УНИВЕРЗИТЕТ „СВ. КИРИЛ И МЕТОДИЈ" - СКОПЈЕ

ФИЛОЗОФСКИ ФАКУЛТЕТ

ИНСТИТУТ ЗА БЕЗБЕДНОСТ ОДБРАНА И МИР

ДОКТОРСКА ДИСЕРТАЦИЈА

Тема:

ИМПЛЕМЕНТАЦИЈА НА СОВРЕМЕНИТЕ БЕЗБЕДНОСНИ СИСТЕМИ И ПРОЦЕДУРИ ВО РАЗВОЈОТ НА ОБЕЗБЕДУВАЊЕТО НА ОБЈЕКТИТЕ ОД ВИТАЛЕН ИНТЕРЕС ЗА РЕПУБЛИКА МАКЕДОНИЈА (СО ОСВРТ НА АЕРОДРОМСКАТА БЕЗБЕДНОСТ)

Кандидат:

М - р Ѓорѓи Алчески

Ментор:

Проф. Д-р. Оливер Бакрески

Скопје, 2016 година

Содржина

Вовед

Прифаќајќи ја реалноста, за ранливоста на државата преку објектите кои се од витално значење за развојот и функционирање на современото општество и фактот дека живееме во време на нестабилни општествено политички услови, каде тероризмот и другите извори на загрозување, како што се: општествените девијации (пр. кражби, измами, индустриски шпиунажи, саботажи, диверзии, злонамерни оштетувања и сл.), потоа, природните катастрофи, техничко технолошките акциденти, човечките пропусти слично, можат да предизвикаат поголеми човечки загуби и материјална штета, отколку разни вооружени конфликти и локални војни.

Специфичниот облик на загрозување, во чии рамки спаѓа и употребата на современите оружја и напредни технологии, вклучувајќи го и нуклеарниот материјал, хемиските и биолошките оружја, претставуваат безбедносни текови, со кој мораме да се соочиме и реално да погледнеме во опасностите кои ги носи денешницата. Фактот дека постои веројатност, таквото оружје да биде употребено во акти на незаконско постапување и врз објектите од витален интерес, односно ,,критичната инфратруктура", ја наметнува потребата од еден посебен безбедносен третман во поглед на креирањето на развојната безбедносна политика.

Во таа смисла, денес предмет на сериозна теоретска критика е потребата од правилно менаџирање со обезбедувањето, кое е директно вклучено во обезбедувањето на критичната инфраструктураи во суштина бара избалансираност, заеднички напор и висок степен на соработка на клучните субјекти за остварување на примарните цели на безбедносниот систем. Тоа ја нагласува потребата за прифаќање на напредните безбедносни системи и процедури во развојот на обезбедувањето, како и постапките кои треба да се превземаат во случај на опасност (вонредни околности), од страна на стручниот персонал, а се со цел создавање на услови за нормално функционирање на државата.Оттука, нашата намера е да се придонесе во креирањето на развојната безбедносна политика на објектите од витален интерес, со кои ќе се обликуваат идните развојни стратегии, инвестиции и едукации, а се со цел навремено, безбедно и ефикасно одвивање на технолошките процеси од една страна и заштитата на објектите од витално значење - ,,критичната инфратруктура" како национален интерес од друга.

Од тие причини, овој труд низ адекватен методолошки пристап и експлицитно поставени цели и задачи на истражување, преку прецизно дефинирање на хипотезата и варијаблите, воедно применувајќи соодветни методи и техники за истражување,во

рамките на девет глави ќе бидат разработени теми и понудени одговори, во насока на унапредување на обезбедувањето на виталните објекти во Република Македонија.

Во вториот дел од оваа докторска дисертација ќе ги анализираме виталните објекти низ една концептуална рамка, во која веднаш на почетокот се наметнува значењето на виталните објекти, но и проблемот со терминолошките дивергенции околу поимот и употребата на се по прифатливиот назив, користен во меѓународната терминологија а тоа е ,,критична инфраструктура", термин кој низ индикативна листа на дефинирани области ќе преовладува во докторската дисертација.

Во третата глава, направен е преглед на областите и објектите од витален интерес-критична инфраструктура, со акцент на воздухопловството, кое во основакако една од порегулираните и пософистицираните области ќе претставува водидилка низ процес кој ќе постави бројни размислувања од аспект на применливоста на напредните технологии и насоки во развој на обезбедувањето на виталните објекти во Република Македонија.

Четвртата глава, се фокусира на потребата од воведување на проценки на ризик низ заканите, ранливоста но и последиците, а сето тоа третирано од аспект на актите на незаконско постапување. Тука, се наметнува потребата од воспоставување на методологии за проценка на ризици, но и утврдување на критериуми за закана и ранливост. Затоа, концептот, моделот и потребата од управување со ризикот, практично само по себе, се наметнува како важен сегмент во целокупното управување со безбедноста на виталните објекти.

Во петото поглавје, акцентот се става врз актите на незаконско постапување, врз безбедноста на виталните објекти, тукасе наметнува нов термин кој во иднина по примерот на воздухопловството би било пожелно да постане општо прифатен, кога станува збор за криминалните дејствија, односно кривичните дела преставени во повеќе форми вклучувајки го и тероризмот како најекспонирана област. Во овој дел преку анализа на актите на незаконско постапување претставени низ опасните материи, терористичките дејствија, тактика на дејствување, карактеристиките и категориите на теротистичките групи,произлегува коплексноста на обезбедувањетои потреба од примена на напредните технологии и методологии на работа во насока на заштитата на виталните објекти од современите закани.

Следствено на тоа, шестото поглавје се фокусира на мерките за обезбедување во функција на виталните објекти и прашањата поврзани со организацијата, планирањето, службите и агенциите за обезбедување, понатака програми и процедури за работа, улогата на разузнавањето, развојот и примената на напредната

безбедносна опрема за заштита на критичната инфраструктура и сл. Исто така, преставени се сегментите во системот на обезбедување и концептот за обезбедување кој низ четири ефекти коитреба да се постигнат,на еден мошне специфичен начин ја откриваат функција на обезбедувањето на виталните објекти. Како што беше напоменато, во оваа глава понудена е применливоста на мерките за обезбедување од воздухопловството,за потребите во останатите критични инфраструктури, така што, низ еден прилагоден и адаптиран пристап ќе придонесат во унапредувањето на целокупната безбедност како на виталните објекти така и на државата во целост.

Предмет на научен интерес во седмата глава беше заштитата на виталните објекти односно критичната инфраструктура, претставена низ призмата на САД, земјите членки на ЕУ со осврт на Германската стратегија и односот на Република Хрватска и Република Чешка кон заштитата на критичната инфраструктура како и Австралискиот концепт кон безбедноста на критичните инфраструктури. Направени беа согледувања, како современите држави најнапред ја дефинираат критичната инфраструктура, но и како истите низ прописи, стратегии, мерки и активности се справуваат со заканите, кои ја пратат денешницата.

Во осмиот дел, анализата се фокусира на критичната инфраструктура во Република Македонија, односно досегашното регулирање на оваа област претставено низ некои критични инфраструктури, како што се на пример: енергетскиит сектор, ИТ безбедноста, водните системи и воздушниот сообраќај како сегмент од транспортниот систем со детална елаборација на процедурите, координацијата, безбедносните закани и ризиците кои се среќаваат во системот на безбедност на критичните инфраструктури. Во оваа глава, направен е и целосен преглед и интерпретација на резултатите од спроведеното теренско истражување, по однапред подготвен прашалник адаптиран за потребите на оваа докторска дисертација.Следствено на тоа, поставени се иницијалните размислувања во поглед на дефинирањето на ,,критичните инфраструктури" во Република Македонија. Од резултатите на спроведеното истражување, беа донесени заклучоци кои понатаму ќе користат во развојот на обезбедувањето на критичните инфраструктури во Република Македонија, со сите специфики и карактеристики, кои ја дефинираат оваа област.

По основ на истражувањето и анализите направени за потребите на оваа докторска дисертација, предожен е можен модел за подобрување на безбедноста и намалување на последиците од актите на незаконито постапување врз објектите од витален интерес во Република Македонија. Затоа, во главата девет претставен еи концепт за изработка на План - ,,ПОКИ", кој низ опишани стандардни оперативни

процедури би придонел во подобрување на безбедноста и намалување на последиците од актите на незаконско постапување врз објектите од витален интерес во Република Македонија,,

На крај, низ заклучоците кои се донесени по основ на сите девет глави, се предлага развивање или надоградување на безбедносниот систем на Република Македонија,со концептот обезбедување на ,,критични инфраструктури" кој имапосебни карактеристики и специфики, и се дава простор за понатамошно доизградување и унапредување на областа.

ГЛАВА I

Методолошки пристап

1. Релевантност на темата

Имплементацијата на современите безбедносни системи и процедури во однос на потребата за оптимален степен за безбедност, кој ќе гарантира нормално функционирање на друштвото, станува врвен приоритет на секоја современа држава. Комплексноста и сложеноста на проблематиката, која го третира овој докторски труд, претставен низ зависноста на државата од виталните објекти и потребата од нивна адекватна заштита, преставува предизвик, на кој во иднина треба да се посвети уште поголемо внимание. Всушност, овој докторски труд претставува еден научен потфат, кој има за цел да одговори на повеќе прашања од областа на безбедноста и да направи анализа за применливоста на напредните технологии, системи и процедури во развојот на обезбедувањето на виталните објекти во Република Македонија.

Новите безбедносни предизвици и нивното влијание врз објектите од витален интерес, а од тука и влијанието врз националните капацитети, кои се од такво суштинско значење што нивното нефункционирање или оштетување можат да имаат директно влијание на националната безбедност, националната економија, здравството и ефикасното функционирање на системите на државата, недвосмислено говорат за сериозниот пристап, кој треба да го имаме кон овој реален проблем и кој во голема мера ја засега безбедноста на секоја држава.

Имајќи ја предвид турбулентната транзиција на Република Македонија, како и се понагласената потреба за заштита и обезбедување на приватната и државната сопственост, истовремено и како земја која треба да ги почитува и имплементира меѓународните стандарди кои се однесуваат на безбедноста, потребно е да се постигне стандардизирано ниво на безбедност и да се усвои сеопфатна безбедносна политика, подржана со законски прописи, кои ќе ги спроведуваат сите субјекти вклучени во безбедноста.

Потребата за следење на современите безбедносни текови, а посебно во сегментот кој се нарекува ,,критична инфраструктура" или кај нас сеуште употребуваниот термин ,,витални објекти", преставува еден од фундаментите на кој се темели безбедноста на модерните општества и ќе се трасираат основните контури во подобрување на обезбедувањето на виталните објекти, но и поттик, кон нови размислувања во безбедносните науки, кон една проблематиката која е составен дел на системот на безбедност на секоја држава.Во оваа дисертација, која се темели на повеќе аспекти преставена низ девет глави, ги обликува клучните перспективи за еден понатамошен сестран развој на обезбедувањето на критичните инфраструктури, низ

сложеноста и комплексноста на современите закани, кои директно влијаат врз националната безбедност, економија, здравство и др.

2. Цели и задачи на истражувањето

Истражувањето на овој проблем има за цел, да ги провери и анализира новите безбедносни предизвици, нивното влијание и моделирањето на новите безбедносни текови, кои претставуваат значаен сегмент во заштитата на објектите од витален интерес (критична инфратруктура) за националната безбедност. Основата на истражувањето, беа всушност новите безбедносни предизвици и нивното влијание врз овие објекти, а од тука и влијанието врз националните капацитети, кои се од толкаво витално значење што нивното нефункционирање или оштетување, можат да имаат директно влијание на националната безбедност, националната економија, здравството како и ефикасното функционирање на системите на државата.

Елаборацијата која е направена во овој труд, содржи два елементи: прво, се прави согледување на критичната инфраструктура од аспект на нејзиното значење врз националната безбедност и второ, анализата е направена за да се согледа какви чекори се прават или треба да се направат, за да се обезбеди нејзина соодветна заштита.

Ако се земе предвид сложеноста на истражувачкиот проблем, кој се темели преку испреплетување на обврските на повеќе субјекти, кои што учествуваат во обезбедувањето на објектите од витален интерес (критичната инфратруктура), акцент беше ставен и на деталната проценка на факторите, кои што доведуваат до неефикасност на безбедноста.

Во сегашните околности, опасностите кои се детектирани бараат примена на дополнителни мерки за безбедност, кои треба да се прилагодат на условите и истите мораат континуирано да се ревидираат и надградуваат, со цел да се постигне оптимално ниво на нивната ефикасност. Во тој поглед, направена е анализа на настани, кои во голема мера влијаеле во развојот на имплементацијата на напредните системи и процедури и даден е опис на клучните фактори кои предходеле на настаните, а кои во голема мера завршувале со фатален исход.

Имајки ги предвид, случувањата од 11 Септември 2001година и потребата за што посигурна заштита на цивилното воздухопловство, Република Македонија е обврзана да ги почитува и имплементира меѓународните стандарди кои се однесуваат на безбедноста на цивилната воздушна пловидба. За да се постигне стандардизирано ниво за безбедност на воздушната пловидба, нашата држава ја гради својата

платформа за безбедност на воздушниот сообраќај преку, градење сеопфатна политика, подржана со законски прописи, кои ќе ги спроведуваат сите субјекти вклучени во која било безбедносна структура во цивилното воздухопловство. Оттука, ова истражување дава еден конкретен придонес, како во општото и теоретско доизградување на оваа област, така и во разрешувањето на практичните аспекти за примена на методологијата на системот за безбедностприменета во воздухопловството, да се доизгради на уште повисоко ниво и да се примени или во најмала рака да се приближи и во обезбедувањето на останатите објекти, кои се од витален интерес (критичната инфратруктура) за Република Македонија.

2.1. Научната цел на истражувањето е базирана врз основа на општите и теоретските постулати за обезбедувањето на виталните објекти во Република Македонија, а со тоа да се воспостави методолошки пристап во менаџирањето со обезбедувањето, посебно во делот на приватното обезбедување, како еден релативно нов - дополнителен сегмент во националниот систем за безбедност на Република Македонија.

Исто така, вниманието беше насочено кон доградбата на теоретските и практичните решенија, во областа на справувањето со заканите во функција на безбедноста, согледување, изнаоѓање и дефинирање на можностите и условите за применливоста на напредните процедури и системи, имплементирани во развојот на обезбедувањето на објектите од витален интерес за Република Македонија.

Со оглед на научната цел, **посебните цели на истражувањето** беа насочени кон:

- добивање на научни сознанија, со кои ќе се утврдуваат безбедносните појави, нивната структура и поврзаност,
- дефинирање на критичната инфраструктура, како нов термин во рамките на безбедносниот сектор во Република Македонија,
- откривање на непознатите појави од аспект на безбедноста, нивните својства, причинители, состојби и тенденции кои ги сочинуваат објектите од витално значење,
- 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 објектите од витален интерес – критичната инфраструктура,

- воспоставување и развивање на плановите за вонредни ситуации и после кризно опоравување,

- компаративна анализа на безбедносните системи и процедури на различната критична инфраструктура,

- утврдување на применливоста на одредени напредни системи и процедури во различни инфраструктури,

2.2. Практичната цел на истражувањето

Практичната цел на истражувањето беше развојно ориентирана, која за основа имаше фундаментално унапредување на научните сознанија и применети истражувања, (да се унапредат научните сознанија меѓутоа да се унапредат првенствено практичните цели) за да се дојде до релевантни сознанија, кои се во врска со влијанието на терористичките и другите видови на закани и оттука мерките, процедурите, опремувањето, екипирањето, структурата итн. кои треба да бидат спроведени со цел навремено, безбедно и ефикасно функционирање на објектите од витален интерес – критичната инфраструктура во Република Македонија.

Важен критериум на функцијата на истражувањето, беше акционо истражување, чија задача беше да се даде одговор на конкретниот проблем, со конкретно оперативно решение и да се понуди модел за обезбедување, применлив во голем дел од дефинираните критични инфраструктури. Да се даде прецизна насока во поглед на применливоста на технолошките безбедносни решенија од една во друга критична инфраструктура, а се со цел намалување на загубите и штетите, како на компаниски така и на национален план.

2.3. Општествена цел на истражувањето

Општествената цел на истражувањето беше, обезбедување на научни сознанија за состојбата, содржината, методите и насоките за развој и усовршување на системот за справување со актите на незаконито постапување во Република Македонија, со што се обезбеди, пред се научно, стручно, рационално и ефикасно работење во оваа област,

како и применливоста на одредени напредни системи и процедури во различни објекти од витално значење –критична инфраструктура.

Истражувањето кое беше спроведено во овој труд, се обиде да ги пронајде каузалните врски помеѓу заканите во овој случај (саботажа, диверзии, киднапирања, анонимните закани, поставени експлозиви во објектите и др.) со нормалното функционирање на процесите на работа на виталните објекти, а воедно се даде објаснување за инвестиционите вложувања во безбедноста, се со цел, намалување на последиците од заканите.

2.4. Општествена и научна оправданост

Научен придонес на оваа дисертацијата ќе биде, отворање на нови видици и нови можности, за практичната примена на одредени меѓународни развојни проекти, од областа на обезбедувањето во Република Македонија, кои ќе се однесуваат на унапредување на обезбедувањето, како составен дел на безбедносните капацитети на државата, а кои се верификувани од страна на релевантните меѓународни организации и веќе применети и потврдени во одреден број на европски држави.

Теоретски, до овој момент не постојат и не се вршени истражувања за евентуална поврзаност и применливост на одредени напредни системи и процедури во различни објекти од витален интерес. Со соодветна анализа, се изврши согледување, изнаоѓање и дефинирање на можностите и условите за применливоста на мерките за безбедност во различни објекти од витално значење – критична инфраструктура, со цел добивање на повисок степен на безбедност, менаџирање на безбедноста и взаемната поврзаност.

Резултатите од практичната примена на истражувањето, ќе придонесе да се влијае врз припадниците на сите инволвирани субјекти во безбедноста, да бидат подготвени, стручно оспособени и опремени за навремено, ефикасно, безбедно и стручно реагирање и делување, при секаква евентуална појава, која би ја загрозила безбедноста на објектите од витален интерес –критичната инфраструктура. Тоа посебно се однесува на стручниот персонал, кој извршува работи поврзани со обезбедувањето, да носат навремени и прецизни одлуки во справување со заканите кои го следат функционирањето на објектите од витален интерес за Република Македонија. Затоа,субјектите кои се инволвирани во обезбедувањето на објектите од витален интерес, како фундаментален предуслов за непречено функционирање на државата, ќе треба да имплементираат постапки (процедури) за обезбедување, кои ќе бидат понудени во докторската дисертација, со цел за посериозен пристап кон проблемите, кои ја засегаат оваа област.Водејќи сметка за ова, научното истражување

ќе даде насоки во поглед на обезбедување на адекватни услови за справување со заканите, а се со цел да се добие најбезбеден, најсоодветен и намјалку конфузен резултат.

3. Појмовно определување на основните поими на истражување

Во текот на изработката на докторската дисертација, беа анализирани повеќе документи, прирачници, планови, програми, процедури, списанија, објавени написи од службени документи, со кои располагаат објектите, кои се предмет на истражување, а кои се во директна врска со обезбедувањето.

Содржините во дисертацијата се базирани, пред се, врз документите на меѓународните организации, кои пропишуваат стандарди и препораки што се однесуваат на безбедноста а исто така, обработените содржини се во согласност со важечките законски и подзаконски прописи од оваа област во Република Македонија.

Во докторската дисертација застапени се следните основни поими:

- **Аеродром** е определена копнена или водна површина со површини за маневрирање и површини за полетување и слетување, платформи, објекти, уреди и опрема наменети за безбедно движење, слетување, полетување и престој на воздухоплови;
- **Аеродромски услуги** се услуги што се даваат на воздухопловното пристаниште значајни за безбедно одвивање на воздушниот сообраќај и опфаќаат:
  - а) прифаќање и испраќање на воздухоплови, патници, багаж, стока и пошта,
  - б) противпожарна заштита,
  - в) медицински услуги за членови на екипаж и патници,
  - г) опслужување на воздухоплови со гориво и мазиво и
  - д) обезбедување од дејствија на незаконско постапување;
- **Анализа на ризик** преставува согледувања на можните загрозувања, закани, со што би се оценила ранливоста или пореметување на нормалното функционирање на критичната инфраструктура,
- **Безбедносна програма** е збир на мерки и активности, коишто се применуваат на национално ниво и на ниво на аеродром, дадени во писмена форма, што се усвоени од надлежниот орган, со цел заштита на цивилниот воздушен сообраќај, од акти на незаконско постапување;
- **Безбедност/ обезбедување** (Security) е збир на мерки и активности, кои што претставуваат комбинација на човечки и материјални средсва, наменети за заштита од акти на незаконско постапување.

- **Безбедносна контрола** значи,примена на средства и методи, со кои може да се спречи внесување на оружје, експлозиви и други опасни направи, предмети и субстанци, кои можат да се искористат за извршување на незаконски дејствија.
- **Безбедносен преглед** значи примена на технички или други средства, кои се наменети за идентификување и /или откривање на забранети предмети,
- **Безбедносна анализа -** проценка на безбедносните потреби, вклучувајќи го и откривањето на чувствителните делови, кои можат да бидат искористени за извршување на дејство на незаконско постапување, и препораката за преземање на корективни активности.
- **Безбедносно ограничени зони**: Оние области кои се идентификувани како приоритетно ризични зони, а каде во дополнување на пристапната контрола, се применуваат други контроли.
- **Безбедносна проверка на лице** значи документирана проверка на идентитетот на едно лице, вклучувајки и било какво криминално досие, како дел од проценката на подобноста на едно лице за непридружуван пристап до безбедно ограничените зони,
- **Важечки стандард** е документ подготвен со консензус и усвоен од страна на признато тело, со кој, поради заедничка и повторлива употреба се обезбедуваат правила, упатства и карактеристики за определени активности или резултати од тие активности, чија цел е, постигнување најповолен степен на уредност во определено подрачје. Во случај на непостоење на домашен важечки стандард ќе се примени меѓународен;
- **Вредност на целта** е проценката колку објектот е значаен за остварување на крајните цели на терористите;
- **Демаркирана зона** значи зона која е оделена преку контрола на пристапот од безбедносно ограничените зони, или ако самата демаркирана зона е безбедносно ограничена зона, од други безбедносно ограничени зони,
- **Дејствија на незаконско постапување во воздухопловството**: Ова се дејствија или обиди за вакви дејствија со цел да се загрози цивилното воздухопловство и воздушниот транспорт, т.с.:
  - незаконско грабнување на воздухоплов во лет;
  - незаконско грабнување на воздухоплов на земја,
  - земање на заложници во воздухопловот или на аеродромите,
  - насилно влегување во воздухополов, на аеродром или во простории на воздухопловните објекти,

- внесување во воздухоплов или на аеродром на оружје, опасна направа или материјал, со намера да се употреби во криминални цели,
- соопштување на погрешни информации, со цел да се загрози безбедноста на воздухопловот во лет или на земја, или на патниците, екипажот, персоналот на земја или општата јавност, на аеродромот или во просториите на цивилните воздухопловни објекти.

