не постои дефинирана процедура за поделба на компанијата во дефинирани зони на движење, видот, изгледот и начин на употреба на идентификационите картички, поднесување барање за издавање, носење и враќање на идентификационите картички, евиденцијата како и надзорот за носење и поседување на идентификационите картички. Контролата на документите и на идентификационите картички потребно е да се спроведуваат на сите контролни пунктови при влез во ограничените зони на компанијата и тоа би можело да се реализира со по-

мош на електронски системи што го ограничува пристапот или пак од овластено лице што врши контрола на пристап. Во основа, сите компании издаваат пропусници и водат евиденции за движење на возилата, но не се прави детална проверка врз основа на процедура или упатство за оваа намена од аспект на противдиверзиона контрола. На аеродромите ова е прецизно регулирана постапка со посебни процедури за работа и специјална опрема за контрола на возилата. Сите возила што имаат пристап во безбедносните зони на аеродромот подлежат на проверки и спроведување на постапки, мерки и дејства што ги преземаат работниците за обезбедување во согласност со нивните надлежности.

Анализата потврди дека во делот на техничкото обезбедување пристапот до ограничените зони во сите компании се применува врз техничка опрема врз основа на моменталните потреби на компаниите. На аеродромите постои јасно дефинирана опрема што се користи и треба да биде поставена во определени простори и кои карактеристики е потребно да ги задоволува. Голем дел од компаниите имаат пропишано и применуваат процедури за постапување со забранети предмети, но не постојат адекватни опреми за нивно откривање следење и неутрализирање. Генерално, најголем број од компаниите се темелат на мониторинг системите што не се доволни за откривање на прикриени предмети.

При опсервација на движењето на персоналот и другите лица што своите должности ги извршуваат во безбедносно ограничените зони во компаниите што беа предмет на опсервација, минуваа низ премини што се контролирани, меѓутоа вработените не подлежат на дополнителни безбедносни контроли. На аеродромите оваа активност е регулирана со службени влезови и постојана контрола со помош на уреди и техники за против-диверзиона контрола (ПДЗ), а сè со цел остварување на стандардизиран, квалитетен и одржлив систем на мерки и техники на обезбедување што се применливи и мерливи по интензитет и квалитет. Дефинирани се локациите за преглед, надлежностите, постапките за спроведување на ефикасен и темелен преглед како и адекватно користење на опремата за таа намена. Безбедносниот преглед на лицата треба да им се изврши со едно од следните средства: рачен претрес, метал – детекторска врата, кучиња за откривање експлозиви, системи за откривање траги од експлозиви (ETD), скенери за обезбедување кај кои не

се употребува јонизирачка радијација и систем за откривање траги од експлозив во комбинација со рачни метал детектори. Како најчести методи за преглед на предметите кои се носат се: рачен претрес, рентгенска опрема, систем за откривање на експлозив (EDS), кучиња за откривање на експлозив, системи за откривање на траги на експлозив и сл.

Анализата на одговорите констатира слабости во примената на некои од применуваните техники и опреми во реализацијата на откривање на експлозиви и опасни материи. Исто така, најголемиот број испитаници од трите категории посочија дека контролните места за проверка на возилата со исклучок на аеродромите се сведува само во однос на евидентирање на влезот без соодветна примена на методи и техники за контрола на возилата како што е на пример рачен претрес, кучиња за откривање на експлозиви, опрема за откривање на траги од експлозиви и сл. Физичкото обезбедување кое е застапено во компаниите во основа се остварува со работење на определен број работници за обезбедување во согласност со законската регулатива, но контролите се реализираат главно во сите компании со цел откривање на сомнително однесување на лицата, откривање на неовластени упади во компаниите и оневозможување на преземање на дејства за нарушување на нормалното функционирање на компаниите. Зачестеноста во реализација на овие активности се извршуваат врз основа на проценетите опасности, засновани на методот на непредвидливост, секако поткрепено од мониторинг системите што се имплементирани во некои компании.

3.5. Професионализмот и професионалното работење

Во основа денес сме сведоци на ограничените дискусии за професионализацијата, односно дискусиите за ваквите прашања се сведуваат на минимум што секако дека е неоправдано. Одредени дискусии може да ги оцениме дека се во рамките на класичниот пристап што ги дава основните елементи за безбедносната ориентација што значи дека тие ја гледаат професионализацијата низ призмата на когнитивните сознанија кои пак, во основа имплицираат знаење за безбедноста, за безбедносниот сектор, за приватната безбедност итн.

Други размислувања се во насока на давање одредени размислувања и судови за сензитивноста во работата врзана со заштитата на критичната инфраструктура, додека пак трети особено место им даваат на интеракцијата и меѓузависноста на односите кои главно вклучуваат и комбинации на вредности, стандарди и критериуми. Сите размислувања не ја намалуваат научната вредност на овој концепт, но во основа мора да се направат и дополнителни напори за да се надомести инсуфициентноста во актуелната состојба.