- **ЕКИ (Европска Критична Инфраструктура)** значи критична инфраструктура, лоцирана во државите членки на Европската Унија, чие што оштетување или уништување би имало значајни последици во најмалку две земји членки. Значењето на последиците се оценува во услови на взаемни критериуми. Тоа вклучува и последици од меѓусекторските зависности меѓу други типови на инфраструктура.
- **Јавна зона** значи оние делови од објектот, соседниот терен и зградите или делови од нив, кои не се безбедно ограничени зони,
- **Контрола на пристапот** значи примена на средства, со кои може да се спречи влез на неовластени лица или неовластени возила, или на двете,
- **КИ- Критична Инфраструктура - според Директива** *114 од 2008 на ЕУ,* означува систем или негов дел лоциран во земјата членка, кој е од основно значење за виталните општествени функции, за здравјето, сигурноста, безбедноста, економската и социјалната добросостојба и чии што оштетување или уништување би имало значителни последици во земјата членка како резултат на неможноста да се одржат тие функции.
- **Критичност на целната локација** е користа што објектот или местото ја има за населението, за економијата или државата;
- **Капацитет на локацијата за луѓе** е можноста од масовни жртви врз основа на проценката на максималниот број на лица на локацијата во дадено време.
- **Објект од витално значење** е објект кој поради својата функција, политичко, безбедносно, економско, историско или културно значење, местоположба, престој или движење на голема маса луѓе би можел да биде цел на терористички напад или закана, а самото изведување на терористички акт врз ваков објект, би предизвикал тешки последици врз безбедноста на државата, животот, здравјето и имотот на граѓаните.
- **Ограничена зона** значи зоната за движење во објектот или соседниот терен и згради или нивни делови, до кои пристапот е ограничен,

- **Напад** Претставува директно или индиректно загрозување на работникот за обезбедување, на објектот, или на лицето што го штити,
- **Непосреден напад** претавува оној напад што трае или предстои,
- **Опасни материи** Материи или предмети кои можат да претставуваат значајна опасност, за здравјето, безбедноста или имотите,
- **Сопственици / оператори на ЕКИ** значат онисорганизаци одговорни за инвестирањето или одржувањето на определен елемент систем или негов дел согласно Директивата (ЕУ 114 2008).
- **Субјект**означува лице, организација или претпријатие, различно од оператор;
- **Забранети предмети** значи оружје, експлозиви или други опасни направи, предмети или супстанции, кои можат да се искористат за да се извршат дејствија на незаконито постапување, кое ја загрозува безбедноста,
- **Закана од штетни влијанија** е присуството на опасни материи, средства и оружје во објектот.
- **Заштита** значи сите дејствија, кои се превземаат за заштита на функционалноста, континуитетот и интегритетот на КИ,со цел откривање, спречување и неутрализирање на закана, ризик или ранливостм (ЕУ Директива 114/ 2008).
- **ПДЗ Екипа** тим за противдиверзиона Заштита. Се состои од посебно обучен перонал, ангажиран да изврши проверка (претрес) на одредени простори, објектии простории со задача да откриеексплозивни средства. Персоналот на ваквиот тим е обучен и има познавања во сверата на експлозивите,
- **Периметар** Замислена или обележана линија, која го одделува штитениот простор, имот, објект, од останатиот простор. Најчесто по должината на оваа линија се поставува ограда и за работникот преставува граница, во која ги применувазаконските овластувања.
- **Потенцијал за колатерална штета** е штетата што би можела да биде предизвикана врз околината и верижните последици од евентуален терористички напад.
- **ПДЗ контрола**: примена на технички или други средства наменети за идентификација и / или откривање на оружје, експлозиви или други опасни средства, предмети и субстанци кои можат да се користат за извршување на незаконски дејствија.
- **Техничка заштита** преставува континуирано набљудување и следење на состојбите на одреден простор / објект, со помош на електронско-технички средства и уреди

- **Узбуна поради бомба**. Состојба, која ја имаат прогласено одговорните тела, со цел, активирање на план за спречување или санирање на евентуалните последици од најава за бомба, анонимна или не, или последиците кои можат да настанат после откривање на сомнителна направа или друг сомнителен предмет.
- **Чуствителна информација поврзана со заштитата на КИ** значи информација поврзана со критичната инфраструктура, која ако се открие може да биде употребена за планирање или извршување на дејствија со цел оштетување или уништување на КИ.

4. Хипотези на истражувањето

Општа хипотеза

Со добрата организација, обученост на персоналот, воспоставување на напредни системи, правилни процедури и навремена реакција во случај на вонредни ситуации, предизвикани од акти на незаконско постапување, ќе овозможи ефикасност во менаџирањето со заканите, кои негативно влијаат врз безбедноста на објектите од витален интерес (критична инфраструктура). Исто така, правилното менаџирање ќе резултира со зголемување на нивото на безбедност на објектите од витален интерес, и на тој начин ќе биде постигнато унапредување, дополнување и зголемување на националната безбедност.

Посебни хипотези:

- Имплементацијата на современите безбедносни технологии и техники, со цел зголемување на нивото на заштита, ја намалува можноста од изведување на актите на незаконското постапување.

- Воспоставување на адекватни превентивни безбедносни мерки во развојот на обезбедувањето, од акти на незаконско постапување кај објектите од витален интерес (критичната инфраструктура) ја намалува ранливоста на објектот кој е предмет на заштита.

- Строгата примена на прецизни инструкции и процедури во обезбедувањето на објектите од витален интерес, ја зајакнува безбедноста и ги ублажува, колку што е можно, штетните ефекти.

- Правилна проценка на заканата, придонесува за избалансиран, соодветен и правилен развој на настаните.

- Спроведувањето на адекватна обука на персоналот за обезбедување, врз основа на карактеристиките на објектите од витален интерес – критична инфраструктура, ќе придонесе до зголемување на целокупната безбедност,

- Доколку на заканите се регира прерано и/или ако се реагира неадекватно, може да се предизвика штетен ефект на безбедноста и функционирањето на објектите од витален интерес.

- Ако безбедносниот персонал е запознаен со упатствата што се поврзани со ситуации кога постои закана, тогаш ќе постои и успех во справувањето.

- До колку пребарувањето на објектите од витален интерес, со цел за пронаоѓање на сомнителни експлозивни направи поради закана, го врши обучен персонал, тогаш се намалува опасноста од последиците кои би можеле да бидат фатални.

5. Варијабили во истражувањето

Во рамките на ова истражување, се издвојуваат следните варијабили:

- Ранливоста на виталните објекти која може да биде предизвикана од тероризам и други акти на незаконско постапување, како независни варијабили:
  - саботажа,
  - киднапирање,
  - анонимна закана
  - подметнат експлозив,
  - кражби,
  - индустриски шпиунажи,
  - диверзии,
  - природните катастрофи
  - злонамерни оштетувања
  - човечки пропусти
  - технолошки недостатоци и пропусти

- Влијанието врз националната безбедност, како зависна варијабила:

1. Безбедно функционирање на виталните објекти – критичната инфраструктура
2. Нормално одвивање на технолошките процеси односно намената на критичната инфраструктура

6. Методи и техники на истражувањето

Од методолошки аспект, ова истражување е насочено кон проценката на загрозеност на објектите од витален интерес (критичната инфраструктура) од акти на незаконско постапување и влијанието врз нормалното функционирање на државата.

Методите на истражување беа комбинирани и беше применет квантитативен и квалитативен пристап. Податоците за начинот на обезбедување, бројот на заканите, безбедносниот ризик, зачестеноста на заканите, беа обезбедени преку институциите, кои се задолжени за обезбедување на објектите од витален интерес.

Квантитативниот пристап опфати спроведување на научно мулти варијантна анализа, каде беа применети методолошки варијанти набљудување и интервју за собирање на податоци за безбедносната состојба, во која се наоѓаат објектите од витален интерес, учесниците во обезбедувањето, активностите кои се превземаат, како и резултатите.

Се изврши систематска постапка за собирање на објективни, прецизни, и сигурни податоци за појавите, кои беа предмет на анализа.

Квалитативниот пристап опфати собирање на реални податоци, која со некои извори на случаи самата открива и евидентира присуство на одредена содржина и ги утврдува нејзините квалитативни својства.

За идентификација на одредени аспекти од постоечката безбедносна состојба, беа користени принципите за прибирање на податоци за безбедноста и начинот на обезбедување на аеродромите во Република Македонија и другите објекти од витален интерес како и начините на обезбедување на критичната инфрастрктра и препорачаните практики во земјите од ЕУ,САД и Австралија.

Посебна примена во истражувањето најдоа следните методи:

Компаративниот методкој обезбеди, компаративен (споредбен) пристап меѓу анализираните содржини, во однос на анализите на безбедносните системи и процедури во различните објекти од витален интерес. Овој метод, всушност овозможува објективен, систематски и квантитативен опис на очигледната содржина.Суштински, сознајна улога на методот споредување, т.е. компарација се состои во тоа што, без споредување не е можно да се констатираат ниту сличностите, ниту, пак, разликите и спротивставеноста на својствата на појавите.

Анализа на содржината, се спроведе комбинирано со нормативните и законските акти.

Како методолошка постапка за анализа на податоците беше спроведена, муливаријантна методолошка постапка со примена на набљудување и интервју.

При оваа методолошка постапка, паралелно се собираа податоците по пат на сетилно восприемање со цел проширување на примарното искуство, стекнување на представа и сознанија за целината на настанот или појавата што се набљудува и нејзино разбирање, како и проверка на одредени искуствени податоци, добиени или создадени со други методолошки постапки или извори кои настанале од практични потреби.

Според начинот на кој се вршеше набљудувањето беше непосредно (директно) набљудување, според времето на набљудување тоа беше етапно, а според бројот на набљудувани случаи беше масовно.

Со интервјуто, како методолошка постапка, се дојде до искуствени податоци, по пат на вербално комуницирање помеѓу интервјуерот и интервјуираните лица во случајов со носителите на активностите за обезбедување на објектите од витален интерес.

За потребите на истражувањето се собираа објективни и проверливи податоци за загрозеноста и обезбеденоста на објектите од витален интерес во Република Македонија. За овие потреби беше изготвен прашалник. Беа спроведени интервјуа со повеќе од 30 испитаници (раководители на сектори и служби), а исто така се спроведуваа и разговори со непосредните извршители на работните обврски поврзани со обезбедувањето, со цел да се изврши компарирање на податоците. Анализата, обработката и донесувањето на заклучоци, од овој дел на истражувањето, претставуваа добра основа за понатамошни постудиозни проучувања, а исто така ианализа на ефективноста од примената на напредните системи и процедури, во поглед на безбедноста.

7. Просторно и временско определување на истражувањето

Квантитативното истражување се спроведе на аеродромот Александар Велики – Скопје, аеродромот Св. Апостол Павле – Охрид, Термоелектраната РЕК Битола, Хидроелектраната Глобочица, Меѓуопштинското претпријатие за водоснабдување Проаква - Охрид, Рафинеријата ОКТА и други објекти од витално значење во Република Македонија – критична инфраструктура, согласно планот и опфати набљудување на тековните активности и интервјуирање на директните учесници во

обезбедувањето. Беше разгледана целокупната архивска документација и евиденција, која се води од аспект на безбедноста и извештаите, кои ги карактеризираат настаните поврзани со безбедноста.

Активностите од истражувањето беа спроведени во период од 2 години. А, беше употребувана однапред подготвена чек листа.

ГЛАВА II

Витални објекти

(критична инфраструктура)

1. Општо за виталните објекти

Безбедноста на луѓето, како уставно загарантирано право, несомнено зависи од повеќе фактори, вклучувајки ги ивиталните објекти и инфраструктурите кои во суштина, преставуваат движечка сила на современите и ефикасни општества. Давањето на значење ,,критичност" на определени инфраструктури, пред се, тргнува од потребата да се обезбедат виталните функции на државатаи да се обезбеди стабилна меѓузависност помеѓукритичните инфраструктури во општествениот живот. Важноста на заштитата на критичната инфраструктура посебено е видлива по терористичките напади од 11 Септември 2001 година, каде уште еднаш се потврди потребата за подобра безбедност на критичните инфраструктури[1]

Поради промената на општествените случувања и тензиите кои ги носи брзиот технолошки развој, одделни општества се затекнати неподготвени за справување со новата глобална безбедносна ситуација. Традиционалните национални капацитети и механизми повеќе неможат да бидат ефективни во фазата на справување со новите безбедносни закани од причина што денешното модерно општество во целост зависи од технологиите, така штодржавата станува се поранлива на ризиците и заканите во поглед на функците на критичните инфраструктури. Оттука оние инфраструктури кои 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 биджат третирани како на национално така и на меѓународно ниво[2].

Националната критичната инфраструктура е столбот на секоја држава затоа што таа се поврзува со националната безбедност, економијата, индустријата и здравјето на граѓаните[3]. За граѓаните во основа тоа е електричната енергија која ја користат во своите домови, водата која 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, кои се од витално значење за државата и нивното онеспособување и

[1] National critical infrastructure protection – regional perspective- Belgrade, December 2013 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, str 203.
[2]http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html,Преземено 14.03.2014
[3]http://www.dhs.gov/what-critical-infrastructure Преземено на 26.03.2015г.

уништување, ќе предизвика ослабувачки ефект на безбедноста на државата, националната економска сигурност, јавното здравје, јавната безбедности сл.[4]

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

2. Витални објекти наспроти критична инфраструктура – синергија или дијалектика

Различни земји ја дефинираат критичната инфраструктура на различен начин, но на крај генерално,најчесто секогаш се сведува на инфраструктура, системи и ресурси кои се од витално значење за општеството. Концептот, безбедност на критична инфраструктура, претставува се поексплоатиран безбедносен термин кон една релативно ,,нова" безбедносна дисциплина, диференцирана со свои специфики во однос на останатите безбедносни гранки.

На прашањата: Што преставува ,,критична инфраструктура"?и како до соодветна заштита на истата?,одговорот се врзува со инфраструктура и области кои се сметаат од толку голема важност за функционирањето на современите општества, така што нејзината неисправност или уништување ќе резултира со постојани пореметувања во целокупниот систем. Токму поради тоа, терминот ,,критична инфраструктура" се прифаќа во сите подрачја, како во науката така и во праксата и продираат во

[4]http://www.morm.gov.mk Славески С. Предизвик на современите општества, Преземено 30-05-2015

терминолошката конверзација која е се поприфатлива во сите држави. Од аспект на нејзината заштита,критичната инфраструктура е сама по себе многу сложена и тешка активност која несомнено предизвикува голем интерес за проучување на безбедноста на критичните инфраструктури како одраз на се поголемото значење на неговата улога во општеството. Оттука поимот ,,витален" може да се замени со поимот ,,критичен",посебно во сферата на дејностите кои се во директна корелација со цивилниот сектор и потребите за нормално функционирање на современото општество.

Фактот дека постои се поголемата зависност на современиот живот од се посложените инфраструктури наметнува потреба од поголемо внимание по однос на прашањата поврзани со обезбедувањето и безбедноста во целост и во тој контекст потребно е да се откријат слабостите, да се намали ранливоста, да се ублажат последиците од загубите на критичните инфраструктури, со поврзување на бизнисот, науката и безбедноста преку интердисциплинарни проекти.[5]

Опасностите кои следат современото општество низ призмата на критичните инфраструктури бара перманентно, стручно и професионално спротивставување на заканите, применувајќи мерки и активности за јакнење на безбедносните капацитети на државата, вклучувајќи ја и приватната безбедност како составен сегмент во системот за национална безбедност.Заедничкото делување, институционалната соработка и координираноста во полето на безбедносните активности го прави синергичниот пристап доминантен кога се во прашање критичните инфраструктури пред се поради комплексноста на областите, интердисциплинарноста и сложеноста во кои функционира критичната инфраструктура.Затоа, кога станива збор за Безбедноста на виталните објекти - критична инфраструктура и последиците од нивната нефункционалност, без сомнение имплицира потреба од еден посебен концепт на системски пристап кон развивање на безбедноста во целост.

3. Поим, значење и дефинирање на виталните објекти - критични инфраструктури

Генерално, постојат повеќе размислувања за тоа што е критична инфраструктура. Како општо прифатена дефиниција за критична инфраструктура во рамките на Европската Унија е претставена во Директивата 114 од 2008 година. Тука, Европската

[5] Matka D. Energetska sigurnosti kri čna infrastruktura –pregled rezultata istraživanja Zbornik radova: Krajcar, S. (ur.)(2009.), Energetska sigurnost i kri čna infrastruktura, Sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb.

Комисија ја дефинира критичната инфраструктура, како систем или негов дел лоциран во земјата членка кој е од основно значење за виталните општествени функции, здравјето, сигурноста, безбедноста, економската и социјалната благосостојба и чие што оштетување или уништување би имало значителни последици во земјата членка како резултат на неможноста да се одржат тие функции[6].

Анализирајќи ги сите аспекти кои ги детерминираат критичните инфраструктури, а имајќи ги предвид сложеноста, динамичноста и специфичноста која ја третира оваа област, несомнено најчесто тие претставуваат физички средства, мрежи или организации, чие нарушување или оневозможување ќе предизвика сериозна, трајна штета на општествениот и економскиот живот. Различните национални власти имаат подготвено листи на стопански гранки, односно сектори кои се опфатени со оваа дефиниција. Тие обично вклучуваат енергија, вода и храна, управување со отпад, клучните транспортни системи (аеродроми и железници), финансиски институции, здравството, државните институции за справување во вонредни ситуации и др.[7] Оттука произлегуваат и начините на нивното обезбедување и заштита. Во повеќето земји тоа преставува мешавина на државните органи (полиција, специјализирани заштитни сервиси и повремено војската), компании за приватно обезбедување и други служби и сервиси.[8]

Како важен критериум на проценката е критичноста како релативна мерка за значењето на дадената инфраструктура во однос на влијанието врз снабдувањето, односно обезбедување на општеството со важни стоки и услуги, можат да бидат преставени како:

- инфраструктури во врска со нивните технички, структурни и функционални особености, се класифицираат како од витално значење (апсолутно суштинско значење) - технички основна инфраструктура;
- витално значење (апсолутно суштинско значење) како социо-економска инфраструктура.[9]

Со цел квалитетно дефинирање, контролирање и развивање на критичните инфраструктури потребен е институционален пристап, кој ќе ја преземе одговорноста во својство на стратегиска рамка,пред се поради новите интеграции на државите но и поради новите технолошки достигнувања кои на големо ги менуваатгледиштата кога

[6] Директива наЕУ2008/114/23.12.2008 EN Official Journal of the European Union L 345/75"
[7] Critical Infrastructure Security and Protection The Public-Private Opportunity- White Paper and Guidelines by CoESS And its Working Committee Critical Infrastructure December 2010 str. 5
[8] Ibid., p.6
[9] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of GermanyFederal Ministry of the Interior Berlin, 17th June 2009, p.7

се во прашање критичните инфраструктури. Мораме да земеме во предвид дека технолошкиот развој го промени начинот на работење, управување и водење на политика, па оттука и концептите за водење на националната и јавната безбедност потребно е да се прилагодат на новите услови Исто така, технологијатастана се поевтина, пософистицирана и се подостапна што ја трансформира во потенцијално опасен инструмент, кој е тешко да се следи[10]. Поради тоа, потребно е да се создадат предуслови за намалување на ризиците од негативните активности и последици на критичните инфраструктури континуираното дејствување на институциите затоа штокако последица можат да имаат крајно штетно влијание на одбранбената и економската безбедност на државата.[11]

Со примена на разновидни информации и знаења, кои може да се најдат во повеќе извори, на пример: академски трудови, регулативи, програми за безбедност, печат, проценки, студии на случај, концептуални модели, лични сведоштва, мислења во социјалните медиуми, истражувања и анкети, етнографски студии и друго, како главни цели во дефинирањето изаштитата на критичната инфраструктура низ призмата на Европските стратегии се пфреставени:

- идентификување на релевантните (тековните и новите) сектори на инфраструктурите. Во релевантни сектори водени според Зелената книга на Европската комисија (2005) се: енергија, нуклеарната индустрија; информации и комуникациски технологии; вода; храна; здравјето на луѓето; финансии; транспорт; хемиската индустрија; истражувачки капацитети, како и надополнување на листата по основ на резултатите од европските дебати за тоа каков тип на инфраструктура може да се смета за нов, за ,,критична", која вклучува управување со отпади; управување со кризи и кризен менаџмент; националните симболи и др.
- идентификација на зависностите како и ланците на снабдување;
- истакнување клучните улоги во ЕУ, регулаторни елементи и влијанијата на егзогените закани;
- давање на приоритети по основ на: специфични закани, проценки на ризик разни сценарија и други користени методи и предвидувања во функција за потребите на безбедноста;

[10]Методологија избора критичне информатичке инфраструктуре – Министарство за информационо друштво и телекомуникације Црне Горе, 2014.
[11]Методологија избора критичне информатичке инфраструктуре – Министарство за информационо друштво и телекомуникације Црне Горе, 2014, стр 6.

- препознавање на постојните политики и оперативните практики, кои ја градат отпорноста во системите под нормални услови;
- развивање на дискусии за потребите и правилата за оперативност на системите во услови на вонредни и критични ситуации;
- концепирање на услови за работа на ЕУ во функција на носење на стратешки одлуки;
- обезбедување на главни ресурси и клучни дефиниции поврзани со големи теми поврзани со заштита на критичната инфраструктура и снабдувачките капацитети;
- обезбедување на различни чинители, посебно групи за во иднина, со сет на податоци и информации за развивање на идни сценарија.[12]

Комплексноста на кризните ситуации, посебно фактот дека можат да бидат загрозени и критичните инфраструктури и нивните капацитети кои се од огромно значење за функционирањето на државата, наметнаа потреба голем број на држави да развијат свои активности кои имаат за цел:

- Дефинирање на елементите на критичност и ранливост на различните инфраструктури;
- Дефинирање на мерките за смалување на ранливоста;
- Воспоставување на планови за кризни и вонредни состојби и послекризно опоравување;
- Потик за развој кај јавните и приватните оператори во поглед на заштитата на критичната инфраструктура;
- Подржување на меѓународната соработка[13];

Во истиот контекст, а во поглед на мерките за заштита на критичната инфраструктура, државите треба да утврдат редослед и постапки за:

- Идентификација на критичната инфраструктура;
- Изработка на карти – мапи на критичните инфраструктури;
- Размена на информации;
- Оспособување на лицата кои се ангажирани во критичните инфраструктури;
- Вежбовни активности за заштита на критичните инфраструктури и опоравување од кризни и вонредни состојби и сл.[14]

[12]D5.1 – Problem space report: Critical infrastructure & supply chain protection Cross-border Research Association (CBRA)January, 2012,P.11

[13]Jakovljević V., Gačić J. Zastita kriticne infrastructure u kriznim situacijama - Medunarodna naucna konferencija Menadzment 2012 Mladenovac, Srbija, 20-21. april 2012

Исто така потребно е да се откријат слабостите, за да се намали ранливоста и за да се ублажат последиците од загубите на критичните инфраструктури. Тоа може да се постигне со поврзаност на бизнисот, науката и безбедноста преку интердисциплинарни проекти.[15]

Од изнесеното може да се заклучи дека, определувањето на критичните инфраструктури не само што го прават безбедносниот апарат да биде по ефектен, туку и го прават поефикасен и поодговорен како во внатрешната така и во надворешната безбедност пред се во поглед на градење на адекватни безбедносни стандарди поткрепени со домашни и меѓународни практики и регулативи.

4. Терминолошки дивергенции околу поимот и улогата на терминот критична инфраструктура

Терминот ,,критична инфраструктура" е релативно нов израз, кој во голема мера ги заменува долго експлотираните називи кои што беа применувани во повеќе држави. Тие најчесто беа именувани како: витални објекти за функционирање на државата, материјално техничка база на државата и сл.

Комплексноста на овој безбедносен концепт, доаѓа од потребата за имплементација на голем број мерки и активности, кои навлегуваат во различни струки и дејности, а сето тоа обединето во рамките на безбедноста.

Истражувањето кое е направено за потребите зазаштита на критичната инфраструктура и синџирот на снабдувањепретставено во табела бр.1 дава еден сублимат на дефиниции кои се применуваат во повеќе држави.

[14]Jakovljević V., Gačić J. Zastita kriticne infrastructure u kriznim situacijama - Medunarodna naucna konferencija Menadzment 2012 Mladenovac, Srbija, 20-21. april 2012 str 282 – 283.

[15]Dario Matka Energetska sigurnosti kri čna infrastruktura –pregled rezultata istraživanja Zbornik radova: Krajcar, S. (ur.)(2009.), Energetska sigurnost i kri čna infrastruktura, Sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb.

РЕПУБЛИКА ЧЕШКА	,,Критична инфрструктура" е инфраструктура неопходна за нормално живеење како и за вонредни и критични ситуации. Составена е од: систем за снабдување со електрична енергија, вода, канализација, транспортна мрежа, комуникациски и информациски систем, банкарски и финансиски сектор, службите како што се: полицијата, против пожарната служба, здравство, основни услуг (снабдување со храна, комунални услуги, социјални услуги и сл.), индустрија и земјоделие, државната, регионалната и локалната администрација. (Czech Republic, 2002)
АВСТРАЛИЈА	,,Критичната инфраструктура" е дефинирана со оние физички капацитети, системи за снабдување, информациски технологии и комуникациски мрежи кои ако се уништат оштетат или онеспособат за подолг период би имале значително влијание врз социјалниот живот и економската благосостојба на нацијата или би ја нарушиле способноста на Аустралија да ја раководи националната безбедност и да обезбеди сигурност. (Australian National Security)
КАНАДА	,,Канадската критична инфраструктура" се состои од оние физички капацитети, системи за снабдување, информациски технологии и комуникациски мрежи кои ако се уништат оштетат или онеспособат, би имале сериозни последици здравјето сигурноста, безбедноста и економската благосостојба на Канаѓаните или на ефективното функционирање на владата на Канада. (Public Safety Canada).
БУГАРИЈА	,,Критична инфрструктура" Систем на објекти, услуги и информациски системи, чие откажување или уништување би имало сериозно негативно влијание по здравјето и безбедноста на популацијата, животната средина, националната економија или на ефективно функционирање на владата. (Закон за справување со кризи). Друг извор ја нагласува критичната инфраструктура како компонента, систем или нивни делови кои се неопходни за одржување на виталните општествени функции здравјето, сигурноста и безбедноста, економски или социјални благосостојби и онеспособувањето или уништувањето би имало значителни последици за Р. Бугарија. (Ordnance18: on the establishment and designation of European Critical Infrastructures in Bulgaria and measures for their protection, 2011).
ХРВАТСКА	Национална критична инфраструктура ги има дефинирано составите, мрежите и објектите од национална важност, чие прекинување или престанок на испорака на роба или услуга која може да има сериозни последици по националната сигурност, здравјето и животот на луѓето, имотот, околината, безбедноста и економската стабилност и непречено функционирање на власта. (Закон за критичната инфрструктура,, 2013 год).

ГЕРМАНИЈА	,,Критична инфраструктура" се организации или објекти од витално значење за општеството, чие откажување или оштетување би предизвикало значително намалување во снабдувањето, нарушување на јавниот ред или други сериозни (драматични) последици. (Федерална канцеларија за информации и безбедност).
ХОЛАНДИЈА	,,Критичната инфрструктура" се однесува на, продукти, услуги и придружни процеси кои, во случај на оштетување или онеспособување, може да предизвикаат големи социјални нарушувања. Ова може да биде во форма на значителни жртви и огромна економска штета.. (Министерство за Внатрешни работи 2005).
ВЕЛИКА БРИТАНИЈА	,,Критична национална инфрструктура" ги вбројува оние средства, услуги и системи кои го подржуваат социјалниот, економскиот и политичкиот живот и чие значење е такво што при нивно уништување може: да предизвика жртви, да има сериозно влијание врз националната економија, да има други социјални последици или да стане главна грижа на владата. (Биро за безбедност на Велика Британија)
САД	,,Критична инфрструктура" се системи и средства, физички или виртуелни, толку значајни за САД што нивното онеспособување или уништување би имало значително влијание на безбедноста. (Department of Homeland Security , 2006).

Табела бр 1 : Problem space report: Critical infrastructure & supply chain protection[16]

Од анализата на терминот ,,Критична инфраструктура"посматрано низ потребата од нејзина адекватна заштита, заклучено е дека постојат мали разлики во националните дефиниции на државите, имено во основа се истакнуваат системите, средствата, имотите, услугите, продуктите и сл. кои се клучни за нормално функционирање на државата во поглед на економските, социјалните, здравствените и безбедносните потреби.

[16] FOCUS D5.1 – Problem space report: Critical Infrastructure & Supply Chain Protection - Cross-Border Research Association (CBRA) January, 2012.

Дивергенциите кои се појавуваат околу терминот критична инфраструктура се однесуваат пред се поради спецификите поврзани со географската поставеност на државите, политичко социјалните услови, техничко технолошкиот развој, природните богатства, економските параметри, безбедносните состојби и слично, кои во голема мера ги детерминираат и стратегиите за националната безбедност како важен приоритет на секоја држава.

5. Потреба од заштита на критичните инфраструктури

Секој сектор од критичната инфраструктура има уникатни карактеристики, оперативни модели и профили на ризик, кои имаат институционално значење и специјализирана експертиза во врска со наведениот сектор.[17]

Што се однесува до заканите за критичната инфраструктура, тие можат да бидат вештачки, како резултат на тероризам или други криминални активности, но можат 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.[18]

Можни методологии кои помагаат во идентификацијата на неопходните капацитети потребни за да се соочиме со посебни 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 во предвид ги земаат идните трендови. 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;
- проценка на ризикот: потребно е да се создаде листа на постоечки веродостојни ризици, во зависност од потенцијалните ризици во однос на нивната кауза, природата, потенцијални цели, како и оценка на влијание.[19]

---

[17] Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013

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

[19] National critical infrastructure protection – regional perspective- Belgrade, December 2013 UDC726.9:75.041.5 ID176374796, M. Marjanović I. Nađ: Assesment of threats to critical infrastructure facilities from serious and organized crime, p. 78.

Може да се каже дека корпоративната безбедност како една од важните процеси во организациите, има значајна улога во делот нафункционирање на ситемите.Стратешкото планирање и оперативните мерки кои произлегуваат од истото, мора да обезбедат одговори на голем број загрозувања и ризици со кои се соочуваат компаниите посебно во сегментот кој се нарекува критична инфраструктура. На тој процес потребно е да се посвети многу повеќе внимание и свесност на ниво на највисок менаџмент во компаниите[20]. Клучните кадри, на полето на корпоративната безбедност, мораат да ги завземат едни од доминантните позиции пред се поради зависноста на државатаод овие компании во областите детерминирани како критична инфраструктура. Државите се одговорни за заштита на јавноста и обезбедување на одредено ниво на социјалната функционалност и безбедност, но фактот дека дел од критичната инфраструктурата 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 наметнува потреба од еден мулти вариантен пристап на државата и операторите. Многу западни земји го имаат поголемиот дел од критичните инфраструктури во приватна сопственост, а државата со цел да се обезбеди непречено работење и функционирање на критичните инфраструктури - вложува големи напори во соработката на државните структури и приватни лица.[21]

Во Германија четири петтини на критичната инфраструктура се во приватни раце [22]. 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[23].

Што се однесува во однос на потребата од заштита на критичните инфраструктури во ЕУ, потребно е да се спомене дека Унијата својата безбедност ја насочува и кон соседите, затоа што негативните последици од уништување или онеспособување на критичната инфраструктура може да биде взаемна, од тие причини потребно е да се постигне стандардизирано ниво на безбедност на критичните инфраструктури кои ќе го минимизираат ризикот од пореметување на нормалните функции на државите

[20]http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja - Denis Caleta - Kritična infrastruktura i značaj osiguravanja njenog neprekidnog djelovanja, Превземено на 17.09.2015г.

[21]National critical infrastructure protection – regional perspective- Belgrade, December 2013 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.

[22]http://www.bmi.bund.de/EN/Topics/Civil-Protection/Critical-Infrastructure-Protection/critical-infrastructure-protection_node.html 2015г.

[23] P. Auerswald, L.M. Branscomb, T.M. La Porte, E.Michel – Kerjan – The Chalenge of Protecting Critical Infrastructure – issues in science and tehnology FALL 2005 p. 77

членки на Унијата. Генерално гледано тоа се остварува преку соработка во различни форми и концепти на надворешната соработка но примарно фокусирано конпоради глобалната поврзаност на одредени сектори, кои бараат по различен пристап, дијалог и размена на најдобрите практики.

Ако ја разгледаме потребата од заштита на критичната инфраструктура во САД, преку управувањето со ризици ќе видиме дека таа е многу широка и составена 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 сајбер закани врз критичната инфраструктура бара интегриран пристап во поглед на:

- идентификување, спречување, откривање, и подготовка за закани и опасности на критичната инфраструктура;
- намалување на ранливоста на критичните средства, системи и мрежи; и
- ублажување на можните последици од инциденти или негативни настани кои се случуваат врз критичните инфраструктури[24].

Успехот на овој интегриран пристап зависи од целиот спектар на способности, експертизи и искуства во инфраструктурите и придружните засегнати страни.[25]

Во Директивата на САД што ја третира оваа област ги идентификува енергетиката и комуникацискиите системи, како уникатни критични инфраструктури, поради поврзаноста со функциите кои ги обезбедуваат во сите критични сектори.

Сојузниот пристап се води низ три стратешки императиви:

1. насоченост кон јасни функционални односи низ Сојузната влада за унапредување на националното единство и зајакнување на безбедноста и флексибилноста на критичната инфраструктурата;
2. овозможување на ефикасна размена на информации со идентификување на основните податоци и системи за Сојузната влада; и
3. да се спроведе имплементацијата и интеграцијата на анализите,низ операциите за донесување на одлуки, поврзани со критичната инфраструктура[26].

За ефикасна имплементација на Директивата се бара национално единство и напор во согласност со стратешките насоки од секретарјатот за национална безбедност. Националните напори вклучуваат експертиза и од специфични секторски агенции, како и специјализирани или поддршката е овозможена од другите федерални

[24] NIPP 2013 Partnering for Critical Infrastructure Security and Resiliencehomeland security - USA
[25] Ibid, p. 7
[26] Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013

министерства и агенции, како и силна соработка со сопствениците на критичните инфраструктури и оператори.

И покрај тоа што во САД и ЕУ постојат различни ставови по однос на ризиците и заканите кои можат да ја загрозат општата безбедност на нацијата и критичните национални добра, набрзо е формирано заедничко определување на две нивоа кои се дефинирани:

- кои ресурси преставуваат критична инфраструктура,
- кои мерки се потребни за нивна заштита[27]

Во процесот на идентификација на критичните инфраструктури ЕУ низ критериумот разгледуван преку (ang. cross-cutting) се темели на три фактори а тоа се:

1. човечки загуби, во кој се проценува потенцијалниот број на човечки загуби или повреди;
2. економскиот ефект, се проценува значението и големината на економските загуби и или деградација на производите или сервисите вклучувајки ги и негативните ефекти врз човековата околина;
3. друштвениот ефекти, се проценуваат ефектите на јавната самодоверба, физичката загриженост и пореметување во секојдневното живеење, вклучувајки ги и основните сервиси.[28]

Со оглед на големиот број на критични инфраструктури, се појавуваат значителни предизвици и тешкотии во остварувањето на заштитата, а тука како по карактеристични би нагласиле:

- 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 на аеродроми, морски пристаништа, голем број мостови и слични структури.
- недостаток на надлежност и одговорност во секторите каде што се ангажирани повеќе државни и приватни институции;
- недоволна размена на информации меѓу институциите , што доведува до нова ранливост и влијае на ефикасноста на одговорите за заштита на критичната инфраструктура;

[27] Zastita kriticne infrastructure I osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ESMirko ŠkeroBezbedno-informativna agencijaVladimir AteljevićVlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrane стр.197

[28]Metodologija izbora kriticne informaticke infrastructure , Ministarstvo za informaciono društvo Itelekomunikacije Crne Gore - Oktobar 2014 str. 8

- сложеност на знаење во поглед на голема количина на посебни вештини кои треба да се познаваат и пред политиките и пред стратегиите во областа на заштитата на критичната инфраструктура;
- меѓузависноста на одделните сектори на критичната инфраструктура. Овој проблем дополнително влијае на комплексноста на заштита на критичната инфраструктура;
- несовршеноста на алатките за анализа на критичната инфраструктура и неговата ранливост. Науката обично се фокусира на општите пристапи, алатки и решенија.
- асиметричните конфликти и сл.[29]

Визијата и мисијата зависи од постигнувањето на целите, кои претставуваат стратешка насока кон кои критичните инфраструктури треба да се фокусираат:

- проценка и анализа на заканите, ранливоста и последиците на критичната инфраструктура и информирање поврзани со управување со ризик;
- безбедна критична инфраструктура од човечки, физички и сајбер закани преку одржлив ризик, од аспект на трошоци и придобивки од инвестициите за безбедност;
- подобрување на отпорноста на критичната инфраструктура со минимизирање на штетните последици од инцидентите преку однапред планирање и ублажување.
- споделување на релевантни информации во критичната заедница за да се изгради свест и да им овозможи донесување на одлуки; и
- едукација и вежби за време и по инцидентите ситуации[30]

6. Индикативна листа на критичната инфраструктура

Голем број држави имаат направено прецизна спецификација на критичните инфраструктури, генерално земено, тоа се исти или слични сектори, кои се повторуваат во голем број држави со надополнување на оделни специфични сектори, карактеристични за ,,посилните" држави.

Во наведената индикативната листа на водечките земји во светот, како критични инфраструктури се претставени на следниот начин:

[29] Prezelj, I., Konceptualna opredelitev kritične infrastrukture,FDV, Ljubljana, 2008. str. 13. - National critical infrastructure protection – regional perspective- Belgrade, December 2013 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.

[30] Исто стр 11.

Во Канада индикативната листа вклучува: енергија (објектите на електрична и нуклеарна енаргија, природен гас и нафта, производни и транспортни системи), комуникации, сервиси (финансии, дистрибуција на храна, јавно здравство, транспорт (воздушен, морски и копнен), безбедност – сигурност (нуклеарна сигурност, служби за спасување, итни служби), влада (важни владини објекти, служби и информатички состави и мрежи).

Во Велика Британија листата се однесува на: енергија, телекомуникации, здравствените служби, финансиите, транспорт, итни служби, средишна власт, вода и одводни системи. Додека во Австралија спаѓаат: енергија (гас, нафта и производи од нафта, производство и дистрибуција на електрична енергија), комуникации (телекомуникации: тел, 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 дистрибуривни центри), Владини служби (објектите на одбраната, и безбедносни служби), Парламент, важни министерства, странски дипломатски и преставништва и резиденции, хитните служби (полиција, противпожарни, медицински и други служби), услуги (вода, одводување и прочистување на отпадните води), производство (војна, тешка и хемиска индустрија), Национални вредности (градежни, културни, спортски и туристички вредности).

Примерите во САД, Германија, Шведска, Холандија итн. немаат некои поголеми сигнификантни разлики во листата. Така, во **САД** листата вклучува: енергија, информации и телекомуникации, јавно здравство, храна, земјоделство, банкарство и финансии, службите за хитна помош, власт, основна одбрамбена индустрија, вода, хемиска индустрија и опасни материи, пошти и достава на роба, а во **Германија:** енергија (електрична, нафта и гас), телекомуникации и информатичка инфраструктура, јавно здравство (вклучувајки и снабдување со вода и храна), банкарство, финансии и осигурување, транспортни системи, хитни и спасувачки служби, Власт и јавните служби (вклучувајки: 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, друштвени вредности.

Во **Норвешка** листата вклучува: енергија и објекти, снабдување со нафта и гас, телекомуникации, јавно здравство, банкарство и финансии, транспорт, спасувачки служби, одбрана, полиција, јавна безбедност, во **Холандија:** енергија и 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 вклучува: објекти и служби, телекомуникции, дистрибуција на информациите, јавно здравство, храна, финансии, транспорт, цивилна одбрана, администрација, војна одбрана, снабдување со вода, социјална безбедност, индустрија, истражување и образование.[31]

Врз основа на целокупните анализи околу поимот и терминот ,,критична инфраструктура" разгледуван низ призмата на безбедноста и понудените индикативни листи за критични инфраструктури од западната провиненција, а водејќи се пред сè по насоките дадени од страна на Европската Унија може да кажеме дека: Критична инфраструктура преставуваат објекти, уреди, инсталации, продукти, услуги и сите системи кои се во директна или индиректна поврзаност со нормалното функционирање на државата така што нивното откажување би предизвикало сериозни последици врз националната безбедност, економија, здравството, функционалноста на државниот апарат, социјални или друг вид на последици.

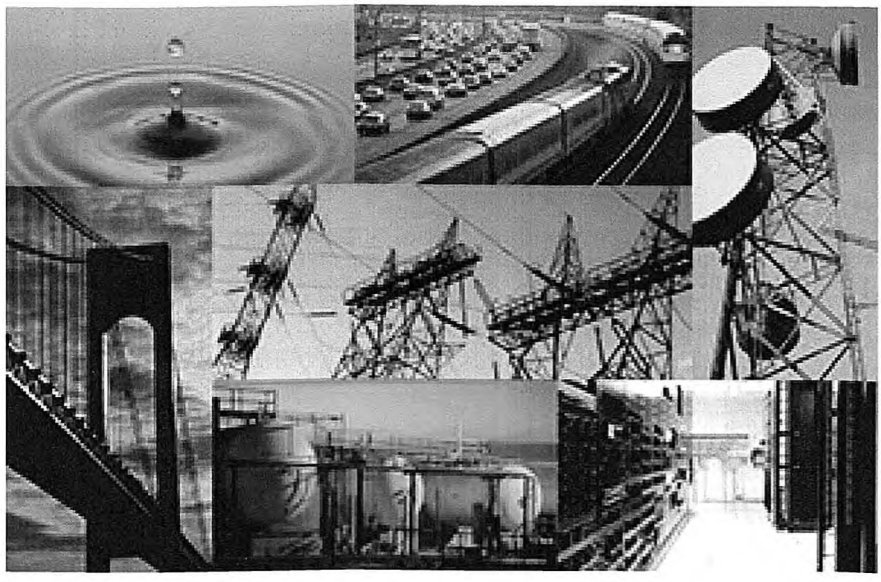
Во тој контекст како области во целост би ги прифатиле идентификуваните области од страна на Европската комисија а тоа се: енергијата, информациските и комуникациските технологии, водата, храната, финансиите, јавната и законската заштита, јавната администрација, транспортот, хемиската индустрија, истражувачките дејности[32], со сите нивни капацитети и дејности, производи или услуги.

[31]Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljamaZdenko Kljaic, dipl.ing. Member, IEEE, Sadko Mandžuka, dr.sc. Member, IEEE, Pero Škorput, mr.sc. Member, IEEE 18. Telekomunikacioni forum TELFOR.

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

ГЛАВА III

Области и објекти од витален интерес – критична инфраструктура со осврт на воздухопловството



1. Општи претпоставки

Секоја критична инфраструктура има силно влијание во одредени функции на современото општество. Идентификуваните области и објекти од витален интерес – критична инфраструктура,претставен од страна на Европската комисија прикажан во Табела бр.2, ја има комплетирано индикативната листа за секторите од критичната инфраструктура, вметнувајќи големо значење на заштита на критичната инфраструктура за многу функции на соврменото општество. критична инфраструктура,претставен од страна на Европската комисија прикажан во Табела бр.2, ја има комплетирано индикативната листа за секторите од критичната инфраструктура, вметнувајќи големо значење на заштита на критичната инфраструктура за многу функции на соврменото општество.

СЕКТОР	ПРОИЗВОД ИЛИ УСЛУГА
1. ЕНЕРГИЈА	• Производство на нафта и гас, рафинирање, одржување и чување, вклучувајќи и водови • Производство на ел. енергија • Пренос на ел енергија, нафта и гас. • Дистрибуција на ел енергија, нафта и гас.
2. ИНФОРМАЦИСКИ И КОМУНИКАЦИСКИ ТЕХНОЛОГИИ	• Заштита на информациските системи и мрежи • Инструментализација, автоматизација и контролни системи. • Интернет • Обезбедување на фиксната телекомуникација • Обезбедување на мобилната телекомуникација • Радио комунукација и навигација • Сателитска комуникација • Емитување
3. ВОДА	• Обезбедување на вода за пиење • Контрола на квалитетот на водата • Контрола на количество на вода
4. ХРАНА	• Снабдување со храна, обезбедување и заштита на храната
5. ФИНАНСИИ	• Платежни сервиси и структури • Владини финансиски структури
6. ЈАВНА И ЗАКОНСКА ЗАШТИТА	• Одржување на јавен ред и мир, обезбедување и безбедност • Судска администрација
7. ЈАВНА АДМИНИСТРАЦИЈА	• Владини функции • Оружени сили • Цивилна администрација • Служби за хитни ситуации • Пошти

8. ТРАНСПОРТ	• Патнички сообраќај • Железнички • Воздушен • Внатрешен воден сообраќај • Океански и морски сообраќај
9. ХЕМИСКА И НУКЛЕАРНА ИНДУСТРИЈА	• Производство, чување и процесирање на хемиски и нуклеарни супстанции • Дистрибуција на опасни матери (хемиски супстанции)
10. ПРОСТОР И ИСТРАЖУВАЊЕ	• Простор • Истражување

Табела бр2 . Дефинирани сектори во Европската критична инфраструктура[33]

2. Енергетика

Енергетиката е основа на сите фундаментални процеси за функционирање на современото општество. Долгорочното, односно долготрајното нарушување на овој систем би довел 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. [34]

Менаџирањето со безбедносните ризици според принципот за превенција од штети и загуби како и задржување на висок степен на општествена одговорност е од есенцијална важност.Енергетскиот сектор има потреба да биде уреден со соодветна безбедносна политика и стандарди.Затоа, аво контекст на обезбедувањето на критичните инфраструктури, потребно е да се воспостави еден поширок опсег на заштита, не само во делот на физичката и техничката заштита, туку и во целосниот безбедносен систем кој е законски регулиран со адекватна безбедносна политика во сите области.[35]

Важен аспект на заштитата на критичната инфраструктура е разбирањето на концептот за енергетска безбедност, кој 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

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

[34]http://www.dhs.gov/energy-sector - преземено Јануар 2016

[35]Milan Vrsec: 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, p.125

енергетска безбедност. Фактот што енергетската безбедност е комплексен концепт, обично Европската Унија годели на долгорочна безбедност (стабилна енергетска политика во ЕУ како и помеѓу ЕУ и земјите снабдувачи) и краткорочна безбедност (градење на способност да се избегнат нарушувања во снабдувањето со енергија во вонредни ситуации)[36]. Енергетскиот сектор, секако претставува глобален проблем кој ги надминува националните граници, мрежата на енергетската инфраструктура пример во Европската унија ги надминува границите на ЕУ така што во комплексноста на синџирот на снабдување треба да се нагласи и меѓусебната зависност.

Заштитата и подобрување на отпорноста од опасности предизвикани од вештачки или природни катастрофи бара континуирана будност, планови и обуки во комбинација со сеопфатни мерки за подготвеност, како од физички така и од сајбер заканите,така што покрај државата, значајна улога во безбедноста на енергетскиот сектор секако имаат и сопствениците на енергетската инфраструктура, без оглед на локацијата.

Ако ги анализираме САД како водечка сила во поглед на заштитата на киритичната инфраструктура во делот на енергетиката, ќе видиме дека таму преку Министерство за енергетика и нејзините партнери, кој покрај другото се залагаат за една стабилна и еластична енергетска инфраструктура низ Програмаодржува континуитетот на бизнисот и услугите. Во таа смисла, преку безбеден и сигурен систем кој опфаќа споделување на информации, ефективни програми за управување со ризици, координирани активности за одговор и доверлив однос помеѓу јавниот и приватниот сектор на сите нивоа, како цели во рамките на секторот, САД во својата Програма ги нагласува:

- Воспоставување на свесност за енергетскиот сектор преку навремено информирање и безбедна размена на информаци помеѓу јавниот и приватниот сектор;
- Користење на принципи за справување со ризици со имплементација на физички и информатички мерки, заради подобрување на подготвеноста, обезбедувањето, еластичноста (флексибилноста);
- Спроведување на ефикасно планирање при вонредни ситуации и катастрофи, вклучувајки обуки и вежби за да се подобри реагирањето во ваквите ситуации;
- Јасно дефинирање на улогата на заштитата на критичната инфраструктура и одговорностите на федералните, локалните, државните и приватните сектори во насока на подобрување на координацијата помеѓу партнерите;

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

- Разбирање на важноста на меѓузависностите и соработка со други сектори и имплементирање на знаењето во планирањето и операциите;
- Зајакнување на јавната доверба и довербата помеѓу партнерите, заради зајакнување на способноста на секторите за да се справи со ризици и имлементирањето на ефективните мерки за обезбедување и послекризно опоравување[37].

2.1. Профил на секторот

Како што споменавме предходно, енергетскиот сектор вклучува три клучни енергетски извори: електрична енергија, нафта и нафтени деривати и природен гас. 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 од некои типови на корисници како што се големи индустриски и финансиски институции.[38]

Во следната табела, претставени се трите клучни енергетски извори дефинирани од страна на Националната безбедност на САД:

ЕЛЕКТРИЧНА ЕНЕРГИЈА	НАФТА	НАФТА

Производство
• Фосилни горива
  • Јаглен
  • Природен гас
  • Нафта
• Нуклеарни горива
• Хидро електрични
• Обновлива енергија
Пренос
• Базни станици
• Мрежи
• Контролни центри
Дистрибуција
• Базни станици
• Мрежи
• Контролни центри
Контролни системи
Пазари на електрична енергија
	Сирова нафта
	• Внатрешни нафтни полиња
	• Надворешни нафтни полиња
	• Терминали
	• Транспорт (нафтоводи)
	• Складирање
	Објекти за преработка на нафта
	• Рафинери
	• 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.3 сегменти на енергетскиот систем[39]

[37] EnergySector-Specific PlanAn Annex to the National Infrastructure Protection Plan2010 Homeland Security – United States Department of Energy
[38] Ibid
[39] EnergySector-Specific PlanAn Annex to the National Infrastructure Protection Plan2010Homeland Security – United States Department of EnergyTable 1-1: Segments of the Energy Sector стр. 19

Може со сигурност да потенцираме дека енергетскит секторбара стабилнаи еластична (флексибилна) енергетската инфраструктура, во кои примарна цел ќе има континуитет на бизнисот и услугите преку безбедна и сигурна размена на информации, ефективни програми за управување со ризици, координиран одговор и прецизна соработка помеѓу јавниот и приватниот сектор на сите нивоа на индустријата и владата.