Во рамките на нашите размислувања особено е важно прашањето за самиот пристап кон овој проблем кој имплицира сложен процес внатре во самата држава, како и прашањето за вкупната безбедносна култура, која има бројни димензии почнувајќи од заедничките интереси, заедничките вредности, политичко-безбедносните процеси, сложениот однос во безбедносната заедница, но и од околностите во кои човекот живее и работи. Единствената важна интерпретација на општествената природа на човекот е онаа која човекот го сврстува во општествената целост и како дел од таа целовитост тој ги остварува своите интерси, а исто така и живее во една уредена демократско-безбедносна средина во која има изградена хиерархиска структура и се бара апсолутна покорност од своите делови кои заедно го сочинуваат идиличното богатство на заемната помош на совршената власт. Значи, тука споменатите амбиваленции неминовно се одразуваат и на самите поединци кои се ангажираат за извршување на одредени заштитни активности со што се влијае на оформување на нивниот пристап и самата имплементација на стандардите во безбедносната пракса. Оттука, само општествено активен однос спрема оваа проблематика ќе придонесе кон афирмација и развој на основните постулати во кој професионализацијата ќе доведе до акумулација на безбедносно културниот капитал од индивидуата до самото општество.

Со цел да се види што значи професионализацијата и професионалното работење во заштитата на критичната инфраструктура беше поставено прашањето: *„Дали сметате дека поголема професионализација значи и посоодветна заштита на критичната инфраструктура?“*. На ова истражувачко прашање, голем дел од испитаниците, претставници на сите категории се изјасниле дека согледувањето на проблемот на професионализацијата единствено е можен само преку детално познавање на сложените, испреплетени

внатрешни односи, како и преку разгледување на клучните елементи што ја имаат централната улога во креирањето соодветен амбиент за работа почнувајќи од средината, достигнатото ниво на образование, нивото на свеста, повеќеструктурните форми на комуникација итн.

Ако ги синтетизираме одговорите ќе видиме дека испитаниците-претставници на академската заедница сметаат дека професионализацијата значи партиципативно учество и придонес, но и проактивен пристап за себе, заштита на другите, одговорност кон државата, одговорност кон фирмата, одговорност кон претпоставените, одговорност кон објектите што се штитат итн. Дел од експертите сметаат дека професионализмот не смее да се врзува за дискриминаторно, корумпирано или насилно искористување на својата моќ.

За разлика од испитаниците-претставници на академската заедница, поголем дел од испитаниците-претставници на енергетскиот сектор сметаат дека професионализмот се заснова на системски пристап и основи и сметаат дека повеќе е од потребен, затоа што тој е во функција да го обезбеди потребниот квалитет во работењето. Мал дел од испитаниците од оваа категорија се изјасниле дека треба да се зајакне професионализмот, односно да се надогради со имплементирање на нови практики и да се проучат странските искуства за да се имплементираат и во Република Македонија, според нашите можности и потреби.

Слични ставови имаат и претставниците на секторот води и транспортниот сектор со тоа што тие сметаат за да има висок степен на професионализам дека треба најнапред поставувањето минимум стандарди што се основа за развој и за професионализацијата на овој сектор.

Општиот впечаток во одговорите на испитаниците е дека професионализмот и професијата како категоријални црти може да се изградат со многу знаење и искуство и дека тоа може да се стекне во образовниот процес, во работењето, во однесувањето, во претставувањето, во комуницирањето, во непосредниот однос, во пристапот итн.

3.6. Образование, стручна подготовка и обука на персоналот

Образованието е клучен фактор и заедно со обуките и усовршувањата ќе придонесат за поголема професионализација и развој на заштитната дејност. Знаењето што се добива од образовниот процес е главна детерминанта во развојот затоа што се темели на совладување и на стекнување комплексен корпус од компетенции, способности и вештини. Тоа е вокација во која знаењето или праксата се користат за давање услуги на други. Оваа приврзаност значи изразеност, алтруизам и промоција на јавното добро во сопствениот домен на работа. Таа приврзаност ја обликува основата за општествениот договор помеѓу професиите и задачите, што за возврат осигурува професионална автономија во практиката и привилегија на саморегулација.

Во основа, професионалните компетенции и доаѓањето до нив е условено од практичното извршување на задачите, а тука до израз доаѓа стекнатото знаење. Ова значи прво, да се стремат агенциите за обезбедување, но и фирмите што имаат обезбедување за сопствени потреби за адекватно кадровско планирање и да се избираат најдобрите кандидати заради специфичноста на дејноста и професијата и второ, овој концепт треба да опфаќа стручни профили кои треба да подлежат на континуирано стручно усовршување, нивна соодветна подготовка за извршување на секојдневните задачи и работењето. Тоа знаење треба да се базира на високите стандарди за реализација и однесување.