2.2. Проценка на заканите за енергетските компании

Проценката на заканите на енергетските компании, бара размислување за специфични карактеристики на енергенсите (електрична енергија, нафта и гас), закони поврзани со енергетиката, 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 проценка на заканите во енергетската компанија опфаќа:

- Презентација на 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 на матрица на закана;
- Идентификација на потребите за обезбедување.[40]

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

- Заштита на мобилни и дистрибутивни мрежи, складишта, транспорт на енергија, и целосна логистика (одржување на инсталациите за нафта и гас, сигурносни аларми за заштита на критичките точки во инсталациите, хеликоптерска контрола на инсталациите, употреба на сателитска навигација и др.);

[40]Milan Vrsec: 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 периметар и локации на енергетските компании. (огради, врати, контрола на влез и излез, видео надзор контрола на паркинг, итен пристап и сл.);
- Заштита на енергетски објекти згради, опрема и процеси (контрола на пристап и видео надзор);
- Заштита на влезовите на објектите (заштита од провала, контрола на пристап и видео надзор во однос на заканата;
- Заштита во објектите – просториите (физичка и електронска заштита на компјутерската опрема, класифицирана документација, податоци, информации, архиви и електронски комуникации).[41]

2.3. Воспоставување на интегрален систем за обезбедување во рамките на ЕУ

Европската енергетска политика, ги наведува членките на ЕУ да ги подобрат системите за обезбедување во областа на енергетиката. Директивата на европскиот совет е конкретен Европски документ за идентификација на европската критична инфраструктура и проценката за потребата за подобрување на заштитата[42].

Нити една држава во меѓународната заедница, независно од нејзината моќ и напредна технологија, не е во можност да се заштити во целост и да биде не ранлива на современите закани кои кои го пратат енергетскиот сектор.

Во таа насока ЕУ ја зголемува безбедноната политика во областа на енергетиката за што постои Директива на Европскиот совет кој преставува конкретен Европски документ за идентификација и одредување на Европската критична инфраструктура но и потребата да се унапреди заштитата. Главните насоки на оваа Директива се:

- Терористичките борбени закани се приоритетна задача за секој кој менаџира со критичните инфраструктури,
- Заштита на сите опасности кои доаѓаат од човечки или технолошки закани како и заканите кои доаѓаат од природни катастрофи,
- Примарната и конечната одговорност во безбедносниот систем на критичната инфраструктура е даден на државите членки на ЕУ и сопствениците и операторите со овие инфраструктури,

[41]Milan Vrsec: 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, p. 126
[42]Ibid p.124

- Операторите на критичните инфраструктури треба врз база на проценката на закани и безбедносни ризици да направат сигурносни планови кои 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 ранливостите на критичната инфраструктура,
- Потребно е да се заштитат и класифицираните податоци во согласност со актите на Унијата,
- Сопствениците и операторите на КИ треба да ги пратат докажаните пракси при воспоставување на сигурносните механизми во енергетиката и транспортот а кои се дефинирани од членките на ЕУ,
- Секоја членка на ЕУ треба да определи офицер за безбедност кој е овластен за координација со останатите земју 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[43].

За да се подобри обезбедувањето на критичните инфраструктури, 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 вклучувајки го и енергетскиот сектор,потребно е да ја следат добрата практика за воспоставување на безбедносни системи регулирани согласно актите на ЕУ преку воспоставување на офицер за соработка кој ќе биде главен за координација со другите држави, контрола, обезбедување на совети за државните оператори на критичните инфраструктури[44].

Функцијата на корпоративната безбедност во сегментите на производството на енергија, мобилна и дистрибутивна мрежа, складиштата, транспортот на енергијата, енергетските објекти и опремата, процесите и персоналот вработен во енергетската компанија се реализира воглавно низ физичка, техничка и електронска заштита. Корпоративната безбедност е менаџирана низ безбедносен менаџмент регулиран со закон, проценка на закана, безбедносна политика и стандарди. Затоа, таа наметнува

[43]Milan Vrsec: 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 p.124 - 125

[44] Milan Vrsec: 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

адекватни методи за менаџирање на безбедносните ризици според принципот за превенција од штети и загуби, како и задржување на висок степен на општествена одговорност.[45]

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

3. Информатички и комуникациски технологии

Електронската комуникациска мрежа е преносен систем и таму каде што е применливо овие комуникациски или насочувачки опреми и други средства коишто 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, доколку се користат за пренос на комуникациски сигнали, радиодифузни мрежи и кабелски телевизиски мрежи, независно од видот на информациите што се пренесуваат.[46]

Секторот за информатичка технологија е од централно значење за безбедноста, економијата, јавното здравство и безбедноста на нацијата. Бизнисот, стопанството, владата, академските институции и граѓаните се се повеќе зависни од информатичка технологија[47]. Од тие причини, безбедноста на овој сектор потребно е да се темели на:заштита на информацискиите системи и мрежи,инструментализација, автоматизација и контролни системи, интернет, обезбедување на фиксната телекомуникација, обезбедување на мобилната телекомуникација, радио комунукација и навигацијата, сателитска комуникација, емитувањето и др.Комплексноста и динамичниот развој на секторот го прави дотолку сложен од аспакт на идентификување на заканите и слабостите што бара огромна компаниска соработка и креативен начин на заштита. Иако, инфраструктурата која се однесува на информатичката технологија има одредено ниво на својствена еластичност, поради

[45]Ibid
[46]Законзаелектронскитекомуникации http://mio.gov.mk/files/pdf/dokumenti/zakoni/ 15102015.pdf
[47]https://www.dhs.gov/information-technology-sector, Превземено на 24.10.2015 год.

големите меѓузависности 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 на закани е многу комплицирана задача на сите критични инфраструктури, која ги обединува оваа област.

Сајбер тероризмот е во постојан развој и потенцијалот на терористичките организации и поединци и во иднина постојано ќе се зголемува заедно со промените во информатичко – комуникациските технологии. Сајбер тероризмот во основа претставува напади и закани насочени кон компјутерските системи, мрежи и информатичките опреми за чување на податоци со цел на заплашувањеи влијание врз властите и јавноста во политичкиот и социјалниот живот[48]. Справувањето со ваков вид на закани е многу комплоцирана задача, затоа што самиот сајбер простор е многу големо и несигурно подрачје кое е тешко да се разграничи и дефинира, така што, компјутерските системи се постојана цел на терористичките организации вклучувајки ги иинформатичките системи на големите светски компании.

Информатичко општество во основа се темели на заења и иновации, такашто голем број на граѓани преку електронските комуникациски инфраструктури и дигиталните технологии имаат лесен и евтин пристап до информациите и знаењето. Но покрај позитивната страна потребно е да се соочиме и со негативните последици пред се поради зависноста на општествата од напредната технологија, како што се информатичките и комуникациските системи. Комплексните закани претставени низ современите ризици и закании манифестирани преку сајбертероризмот,претставуваат напади на компјутерски системи како и на комуникациските мрежи кои се од стратешко значење за државите. Нападите врз комуникациските и информатичките системи најчесто доаѓаат од хакерите, терористичките организации а многу чести се и нападите поради индустриска шпиунажа. Нападитеисто така можат да бидат насочении кон системите на националните критични инфраструктури, со што и тоа како ја прави ранлива државата.

Глобалното вмрежување во ситемот на комуникациската и информатичката технологија стана основа на функционирање 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 дејствија, крадење на податоци или хакирање,

[48] https://sr.wikipedia.org/wiki/Sajber_terorizam. Превземено на 03.04.2015 год.

предизвикување на насилсва, регрутација и радикализација на корисниците на овие мрежи и др.

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)[49].

Покрај улогата на државата во поглед на заштитата на критичната инфраструктура од областа на ИТ безбедноста, клучен фактор во заштитата секако спаѓаат и операторите, односно компаниите кои стопанисуваат со овие критични инфраструктури.

Нападот на информатичкиот систем може да се дефинира како директна акција против мрежата или информатичкиот систем со цел неовластено да се пресретне или да се прекине некојаоперација, да се преземе контрола и да се уништи, да се промени или да се корумпира податокот (со меморирање или обработка).[50]

Затоа безбедноста на компаниите во делот на ИТ заштитата преставува примарна дејност каде што најчесто опфаќаполитика односно стратегија за ИТ безбедност поткрепена со регулативи и нормативно правни акти а опфаќа:

- Управување со физичкиот пристап - обезбедување на физички пристап до клучните компоненти само за ИТ персоналот, вклучувајќи ја и можноста за надзор. Оваа област е испреплетена со системите за физичка заштита.
- Одделни услуги, автентикација и авторизација - централна база на податоци на корисници, овозможува управување со нивните податоци за идентификација и пристап, вклучувајќи логирање и следење на пристап. Потенцијална експанзија може да претставуваат системи за управување со идентитетот, единечно најавување, или системи за мулти-факторска проверка.
- Безбедносен надзор и управување со системот - важен елемент на сигурноста која овозможува собирање на информации за настани од разни системи, обединети на едно место, и потоа оценување на истите.
- Проверка на сите оперативни активности или мерки во рамките на безбедност, мора да се проверат од аспект на водење на утврдената политика за безбедност

[49] Stallings William, Network and Internetwork Security – Principles and practices, Prentice Hall, Englewood Cllifs, New Jersey 1995., pp 29 – 30 / Бакрески О. Триван Д. Митевски С. Скопје 2012 – Корпорорациски безбедносен систем стр.243

[50]Stallings William, Network and Internetwork Security – Principles and Practice, Prentice Hall, Englewood Cliffs, New Jersy 1995., pp. 29 -30 Бакрески О. Триван Д. Митевски С. Скопје 2012 – Корпорорациски безбедносен систем стр.243

или 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 опасен код во насока на информативниот систем на организацијата, односно повеќе-слојна антивирусна заштита. Суштински елемент е централно управување и следење на антивирусните решенија и понатаму заштита од нови видови на 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 - филтрирањето 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 на податоци - VPN.
- Заштита на мобилни уреди - користењето на преносна опрема бара, посебен акцент на безбедноста, бидејќи овие уреди се надвор од стандардното разбирање за периметарска заштита на компјутерските мрежи[51].

Според некои автори, можат да се разликуваат три видови напади на информатичкиот систем:

- Физички напад, насочен кон расположливоста на нападнатиот систем (употреба на конвенционални оружја против инфраструктурата, во кој се наоѓаат информатичките системи или против линијата на преносот на информацијата)[52]
- Електронски напад (користење на електронско оружје кое е во можност да емитуваелектромагнетна енергија концентрирана во снопови со автоматски или субавтоматски честички или оружје, кое испушта електромагнетни импулси со

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

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

цел да се преоптоварат или да се онеспособат електричните споеви на системот.[53]

- 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 чуствителни податоци).[54]

Според Црногорската методологија, за избор на критична информатичка инфраструктура, во поглед на мерките кои можат да доведат до заштита на критичната информатичката инфраструктура, можат да се дефинираат на следниот начин:

- Да се обезбедат средства за превентивно делување, вклучувајки вежби и обуки (превенција, вежби и обука);
- Да се обезбеди нај ран одзив на инцидентот (ублажување);
- Обезбедување на капацитети за брза детекција на тековниот инцидент (детекција и рано предупредување);
- Соочување со последиците во текот на инцидентот;
- Што поскоро враќање на системите во нормално функционирање (опоравување);
- Извлекување на поука од случувањето.[55]

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, изнаоѓање на 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 на соодветен одговор на нападите и брзо враќање во функција на нападнатите системи и мрежи се приоритетни задачи за националните влади[56].

4. Сообраќајот и транспортот како критична инфраструктура

Влијанието на сообраќајот во стопанскиот живот на секоја земја е повеќекратна и многу значајна. Постои цврста взаемна зависност помеѓу степенот на развој на сообраќајот во една држава со развојот на економијата. Сообраќајот е резултанта на

[53]Бакрески О. Триван Д. Митевски С. Скопје 2012 – Корпорорациски безбедносен систем стр. 243

[54] Петковоќ Тодор оп.цит.стр.293 преземено од:Бакрески О. Триван Д. Митевски С. Скопје 2012 – Корпорорациски безбедносен систем стр. 243

[55]Методологија за избор на критична информатичка инфраструктура- *Ministarstvo za informaciono društvo i telekomunikacije Oktobar 2014 cmp.7*

[56]http://morm.gov.mkПредизвик на современите општества – С. Славески, 30.05.2015год.

одредено ниво на развој на стопанството од една страна и од друга страна сам врши влијание на стопанскиот развој на секоја земја.[57]

Различноста и големината на транспортниот сектор го прави витален за националната економија и безбедност. Оваа инфраструктура е обемна, развивана со години како во приватниот така и во јавниот превоз. Различните транспортни модели обезбедуваат мобилност на популацијата и придонесуват за личната слобода.

Сообраќајот е значаен услов за стопанскиот развој на секоја земја како и оделни региони. Сообраќајната инфраструктура: патиштата, пругите, реките и каналите, со основните инфраструктурни објекти го овозможуваат 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 оценка на ефикасноста на инвестицијата и развојот и модернизацијата на сообраќајниот систем на една држава.[58]

Од аспект на значењето на сообраќајот разгледано преку функциите кои ги има во однос на нормалното функционирање на општеството, потребно е да се напомене зависноста на производството и потрошувачката преку развивање на подоброто искористување на суровините, енергетските горива, рационално и подобро користење на работната сила во поедини подрачја и сл.

Од поважните економски и општествени функции, сообраќајот во секоја држава, има првостепено политичко и општествено значење. Со самото тоа што поврзува оделни 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 допринесуваат во претварање на туризмот од индивидуален во масовен феномен. Изградбата и модернизацијата на градскиот сообраќаен систем ја условува општествената поделба на работата и развој на нови индустриски гранки. Историскиот развој на многу земји покажува дека, сообраќајот игра значајна улога во формирање на начините на живеење, изградбата на сообраќајниците и сообраќајните

---

[58]Ibrahim Jusufranić, Osnove drumskog saobracaja , Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje. – Травник 2007

превозни средства влијаеле отсекогаш па и денес влијаат на формирање на големината на населените места и на процесот на урбанизација.

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 повторно во 2004 и 2005 година, Мадрид и Лондон, Брисел 2015, каде што цели на напади беа транспортните системи.

Сообраќајот може да се врши на повеќе начини. Како критериум на поделбата, можат да ни послужат некои технички карактеристики, понатака начинот на превоз, како и некои економски функции на поедини сообраќајни дејности.

Транспортниот систем според начинот на превоз и превозните средства може да се подели:

- копнен сообраќај, кој се дели на патен, железнички, цевоводни и сообраќај со преносни траки.
- воден сообраќај, кој го делиме на поморски, речен, езерски и канален
- воздушен сообраќај
- поштенски сообраќај
- телекомуникациски сообраќај[59]

По дефиниција, сообраќајот претставува систем, кој се состои од поедини сообраќајни гранки, кои имаат карактеристики на подсистеми во однос на сообраќајот како систем.

4.1. 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 подсистеми: аеродроми (воздухопловни пристаништа), воздушни превозници (воздухопловни превозни средства) и контрола на летање (управување и контрола на воздушниот сообраќај). Секој од овие подсистеми се состои од повеќе функционални елементи: корисник на системот, инфраструктура, управувачки елементи, технолошки процедури, технички и кадровски ресурси, законска регулатива, меѓународна легислатива итн[60]. Фигуративно претставено, воздушниот сообраќај се реализира во воздух (воздухоплови) и на земја (аеродроми), со меѓусебна интерактивна поврзаност преку системите за негово управување и контрола.Воздухоплов е секоја направа која може да се движи или одржува во атмосферата поради реакција на воздухот, освен

[59] Ibrahim Jusufranić, Osnove drumskog saobracaja , Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje. – Травник 2007

[60] Т. Тунтев, Аеродромски Прирачник за прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.13

реакцијата на воздухот што се одбива од површината на земјата[61]. Без оглед на неговите конструктивни и технички карактеристики, перформанси или неговата намена, за секој воздухоплов е пропишан начин за утврдување на неговата способност за безбедна воздушна пловидба. Воздушен сообраќај претставува летање на воздухопловот или негово движење по маневарските површини на аеродромот[62]. 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[63].

Гледано од страна на аеродромската проблематика од подсистемот на инфраструктура може да се издвои аеродромскиот подсистем. Делот на аеродромскиот подсистем, кој 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 кои често го одредуваат капацитеот на полетно слетната патека по по тоа и самио аеродром), па се до присанишната плаформ[64]. Делот на системие каде што не се појавуваат воздухопловите, т.е делот од плаформата и пристанишната зграда до градскиот терминал се нарекува земна или градска страна (landside).[65]

Во современата воздухопловна терминологија, согласно меѓународно прифатената дефиниција, поимот ,,аеродром" се користи за дефинирање на копнената или водената 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 поимот ,,воздухопловно пристаниште"[66].

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

[61]Закон за воздухопловство Сл весник на Р.М, бр 155 од 2012год.
[62]Исто член 4
[63]Тунтев Т. ,,Аеродроми,,Технички факултет, Битола, 2005
[64]Б.Мирковиќ, В. Тошиќ, Воздухопловна пристаништа II, Универзитет у Београду, Сообраќаен факултет – Београд 2012год
[65]Б.Мирковиќ, В. Тошиќ, Воздухопловна пристаништа II, Универзитет у Београду, Сообраќаен факултет – Београд 2012год.
[66]Тунтев Т. ,,Аеродроми,,Технички факултет, Битола, 2005

серија на летови за превоз на патници, карго и / или пошта за надомест или закупнина.[67] 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[68].

Суштинската разлика помеѓу поимите ,,аеродром" и ,,воздухопловно пристаниште" се состои во законски регулираната обврска за организирање и 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: 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 на објекти, уреди и инсталации кои се од значење за безбедноста на воздушната пловидба[69].

Воздухопловните пристаништа можат да се користат и за меѓународен воздушен сообраќај (во тој случај мора да биде организирана пасошка и царинска контрола), што не е случај со другите аеродроми. Аеродромите на вода, што се користат за оперирање на хидроавиони, се нарекуваат хидродроми, а аеродромите наменети за оперирање на хеликоптери се нарекуваат хелиодроми.

4.2. Организација на цивилното воздухопловство

4.2.1. Меѓународни воздухопловни организации и здруженија

Под поимот воздухопловни организации се подразбираат разни облици на здружување и делување било на држави било на други правни субјекти, заради постигнување на одредени заеднички цели во областа на воздухопловството. Меѓу поистакнатите меѓународни воздухопловни организации и здруженија ќе ги анализираме (ICAO, IATA, ACI, ECAC, EUROCONTROL, JAA)

[67]Закон за воздухопловство Сл весник на Р.М, бр 155 од 2012год. член 4
[68]Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.13
[69]Тунтев Т. ,,Аеродроми,,Технички факултет, Битола, 2005

а) ICAO - International Civil Aviation Organisation - меѓународна Организација за Цивилен Воздушен сообраќај - основана е со Конвенцијата за меѓународно цивилно воздухопловство, потпишана во Чикаго на 7 Декември 1944год. а стапува на сила од 1947год[70]. Седиштето на оваа организација е во Монтреал, Канада и нејзина задача е, во соработката со нејзините земји членки, да обезбеди меѓународното цивилно воздухопловство да се развива на сигурен, безбеден, редовен и ефикасен начин, а врз основа на принципот на еднаквост и рамноправност на сите субјекти, учесници во воздушниот сообраќај[71]. Во моментов во неа членуваат 190 земји. Во моментов во неа членуваат 190 земји, Република Македонија стана членка на оваа Организација на 09.01.1993 г.одина со прифаќање на Меѓународната конвенција за цивилно воздухопловство (тн. Чикашка Конвенција) согласно Уставниот закон од 1991 година.[72].

Целите на **ICAO** се следните: развивање на основните начела и техниката во меѓународната воздушна пловидба и унапредување на меѓународниот воздушен транспорт, спречување на било каков вид на дискриминација во меѓународниот воздушен сообраќај, унапредување на безбедноста на воздушната пловидба, поттикнување и развој на воздушните патишта, обезбедување на урамнотежен развој на воздухопловсвото во светот, спречување на нелојалната конкуренција помеѓу членките, донесување на стандарди и препораки во сите области во цивилното воздухопловство, поттикнување и развој на аеродромите и воздухопловите, грижа за рамноправни можности на сите членки во одржувањето на меѓународните воздушни линии и др.

ICAO има три основни функции и тоа: административна, легислативна и судска. Најважни органи се: Собранието, Советот, Секретаријатот и Генералниот секретар. Пропишаните правила и одреби на ICAO се издаваат преку редовни и повремени публикации, во форма на стандарди или препораки, содржани во анекси и прирачници. Државите членки на ICAO се обврзани да ги почитуваат и применуваат ваквите одредби, преку сопствената законска регулатива[73].

Одредбите кои ги пропишува ICAO и кои се однесуваат на сите учесници во глобалниот систем на воздушниот транспорт, се издаваат во форма на препораки и стандарди, кои се содржани во разни Анекси и Прирачници. Државите членки се

[70] http://www.icao.int/Pages/default.aspx Превземено на 17.09.2013
[71] http://www.caa.gov.mk/86/Chlenstvo_vo_megjunarodni_organizacii.html Превземено на 18.10.2015год.
[72] Ibid. http://www.caa.gov.mkПревземено на 18.10.2015год.
[73] Т. Тунтев, Аеродромски Прирачник за прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид.

должни да ги почитуваат овие препораки и стандарди, па затоа секоја држава членка , ги разработува низ својата сопствена легислатива[74].

Анексот 17 на ICAO ги обработува Меѓународните стандарди и препорачани практики за безбедност во врска на заштитата на цивилното воздухопловство од акти на незаконито постапување. Така, секоја договорна земја за примарна цел ќе ја има безбедноста на патниците, екипажите, персоналот и јавноста во работите поврзани со заштита на цивилното воздухопловство од незаконски дејствија. Договорната земја ќе воспостави и имплементира регулативи и практики и процедури заради заштита на цивилното воздухопловство од незаконски дејствија со водење сметка за безбедноста, уредноста и ефикасноста на летовите и ќе осигура дека таквата организација, таквите регулативи, практики и процедури:ќе ја заштитат сигурноста на патниците, екипажите, земниот персонал и општата јавност во целост во работите поврзани со обезбедувањето од незаконскии дејствија да се способни брзо да одговорат на зголемените закани по безбедноста[75].

б) IATA - International Air ransport Asossiation - Меѓународна Асоцијација за Воздушен Транспорт – основана е во Хавана, 1945 година, со седиште во Монтреал, со подрачни уреди во Њујорк, Париз и Сингапур и комора за пресметувања во Лондон. Меѓународната асоцијација за воздушен транспорт (ИАТА) преставена со околу 260 авиокомпании или 83% од вкупниот број во воздушниот сообраќај, поддржува многу области на воздухопловството.[76]

Целите на постоењето и функционирањето наIATA се: унапредување на безбедноста, редовноста и економичноста на воздушниот транспорт, проучување на проблемите во одвивањето на воздушниот транспорт од страна на воздухопловните превозници – членки, развој на меѓусебната соработка за потикнување на меѓународната воздушна трговија, воспоставување на безбедни воздушни транспорти и др[77].

в) ACI - Airports Council International - Меѓународен Совет на Аеродроми – основане на 01.01.1991, под името AACI - Airports Association Council International од страна на двете дотогаш постоечки меѓународни организации AOCI - Airport Operators Council Internationalil CAA - International Civil Airports Association. Со нивното соединување,

[74]Т. Тунтев,,Аеродроми,,Технички факултет Битола 2005 година.
[75]ICAO – Анекс 17 International Standards and Recommended practices Marth 2011
[76]http://www.iata.org/ Превземено на 17.09.2015
[77]Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид,стр.11.

заедно со AACC - Airport Association Coordinating Council, настанува најголемата меѓународна асоцијација на аеродроми, која на 11.11.1992 година, на заседанието на Генералното собрание во Мадрид го добива своето конечно име ACI. Седиштето на оваа организација се наоѓа во Женева. Членките на ACI се аеродромските оператори од целиот свет, како и некои други компании (комерцијални претпријатија, национални асоцијации, образовни институции и сл.) и тоа како редовни или како вонредни придружни членови. Целите на основање на оваа организација се: развој и унапредување на цивилните аеродроми и нивната меѓусебна соработка, признавање на статусот на аеродромите како еден од основните елементи на цивилното воздухопловство, претставување и промовирање на интересите наработата на другите меѓународни организации, формулирање на сопствена политика која ќе овозможи рамноправно учество на аеродромитекако еден од најважните субјекти во цивилното воздухопловсво, заедно со другите меѓународни субјекти, за обезбедување на безбедна, ефикасна и еколошки прифатлива воздушна пловидба во рамките на глобалниот транспортен систем, развој и унапредување на аеродромскиот менаџмент и размена на информации кои се однесуваат на унапредувањето на аеродромската инфраструктура, заштита на човековата околина, финансирањето, маркетингот, техниката и технологијата, стручното работење и одржувањето[78].

Оваа светска професионална асоцијација на аеродроми ги застапува интересите на голем број на аеродроми, од јануари 2014 година ACI вклучува 1.861 аеродроми од 177 земји. АЦИ е непрофитна организација, чија примарна цел е да се унапредат интересите на аеродромите и да се промовира професионален квалитет во управувањето и работењето на аеродромите.[79]

Аеродромите во Охрид и Скопје се членки на ACI Европа од Септември 1993година и делегираат свои преставници во работата на комитетите[80].

г) ECAC (European Civil Aviation Conference)

Европска Конференција за цивилен воздушен сообраќај основана е во 1955 год. од страна на неколку европски држави, со седиште во Париз, која работи преку одржавање на редовни и вонредни пленарни сесии, на ниво на директори на цивилните воздухопловни власти на државите членки или на ниво на Министри за

[78]Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.13

[79]http://www.aci.aero/About-ACI/Overview/Mission-Objectives-Structure Преземено 11.12.2015

[80]Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.14

сообраќај. Мисијата на ECAC е промоција на континуираниот развој на безбеден, ефикасен и одржлив Европски воздушен сообраќај.[81]

Основните цели на ECAC се: почитување и грижа за интересите на државите – членки од областа на цивилниот воздушен транспорт во Европа, изнаоѓање решенија за решавање на нивните меѓусебни проблеми и недоразбирања, соработка со телата на Европската комисија и ICAO, унапредување на европскиот воздушен сообраќај и безбедноста на европското небо, обезбедување на меѓусебна соработка во развојот и имплементацијата на заедничките стандарди и процедури од областа на цивилното воздухопловсво.[82].Република Македонија стана земја членка на Организацијата на 03.07.1997 г. Во неа членуваат 44 земји, речиси цела Европа[83].

Политиката на ECAC на полето на воздухопловната безбедност го има разработено и имплементирано Doc. 30 кој е развиен со цел сите земји членки, како и сите други земји чии што превозници и аеродромитреба да одржат прифатливо и еднообразно ниво на безбедност, при утврдувањето на обемот на мерките, методите, исти принципи, процедури, спецификации, критериуми, материјали,податоци и сл. Се очекува сите земји членки на ECAC да продолжат со примена на одредбите од Анекс 17 и одредбите од другите анекси на ICAO во соодветните Резолуции на Собранието на ICAO и материјалите од прирачникот за безбедност на ICAO, Doc. 8973. Бидејќи сегашниве околности, опасноста која го демне цивилното воздухопловство бара примена на дополнителни мерки за безбедност, кои мораат да се прилагодат на условите кои континуирано се менуваат и кои мора постојано да се ревидираат со цел да се постигне оптимално ниво на нивна ефикасност[84].

д) EUROCONTROL - Европска Организација за безбедност на воздушниот сообраќај – со седиште во Мастрихт , Холандија, делува на ниво на експертски тимови, преку развој и имплементација на голем број проекти, програми и процедури од областа на воздушниот сообраќај (навигација, контрола на летање, управувачки безбедносни системи, хармонизација на системите за контрола на летањето, интеграција на воздухопловните сегменти, централизација во управувањето со сообраќајот,

[81] https://www.ecac-ceac.org/about-ecac Преземено 11.12.2015

[82] Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.14

[83] http://www.caa.gov.mk/86/Chlenstvo_vo_megjunarodni_organizacii.html Превземено на 18.10.2015год.

[84]. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.14

безбедносно користење на воздушниот простор и др)[85]. Европската организација за безбедност на воздушната пловидба, е меѓувладина организација со 41 земји-членки, посветени на градење, заедно со своите партнери единствено европско небо и со задача да ја зголеми ефикасноста на управувањето со воздушниот сообраќај.[86]Таа е сочинета од 38 земји и Европската Заедница. Република Македонија стана земја членка на оваа Организација на 01.11.1998 година[87].

ѓ) JAA (Joint Aviation Authorities) - Здружени воздухопловни власти – придружно тело на ECAC, како посебно неформално здружение на цивилните воздухопловни власти на земјите – членки на ECAC, со седиште во Хофдорт, Холандија, чија основна цел е обезбедување на меѓусебна соработка помеѓу државите – членки, во развојот и имплементацијата на заедничките стандарди, правила прописи и процедури, од областа на цивилниот воздушен сообраќај и транспорт на Европско небо[88].Агенцијата за цивилно воздухопловство на Република Македонија стана членка на ова тело на 03.12.2008 година кое згасна како такво на 30 јуни 2009 година, но истото премина во Европската агенција за воздухопловна безбедност (European Aviation Safety Agency - EASA)[89].

4.2.2. Карактеристични случки во примена на актите на незаконско постапување во воздушниот сообраќај

Примената на актите на незаконско постапување во цивилниот воздушниот сообраќај покажува дека е честа мета на на разни видови на насилство или терористички акти.[90]Последиците, односно штетите нанесени на цивилниот воздушен сообраќај обично се многу тешки со губење на 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 на аеродромите со криумчарење на огнено оружје или експлозивни направи, сама по себе ја зголемува опасноста од тероризмот кој претставува најекспониран причинител на загрозувањата на цивилниот воздушен сообраќај, кој датира уште со самите почетоци на воздушниот транспорт. Низ историјата на цивилното воздухопловство се забележани голем број на терористички напади и закани. Тие се разликувале по тоа какви цели се сакани да се постигнат и по тоа какво средство се користело при

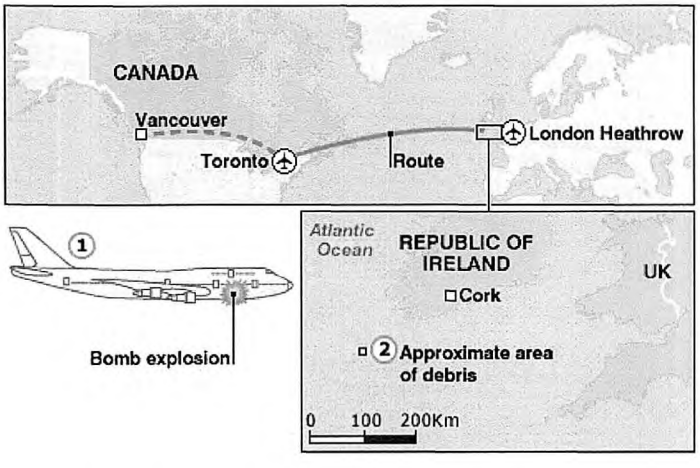
[85]Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.14
[86]https://www.eurocontrol.int/articles/who-we-are Преземено на 14.12.2015
[87]http://www.caa.gov.mk/86/Chlenstvo_vo_megjunarodni_organizacii.html Превземено на 18.10.2015год
[88]https://en.wikipedia.org/wiki/Joint_Aviation_Authorities Преземено 11.12.2015
[89]http://www.caa.gov.mk/86/Chlenstvo_vo_megjunarodni_organizacii.html Превземено на 18.10.2015год
[90]Аеродромска тренинг програма за заштита на цивилното воздухопловство Скопје 2008 – група автори

извршувањето на нападите или за превземањето на цивилниот лет.[91]Актуелноста на авиосообраќајот секогаш го привлекуваат вниманието и на обичните луѓе, кои најчесто преку средствата за јавно информирање делумно се инволвираат, односно запознаваат со еден многу широк и комплексен поим наречен безбедност во воздухопловството. Ова чувство на безбедност е присутно кај секој еден патник,кој што треба да отпатува на одредена дестинација користејќи ги услугите на воздушниот сообраќај. Оттука, задолжителното ставање ацент на безбедноста како фактор во авиосообраќајот, како и настаните од поблиското минато, имаат директен импакт врз создавањето на одредени безбедносни системи и процедури, кои до ден денес се усовршуваат и надополнуваат, со цел да се елиминираат сите можни пропусти.

Во овој контекст, како покарактеристични случаи ќе ги спомнеме, уривањето на Кулите Близначки, односно со грабнувањето на четирите патнички воздухоплови, *Boeing 767-223ER*и *Boeing 767–222*кои беа срушени во Светскиот трговски центар во Њујорк, и *Boeing 757-223*и *Boeing 757–222*, кои беа срушени близу пред својата однапред координирана цел од страна на киднаперите поставија едно ново поглавје во науката која го третира тероризмот.Во оваа насока потребно е да се спомене и примерот кој датира од 1988 година,а тоа е немилиот настан што се случи над небото на Локерби во Шкотска, кога воздухопловот Boeing 747-121A на Pan American Airways на интерконтиненталниот лет од Лондон до Њујорк беше соборен во воздух што резултираше со 270 жртви од кои 11- случајни жртви, односно не биле патници[92]. Пред настаните од 11 Септември во 2001 година, овој терористички акт што се случи над Локерби важеше за најкрвав чин на терор против Америка и најтежок терористички акт во британската историја. Комплексноста на случајот, на почетокот истрагата била насочена кон Popular Front for the Liberation of Palestine, затоа што на овој настан во 1970 година му претходел и друг настан, каде што биле грабнати три авиони и принудно слетани во базата Dawson Field, во близина на градот Ал Зарка во Јордан. Авионите во сопственост на компаниите *Trans World Airlines,*кој се обраќал од Франкфурт,*Swissair* кој се обраќал од Цирих и третиот на *British Overseas AirwaysCorporation* кој се обраќал од Бахреин. После неколку дневни преговори помеѓу владите на државите и грабнувачите од познатата палестинска организација Black September, 310 патници кои биле држени како заложници биле ослободени, а на авионите од типот *Boeing 707*, *Douglas DC-8* и *Vickers VC10* им биле поставени експлозивни направи и истите биле јавно демолирани пред очите на целата светска

[91]http://www.airserbia.com/magazin/vuk/terorizam_u_vazduhu/terorizam.htm,Преземено: 15.04.2010
[92]http://en.wikipedia.org/wiki/Pan_Am_Flight_103, Преземено 17.02.2015

јавност, бидејќи целиот настан бил пренесуван преку BBC[93]. Преговорите за ослободување на патниците, бил еден вид на поставен ултиматум за ослободување на Лејла Калед, која што била држена како затвореник, заради обид за грабнување на израелскиот авион во Амстердам на компанијата *El Al.* Всушност, во целиот настан вкупно пет патнички авиони биле цел на членовите од фронтот за слобода на Палестина, еден од нив е и авионот на *Pan Am* од типот *Boeing 747,* кој бил принудно присилен да слета во Каиро, но исто како и случајот со израелскиот авион и овој обид завршил неуспешно, бидејќи еден од грабнувачите бил ранет. Заради овој настан, потрагата за вистинскиот виновник за Локерби се одолговлечила цели 11 години, водени од претходното искуство кое се случило во 1970 година, по асоцијација случајот бил посочен кон друга страна.Летот 182 на Ер Индија во 1985 година во историјата на авионските несреќи/незгоди, засекогаш ќе остане запомнат како негативен пример за пропустот кој што е направен од страна на аеродромските служби.[94] Имено, на летот кој се обраќал на рутата од Монтреал, Лондон и Њу Делхи е пропуштен багаж без придужба, а бидејќи скенерот на тамошниот аеродром во моментот кога се товарал авионот бил надвор од употреба, вработените при рачното скенирање на багаж, направиле пропуст заради недоволна обученост за работење со детекторите за откривање на сомнителни направи, оружје, ескплозивни средства и слично.



Слика 1. Приказ на рутата на летот 182[95]

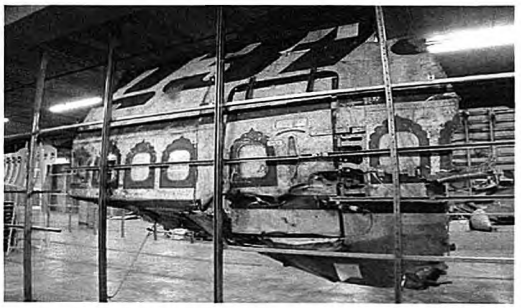
Ваквиот пропуст доведува до фатален исход, после четири часовниот лет над Атланскиот океан, само половина час пред слетувањето во Хитроу, кога авионот бил над водите на Ирска, на височина од 31 000 фити, исчезнува од радарската контрола,за да после неколку минути од страна на поморските служби било пријавено дека остатоци од авион и тела пловат во водите на Атлантикот Океан[96].

[93] http://en.wikipedia.org/wiki/Dawson's_Field_hijackings,Преземено 17.02.2015
[94] http://en.wikipedia.org/wiki/Air_India_Flight_182
[95] http://en.wikipedia.org/wiki/Air_India_Flight_182
[96] Исто

Манипулацијата која што е направена од страна на саботерот е добро осмислена стратегија, со цел да го реализира својот план за внесување на експлозивна направа и активирањена истата, без негово присуство во воздухопловот. Неговата стратегија била заснована на претходни сознанија за пропустите, кои што настанувале при чекирање на патниците и багажот и по подолго анализирање, тие сознанија биле искористени за реализација на планот.

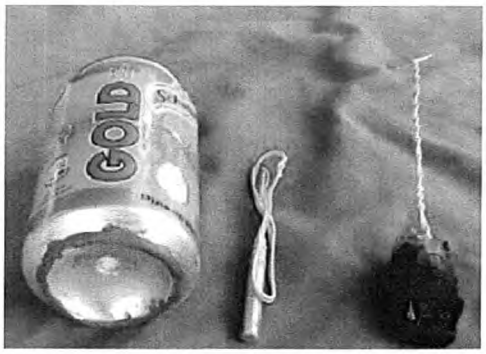
Исходот од ваквите последователни грешки, кои се случиле заради низа на околности, довеле до најнепосакуваните ситуации во авијацијата, пропустите во цивилната авијација, каде што директно се загрозува безбедноста како на патниците, така и на членовите на екипажот се недопусливи и не треба никогаш да се повторат, затоа што секоја една грешка ненамерна или намерна, без разлика дали е поврзана со безбедноста или некој друг сегмент од воздушниот сообраќај, доведува до фатален исход.

Сл2:Приказ на Слика собирањето на остатоците [97]



Слика3: Реконструкција на остатоците[98]

Во овој дел потребно е да се спомене несреќата која се случила на 31.Октомври, 2015 година на авионот Airbus A321-231 на компанијата Metrojet, кој летал на рутата Шарм ел Шеик до Ст. Петерзбург. На околу 25 минути по полетувањето од аеродромот во Шарм ел Шеик, авионот беше соборен од рачно изработена експлозивна направа, при што загинаа 224 патници и членови на екипажот[99]. На летот најголем број на патници беа руски државјани 219, а одговорноста за нападот е преземена од страна на терористичката организација (ИСИЛ).



Слика бр 4. Импровизирана Експлозивна Направа (ИЕН) поставена во лименка.

[97] http://en.wikipedia.org Преземено 04,01.2015
[98] Исто, Преземено 04,01.2015
[99] http://www.planecrashinfo.com/2015/2015-16.htm Превземено: 04.01.2016год.

Од анализите кои се направени од страна на руската служба за безбедност и истрагата која се спроведувала заклучено е дека, се работи за ,,терористички чин" откако беа пронајдени траги од експлозив во остатоците. Според руските официјални лица, се работи за импровизирана експлозивна направа со моќност еквивалентна на 1килограмТНТ. На 18 ноември 2015 година, ИСИЛ објави слики од она што го тврдешедека е бомба. Осомничени за поставување на бомбата на летот биле вработени на аеродромот, поврзани со терористичката организација[100].

Во следната табелахронолошки се претставени настани, кои што се поврзани со грабнување на воздухоплови.

[100]https://en.wikipedia.org/wiki/Metrojet_Flight_9268, Превземено04.01.2016 год.

ДАТУМ	АВИО ПРЕВОЗНИК/БРОЈ НА ЛЕТ	ТИП НА АВИОН
1-ви Јуни 1943	British Overseas Airways Corporation/Лет 777	Douglas DC-3
23-ти Јули 1968	El Al Israel Airlines /Лет 426	Boeing 707
11-ти Декември 1969	Korean Air Lines	NAMC YS-11
31-ви Март 1970	Japan Airlines/Лет 351	Boeing 727-100
6-ти Септември 1970	El Al Israel Airlines/Лет 219	Boeing 707
6-ти Септември 1970	Pan American World Airways/Лет 93	Boeing 747
6-ти Септември 1970	Swissair/Лет 100	Douglas DC-8
6-ти Септември 1970	Trans World Airlines/Лет 741	Boeing 707
9-ти Септември 1970	British Overseas Airways Corporation/Лет 775	Vickers VC10
24-ти Ноември 1971	Northwest Orient Airlines/Лет 305	Boeing 727
12-ти Јануари 1972	Braniff International Airways/Лет 38	Boeing 727
22-23 ти Февруари 1972	Lufthansa/Лет 649	Boeing 747-200
29-ти Октомври	Lufthansa/Лет 615	Boeing 727-100
23-ти Јули 1973	Japan Airlines/Лет 404	Boeing 747-200
15-ти Септември 1974	Air Vietnam/Лет 706	Boeing 727
27-ми Јуни 1976	Air France/Лет 139	Airbus A300
28-ми Септември 1977	Japan Airlines/Лет 472	Douglas DC-8
13-ти Октомври 1977	Lufthansa/Лет 181	Boeing 737
4-ти Декември 1977	Malaysia Airlines/Лет 653	Boeing 737
30-ти Август 1978	Polskie Linie Lotnicze/Лет 165	Tupolev Tu-134
18-ти Ноември 1082	Aeroflot – Russian Airlines/Лет 6833	Tupolev Tu-134
21-Јуни 1982	Braathens South American & Far East Airtransport A/S/Лет 139	Boeing 737
23-ти Ноември 1982	EgyptAir/Лет 648	Boeing 737
5-ти Септември 1986	Pan American World Airways/Лет 73	Boeing 747
25-ти Декември 1986	Iraqi Airways/Лет 163	Boeing 737
7-ми Декември 1987	Pacific Southwest Airlines/Лет 1771	British Aerospace Bae 146-200A
5-ти Април 1988	Kuwait Airways/Лет 422	Boeing 747
2-ри Октоври 1990	Xiamen Airlines/Лет 8301	Boeing 737-247
26-ти Март 1991	Singapore Airlines Flight/Лет 117	Airbus A310
24-ти декември 1994	Air France/Лет 8969	Airbus A300
23-ти Ноември 1996	Ethiopian Airlines/Лет 961	Boeing 767
24-ти Јули 1999	All Nippon Airways/Лет 61	Boeing 747-400
24-ти декември 1999	Indian Airlines/Лет/Лет 814	Airbus A300
20-ти Декември 2000	British Airways/Лет 2069	Boeing 747-400
23-ти Јануари 2001	Yemenia/Лет 448	Boeing 727
11-ти Септември 2001	American Airlines/Лет 11	Boeing 767-200ER
11-ти Септември 2001	United Airlines/Лет 175	Boeing 767–200
11-ти Септември 2001	American Airlines/Лет 77	Boeing 757–200
11-ти Септември 2001	American Airlines /Лет 93	Boeing 757–200
8-ми Февруари 2008	Eagle Airways/Лет 2279	BAe Jetstream 32
9-ти Септември 2009	Aeroméxico/Лет 576	Boeing 743-800
29-ти Јуни 2012	Tianjin Airlines/Лет 7554	Embraer E-190

Табела 4. Приказ на грабнати авиони[101]

Во продолжение претставена е табела, во која хронолошки се подредени настани кои што се поврзани со бомбашки напади на воздухоплови.

ДАТУМ	АВИО ПРЕВОЗНИК/БРОЈ НА ЛЕТ	ТИП НА АВИОН
12-ти Октомври 1967	Cyprus Airways /Лет 284	de Havilland DH 106 Come
26-ти Јануари 1972	JAT/Лет 367	Douglas DC-9
15-ти Јуни 1972	Cathay Pacific/Лет 7003	Convair 880
17-ти Декември 1973	Pan American World Airways/Лет 100	Boeing 707
8-миСептември 1974	Trans World Airlines/Лет 841	Boeing 707
1-ви Јануари 1975	Middle East Airlines /Лет 438	Boeing 720
23-ти Јуни 1982	Air India /Лет 438	Boeing 747-237B
2-ри Април 1986	Trans World Airlines/Лет 840	Boeing 727
19-ти Јули 1994	Alas Chiricanas /Лет 00901	Embraer EMB-110
11-ти Декември 1994	Philippine Airlines /Лет 434	Boeing 747
22-ри Декември 2001	American Airlines /Лет 63	Boeing 767

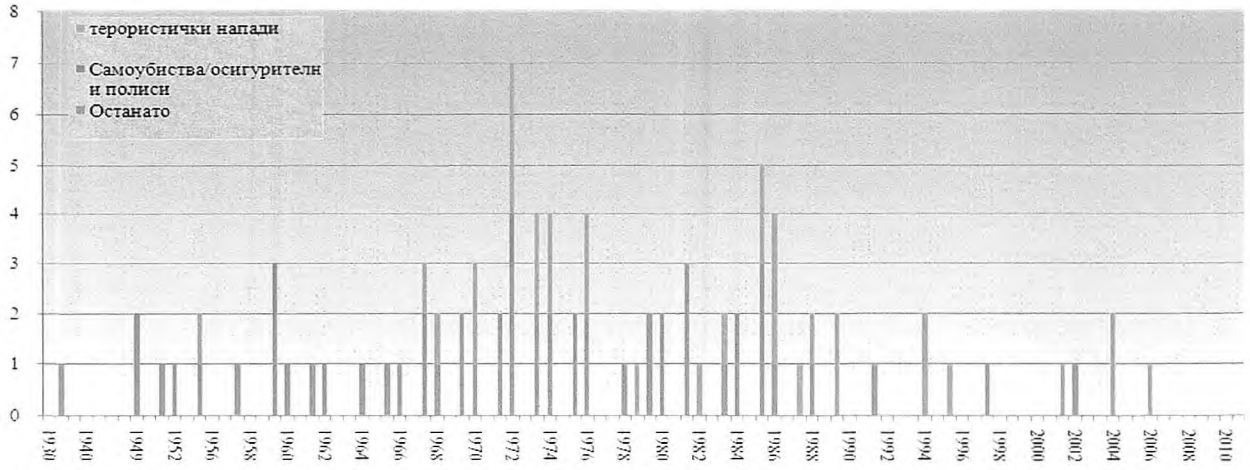
Табела бр.5 Приказ на воздухоплови поврзани со бомбашки напади[102]

Претставениотграфички приказ кој се однесува на експлозивните направи кои биле поставени во комерцијалните воздухоплови во текот на изминатите 70 години, од сите можни евидентирани инциденти односно од 88 кривични дела, биле уништени 50 авиони, 32 биле оштетени и сето тоа резултирало со 2790 жртви и 129 повредени лица. Од сите настани, 33 се однесуваат на терористички напади, 14 се комбинација од самоубиства, поврзани со полиси на животни осигурувања. Четири бомбашки напади се резултат на разни или случајни причини, а мотивот зад останатите 37 е неодреден. Во оваа статистика се сумирани настаните по години. Нападите со бомба во комерцијалната авијација, својот максимум го достигнуваат во 70-тите и 80-тите години од 20-тиот век, во период од 1964 година до 1989 година, секоја година се случувало по еден ваков настан, со исклучок на 1977 година. Една од најлошите години, во која била загрозена комерцијалната авијација е 1985 година, кога се случиле 5 напади, кои резултирале со 332 жртви, од кои 182 се превезувале во авион на индиската авиокомпанија Air India. Нападите со бомба се намалиле во текот на 90-тите години, па се до ден денес, но тероризмот сеуште претставува сериозна закана за цивилниот воздушен сообраќај, без разлика дали станува збор за грабнување на

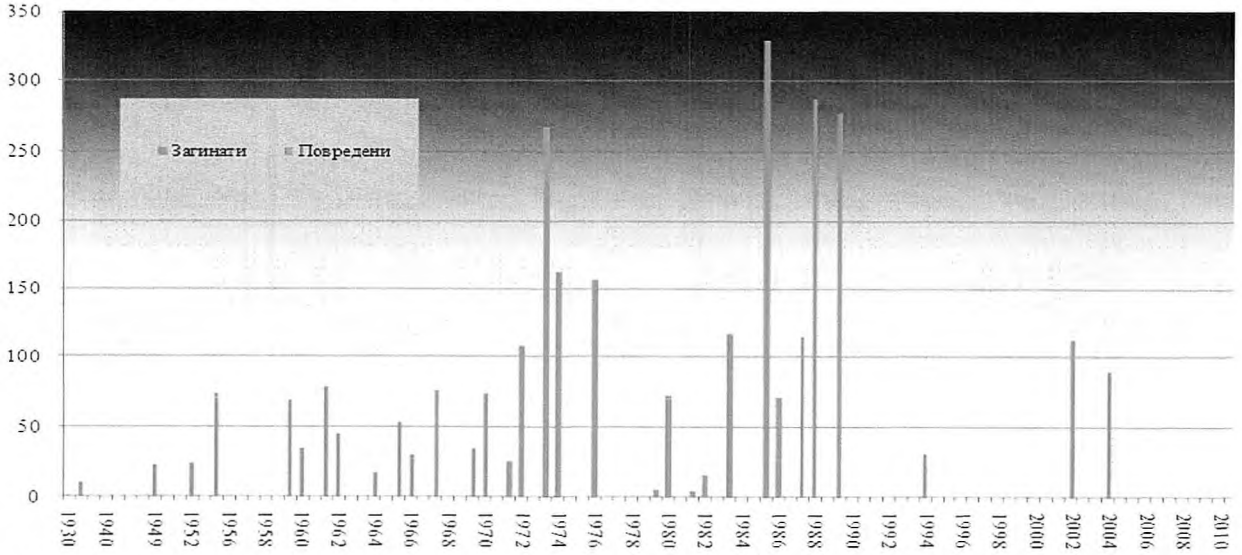
[101] http://en.wikipedia.org/wiki/List_of_accidents_and_incidents_involving_commercial_aircraft, Превземено на 04.10.2014 година.