Одговорите од најголемиот број испитаници од сите категории упатуваат дека Законот за приватно обезбедување предвидува можност за обука на персоналот и дека на ова прашање повеќе треба да посвети самата агенција и/или компанија што има сопствено обезбедување. Тоа значи дека по примерот на аеродромите како што наведуваат и испитаниците претставници на транспортниот сектор дека покрај обврските што произлегуваат од Законот за приватно обезбедување треба да постојат и дополнителни обуки на персоналот, во согласност со одобрените програми за обука и од позитивните практики каде што главен акцент се става: на селекција на персоналот, на минималните квалификации за одредени овластувања како и на обврските што произлегуваат од до-

машната и од меѓународната регулатива во поглед на квалитетот и спроведувањето на обуките. Персоналот чии должности вклучуваат: преглед со помош на технички средства или рачен претрес на лица, предмети и сл., преглед и проверка на зоните и објектите што се предмет на посебна контрола, контролата на пристап до ограничените зони на критичните инфраструктури, издавање на идентификациони картички и пропусни документи т.е. персоналот што е директно вклучен во примената на специјалните мерки за обезбедување, потребно е да помине низ специјализирана обука во однос на прашањата што ги третираат: одговорностите и селекција на персоналот за обезбедување, имплементација и спроведување програма за обука, критериуми за селекција на персонал задолжен за обезбедување на критична инфраструктура, барањата за обука, процедури за сертификација на операторите, определување на целите, времетраењето и периодичноста за одржување на обуките и сл.

Важен елемент на кој треба да се посвети потребното внимание како што посочија најголем број од испитаниците претставници на трите категории е делот на човечките ресурси. Тука важен елемент е селекцијата на персонал, што треба да биде сразмерен на специфичните потреби и задачи. Во голем број компании што беа предмет на истражување при процесот на селекција, потврдија дека не се спроведуваат безбедносни проверки на лицата, ниту пак, проверките се повторувани во одреден временски период според примерот на воздухопловната безбедност, каде што ваквите проверки се прават на секои две години. Безбедносните проверки треба да вклучат проверки на идентитетот на лицето кое се пријавува за работа во поглед на претходното однесување, вклучувајќи какво било криминално поведение како критериум за негова подобност.

Испитаниците од академската заедница целосно се согласуваат дека постои длабоко врска меѓу стручната подготовка на поединците со работната должност, односно вршењето на работните задачи. Но, за разлика од трите категории испитаници тие сметаа дека професионализмот и стручната подготовка како исклучително важни елементи наспроти професијата дека оваа врска е одамна прекината. Еден од испитаниците на академската заедница посочува дека проблемот постои уште од моментот на вработувањето. Според него неводењето сметка за стручноста и за компетентноста

на кадарот ја уништуваат професионалноста и директно влијае врз професионалноста во извршувањето на работните задачи од страна на поединците, бидејќи изборот на кандидатите треба да се прави исклучиво врз основа на квалитетот на образованието. Генералниот заклучок е нема дилеми дека стручната подготовка влијае врз правилно вршење на работните задачи и работењето.

3.7. Планови и процена на ризик

Вообичаено, програмите за процена за заштита на добрата и имотот и нивната реализација започнуваат со дефинирање на тоа што треба да биде заштитено. Затоа првата фаза од овој процес се вика идентификација на средствата или анализа на мисијата. На овој начин се добиваат повеќе податоци и се одредува вредноста и значењето на нешто, врз основа на конкретниот придонес во даден систем и посакуваните резултати и исходи. Втората фаза се однесува на закани и извори што може да го нарушат процесот. Со чекорите во овие фази се создава основа за тврдења и процени дека нешто е ризик, или „можност за штета или повреда“ на „фактор со вредност на добро и ранливост“.

Во основа, проценатa на ризик опфаќа примена на логични и систематични методи за: комуницирање и консултации во текот на овој процес; воспоставување организациски контекст за идентификација, анализа и процена на ризикот поврзани со која и да е активност, производ, функција или процес и адекватно известување и архивирање во врска со резултатите од проценатa. За да може организацијата да изврши ефективна процена на ризикот, претходно мора да го дефинира контекстот на проблемот. По завршената процена организацијата треба да изврши третман на ризикот. Целта за изработка и примена на проценатa на ризикот е создавање услови за донесување ефикасни и ефективни одлуки во процесот на заштитата на лица, имот и работење втемелени врз сеопфатната процена на ризикот.[299]

[299] Бакрески О., Триван Д., и Митевски С., *Корпорациски безбедносен систем*, Комора на РМ за обезбедување на лица и имот, Скопје, 2012.

Контекстот во проценатa на ризикот може да варира во однос на потребите на организацијата, во зависност од тоа дали се дава или се бара услугата за заштита на лица, имот и работење. Контекстот може да вклучува, но не е ограничен на:

- определување одговорност;
- определување длабочина и широчина на активноста за процена на ризикот што треба да се спроведе;
- определување обем на проектот, процесот, функцијата или активноста во поглед на времето и локацијата;
- дефинирање на проектот, процесот, функцијата, активноста и нивните цели и предмет;
- определување однос помеѓу одреден проект или активност со други проекти или активности на организацијата;
- одредување барање за методологијата на процена на ризикот;
- утврдување на начинот на кој се проценува ефектот од проценатa на ризикот;
- идентификација и спецификација на одлуките што треба да се донесат;
- идентификација на неопходни студии за рамките и обемот, нивниот опфат, цели и ресурси неопходни за таква студија.[300]

Анализата од истражувањето посочува дека компаниите кои беа предмет на истражување генерално сите имаат планови за работа во вонредни ситуации, што начелно се засноваат на соодветните закони за заштита и спасување и на законот за управување со кризи, но, како посебни планови што ја третираат само областа од обезбедување и што генерално е засегната службата за обезбедување во делот на вооружени напади, нарушување на јавен ред и мир од поголеми размери, подметнувања на експлозивни направи, анонимни закани, саботажи, диверзии и сл., не се предмет на посебен план. Сепак, аеродромите поседуваат повеќе планови за постапување во вонредни ситуации како и план за постапување при акти од незаконско постапување, што се одобрени од релевантните институции, усогласени, истренирани и практично си-

[300] Исто., стр. 45-156.

мулирани. Од тие причини според примерот на воздухопловната безбедност, испитаниците посочија дека треба критичните инфраструктури да изработат компаниски планови за вонреди ситуации предизвикани од акти на незаконско постапување, што ќе имаат оперативен карактер со цел управување со мерките, со активностите и со постапките, со цел справување со вонредните состојби, спречување на понатамошна ескалација и намалување на ефектите од незаконските дејства против безбедноста на критичната инфраструктура со планско преземање на сите мерки и активности заради разрешување на состојбата. Ваквите планови ќе имаат за цел и обезбедување на навремено и усогласено постапување со сите надлежни субјекти во доменот на справување со вонредната ситуација, почитувајќи ги сите меѓународни и домашни стандарди. Во плановите многу е важно прецизното дефинирање на надлежностите и одговорностите, службите за реагирање при вонредните состојби, организациските структури во вонредни состојби, пристап до критичната инфраструктура, прецизно дефинирање на сите вонредни состојби кои можат да се случат во критичната инфраструктура, како и организација на тренинг активности за увежбување на оперативните планови од страна на сите инволвирани субјекти.

Од анализата на збирните одговори може да се воочи недоволното значење што правните лица му го придаваат на планирањето и на изработката на плановите и проценатa на ризикот, што е всушност и важна претпоставка за соодветна заштита на критичната инфраструктура.

Анализата и толкувањето на некои одговори од делот на корпоративното управување, карактеристиките на приватното обезбедување и офицерот (раководителот за безбедност), укажуваат на некои изненадувачки, а во некоја мерка и загрижувачки појави, коишто може да се карактеризираат како импровизација или како недоволно познавање на важноста на одредени прашања од суштествено значење за правните лица што управуваат или ја штитат критичната инфраструктура (тука во преден план е неизготвувањето на плановите за обезбедување, несоодветното искуство на офицерите за безбедност, како и нивната образовна несоодветност, а со тоа и некомпетентност).

4. КАКВИ СОГЛЕДУВАЊА НУДИ АНАЛИЗАТА ЗА ЗАШТИТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Колку што функционирањето на одредена инфраструктура е од клучен карактер, толку е критичен и прекинот на нејзино функционирање. Токму поради таа критичност, одредена инфраструктура добива на важност како критична.

Истражувањето супстанционално потврди дека појдовен елемент во анализата и синтезата на ова прашање претставува определбата на Европската унија што јасно го изразува ставот дека заштитата на националната критична инфраструктура претставува исклучива одговорност на националните држави. Оттука, најнапред потребно е прифаќање или адаптирање на европската дефиниција за критична инфраструктура, односно врз нејзина основа градење соодветен дефиниciски пристап што треба да биде значаен елемент за современата заштита на компаниите и државата во целост. Дополнително, со цел да се унифицира имплементацијата на секторскиот и на потсекторскиот пристап кон заштита на критичната инфраструктура, потребно е да се воспостави заедничка листа на сектори, што ќе овозможи кохерентна имплементација на мерките и на постапките за заштита на критичната инфраструктура.

Оттука за да може критичната инфраструктура квалитетно да се дефинира и да се развива, потребен е најнапред институционален приод, односно стратегиска рамка во поглед на дефинирањето, а аналогно на тоа, потребна е поприфатлива методологија за заштита и намалување на заканите врз критичната инфраструктура, што претставува услов за стабилно општество и сигурно извршување на основните функции на државата.

Во тој контекст, идните развојни стратегии како врвен приоритет треба да ја имаат заштитата на критичната инфраструктура. Во таа насока потребно е првичниот приод да биде фокусиран на:

- дефинирање на поимот „критична инфраструктура“ и поимот „заштита на критична инфраструктура“;
- давање опис со кој се утврдуваат безбедносните појави, нивната структура и поврзаност со критичната инфраструктура;
- класификација на безбедносните појави и прогнозирање на ризиците врз критичните инфраструктури;

- разбирање за елементите на критичност и ранливост на објектите од витален интерес – критичнатата инфраструктура;
- потикнување кон развојот на јавните и приватните оператори во поглед на обезбедувањето на критичната инфраструктура;
- воспоставување и развивање на програмите за обезбедување, вклучувајќи ги и плановите за вонредни ситуации и покризно закрепнување;
- поддржување и развивање на меѓународна соработка и др.