[102] http://en.wikipedia.org/wiki/List_of_accidents_and_incidents_involving_commercial_aircraft, Превземено на 04.10.2014 година.

воздухоплов, подметнување на експлозивни направи и слично, ваквите девијантни појави се строго дефинирани во документацијата од страна на ICAO, разработени во Анекс 17 на Чикашката Конвенцијата за меѓународното цивилно воздухопловство во кој се препорачани меѓународните стандарди и практики за безбедноста.



Слика бр 5. Хронолошки приказ на напади со бомба[103]



Слика бр. 6 Хронолошки приказ на загинати и повредени[104]

Хронолошки актите врз цивилното воздухопловство генерално според мотивите можат да се поделат во три фази:

Фаза 1: Од 1948 – 1968 год. каде основен мотив е избегнување од судски прогон. Главни карактеристики на овој вид на тероризам е воздухопловно пиратство, каде индивидуалци грабнуваат воздухоплови, се обидуваат со бегство да го избегнат судскиот прогон,а грабнувањето на воздухоплов е најбрз и едноставен начин на остварување на овие цели.

[103] http://www.aerospaceweb.org/question/planes/q0283.shtml Превземено 15.05.2013год.
[104] http://www.aerospaceweb.org/question/planes/q0283.shtml Превземено 15.05.2013год.

Фаза 2: Од 1968 – 1994 год. каде основен мотив се остварување на политички цели и ја карактеризира: Поставување на противниците на актите на незаконско постапување во нелагодна состојба (Влада и други државни институции), нанесување штети на државата на економски цели,користење на нападот, како средство за изнудување, во ослободување на осудени лица (со исти идеолошки цели) или од материјални цели.

Фаза 3: воздухопловот е средство (оружје) за извршување на напади[105].

За почеток на оваа фаза се зема 24.12.1994 год. каде Алжирските терористи го грабнуваат воздухопловот на авио компанујата Air France, лет 8969, на линија од Алжир до Париз . Терористичката група инсистирала грабнатиот воздухоплов да слета во Париз, но Француската влада не дозволила воздухопловот да слета на аеродромот во Париз, бидејќи имала разузнавачки информации дека терористите имале намера да активираат експлозив над градот, го пренасочиле воздухопловот кон аеродромот во Марсеј каде полициските сили интервенираат и ги ослободуваат патниците и посадата. На 11.09.2001 год. четири воздухоплови се симултано грабнати од аеродромите во Соединетите Американски држави, од кои два се насочени кон зградите на светскиот трговски центар во Њујорк, каде удираат во нив и по еден час зградите се рушат како последица од силната експлозија која е настаната при ударот, каде што настрадаа 2800 лица. Третиот воздухоплов е насочен кон зградата на Пентагон (главниот штаб на Американската армија) во Вашингтон каде се руши и нанесува човечки жртви и материјални штети на објектот. Главни карактеристики на оваа Фаза 3 се: Намера да се нанесе максимална штета и човечки загуби, Оваа фаза се смета за најопасен за цивилниот воздушен сообраќај и најтешка за одбрана од тероризмот.[106]

Нападите врз цивилните аеродроми, поврзани со терористички бомбашки напади случени во 18.07.2012 година, на аеродромот во Бургас, како и најновиот напад на 22.03.2016 на аеродромот во Брисел ја покажува ,,атрактивноста" на аеродромите како мета. И во двата случаи, нападите се реализирани во јавните зони на аеродромите, без целта да биде определен воздухоплов, со што се потврдува фактот дека терористичките стратегии се насочени и кон најчуваните и најобезбедените витални објекти, со цел да се манифестираат целите на терористичките организации во поглед на предизвикување на страв, несигурност во системите на државата, нанесување на голем број жртви, но и предизвикување на голем медиумски ефект.

[105]Аеродромска тренинг програма за заштита на цивилното воздухопловство Скопје 2008 – група автори
[106]Исто стр.4

Нападот на аеродромот во Бургас се случил на 18 јули2012 година, во кој седум лица загинале и дваесетина биле повредени, во терористичкиот напад што се случил околу 17.23 часот на паркинг пред аеродромот. Според извештаите од бугарските медиуми, целта на нападот биле 150 израелски туристи, кои на половина час пред експлозијата долетале од Тел Авив и влегле во три автобуси со кои требало да заминат на црноморското крајбрежје. Според очевидци, во еден од автобусите влегол бомбаш кој активирал експлозив. Разузнавачки извори укажуваат на вмешаност на Хезболах во бомбашкиот напад[107].

Координираните бомбашки напади на аеродромот во Брисел, беа реализирани со две експлозии во терминалната зграда на аеродромот, но пронајдена беше и една експлозивна направа во текот на пребарувањето на аеродромот, која подоцна била уништена . Во овој немил настан бомбаши-самоубијци активиралеексплозиви утрото на 22 март 2016 година, во три бомбашки напади: две во аеродромот во Брисел во Завентем, а еден во Maelbeek метро станица во Брисел. Во овие напади предизвикале 32 жртви, а повеќе од 300 лица беа повредени. Исламската држава Ирак и Левант (ИСИЛ) ја превзела одговорноста за нападите[108].

5. Водните системи како критична инфраструктура

Водата е во основа на одржливиот развој. Водните ресурси, и опсегот на услугите што ги нудат, поткрепуваат намалување на сиромаштијата, економски раст и одржливост на животната средина. Од безбедност на храната и енергијата до здравје на луѓето и животната средина, водата придонесува за подобрување на социјалната благосостојба и инклузивниот раст, кои влијаат на животот на милијарди луѓе[109].

Виталната зависност на современото општество од водните системи претставена низ призмата на заканите од акти на незаконско постапување е постојано присутна. Можните сценарија за напад кои се присутни во секојдневното живеење, предизвикуваат загрижувачки размери поради опасните агенси кои можат да бидат внесени во организмот преку водата и да предизвикаат големи последици.

Секторот вода и отпадните водни системи е подложен 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 на жртви, заболени и материјални загуби. Откажувањето на снабдување со вода,

[107] https://en.wikipedia.org/wiki/2012_Burgas_bus_bombing Превземено на 12.03.2016година.
[108] https://en.wikipedia.org/wiki/2016_Brussels_bombingsПревземено на 12.03.2016година.
[109] http://www.iph.mk/svetski-den-na-vodata-2015-vodata-i-odrzliviot-razvoj/Превземено на 12.03.2016година

исто така ќе влијае на јавното здравје и економска виталност на државата. Голем број услуги вклучувајќи ги, здравството, енергетиката, земјоделството, прехранбениот сектор, транспортните системи, службите за во итни ситуации и други ќе трпат негативни последици од нарушениот систем.[110]

Ако го посмараме секторот води низ системот на заштиа кој е утврден од страна на САД преку специфичниот План за секторот води, кој ги опишува процесите и активностите за заштита и опоравување на секторската инфраструктура ќе видиме дека главен акцен се става на:

- *Профилирање на секторот и целите и тоа*:
- Профили (вода за пиење, отпадни води, клучни авторитети)
- Субјекти: агенци, сопственици и оператори, државната безбедност, други ферерални оддели, регионални субјекти и меѓународни организации и странски држави,
- Цели (елементи и карактеристики)
- Визијата на секторот води е обезбедување и подобрување на водата за пиење и отпадните води, заштита на таа инфраструктура преку ефективни програми за подготвеност, безбедносни практики и мерки.

- *Идентификување на објекти системи и мрежи*, Преставува сет од системи на вода за пиење и отпадни води. Ажурирање на податоците поврзани со системот, кој се прави преку периодични истражувања и контроли од страна на надлежните институции.
- *Ризици,* Секторските објекти се ранливи при поединечни 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 и др, природните катастрофи како што се земјотресите, пандемиите и ветровите, исто така, преставуваат закани за секторот вода.
- *Приоритетни делови на инфраструктурата*, Сопствениците и операторите при проценката 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 деловите на инфраструктурата и тоа: колку популација се опслужува, количина на складиран Хлор, економски инпакт, критична маса на потрошувачи и др.

[110] http://www.dhs.gov/water-and-wastewater-systems-sectorПревземено на 14.07.2015 година.

- *Развој и имплементација на иницијативи, стратегии за заштита и опоравување*, Пристапи при изработка и имлементирање на стратегии за заштита и опоравување вклучуваат обуки, вежби, техничка асистенција, меѓусебна регионална помош, шланирање на заштита на информатичките системи и припреми при пандемии.
- *Развојни мерки*
- *Истражување и развој на мерките за заштита*
- *Менаџирање и координација на секторските одговорности*[111]

6. Храната како критичен енергенс

Една од потенцијалните мети на терористичките организации претставува и храната, поради можноста од насочување на акциите кон широката популација и лесно предизвикување на паника. Во поново време, ваквите инциденти не се реткост, сценариото за можен терористички напад на некој од синџирите на исхрана веќе не делуваат само како теорија. Светската здравствена организација (WHO), го дефинира тероризмот во однос на храната, како активност или закана за намерна контаминација на храната со биолошки, хемиски, физички или радиоактивни материи во насока на предизвикување на ранување или смрт на цивилното население или загрозување на социјалните, економските или политичката стабилност. При тоа, како биолошки агенси се подразбираат: вируси, бактерии и паразити. Хемиски агенси можат да бидат вештачки или природни токсини, додека физички агенси можат да вклучат широк спектар на различни делови како што се стакло, игли, и парчина на метали. Радионуклидни материјали дефинирани се 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 на терористички активности ако е наменета кон економски искористувани животни, кои 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 е наменето за загадување на големи количини на храна со опасни агенси, како би се нанеле големи човечки загуби, целта е иста, а тоа е внесување на неред. Во таа насока, во последните години се придава

[111] WaterSector-Specific PlanAn Annex to the National Infrastructure Protection Plan 2010 United States Environmental Protection Agency – Homeland security

големо значење, а посебно со воведување на стандарди и воведување на превентивен систем на заштита[112].

Секторот за храна, претставува еден од покомплесните сектори од аспект на обезбедување. Комплексноста доаѓа од неговата обемност, отвореност, разновидност од аспект на загрозување, како и огромната зависност од останатите сектори. Прехранбените производи се движат брзо во трговијата до потрошувачите и времето кое е потребно за откривање и идентификација на опасноста и еколошката штета, како што се опасностите од животинско или растително потекло од аспект на болести или контаминација на храната, може да биде долго и комплексено[113]. Загрозувањата можат да резултираат со огромни последици и од тие причини,заштита вклучува широк спектар на активности со голем број на инволвирани субјекти.

Низ историјата, храната често пати била средство кое се користело за постигнување на цели во војна или терористички напади насочени кон војските или цивилите. Заканите на терористичките организации со посредство на храната можеби не доаѓа во преден план во однос на нападите кои се реализираат со експлозивни материи и завземаат главен медиумски простор и кои за жал, се многу чести во последно време. Како по карактеристични би ги издвоиле:

Примерите од 1984 година кога членови на религиска секта ги имаат заразено со бактеријата *Sallmonela typhimurium*, повеќе ресторани во САД, со што се предизвикани 751 случај на заболувања од салмонелоза, кој воедно бил како пробен нападпред поинтензивниот напад, чија цел била спречување на одржување на локалните избори, во 1996 година, незадоволен работник намерно ја заразил храната со бактеријата *Shigella dysenteria* тип 2, предизвикувајки заболување кај дванаесет лица, во 2003 година во Кина, училишниот доручек е затруен со отров за штетници како и последен познат пример на намерна контаминација на храна во САД во 2011година, кога поради конкуренција сопственикот на пицерија поставил торби со штетници во соседните пицерии[114]. Ова се само некои примери за труење со храна, гледано во светски размери, намерното труење со агенси не изгледа големо, но тоа незначи дека нетреба да се преземаат адекватни мерки на заштита. Бројните примери за ненамерно труење со храна говорат за потенцијалот кој го поседува храната како терористичко оружје.

---

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

[113] http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf, Преземено 11.01.2016год.

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

Тука треба да се спомене ширењето на хепатитисот А на 300000 луѓе во Шангај – Кина, после конзуминирањето на контаминирани ракови, кој воедно се смета за најголем инцидент во историјата на инциденти со храна[115]. Генерално, храната преставува многу лесно подрачје за контаминација во функција на биотероризмот, за што постојат голем број на сомнителни контаминации,било тоа да се од економски или други побуди, сепак прехрамбената индустрија преставува висок ризик кога станува збор за актите на незаконско дејствување.[116] Од тие причини, потребно е адекватен приод кон проценките на ризици, а се со цел спречување на контаминацијата на храната во сите облици на користење. Проценката на ризик од терористички напади по пат на храна ги содржи следните компоненти: идентификација на опасноста, карактеризацијата на опасноста, проценка на изложеност и карактеризација на ризикот. Оваа постапка е разиена во Агенцијата за храна и лекови на 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 прехрамбената индустрија, однапред предвидените сценарија кои 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 кој треба да го реализира секоја влада.[117]

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

ГЛАВА IV

Ризици, опасности и загрозувања врз објектите од витален интерес

1. Општо за ризиците, опасностите и загрозувањата врз објектите од витален интерес

Како појдовна основа за определувањето на заканите кон критичната инфраструктура, да ги разгледаме најнапред термините кои се дадени во меѓународните и националните документи, а се однесуваат на загрозувањата.

Според дефиницијата дадена за анализа на ризик од страна на Европската комисија во Директивата 114 од 2008, претставена е како разгледување на соодветни сценарија на опасности со што би се оценале слабостите и потенцијалното негативно влијание врз работењето или уништувањето на критичната инфраструктура.[118]

Во Македонската легислатива, поимот ризици и опасности се претставени како можни манифестации на национализам и верска нетрпеливост и омраза, облици и активности сврзани со меѓународниот тероризам, организиран криминал, недозволена трговија со дрога, оружје и луѓе, последици од средствата за масовно уништување, поседување на големи количини на илегално оружје, корупција, урбан тероризам, тежок криминал, вклучувајки уцени, убиства и напади врз граѓаните и на нивната сопственост, активности на странските специјални служби, насочени кон влошување на безбедносната состојба, последици од судир на интереси за користење на изворите и патиштата на странските енергенси, како и попречување и блокирање на нивниот увоз во Републиката, елементарни и други непогоди, техничко технолошки катастрофи, епидемии и карантински и други заразни заболувања кај луѓето и животните, како и деградација од поголем обем и уништувањена животната средина.[119]

Во истиот Закон, поимот Загрозеност на безбедноста на Републиката, е дефиниран како загрозување од ризици и опасност по добрата и животната средина, здравјето и животот на луѓето, животните и растенијата, имотот и другите материјални добра од поголем обем, стабилноста функционирањето на државата и нејзиниот поредок утврден со Уставот, за кои не постојат услови за прогласување воена или вонредна состојба[120].

Во националната концепција за безбедност и одбрана, кој претставува основен документ на Република Македонија во областа на безбедноста и одбраната во делот на виталните интереси со кои се унапредува безбедносната состојба и со кои се создаваат услови за подобар живот на граѓаните и функционирање на државата и

[118]COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008
[119]Закон за управување со кризи Бр.07-1537/1 од 2005 член 3 став2
[120] Закон за управување со кризи Бр.07-1537/1 од 2005 член 3 став 1

општеството во делот на економскиот развој, се нагласува заштитата на виталната инфраструктура и ресурсите на Република Македонија.[121]Во истиот документ, како ризици и опасности по безбедноста на Република Македонија, меѓу другите се нагласени: можните манифестации на екстремен национализам, расна и верска нетрпеливост; облиците и активностите сврзани со меѓународниот тероризам, организираниот криминал, нелегалната трговија со со дрога оружје, луѓе, стратегиските и матерјалите за двојна употреба, како и последиците од употреба на средстваа за масовно уништување; поседувањето на на големи количини на илегално оружје; транзиционите проблеми како што се: корупција, урбанио тероризам, тешкиот криминал, вклучувајки уцени, рекетирања, убиства и напади врз сопственоста на граѓаните, економскиот криминал, даночнаа евазија. Недоизграденоста на институциитена демократскиот систем, проблемите во функционирањето на судството, социјалните проблеми и невработеноста; акивностите на странските специјални служби насочени кон влошување на безбедносната состојба, а со тоа и забавување на демократските и интегративните процеси, особено оние кон НАТО и ЕУ; последиците од судир на интереси за користење на изворите и патиштата на стратегиските енергенси, како и попречување и блокирање на нивниот увоз во Република Македонија; елементарните и други непогоди, техничко – технолошките катастрофи, заразните заболувања на луѓето и животните предизвикани од домашни и/или надворешни чинители; компјутерскиот криминал, пиратството и злоупотребата на информатичката технологија, посебно во делот на личните податоци на граѓаните, деловната, службената и државната тајна; деградацијата и уништувањето на животната средина.[122]

Генерално земено, сите ризици и опасности наведени во стратегирата се во директна или индиректна зависност со критичните инфраструктури во Република Македонија. Од тие причини и политиката на Националната безбедност преставува сложен и меѓузависен збир на мерки, планови, активности и програми, кои ги превзема Република Македонија, заради заштита, одржување и унапредување на безбедноста, во согласност со расположливите ресурси и со активна соработка со меѓународната заедница.[123]

Во зелената книга на Европската комисија, поврзана со заштитата на критичната инфраструктура, терминот ***ризик*** е преставен како: можност за загуба, штета или повреда, додека пак,***нивото на ризик*** е состојба на два фактори:

[121] Национална концепција за безбедност и одбрана на Р.М стр.3
[122]Исто стр 7
[123]Национална концепција за безбедност и одбрана на Р.М, Дел 3

вредноста на средствата од сопственикот / операторот и влијанието на губење или промена на имотот, и веројатноста дека специфичната ранливост ќе биде искористена за одредена закана[124]

Во истиот документ, терминот ***закана*** е дефиниран како: било каква индикација, ситуација или настан, со потенцијал да ја наруши или уништи критична инфраструктура, или било кој елемент од него. Целокупниот приод кон опасностите вклучува, несреќи, природни непогоди, како и намерен напад. Тоа, исто така, може да се дефинира како намера и способност за преземање на дејствија кои ќе бидат на штета врз имотот.

Поимот ***ранливост*** преставува: карарактеристика на елемент или операција која го прави подложно на уништување или онеспособување од одредена закана врз критичната инфраструктура.

Влијанијата од загрозувањата на критичната инфраструктура би предизвикале голем број на квалитативни и квантитативни ефекти како што се:

• *Опсег* - Загубата на критичен инфраструктурен елемент е детерминиран по основ на географската област, која може да биде под влијание, а тоа може да се однесува на: меѓународно, национално, регионално или локално ниво[125].

• *Сериозност* - степенот на загубата може да се оцени како: незначителна, минимална, умерена или голема.

Критериумите кои можат да се користат за проценка на влијанието се:

- Јавноста - број на население кое е под влијание, губење на животи, медицинска болест, сериозни повреди, евакуација и сл.;
- Економски - ефект на БДП, економска загуба и / или деградација на производи или услуги, прекин на транспортот или енергетските услуги, недостаток на вода и храна,
- Животна средина - ефект врз јавноста и околината;
- Меѓузависноста - меѓу другите клучни инфраструктурни елементи.
- Политичките ефекти - доверба во способноста на владата;
- Психолошки ефекти - можна ескалација и на мали настани[126].

• *Ефекти на време* - Овој критериум констатира во кој момент на губење на елемент може да има сериозно влијание (т.е. моментално, 24-48 часа, една недела, други).[127]

---

[124]GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTUREPROTECTION Brussels, 17.11.2005 COM(2005) 576 final

[125]Ibid Annex 1

[126]Ibid Annex 1

[127] GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTUREPROTECTION Brussels, 17.11.2005 COM(2005) 576 final - ANNEX 1

Ризикот како дефиниционен елемент од оперативен аспект, може да се претстави и како,,иден и од таа причина незизвесен настан кој може да има штетно влијание врз рентабилното работење" или било кој акт, пропуст, односно состојба, која може сериозно да да го попречи текот на активностите на правното лице, да предизвика загуби на имотот и материјалните вредности, вклучувајќи човечки загуби и тешки повреди на персоналот.[128]Базирајќи се на ризиците кои влијаат на критичната инфраструктура, претставени во документите кои ја обработуваат оваа област во националната безбедност на САД, претставени се како комплексен приод, од причини што заканите и ризиците постојано еволуираааат, најнапред како физички закани и природните катастрофи, а сега се повеќе се изложени на сајбер ризиците, која произлегува од зголемената интеграција на информатичките и комуникациските технологии[129]. Стратешките национални Ризици (SNRA) дефинира бројни закани и опасности за националната безбедност, во широки категории претставени како: човечки, природни и технолошки / ненамерни закани.

Критичните средства, системи и мрежи се соочуваат и со многу закани кои се категоризирани по SNRA, вклучувајќи, терористички и други акти преку основните услуги и сајбер напади, пандемии или други здравствени проблеми, како и нарушувањето на работењето на инфраструктурите. Потенцијалот за меѓусебно поврзани настани со непознати последици, додава неизвесност во прилог на анализираните ризици преставени SNRA како дел од познатите ризици.[130]Ефектите од екстремните временски влијанија, претставуваат значителен ризик како на пример: критичните морски нивоа, големите невремиња, екстремни и пролонгирани суши, поплавите и др, претставуваат закана на инфраструктурата која ги обезбедува основните услуги за американската јавност. Тековни и идни измени на климата имаат потенцијал да ги зголеми овие ризици и може да има големо влијание на инфраструктурните операции[131].Меѓузависностите во критичните инфраструктурни системи, особено потпирањето кон информациските и комуникациските технологии, е зголемена и потенцијалната ранливост од физички и сајбер заканите. Фактот дека критичната инфраструктура ги преминува националните граници, потенцијалните влијанија драстично се зголемуваат.

---

[128]Зоран Доревски – Практикум - Обезбедување Јуни 2004 стр.36

[129] NIPP 2013 Partnering for Critical Infrastructure Security and Resilience – Homeland security USA

[130] U.S. Department of Homeland Security, Strategic National Risk Assessment, December 2011, http://www.dhs.gov/xlibrary/assets/rma-strategic-national-riskassessment-ppd8.pdf

[131] The National Security Strategy states that "the danger from climate change is real, urgent, and severe." National Security Strategy, 2010.

Проценката на ризикот треба да се спроведува во рамките на операторите на критичните инфраструктури и таа во принцип се состои од следниве елементи: идентификација и класификација на закани, идентификација на слабости, и евалуација на влијание. Ова е основа на сите постоечки методологии за проценка на ризикот.
Според Риналди[132], постојат четири видови на меѓузависности за критична инфраструктура:

- Физички: работењето на една инфраструктура зависи од материјалниот аутпут на другата инфраструктура
- Сајбер: зависност од пренос на информациите преку преку информацискатa инфраструктура;
- Географски: зависноста на ефектите од локалното опкружување истовремено влијаат на неколку инфраструктури,
- Логичка: било каков вид на зависност не се карактеризира како физички, сајбер или географски .

Ако навлеземе подлабоко во анализата на критичностите и ризиците, ќе констатираме дека ризик секогаш постои во сите состојби и процеси, само што некаде е поголем, а некаде помал. Во тој случај, ризикот од аспект на влијанието врз процесот може да биде неприфатлив, прифатлив или незначителен. Следствено на тоа, потребно е да се дефинираат критериумите на прифатливост односно неприфатливост. Во таа насока, се разработува анализа на ризик и се изработува студија која е насочена кон анализа на технолошкиот ризик, односно ризик од акцидентни ситуации, односно геополитичка и /или економска анализа која е насочена на неповолни сценарија од безбедносното опкружување.[133] Сложеноста со која се соочуваат практичарите бара вклучување на целокупниот државен потенцијал, а пред се индустријата, јавноста, науката, државните институции и целокупниот јавен сектор.

2. Облици на загрозување на безбедноста на објектите од витален интерес – критична инфраструктура

Поимот загрозување, најчесто подразбира општ израз за ситуација во која се јавува опасност дека на некој или некого ќе му биде одземен животот, оштетено здравјето, уништена или оштетена материјална, финансиска или друга сопственост. Изворите на такво загрозување, односно доведување во опасност, може да бидат

[132] Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and AnalysingCritical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, pp. 11-25.
[133] Energetska sigurnosti kri čna infrastruktura –pregled rezultata istraživanja - Dario MATIKA - Zbornik radova: Krajcar, S. (ur.)(2009.), Energetska sigurnost i krična infrastruktura, Sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb.