Што се однесува до заканите и ризиците врз критичната инфраструктура, потребна е сеопфатна анализа што треба да се заснова на три основни фактори, а тоа се: природните непогоди, технички-технолошки акциденти и актите на незаконско постапување, вклучувајќи го и тероризмот.

Во однос на инволвираните субјекти што треба да бидат носители на ваквите активности потребен е интегративен пристап со вклучување на:

- министерствата, агенциите и дирекциите што функционираат во рамките на државата;
- локалните власти;
- инфраструктурните оператори;
- релевантните субјекти кои ги третираат засегнатите критични инфраструктури;
- приватниот безбедносен сектор (агенции, Комора на Република Македонија за приватно обезбедување);
- научната и експертската заедница;
- јавноста и особено делот на медиуми итн.

Анализата потврди дека заканите врз критичната инфраструктура се директно поврзани со глобалните безбедносни предизвици, вклучувајќи го и современиот тероризам. Оттука потребно е преземање соодветни чекори во однос на превенција, подготвеност и одговор на терористички напади врз критична инфраструктура, што ќе бидат во согласност со Европската програма за заштита на критичната инфраструктура. Со оглед на декларацијата на ЕУ, дека оштетувањето или загубата на дел од критичната инфраструктура на една земја членка би предизвикало негативен ефект на други-

те земји членки и европската економија, неопходно е Република Македонија да преземе чекори за кохерентна имплементација на мерки за подобрување на заштитата на критичната инфраструктура и дефинирањето на обврските и должностите на сите субјекти во земјата засегнати со оваа проблематика.

Спроведувањето на мерките е директно поврзано со имањето, односно немањето на соодветна процена која треба да укаже или да претпостави на одредена закана. Проценатa на ризици врз самите критични инфраструктури претставува процес во кој се анализираат собраните безбедносни информации со определување на приоритети по однос на критериумите, евалуацијата и веројатноста.

Слика бр.7. Хиерархија на безбедносно регулирање на критична инфраструктура

Покрај проценатa, исто така, есенцијално е прашањето за конзистентноста и координацијата на сите субјекти вклучени во

обезбедувањето на критичната инфраструктура, односно потребно е да биде реализирана низ тело на државно ниво, составено од сите субјекти засегнати во дадената област на критичната инфраструктура, со цел да се промовира координирана имплементација на стандардите на национално ниво.

БИБЛИОГРАФИЈА

1. Alain, E., Hanno, R., Burkard, S., (edited by Burkard, S), *"Information Security, A new Challenge for the EU"*, Chaillot, Paper no. 76, Paris, 2005.
2. Auerswald, L.M. Branscomb, T.M. La Porte, E.Michel – Kerjan, *The Challenge of Protecting Critical Infrastructure – issues in science and Technology,* FALL 2005.
3. Benjamin R. Barber, "*Jihad vs. McWorld*", *The Atlantic*, March 1992.
4. Bennet, T., B. Understanding, Assessing and Responding to Terrorism. Protecting Critical Infrastructure and Personnel. Wiley/John Wiley and Sons, 2007.
5. Betty E. Biringer, Eric D. Vugrin, Drake E. Warren. Critical Infrastructure System Security and Resiliency, CRC Press, 2013.
6. Bigović, M. & Rakocević, A., *Challenges in Defining Critical Infrastructure in Montenegro., in Denis Caleta & Vesela Radovic*, ed., 'Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection', IOS Press, 2015.
7. Biringer, B., E., Vugrin, E., D., Warren, E. D. *Critical Infrastructure. System Security and Resiliency*. CRC Press, Taylor and Francis Group, 2013.
8. Brian T. Bennett. *Understanding, Assessing, and Responding to Terrorism, Protecting Critical Infrastructure and Personnel*, John Wiley & Sons, Inc, 2007.
9. Čaleta, D., Radović, V., *Comprehensive Approach on "Sine Qua Non" for Critical Infrastructure Protection*, IOS Press, 2015.
10. Čaleta, Denis, *Corporate Security in Dynamic Global Environment – Challenges and Risk*, Ljubljana, 2012.

11. D'Agostino, M., D., *Defense Critical Infrastructure*. GAO, 2009.
12. Dawson, M., Omar, M., *New Threats and Countermeasures in Digital Crime and Cyber Terrorism Information Science Reference*. 2015.
13. Dorfman S., Mark, *Introduction to Risk management and insurance*, Prentice Hall, Englewood Cliffs NJ, 2012.
14. Dyrmishi, A. et all, *A Force for Good? Mapping the Private Security Landscape in Southeast Europe*, DCAF, 2015.
15. Edward G. Amoroso, *Cyber Attacks Protecting National Infrastructure*, Elsevier Inc, USA, 2011.
16. Eriksson, P., Barck-Holst S., *Critical Infrastructure Protection policy in the EU and in Sweden –Comparative analysis*, FOI, Stockholm, 2005.
17. George, Loukas, *Cyber-Physical Attacks- A Growing Invisible Threat*, Elsevier Inc, USA, 2015.
18. Gheorghe, A.V., Masera, M., Weijnen, M.P.C., *Critical Infrastructures at Risk. Securing the European Electric Power System*, Springer 2006.
19. Hadži-Janev, Metodij, *Critical Infrastructure Protection as one of the Key Elements in the Search for an Effective Strategy for Regional Energy Security*, Political thought, Institute for democracy, Konrad Adenauer Stiftung, vol.9, December 2011.
20. Hehir, A., Robinson, N. (eds) "*State Building. Theory and Practice*. London. Routledge", 2007.
21. Holland, G., *Assessing Hurricane Impacts,* Willis Research Network and National Center for Atmospheric Research, 2009.
22. Jakovljević V., Gačić J., *Zastita kriticne infrastructure u kriznim situacijama*, 2012.
23. *Jarlsvik, H., Castenfors, K., Security and Preparedness in the EU, Stockholm, 2004.*
24. John Sullivan, *Strategies for Protecting National Critical Infrastructure Assets A Focus on Problem-Solving*, John Wiley & Sons, Inc., 2007.

25. Johnson, A. Thomas (ed.), *Cyber Security-Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015.
26. Jurišić, D., *Critical Infrastructure Protection in Bosnia and Herzegovina and the Role of Military,* 2013.
27. Karmon, Ely. "*The Risk of Terrorism against Oil and Gas Pipelines in Central Asia*." International Institute for Counter-Terrorism, 6 January 2002.
28. Klaić, Z., S. Mandžuka, P. Škorput, *Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama*, 18. Telekomunikacioni forum Telfor, Beograd, 2010.
29. Klemen, Groselj, *Critical Infrastructure Protection and the Energy Sector Counter – Terrorism Challenges regarding the Processes of Critical Infrastructure*. Ljubljana, September, 2011.
30. Kostadinov, Venceslav, "*Vulnerability Assessment. New Nuclear Power Plants Universal Methodology for Terrorism Threats and Natural Disasters Analyses and Predictions*", in Denis Caleta, Paul Shemella, Iztok Podbregar, Branko Lobnikar, Ljubljana. Institute for Corporative Studies-ICS, Monterey. Center for Civil-Military Relations, 2011.
31. Kostić, V., *Zapalive I druge opsne materije*, Udruzenje publicista Beograd, 1980.
32. Krajcar, S., *Energetska sigurnost i kritčna infrastruktura*. Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb 2009.
33. La Porte, T.R., *Critical Infrastructure in the Face of a Predatory Future. Preparing for untoward surprise,* Vol. 15, No.1, 2007.
34. Laing, Christopher, Badii, Atta, Vickers, Paul, *Securing Critical Infrastructures and Critical Control Systems. Approaches for Threat Protection*, IGI Global, 2013.
35. Larsson, R., *Tackling Dependency. The EU and its Security Challenges*, Swedish Defense Research Agency, 2007.

36. Lawrence, Freeman, "*Out of Nowhere – Bin Laden's Grievances*", *BBC Online*, 20 October 2011.
37. Lazari, A., *European Critical Infrastructure Protection*. Springer, 2014.
38. Lewis, G., *Critical Infrastructure Protection i Homeland Security – Defending a Networked Nation*, John Wiley & Sons Inc. Hoboken, New Jersey (USA), 2006.
39. Lewis, J., *Cyber Attacks Explained, June* 15, 2007.
40. Li, H., et al, Strategic Power Infrastructure Defense, Proceedings of the IEEE, 2005.
41. Lopez, J., Setola, R., Wolthunsen, Critical Infrastructure Protection. Information Infrastructure Models, Analysis and Defense. Springer, 2012.
42. Lundborg, T., Vaughan-Williams, N., *Resilience, Critical Infrastructure and Molecular Security*. the Excess of Life in Biopolitics, *International Journal Political Sociology*, vol. 5, no. 4, 2011.
43. Martellini, M., *Cyber Security. Deterrence and IT Protection for Critical Infrastructure*. Springer, 2013.
44. Massoud, A., "*Security Challenges for the Electricity Infrastructure (Supplement to Computer Magazine)*". *Computer* (IEEE computer society), 2002.
45. Matka, D., *Energetska sigurnost i kritčna infrastruktura – pregled rezultata istraživanja* Zbornik radova, 2009.
46. Krajcar, S, *Energetska sigurnost i kritična infrastruktura*, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb 2009.
47. Montanari, Luca, Leonardo Querzoni (ed.), *Critical Infrastructure Protection*: *Threats, Attacks and Countermeasures*,. Tenace, March 2014.
48. Moteff, J., Parfomak, P., *Critical Infrastructure and Key Assets. Definition and Identification*, 2004.
49. Moteff, T., J., *Critical Infrastructures. Background, Policy and Implementation*. Congressional Research Service, 2010.