природни, вештачки и општествени (а според други автори надворешни, внатрешни и комбинирани)[134].

Извори и облици на загрозување на корпорацијата може да бидат:

- техничко-технолошки инциденти;
- елементарни непогоди;
- кривични дела со кои се нанесува штета на бизнис субјекти (диверзии, тероризам, саботажи, уништување или оштетување на средствата за производство и уништување на производите);
- кривични дела на општиот криминалитет;
- кривични дела на економскиот криминалитет извршени од вработените; најчесто во врска со деловните партнери (злоупотреба, корупција, мито, проневера, кражба, заговор или работење на штета на компанијата);
- кривични дела кои предизвикуваат општа опасност и кривични дела против здравјето на луѓето и животната средина;
- кривични дела со употреба на информатичката технологија;
- сообраќајни несреќи и незгоди;
- оддавање доверливи информации (кршење на работната дисциплина, отстапување од прописите за работа, пречекорување или узурпирање надлежности и овластување, неизвршување или делумно извршување на пропишаните процедури, несовесно работење);
- социјални и други немири во корпорацијата итн[135].

Загрозувањето може да се дефинира како ,,можност или интенција на некој настан/активност, преку битен конкретен фактор неповолно да дејствува со јасно изразена сила на определен простор и продуцира неповолен исход" така што изворите на загрозување се поделени во четири групи:

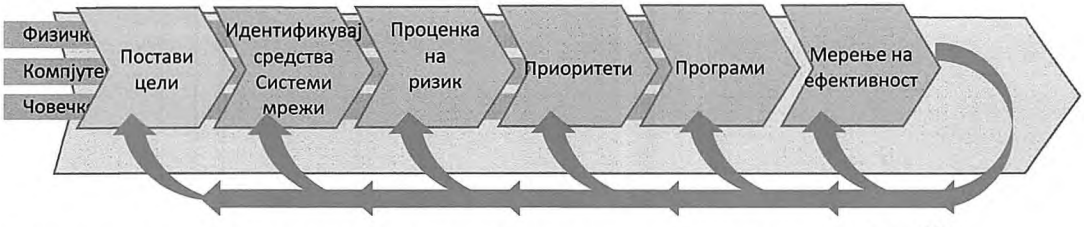
- Природни катастрофи – метеоролошки празнења, силни ветрови, студови – мрзнења, земјотреси, поплави;
- Општествени девијации – кражби, измами, злонамерни оштетувања, индустриска шпиунажа, саботажа, диверзија и др;
- Технички случаи – користење во процесот на несоодветни супстанции , пропусти во заштитата, оштетување на опремата;
- Човечки пропусти – негрижа, неуредност, неупатеност и сл.[136]

[134] Даничиќ Милан, Стајиќ Љубомир . cit. str. 49-50.

[135] Бакрески. О, Драган.Т, Митевски, Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот – Скопје 2012 стр. 56

Природни, односно елементарни несреќи може да се дефинираат како деструктивни и/или антропогени појави, односно како процес со големи размери што претставува опасност за животот и здравјето на луѓето, а може да доведе и до уништување на материјалните добра и на животната средина[137]. Иако природните опасности не може да се избегнат, интеграцијата за процена на ризикот и навременото предупредување, во мерките на превенција и намалување, може даспречат нивно преминување во катастрофа, што значи дека може да се преземаат акции со цел значително намалување на сите последици. Во природни непогоди спаѓаат: земјотреси, поплави, цунами, вулкански ерупции, лизгање земјиште, одрони, урагани, масовни шумски пожари, снежни наноси и лавини, поплави и суши, обилни врнежи, тешки мразови, епидемии, епизоотии, масовно ширење шумски и полски штетници.Силата на земјотресот сама по себе не е доволна да ги одреди големината на загубите, бидејќи ниту големите катастрофи во услови на слаба ранливост и добрата подготвеност на населението како и одличниот менаџмент не подразбираат големи загуби. Во врска со тоа, на специфичноста на проектирање објекти и инфраструктурата на корпорациите, на сеизмички трусни подрачја се состои од потребата за одредување максимално очекуваниот интензитет на земјотресот како и вклучувањето на овие процени во проектот за изградба.[138]

Сликата покажува шест последователни чекори на рамка за управување со ризици. Во рамката се преставени: Поставени цели и задачи; Идентификација на средства, системи, мрежи; Процена на ризикот последици, слабости, закани; Давање на приоритети; Реализација на програми и Мерење на ефективноста. Повратна јамка која се протега од последниот чекор па наназад во првите пет, претставува континуирано подобрување на заштитата. Инпутот во оваа стандардна рамка е преставен низ три елементи на критичната инфраструктура: физички, сајбер, човечки закани[139].



Сл7. воспоетавување на секторски цели во енергетскиот сектор во САД[140]

[136]Зоран Доревски – Практикум - Обезбедување, Комора на Република Македонија за обезбедување на лица и имот Скопје, Јуни 2004 стр.36
[137]Бакрески О. Триван Д. Митевски С. Скопје 2012 – Корпорорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот стр 56.
[138] Исто стр. 57
[139]https://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf Превземено на 11.04.2014год.
[140]https://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf Превземено на 11.04.2014год.

Ваквата рамка претставена од страна на енергетскиот сектор на САД, со мали модификации може да се употреби во голем дел од критичните инфраструктури за управување со ризици. Може да се каже дека, претставува универзален модел за управување, а пред се во елиминирањето на потенцијалните ризици.

Според препораките кои ги дава германското министерство за внатрешни работи, опасностите со кои се соочуваат операторите на критичните инфраструктури се претставени како:

- опасности поврзани со природни настани,
- опасности кои се однесуваат на човечка грешка или технички дефект и
- опасности во врска со тероризмот или кривичните дела[141].

Во истиот документ се споменуваат и загрозувањата на безбедноста на инфраструктурите од страна на реално надворешни влијанија кои можат да бидат предизвикани од соседните објекти, ефектите на меѓузависност и сл.

Од аспект на комплексноста и хетерогеноста на факторите на ризик кои треба да се имаат во предвид, но не со ограничување само на наведените, претставени се:

- **Фактор на ризик – Човек**
  - Несоодветна свесност за безбедност
  - Несоодветно квалификуван персонал
  - Човечка грешка
  - Криминално однесување (саботажа, терористички напади и сл.)
- **Фактор на ризик - Организација**
  - Концентрација на витални ресурси
  - Надворешно управување (Outsourcing) на инфраструктури кои се од клучно значење за компанијата
- **Фактор на ризик: Природа / животна средина**
  - Природни непогоди
  - Епидемии
- **Фактор на ризик - ИТ**
  - Комплексноста на системи
  - Зголемување на ИТ-зависност
  - Опсежност, вмрежување на ИТ системите во целиот свет
  - Кратки ИТ иновациони циклуси
  - Стандардизација на технологијата и компонентите

[141] Protection of Critical Infrastructures –Baseline Protection ConceptRecommendation for Companies – Federal ministry of internal ,www.bmi.bund.de,Превземено 11.11.2015

- Вмрежување / меѓузависности на критичните инфраструктури
- Интернет како нервен систем на критична инфраструктура (поврзување за безбедност во ИТ)[142]

Загрозувањето на компаниите може да настане и како последица на штетното дејствување на луѓето, без разлика дали е тоа направено свесно или несвесно. Во идентификација на овие субјекти на загрозување на компанијата, методолошки е најдобро да се користат нивните поделби на три категории во однос на средината од која потекнуваат, и тоа на: внатрешни надворешни и комбинирани[143].

Внатрешните носители на загрозување произлегуваат од вработените во компанијата. Тие можат да нанесат штета на компанијата свесно (планирано) или несвесно (од невнимание или не знаење). Ваквиот однос на вработените има за цел директно или индиректно нанесување на губиток на компанијата, што негативно влијае на повеќе фактори во процесите на работењето. Додека пак под надворешни носители на загрозување се подразбираат лица кои не се во работен однос во компанијата, а кои со своите штетни влијанија можат да влијаат на нејзината безбедност, условите за работа и да предизвикаат директно или индиректно негативно влијание.[144]

3. Воведување на проценки од аспект на обезбедување

Под безбедносна проценка се подразбира збир на сознание и заклучоци до кои доаѓаат надлежни субјекти за безбедност во корпорациите, кои се одговорни за состојбите на безбедност која се оценува во соодветна постапка. Во таа смисла, безбедносна проценка е аналитичко синтетички заклучок за моментната состојба на безбедноста во компанијата која ги опфаќа сите значајни елементи за оценување на безбедносната состојба (веројатност, и облици на појава на опасности од потенцијален извор на загрозување и др.)[145]

Проценка на ризик е серија на процеси кои ги оценуваат ризиците од собраните / припремените извештаи за опасност и им определува приоритети, вклучувајќи ги оценките за следното:

- тежина, во согласност со критериумите за сериозноста;

---

[142] Source: Bundesverband deutscher Banken (Federal association of German banks), Management von Kritischen Infrastrukturen, 2004, p. 13 Protection of Critical Infrastructures – Baseline Protection Concept Recommendation for Companies – Federal ministry of internal.

[143] О. Бакрески, М. Даничиќ, Ж. Кешетовиќ, С. Митевски – Приватна безбедност – теорија и концепт Комора на Република македонија за приватна безбедност, Скопје 2015 Стр.106

[144] Исто стр.113

[145] Пајковић Д – Обезбеђење одредзених лицности и објеката, МУП Републике Србије, Београд 2003 стр 88. Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – Скопје 2012 стр67 - , Даничиќ М, Сајиќ ЉЈ, оп. цит.стр.47

- веројатност, во согласност со критериумите за веројатност; и
- ризици, во согласност со критериумите за ризик.

При проценка на ризик на критичната инфраструктура, потребно е да биде анализирано најмалку: ризик од човечка грешка, ризик од надворешни фактори, веројатност за штета на лица; веројатност за штета на имот и ризик од други безбедносни средини. Проценката на ризик може да се направи од страна на менаџерите за безбедност, преку рамката на системот за управување со безбедносната (SMS), и треба да донесуваат одлуки во согласност со критериумите за проценка на ризикот[146].

Постапката за проценка на ризик се состои од три главни целини: 1) идентификација на опасноста (hazard identification), 2) проценка на веројатноста (likehood assessment) и 3) проценка на последиците (consequence assessment)[147]. Во секоја од наведените целини се бара одговор на трите поставени прашања. Резултатите од проценката на ризик преставуваат основни влезни податоци за потребите на управувањето со ризикот (risk management). Управување со ризикот е систематична постапка на одлучување во рамките на кои се дефинираат критериуми за прифатливост на ризикот, утврдување на потребите за негова редукција, идентификување на мерки за редукција и прифаќање на најповолните. Постапките за проценка и управување со ризикот се вика анализата на ризикот (risk analysis)[148].

Донесувањето на одлуки е процес за развој на стратегија за намалување или елиминирање на ризикот од опасност, со користење на резултатите од проценката на ризик и воспоставување на детален план за спроведување. Така што, во согласност со критериумите за донесување на одлуки, може да се донесат одлуки за прифатливоста на опасностите и имплементација на стратегии.

При воспоставување на план за имплементација за преземање противмерки, треба дасе земе во предвид следното:

- Причина, место и време на настанување на опасноста;
- Соодветен метод за отстранување или шема за ублажување на причината, вклучувајќи акции, противмерки, и распореди;
- Изводливост, вклучувајќи очекувани придобивки, трошоци, достапност на ресурсите, итн;
- Ниво на ризик и важност по примената на контрамерки; и

[146] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditioПревземено 12.11.2014
[147] https://www.fer.unizg.hr/_download/repository/Davor_Sinka_kvalif_ispit.pdf, Analiza rizika od terorizma za naftovodni sustav - Davor Šinka, ENCONET d.o.o, Превземено 12.11.2014
[148] Ibid

- Контрамерки по појавата на опасноста[149].

Од тие причинипотребно е да се спроведат контрамерки и планови за имплементација, додека извршните менаџери за безбедност треба да го надгледуваат спроведувањето на противмерките и треба да дадат консултации, совети, поддршка, обука, итн. Изборот на контрамерките е заснован на две информации. Првата е добиена од процесот на анализа на ризик (податоци за идентификација на имотот и закани, проценка од можноста дека нешто ќе се случи, проценка на влијанието и фрекфенцијата, како и проценката на соодветно управување со ризик). Другата информација се однесува на природата на работата, целта и филозофијатана управување и култура на корпорациска организација.[150]

Ако го разгледаме одвоено ризикот од тероризам може концептуално да се дефинира како пресек од три параметри: 1) закана(*threat*), 2) ранливост(*vulnerability*) и 3) последица (*consequence*). Постапката за процена на ризик од тероризам наместо идентификација на опасност и процена на веројатноста содржи компоненти под име процена на закани (*threat assessment*) и процена на ранливост (*vulnerability assessment*)[151].

Проценатa на закани опфаќа идентификација на релевантни сценарија на терористички напади, како и утврдување на веројатност за негова појава.

*Процена на заканата*во идеална ситуација се разгледува како интердисциплинарна постапка во која учествуваат 1) познавачите на терористичките организации и начини на нивното делување (разузнавачката служба), 2) познавачи на средствата за кои се верува дека можат да се употребат во терористичките напади, 3) познавачи на работата на технолошкиот процес, 4) познавачи на методологијата за анализа на ризикот[152].

Проценатa на ранливост од добиените резултати на проценката на заканата се однесуваат на почетокот на нападот, а не на негово успешно завршување. Целта на проценатa на ранливост е да се оцени колкава е веројатноста, поединечните сценарија на терористичките напади во случај да се активираат, ќе резултираат со очекувани последици. Значи, како мерка за ранливост на системот, усвоена е

[149] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionПревземено 12.11.2014

[150] Dorfman S. Mark, Introduction to Risk management and insurance , Prentice Hall, Englewood Cliffs NJ., pp 393 – 396 / Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – Скопје 2012 стр67 - , Даничиќ М, Сајиќ Љ, оп. цит.стр.69

[151] Analiza rizika od terorizma za naftovodni sustav - Davor Šinka, ENCONETd.o.ohttps://www.fer.unizg.hr/_download/repository/Davor_Sinka_kvalif_ispit.pdfПревземено 12.11.2014

[152] Isto

веројатноста на успехот од сценариото на терористичкиот напад. Веројатноста на успехот за поедини сценарија на проценка се земаат во предвид, нивото на техничка и физичка заштита на објектот, можност од рано откривање и други релевантни фактори[153].

Процена на последиците подразбира анализа на негативните последици кои би се појавиле како краен резултат на терористичкиот напад[154].

3 .1. Воспоставување на методологија за процена на ризик

Процена на заканата и управување со ризик, заедно ја формираат основата на одржлив и ефективен безбедносен одговор на заканите, кои се насочени кон критичната инфраструктура. Подготовката на ефикасен план за заштита што е во корелација со заканите, а во врска со прецизно идентификување на заканата или заканите треба да биде првиот чекор во процесот.

Методологија за процена на заканата треба да го вклучува фактот дека таа е доволно разноврсна за да се оценат заканите за државата и критичната инфраструктура, користејќи квантитативен аналитички пристап. Методологијата треба да понуди сигурна постапка за идентификација на опасноста, која, пак, им помага на професионалците за безбедност и други носители на одлуки за оптимална распределба на средствата, набавка на опрема за обезбедување и човечки ресурси. Исто така, моделот за процена на ризик потребно е да одговара на особените околности на државата[155].

За време на вршење на безбедносните процени на загрозеност и проценка на безбедносно работење, се идентификуваат бројни закани и ризици со различно потекло. Во таа смисла, одговорноста на вработените, а посебно на оние што се задолжени за безбедност која е поврзана со менаџмент на ризиците,покрај анализите на ризикотсе поставуваати следните задачи: идентификација на лица, објекти и имот кои вредат да се заштитат, идентификација на закани кои можат да доведат до загрозување на безбедноста на имотот на лицата и на работењето на компанијата, проценка да дојде до штетни случувања, влијанието на заканите на процена,

[153] Isto.
[154] Analiza rizika od terorizma za naftovodni sustav - Davor Šinka, ENCONETd.o.ohttps://www.fer.unizg.hr/_download/repository/Davor_Sinka_kvalif_ispit.pdf. Превземено 12.11.2014
[155] https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionAppendix 2THREAT ASSESSMENT METHODOLOGY, Превземено 12.11.2014

можноста за управување со заканите и идентификација на контрамерките на овие закани.[156]

При изготвување методологија за процена на закана, подобро е да се користи систематски и мерлив пристап за да се оцени кои 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 принципи имаат значајна улога во процесот на управување со ризиците[157]. 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 на 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 дејствија 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 нејасни информации кои се достапни. Аналитичарите на овој тип на информации, без разлика дали тие се од обучени разузнавачки специјалисти, полициски службеници или професионалци за безбедноста, треба редовно да ги оценуваат вклучувајки 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[158].

3.2. Утврдување на критериуми за закана и ранливоста

Аналитичарите треба да утврдат критериуми за заканата и ранливоста пред спроведувањето на проценатa, преку одредување на фокусни точки или центри, што може да се дефинираат како фактори или критериуми кои се проценуваат дека имаат

[156]Кековиќ З, Савиќ С. Комазец Н. Милошевиќ М. Јовановиќ Д. Оп.цт стр. 53 - Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – комора на Република Македонија за обезбедување на лица и имот, Скопје 2012 стр.67 - , Даничиќ М, Сајиќ Љ, оп. цит.стр.66

[157]https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionAppendix 2THREAT ASSESSMENT METHODOLOGY, Превземено 12.11.2014

[158] IbidAppendix 2 THREAT ASSESSMENT METHODOLOGY

најмногу тежина или вредност во одреден процес, на пример држава, оператор на воздухоплов, аеродром, или група на луѓе[159].

Повеќето инфраструктури од причини што имаат ограничени човечки и технолошки ресурси, применуваат квантитативен аналитички пристап кој бара помалку информации за формирање на заклучок. Таквата анализа, го насочува аналитичарот да ги смета релевантнте податоци објективно, наместо со субјективни шпекулации.

Процесот користи два аспекти на анализа кои заедно формираат веродостојни средства за оценување на опасноста и утврдување на 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 со цел 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 незаконско дело би било извршено 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 се нарушени од страна на непослушни лица или ментално нестабилен поединец, чии акции не може да се предвидат, а кои се спонтани.

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 критична инфраструктура[160].

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

[159] ICAO - Aviation Security Manual https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditioПревземено 12.11.2014

[160] ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio Превземено 12.11.2014

за оценување на една група која 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;
- Систем од суштинско значење, може да се опише како волја и средства на една група да ги претвори теоретските цели, како политички агенди или религиозни причини во практична примена преку операции на надзор, стекнување на оружје и развој на изворите на финансирање и обука на оперативците;
- Инфраструктура, комбинира неколку елементи, како што се големина и број на келии на групата или под-единици, една основана комуникациска мрежа и ефективна употреба на линии за транспорт и снабдување;
- Бројност се однесува на постоење на голема мрежа на поддршка, составена од локалните симпатизери или други кои можат да обезбедат засолниште, храна и пари за групата, без разлика дали е тоа во согласност со целите на групата, или од страв и принуда;
- Механизам на борбата се членови кои вршат активности со цел за остварување на целите на групата. На пример, членови - киднапери може да бидат сметани за воини и креаторите на бомби може да бидат наведени како техничари[161].

Во рамките на наведените пет атрибути, може да се додадат функционални подкатегории, 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 шестте 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 беа ограничени на оние кои најчесто влијаат на безбедноста.

[161]ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Editio, Table A2-1. Vulnerability Matrix No. 1Превземено 12.11.2014год.

Категориите вклучуваат присуство на група во која би можеле да изврши незаконско дело, историја на напади, постоење на 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 прилагодени за проценката на заканата од страна на државата и операторите.

Откако ќе се соберат сите податоци, аналитичарот ќе примени мерлив метод на предвидување на нивото на закана за целта која се оценува. Ако збирот се комбинира со збирот за профилот на групата, резултатот може да биде директно поврзан со примената на контрамерки за безбедност пропорционален на проценетата закана.

За завршната анализа и комплетирање на матриците аналитичарите треба:

- да наведе 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 спрема бројот на поени со поголем број на поени еднаков на повисоко ниво на закана и ранливост[162].

Треба да се претпостави дека, темелно објаснување со опфаќање на причината за одредени заклучоци треба да ја прати проценатa на закана. Добро втемелено објаснување како резултат го оправдува програмот за управувањето со ризикот, кој ќе се осмисли за да се спротивстави на проценетите закани.Како и со кој аналитички метод, 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.[163]

3.3. Модел на управување со ризици

Двата концепти, проценка на заканата и управување со ризик, кои заедно ја формираат основата на одржлив и ефективен безбедносен одговор на закани врз критичните инфраструктури од аспект на моделот за управување со ризици,

[162]https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionAppendix 2THREAT ASSESSMENT METHODOLOGY, Превземено 12.11.2014

[163]ICAO – Aviation Security Manual - https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditioПревземено 12.11.2014

безбедносните професионалци одамна препознаа дека спроведувањето на зголемени превентивни мерки, пропорционално со повисоко ниво на закана е поврзано со трошоци кои можат да резултираат со големи финансиски оптоварувања на ресурсите на државата или компанијата. Затоа, се смета дека е поефикасно да се употреби одбрана каде и кога тоа е најмногу потребно, наместо тоа да се применува универзално.

Стандардите кои се зададени 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 оглед на типот на заканите кои влијаат врз работењето, со намера да се обезбеди минимум унифицирани стандарди на безбедност. Доколку државата воведува дополнителни безбедносни мерки за да одговори на повисоко нивото 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 кој би можел да се користи и прилагоди според потребите[164].

Ако се претпостави дека потенцијалните сторители на заканата може да го поразат безбедносниот систем, ако им се дадат 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, која може да се опише дека државата има политичка волја и придружни способности да се одржуваат соодветни, сигурни безбедносни практики. Без обврска за одржување на ефективни мерки за безбедност, ефикасноста на другите принципи е намалена. Со преземање на чекори за да се спречи дејствија на незаконско постапување и други криминални активности насочени против критичната инфраструктура, одржливоста на безбедносните мерки треба да се оценува преку инспекции, контроли и прегледи, согласно регулативите кои ги третираат областите.

[164]ICAO – Aviation Security https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionПревземено 12.11.2014

3.4. Потреба од воведување на матрица за управување со ризик

Постојат три нивоа на услови за закана, за кои се поставени сооветни комплети на контрамерки во корелација во матрицата за управување со ризик.

- основно - покажува ниски услови на закана каде што, во отсуство на сигурни разузнавачки информации кои 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 анти-владини фракции;
- средно - разузнавачките информации укажуваат дека постои веројатност еден или повеќе објектида се посочени за напад; и
- високо - разузнавачките информации укажуваат дека еден или повеќе оператори и / се специјално одредени за напад[165].

Пред доделување на противмерки, треба да се разгледаат следните постапки:

- процена на природата и степенот на загрозеност на операторот во согласност со валидна проценка на заканата;
- да се утврди времетраењето на зголемените услови на закана;
- запознавање со изгледот и 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 кои би биле предмет на подобрени безбедносни процедури[166].

Управувањето со ризици претставува исклучително важен дел во целокупното управување на корпорациите и нејзините активности. Практично, непостои компанија која не користи некој облик на проценка на ризик, иако често не е свесна за тоа.[167] 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.[168]

---

[165]https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-Edition, Превземено 12.11.2014

[166]ICAO – Aviation Security https://www.scribd.com/doc/109422672/Doc-8973-05-Security-Manual-Seventh-EditionПревземено 12.11.2014 год.

[167]Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски, Комора на Република Македонија за обезбедување на лица и имот, Скопје 2012 стр.67 - , Даничиќ М, Сајиќ Љ, оп. цит.стр.113

[168]Според: Iackovic M. ,, Upravljanje rizikom ,,kojiko treba ga se bojati u poslovanju?"Empirija Magna d.o.o Zagreb 2009 (http: www.ebizmags.com / kako upravlati rizikom u poslovanju / Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – Скопје 2012 стр67 - , Даничиќ М, Сајиќ Љ, оп. цит.стр.116

ГЛАВА V

Актите на незаконско постапување како извор на закана врз безбедноста на виталните објекти

1. Актите на незаконско постапување против критичната инфраструктура

Во овој дел, предмет на елаборација и анализа ќе претставуваат актите на незаконско постапување во смисол на криминалните активности, односно, кривичните дела кои резултираат со потенцијални или фактички загуби. Тука, пред се, опфатени се општествените девијации претставени низ диверзии, саботажи, киднапирања, пренесување на неточни, односно лажни информации кои би ја загрозиле безбедноста, нарушувања на јавниот ред и мир и др., секако вклучувајќи го и тероризмот како најекспонирана област на загрозување кога се во прашање критичните инфраструктури.