50. Murray, A.T. and Grubesic, T.H., *Critical Infrastructure Reliability and Vulnerability*, Springer-Verlag Berlin Heidelberg, 2007.
51. Nickolov, E., "*Modern Trends In The Cyber Attacks Against The Critical Information Infrastructure*", ITU, Regional Cybersecurity Forum, 7-9 October 2008, Sofia, Bulgaria.
52. Perman, K. and Schurter, T, *Protecting Critical Infrastructure*, 2016.
53. Prezelj, I., *Konceptualna opredelitev kritične infrastrukture*, FDV, Ljubljana, 2008.
54. Pursiainen, C., *The Challenges for European Critical Infrastructure Protection*, European Integration, vol. 31, no. 6. 2009.
55. Radvanovski, R., McDougall, A., *Critical Infrastructure. Homeland Security and Emergency Preparedness*, Third Edition. CRC Press, Taylor and Francis Group, 2013.
56. 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, достапно на. http.//www.cpqd.com.br, http.// www.cpqdusa.com
57. Richardson, Louis, "*Counterterrorism and Democracy*", Harvard Magazine, 2009.
58. Rinaldi, Steven M., Peerenboom, P. James, Terrence K. Kelly, *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, IEEE Control Systems Magazine, December 2001.
59. Sage, P., Andrew, *Systems Engineering for Risk Management*, Norwel MA, 1995.
60. Sawer, Patrick, "*Japan Earthquake. Nuclear Disaster Feared After Power Plant 'Explosion'*", The Telegraph, 12 Mar 2011.
61. Schot, J., *Transnational Infrastructures and the Rise of Contemporary Europe*, working Doc No.1, 2003.

62. Slaveski, Stojan, Bakreski, Oliver, "*Security of Classified Information as Part of the National Critical Infrastructure Protection. Macedonian Experience*", Series NATO Science for Peace and Security Series - D. Information and Communication Security, DOI 10.3233/978-1-61499-478-7-107, E-book Volume 39, 2015.
63. Spyer, John ,"The *Al–Qa'ida Network and Weapons of Mass-Destruction*", *Middle East Review of International Affairs*, Vol. 8, No 3, September 2004.
64. Stephen Flynn, "*America the Vulnerable*", New York. Harper Collins, 2004.
65. Tatalović S., *Energetska sigurnost i zastita kriticne infrastrukture. uticaj na politike i nacionalne bezbednosti* - Zbornik radova, 2009.
66. Vaughan J. Emmett, *Risk Management*, John Wiley & Ins Inc, New York, 1996.
67. Vrsec, M., *Managing Corporate Security in the Energy Sector. Energy as Vital (Critical) Infrastructure for the Functioning of a State, Economy and Civil Society*, во Denis Caleta and Paul Semella, "*Counter Terrorism Challenges Regarding the Process of Critical Infrastructure Protection*", Center for Civil – Military Relations, Monterey, USA, 2011.
68. Wilson, C., Botnets, *Cybercrime and Cyberterrorism. Vulnerabilities and Policy Issues for Congress*, January, 2008.
69. Бакрески О., Даничиќ М, Кешетовиќ Ж. и Митевски С., *Приватна безбедност – теорија и концепт*, Комора на Република Македонија за приватно обезбедување, Скопје, 2015.
70. Бакрески О., Триван Д. и Митевски С., *Корпорациски безбедносен систем*, Комора на Република Македонија за обезбедување на лица и имот, Скопје, 2012.
71. Донева К. Втор национален извештај на Република Македонија кон рамковната конвенција на обединетите нации за климатски промени-Дел. проценка на

ранливоста и адаптација за секторот водни ресурси, Министерство за животна средина и просторно планирање, декември 2006.

72. 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.
73. Кешетовиќ, Ж., *Кризни Менаџмент*, Факултет безбедности, Београд, 2008.
74. Костеска, Миљковиќ Е., *Опасни материи* (Dangerous Goods Manual) Аеродром Александар Велики Скопје, 2007.
75. Милошевска Т., *Модели на поврзаност на тероризмот и на транснационалниот организиран криминал*, Универзитет „Св. Кирил и Методиј“, Филозофски факултет, МАР-САЖ Скопје, 2016.
76. Петровић, Р., С., *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007.
77. Поповски, Јордан, Тероризам и заштита на критична инфраструктура. Случај Република Македонија. *Современа македонска одбрана*, Министерство за одбрана на Република Македонија, Скопје, јуни 2014.
78. Славески С., Сајбер-заканите, предизвик за современите општества, Министерство за одбрана на Република Македонија.
79. “Сигурност и защита на обекти от критичната инфраструктура, Национален военен университет «Васил Левски», София, 2013.
80. Танески, Н., Чаминski, Б., Геополитичкото значење и заштитата на енергетската инфраструктура на Европската Унија од асиметрични закани, *Современа македонска одбрана*, година 14, бр.27, декември 2014.

Документи

81. Bundesministerium des Innern. „Nationale Strategie zum Schutz Kritischer Infrastrukturen“, BMI, Германија, 2014.
82. Center for Security Studies, “*Crisis and Risk Network Critical Infrastructure Protection*”, ETH Zürich, 2009.
83. Centre for European Policy Studies (CEPS) *Task Force report, Protecting Critical Infrastructure in the EU*, 2010.
84. *Checklist-Critical Infrastructure Security and Protection. The Public-Private Opportunity*. White Paper by CoESS – Confederation of European Security Services, 2012.
85. Commission of the European Communities, *Critical Infrastructure Protection in the Fight against Terrorism* (Brussels, 20 October 2004), COM (2004) 702 final.
86. Commission of the European Communities, Green Paper on a European Program for Critical Infrastructure Protection (Brussels, 17 November 2005), COM (2005) 576 final.
87. Commission Staff Working Document on a New Approach to the European Program for Critical Infrastructure Protection Making European Critical Infrastructures more secure, 2013.
88. Commission Staff Working Document on the Review of the European Program for Critical Infrastructure Protection (EPCIP), 2013.
89. Communication on critical infrastructure protection in the fight against terrorism.
90. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008.
91. Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zurich, “Focal reports” (Fokusberichte) on critical infrastructure protection and on risk analysis to promote discussion and inform about new trends and insights, Zurich 2009.
92. Critical Information Protection (CIP) Survey, 2010.
93. Critical Infrastructure Security and Protection The Public-Private Opportunity- White Paper and Guidelines by CoESS And its Working Committee Critical Infrastructure. December, 2010.

94. DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, EУР-lex, 2008.
95. Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan Homeland Security – United States Department of Energy, 2010.
96. European Commission, "*Identification of Critical Infrastructure and Operational Strategic Planning*", Review. Albania-Croatia-Slovenia, European Program for Critical Infrastructure Protection", 2007.
97. European Programme for Critical Infrastructure Protection (EPCIP) COM (2006) 786.
98. European Spatial Planning Observation Network (ESPON), "*The Spatial Effects and Management of Natural and Technological Hazards in Europe*", Luxembourg, 2006.
99. Green Paper on a European Program for Critical Infrastructure Protection.
100. *National critical infrastructure protection – regional perspective* UDC726.9.75.041.5 ID176374796, Z. Keković, S. Vučić, R. Despotović N. Komazec – compliance of education programs with the need of protection national critical infrastructure; Belgrade, December 2013.
101. National critical infrastructure protection – regional perspective, Belgrade, 2013.
102. National critical infrastructure protection – UDC726.9.75.041.5 ID176374796 B. Mihaljević, I. Toth, A. Stranjik University of Applied Sciences, Velika Gorica – impact of critical infrastructure ownership on the national security of the Republic of Croatia regional perspective-Belgrade, December 2013.
103. National Guidelines for Protecting Critical Infrastructure from Terrorism, Australia – New Zealand Counter – Terrorism Committee, Commonwealth of Australia, 2015.
104. National Infrastructure Protection Plan, Homeland Security, 2013.

105. National Oceanic and Atmospheric Administration (NOAA)—*Earthquakes*. NOAA Watch. NOAA's All-Hazard Monitor. National Oceanic and Atmospheric Administration.
106. Nuclear Power and Security Threats", No2, Nuclear Power, January 2007.
107. Partnering for Critical Infrastructure Security and Resilience homeland security NIPP 2013.
108. Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013.
109. Problem space report. Critical infrastructure & supply chain protection Cross-border Research Association (CBRA) January, 2012.

Извори од интернет

110. http.//ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf
111. http.//www.cpni.gov.uk/about/cni/
112. "Explaining Distributed Denial of Service Attacks to Campus Leaders," May 3, 2005.
113. "Frankfurt Shooting, The Kosovo Connection", Economist, March 03, 2011.
114. "Investigating Cyber Security Threats. Exploring National Security and Law Enforcement Perspectives", Frederic Lemieux, Report GW-CSPRI-2011-2, 7 April 2011.
115. "Al Qaeda Calls For Attacks on U.S. Oil Sources." Xinhuanet, 15 February 2007.
116. http.//www.jura.uniaugsburg.de/prof/moellers/materialien/materialdateien/010_europaeische_gesetze/eu_richtlinien/ril_2002_058_eg_datenschutz_en/
117. http.//www.mid.gov.me/en/library/strategije
118. http.//www.nato-pa.int/default.asp?SHORTCUT=1165

119. http.//www.oecd.org
120. http.//www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx
121. https.//www.dhs.gov/what-critical-infrastructure
122. http//www.worldenergyoutlook.org/media/weowebsite/2013/LondonNovember12.pdf
123. http.//europa.eu/lisbon_treaty/full_text/index_en.htm
124. http.//www.noaawatch.gov/themes/quake.php
125. http.//www.nato-pa.int/default.asp?SHORTCUT=1165
126. http.//www.ceps.eu/ceps/download/4061
127. http.//ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf
128. http.//www.unbrussels.org/agencies/unisdr.html
129. http.//searchsecurity.techtarget.com/sDefinition/0.,sid14_gci771061,00.html
130. www.symantec.com

9 786086 599041