Од аспект на општествените девијации – кривичните дела се предизвикани со човечкото поведение, кое законодавецот го смета и го пропишал за опасно, а со кое се нарушуваат определени општествени односи. Истите можат да бидат предизвикани од негрижа или со умисла. Облиците и формите на загрозување, начинит на извршување на кривичните дела и употребените тактики од страна на криминалците може да бидат неограничени. Според битието на делото и објектот на напад, се делата на:

- Кривични дела против животот и телото (пр. убиство, телесна повреда, излагање на опасност и др.)
- Кривични дела против слободите и правата на човекот (пр.присилба, противправно лишување од слобода, грабнување, злоупотреба на лични податоци и др.)
- Кривични дела против имотот (пр. кражба, тешка кражба, разбојништво, оштетување на станбени и деловни згради и др.)
- Кривични дела против државата (пр. шпиунажа, саботажи, диверзии и др.)[169]

Една од подобро регулираните области од аспект на обезбедувањето, секако претставува воздухопловството. Анализирајќи ги дефинициите кои се понудени во регулативите на релевантните воздухопловни организации како акт на незаконско постапување претставени се дела или обиди на акти да ја загрозат безбедноста на цивилното воздухопловство, вклучувајки (но не се ограничени на):

- незаконското одземање (грабнување) на воздухоплови,
- уништување на воздухопловот во сервисот,
- земање заложници во воздухопловот или на аеродроми,
- присилен упад во авион, на аеродромот или во просториите на воздухопловен објект,

[169] З. Доревски – Практикум - Обезбедување Комора на Република Македонија за обезбедување на лица и имот, Скопје, Јуни 2004 стр.37

- внесување во авион или на аеродром на оружје или опасни средства или материјал наменет за кривични цели,
- доведување на воздухопловите во функција на предизвикување смрт, тешка телесна повреда, или сериозна штета на имот или животната средина,
- комуникација на лажни информации кои можат да ја загрозат безбедноста на воздухопловот во лет или на земја, на патници, екипаж, земјата персонал или општата јавност, на аеродром или во просториите на објект за цивилната авијација[170].

Криминалните напади на лицата и имотите се манифестирани, исто така, преку извршување на разни кривични дела од областа на политичкиот, општиот (класичниот) и стопанскиот криминалитет, а во последно време се почесто и во работата на компјутерскиот криминалитет. Најзастапени се делата кои припаѓаат во општ криминалитет, но потребно е да се има во предвид дека многу кривични дела и нивните извршители од доменот на стопанскиот криминалитет никогаш не се откриени. Исто така, некои од карактеристиките својствени за општиот криминалитет се однесуваат и на стопанскиот, при што е важно да се истакне дека одредени специфичности се однесуваат само на стопанскиот. Политичките кривични дела во пракса не се големи, но треба да се има во предвид дека таквите дела се сериозна закана или се општествено опасни појави.[171]

2.Тероризмот како закана за безбедноста на критичните инфраструктури

Основна карактеристика на тероризмот е дестабилизација и загрозување на основните општествени, социјални и политички вредности на државата и општеството. Тероризмот во најголем број случаи ги надминува националните граници и ефектите се чувствуваат во сите сфери на современото живеење.Од тие причини,неопходно е да се познаваат сите видови на поврзаност меѓу терористичките акти и севкупните односи и состојби во домашната и меѓународната политика. Тероризмот како општествено опасна појава го третираат огромен број на правни акти, меѓународни конвенции, директиви, во насока на организирана борба на правната држава против сите видови на тероризам. Во појмовното определување на современиот тероризам присутни се академски и административни дефиниции. И едните и другите го третираат насилството како карактеристичен показател за постоење на современиот

[170] ICAO – ANNEX 17
[171] О. Бакрески, М. Даничиќ, Ж. Кешетовиќ, С. Митевски – Приватна безбедност - теорија и концепт, Комора на Република Македонија за приватно обезбедување, Скопје 2015 Стр.106

тероризам. Со насилството се демонстрира сила, чија деструкција го надминува психичкиот ефект. Покрај тоа што во литературата постои висок степен на согласност за тоа дека насилството е најрелевантна компонента при дефинирање на тероризмот, сепак, поимот физичко насилство во контекст на тероризмот неминовно се надополнува со психолошкото и структурното насилство. Најголем број на автори, кои го проучувале феноменот на тероризмот сметаат дека политичката компонента е една од важните елементи на тероризмот. Ова може да се забележи во билатералните договори, потоа во законодавствата на голем број на држави, како и во документите за репресивните државни органи.[172]

Најчести елементи на академските дефиниции за тероризмот се насилството како *метод*, граѓаните и владата како *мета,* предизвикување на страв и изнудување на политички или социјални промени како *цели,* а огромниот број на жртви кон кои се стремат терористите покажуваат на *спектакуларност* како дефиниционен елемент на тероризмот[173].

Обединетите нации сметаат дека, терорист е секое лице кое, дејствувајќи независно од знаењето на некоја земја, како поединец или член на некоја група, која не е признаена како званично тело или дел на некоја нација, постапува на тој начин што ја уништува имовината на цивилното население или владата за да постигне определена политичка цел. Тероризмот е акт на лишување на животи, ранување или акт на уништување или оштетување на имовината на цивилите и владата, без јасна дозвола на определена влада, од страна на поединци или на група на луѓе кои самостојно делуваат, или влади кои делуваат од сопствени побуди или верувања, за да се постигне определена политичка цел[174].

Европската унија го дефинира тероризмот како намерен акт кој може да предизвика сериозна штета на државата или на меѓународната организација, направен со цел сериозно да се заплаши населението, неоправдано да се принуди владата или меѓународната организација да направи нешто или да се воздржи во некоја активност, сериозно да се дестабилизира или уништат основните политички, економски или друштвени структури со помош на напад на животот или физичкиот интегритет на некоја личност, киднапирање, држење на заложници, киднапирање на воздухоплови, бродови и сл. или со производство, поседување или транспорт на оружје.

---

[172]Управување со вонредни ситуации предизвикани од тероризам во воздушниот сообраќај во Р.М – Институт за безбедност, одбрана и мир, Филозофски факултет УКИМ Скопје-Магистерски труд.
[173]Р. Гачиновиќ Антитероризам – Библиотека на тргу Београд 2006 стр. 19
[174]Исто стр. 21

Дефинициите кои го детерминираат тероризмот најчесто имаат недостатоци од причина што многу често се базираат на конкретни ситуации, па во тој случај генерализирањето не ја намалува применливоста во праксата во однос на друга ситуација. Како и да е, при анализите на поголем број на дефиниции може да се заклучи дека тероризмот е политички мотивиран, многу деструктивен феномен и опасен вид на насилство кој најинтензивно го погодува цивилното население и институциите на државата.

Дефакто, тероризмот се разликува од останатите облици на загрозувања, а како диференцирани компоненти во оваа смисла би ги издвоиле : политичката конотација на актот, насилството или заканата со насилство, психолошкиот ефект кој мора да биде и надвор од конкретната мета, како и организиран од страна на определена организација. Во смисла на дефинирање на тероризмот низ одговор на прашањето: Како против тероризмот, би било: Тероризмот е организирана примена на насилство (или закана со насилство) од страна на политички мотивиран извршител, кои одлучиле низ страв, закана и паника да ја наметнат својата волја врз органите на власта и грѓаните.[175]

Тешкотиите во дефинирањето на тероризмот произлегуваат од фактот што терористичките постапки (без исклучок), предизвикуваат кај жртвите одговор кој е емоционален, секогаш полн со омраза и огромна желба за одмазда. Сепак, огромниот број несогласувања и тешкотии во дефинирањето на тероризмот не значи дека оваа мошне опасна појава темелно не се проучува и дека во меѓународната заедница не постојат дефиниции кои прецизно и сеопфатно го дефинираат овој ,,*феномен на нашето време*".[176]

Според Брајан Џенкинс (Brian M. Jenkins), кој е еден од водечките стручњаци во борбата против тероризмот, всушност тероризмот претставува театар, каде глумците се извршители на нападите и нивните жртви, а публиката е јавноста и власта на која и се пренесува пораката. Според неговиот став, тероризмот се состои од нелегитимна употреба на сила за постигнување на политичка цел, кога невини луѓе служат како мета[177].

Според Волтер Леквер, тероризмот е однапред смислено, намерно, систематско убивање, заканување и заплашување, со цел да се предизвика страв кај невините луѓе

[175]Радослав Гачиновиќ Савремени тероризам, Графомарк Београд 1998 год. Стр 31
[176] Митко Котовчески Современ тероризам, Македонска цивилизација, Скопје 2002 Дел I, стр 26 - 28.
[177]Исто стр. 26

за да се оствари политиката, или тактичката предност и вообичаено да се влијае врз јавноста[178].

Џемс М. Поланд го определува тероризмот како противзаконска употреба на закани и насилство против лица и имот првенствено за реализирање на понатамошни (идни) политички и социјални цели. Обично, се настојува да се заплаши владата, поединци или групи, или да се измени нивното однесување и политика[179].

Според други дефиниции одзападнатапровиненција, тероризмот претставува противзаконска употреба на сила и насилство против лица, против сопственоста, со цел да се заплаши или да се принуди власта, цивилното население, или некој дел од него, за да се постигнат определени политички или социјални цели во периодот што следи[180].

Претходно презентираните дефиниции за тероризмот кои се превземени од ,,западните автори" имаат ,,единствен заеднички именител" според кој тероризмот претставува:

Нелегална, противзаконска примена на закана за употреба на сила и примена на систематско насилство, односно извршување на убиства, закани, сеење на страв од страна на поединци, групи, или организации, насочени против населението (или негови делови), сопственоста и владата со цел, да се промени политичкиот курс и да се остварат нивните политички и социјални цели[181].

Тероризмот претставува и тактика која се користи во мир, при конфликт или војна, или по прецизно, терористичкиот напад може да претставува настан кој ја означува транзицијата од мир во конфликт или војна[182].

Согласно кривичниот закон на Република Македонија, тероризмот како појава е регулиран во членовите 394 а,б,в ,,Тој што ќе изврши едно или повеќе дела на убиство, телесно повредување, грабнување на лица, уништување на јавни објекти, транспортни системи, објекти на инфраструктура, компјутерски системи и други објекти за општа употреба, грабнување на авиони или други средства на јавен транспорт, производство, поседување, транспорт, трговија, набавка или примена со нуклеарно оружје, биолошки, хемиски оружја и други видови на оружја и опасни материи, како и истражувања во насока на развој на биолошко и хемиско оружје, пуштање на опасни радиоактивни, отровни и други опасни супстанции или

[178]Исто стр.26
[179]Исто стр.27
[180]Митко Котовчески Современ тероризам, Македонска цивилизација, Скопје 2002 Дел I, стр 26 - 28.
[181]Исто стр.27
[182]Пошироко види : Митко Котовчески Современ Тероризам Македонска цивилизација 2002 дел I, стр 27, 28

предизвикување на пожар или експлозија, уништување на постројки за снабдување со вода, енергија или други основни природни извори, со намера за загрозување на животот и телото и создавање чувство на несигурност или страв кај граѓаните, ќе се казни со затвор најмалку десет години или со доживотен затвор."[183] Во самиот закон предвидени се санкции и за лицата кои создаваат групи, или друга злосторничка организација за извршување на кривични дела, помагателите, потикнувачите, подржувачите, за лицата кои употребуваат електронски средства за оваа намена и сите форми на соработка поврзани со тероризмот. Финансирањето на тероризмот,исто така, претставува тешко кривично дело опишано во кривичниот закон на Република Македонија со конкретно определени санкции за директно или индиректно финансирање на ваквите дела.

Кога зборуваме за тероризмот низ ефектите кои се постигнуваат преку истиот, а посебно кога се во прашање критичните инфраструктури, најчесто не заради постигнување на ефект врз нападнатата цел, туку повеќе заради драматично влијание врз јавноста или јавното мислење како елемент на терористичките цели, да застрашуваат поединци или групи за да го променат своето однесување или политичко делување. Самата стратегија на терористичките организации за напади врз критични инфраструктури претставуваат и атак врз национален или интернационален репрезент на одредени држави и таквиот акт претставува наводен атак врз државата која во основа е зависна од дадената критична инфраструктура.

Терористичките стратегии во голема мера се детерминираниод ,,стратегиите" на водачите на терористичките организации, од нивните мечтаења и желбата за остварување на проектираните цели[184].

Еден од поважните аспекти на терористичката стратегија претставува публицитетот. Во текот на терористичките инциденти постојат три примарни (клучни) играчи - терористот, владата и жртвата. Двата дополнителни играчи се јавните гласила и ,,публиката"(јавноста). Во овој опасен терористички тријаголник правата цел на тероризмот е интензивно да се влијае на дел од општеството со систематско продуцирање на страв.На секоја успешно извршена терористичка операција, секогаш предходи огромна и макотрпна подготовка и работа, солидна обука и нејзино филигранско планирање.

Терористот, како поединец е личност која поседува посебни психолошки особини, кои содејствуваат со структурните причинители за тероризам и тоа:,,посебни црти на

[183] Кривичен законик на Р.М член 394
[184]Митко Котовчески Современ Тероризам Македонска цивилизација 2002 дел III стр. 297 - 300

карактерот,,(страв, бес, депресија, вина, антидруштвено однесување, големо его, потреба за возбуда, чувство на фрустрација и др.) подложни на здружувања, имаат способност за учење, желба за стекнување на знаења, и др.[185]Просторот на делување на терористичките организации е неограничен, а анонимноста е дополнителен проблем во справувањето. Тактиките и методите на дејствување се секогаш во корелација со напредните технологии со што се зголемува и моќта на организациите. Разноврсноста и заштитената комуникација со примена на шифрирани податоци и ставање во функција на информациските технологии кои се се подостапни, употребата на психотропни супстанции во текот на нивните акции во голема мера ја зголемуваат опасноста од ваквите акти.Исто така, науката и познавањето на многу научни дисциплини, и тоа не само од сверата на безбедносните науки, туку и од областите на психологијата, филозофијата, теологијата, техничките и многу други науки кои ги стават во функција на тероризмот.

Современите терористи се инфилтрирани во нормалните општествени текови на општествата и со ништо не заостануваат, односно разликуваат од останатите во начините на живеење. Мора да се спомене дека, регрутацијата на кадри се прави од страна на специјализирани инструктори уште од најмала возраст, врз основа на длабоки анализи на карактерните особини на поединецот. Мотивациониот аспект може да биде од повеќе природи: религиозни, материјални, националистички, историски, социјални како и политички. Исто така, може да се работи за високо образовани кадри кои се инфилтрирани во голем број компании и критични инфраструктури. Примерот од водачот на исламскиот џихад проф. Др. Рамадан Абдулах Шалах кој долги години беше шеф на катедра и професор на Универзитетот во Јужна Флорида во САД[186] ја потврдува инволвираноста во клучни позиции во општеството. Дека во терористичките напади се застапени не само мажи, потврдува фактот дека во периодот од 1970 година до 1990 година во грабнувањето на 25 авиони учествувале 38 жени терористки.[187] Исто така, верскиот фанатизам кој се појавува во одредени случаи е една од карактеристиките на поедини организации. Огромните средства, пред се финансиски, со кои располагаат терористичките организации ја зголемува професионалноста не само од аспект на материјална мотивација, туку и вложувањата во интелектуална и стручна надоградба на самите извршители.

[185]Михајло Басара, приказ од книгата на Јонатан Вајт ,, тероризам,, војно дело 4/2004 стр. 157
[186]Радослав Гачиновиќ Савремени тероризам Графомарк Београд 1998 год. Стр 156
[187] Љубо Пејановиќ Тероризам и противтерористичка дејства у ваздушном саобрачају – Војно издавачки завод Београд 2003 год. Стр 176

Спремноста, односно подготвувањето за терористичко делување се реализира од разни експерти во тренинг кампови кои ги нудат сите услови за современи обуки.

Базирани главно на варијантите препорачани од авторите во полето на стратешките студии како и прелиминарните идеи истакнати од Брајан Џексон (Brian Jackson), потикот од терористичката иновација, практично, никогаш неможе да биде резултат на еден единствен фактор и во повеќе случаи веројатно е да биде комбинација од неколку варијанти кои ќе ја обезбедат потребната оперативната сила. Фактори релевантни за терористички иновации се: Улога на идеологија и стратегија, динамика на борба, контрамерки, таргетирање на логичките цели, поврзаност со оружје и иновација, групна динамика, поврзаност со други организации, ресурси, отвореност за нови идеи, времетраење и природата на технологиите[188].

Веројатноста за употреба на хемиско, биолошко, радиолошко и нуклеарно (CBRN) оружје од страна на терористичките организации, станува се поактуелна тема за анализи кои треба да бидат разгледани како од страна на научната, така и од страна на практичарите, односно, службите кои што треба да се справат со овие облици на тероризам. Пристапот до ваквите типови на оружје веќе не е предмет на посебни дискусии, нивната достапност и тоа како ги усложнува стандардните методи за обезбедување. Општите трендови во терористичките тактики и технологии не само што може да предизвикаат значителна штета на државата, туку и ескалација, односно, несвесно подржување на тероризмот од страна на дел од граѓанството. Многу важен елемент при организирање и реализирање на деструктивната активност од страна на терористичките организации претставува и моментот на омаловажување, односно, прикажување на слабоста на државата. Од тие причини, критичните инфраструктури кои во основа претставуваат најдобро чувани, односно врз кои се посветува најголемо внимание од аспект на безбедноста, сами по себе претставуваат мети на терористички напади од најмалку два аспекти:Нарушување на угледот и кредибилитетот низ дискриминирање на државните безбедносни капацитети, а од тука и зголемена фрустрацијата на населението кон владините политики.

Големи материјални и човечки загуби со директни импликации и ефекти во сите свери на живеењето и предизвикување на страв и несигурност.

Саботирањето на критичните инфраструктури често се користи како примарен начин на напад. Саботажата овозможува и дискриминација на одрдена група која ја заштитува инфраструктурата, и често се наметнува негативен ефект во лицето на јавноста и чувство на несигурност, што впрочем претставува и една од целите на

[188] Understanding Terrorist Innovation - Technology, tactics and global trends Adam Dolnik 2007 str.13

терористичките организации. Сепаратистичките организации, саботажата ја користат како одличен начин за потценување на властите во очите на јавноста. Од друга страна,влијанието на саботажите кон критичните инфраструктури презентира кон јавностано и кон инвеститорите чувство на несигурност, односно одвраќање од намерите, посебно во државите зависни од туризмот или од странските инвестиции и може да предизвика дополнителни компликации во сите сегменти на живеењето, а посебно економските ефекти доаѓаат во преден план.

Саботажите се противправни дејства, кои преку нанесување на штета на подмолен и прикриен начин, имаат за цел да го попречат нормалното функционирање на компаниите. Најчесто, саботажите претставуваат дел од поголем предходно подготвен напад, независно од тоа дали целта е да се предизвика поголема материјална штета или да се предизвика губење на човечки животи.

Тактиките на герилската саботажасе поделени во три категории: механичка саботажа по примерот на исклучување на ел. енергија, прекин на снабдувањето со вода, минирање на нафтени водови, преместување на шини од возови, уништување на податоци, друг вид на саботажа,исто така, може да биде и контаминацијата,односно, загадување на почвата и водата и сајбер тероризмот, како многу опасен вид на саботажа[189].

Техничките саботажи, или дејствија кои се извршуваат врз објектите со предизвикување на технички дефекти со кој престанува или оневозможува нормалното функционирање на клучните сегменти во компаниите, претставуваат една од целите на сторителите на кривичните дела. Како облици на саботажи на пример во воздухопловството можеме да ги споменеме следните случаи:

Од аспект на воздухопловите: подметнување на опасни, запаливи или ексолозивни направи во критичните системи, всисување на слободни предмети во моторите од воздухопловите поставени - подметнати на полетнослетната патека, намерно неправилно складирање и утовар на робата и багажите со што би се предизвикал дисбаланс во текот на летот, отварање на прозори или врати во тек на летот, погрешно и неправилно преврзување на електричните инсталации за време на сервисот на воздухопловот, оштетување на стојниот трап на воздухопловот посебно гумите, саботирање на квалитетот на горивото со уфрлување на супстанции кои ке го нарушат нормалното функционирање на моторите и др.

Од аспект на саботажите на аеродромските системи и инфраструктури би ги споменале:поставување на лажни сигнални уреди надвор од аеродромскиот простор,

[189]Understanding Terrorist Innovation - Technology, tactics and global trends Adam Dolnik 2007 str.35

уништување, исклучување на важните системи кои им служат на воздухопловите за изведување на безбеден лет, нарушување на комуникациската технологија, посебно на уредите – воздухоплов - контролна кула, оштетување на полетно слетната патека или поставување на препрека за намерен судар при слетување[190].

Поради посебните специфики кои ги карактеризираат критичните инфраструктури, голем дел од саботажите се извршени од страна на лица кои се постојано или времено вработени во компаниите.

Според кривичниот законик на Р.М Член 315, саботажите во овој контекст спаѓаат во делот на кривичните дела против државата,,Тој што во вршењето на својата работна обврска со намера да го загрози уставниот поредок или безбедноста на Република Македонија на прикриен, подмолен или друг начин, ќе предизвика значителна штета за државен орган, установа или правно лице во кое работи или за друг државен орган, установа или правно лице, ќе се казни со затвор најмалку три години,,.[191] Во истиот Закон член 314 правно се регулира и Диверзијата ,,Тој што со намера да го загрози уставниот поредок или безбедноста на Република Македонија ќе уништи или ќе оштети индустриски, земјоделски или друг стопански објект, сообраќајно средство, систем за врски, систем за снабдување со вода, топлина, гас или друг вид енергија, брана или друг објект од поголемо значење за стопанството или за редовниот живот на граѓаните, ќе се казни со затвор најмалку четири години.[192]

Разликата помеѓу диверзија и саботажа е во начин на извршување, диверзијата е планирана и добро организирана акција, додека саботажата е прикриена, се стекнува впечаток дека е случајна и ненамерна, односно несреќен случај. Ефектите од диверзијата се веднаш видливи и предизвикува последици веднаш по извршувањето. Саботажата предизвикува ефекти и последици најчесто многу подоцна.

3. Опасните материи во функција на актите на незаконско постапување

Опасните материи претставуваат хемиски соединенија, смеси на хемиските соединенија или хемиски елементи кои 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 кои ги поседуваат некои материи се контролираат и употребуваат во дејности

[190] Љ. Пејановиќ Тероризам и противтеристичка дејства у ваздушном саобрачају, војноиздавачки завод Београд - 2003г
[191] Кривичен законик на Р.М Глава дваесет и осма кривични дела против државата член 315
[192] Кривичен законик на Р.М Глава дваесет и осма кривични дела против државата Исто, член 314

каде што постои потполна сигурност. Фактот дека ваквите опасни материи многу лесно можат да се најдат во рацете на криминалните или терористичките структури е повеќе од веродостојно. Влијанието понатаму може да биде повеќекратно како врз живите организми така и врз материјалните добра, 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 на материи каде што не се во голема мерка познати опасните особини, во одредени услови и тие можат да се трансформираат во опасни, сепак, во овој дел поделбата на опасните материи во оваа насока е поделена во четири групи:експлозивни,запаливи,радиоактивни,токсични (ортовни) материи[193].

Во рамките на сите поделби на опасните материи примарно место завземаат експлозивните материи, што преставува и показател дека се работи за најопасната материја. Нивното опасно дејство е засновано на особината на овие материи,така што под влијание на некоое надворешно дејство (средство за иницирање), многу брзо се разлагаат со ослободување на голема енергија и продукти од разлагањето. Експлозивите тоа едноставно и многу ефикасно го извршуваат, без посебни механизми за трансформација на својата хемиска енергија во механичка работа. Трансформацијата се извршува многу брзо, што има за последица способност на извршување на огромно дејство во краток временски интервал. Тоа дејство предизвикува разорување, рушење и уништување со што се прикажува опасната особина на експлозивните материи.

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 смисол на палење, односно предизвикување на пожари.

Радиоактивните материи се посебна врста на 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.

Токсичните материи, кои при оваа подела го завземаат четвртото место, спаѓаат исто така во многу опасни материи. Токсичноста е многу значајна карактеристика на хемиските материи, а посебно тоа што може да се манифестира на различни начини.

[193]Група автори:Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998

Хемиските материи, меѓусебно се разликуваат по својата отровност. Одреден број на хемикалии воопшто не е токсичен, многу се токсични само незначаен број, додека некои се токсични во таа мерка што ракувањето со нив представува голема опасност.[194]

4. Опасните материи во функција на терористичките дејствија од аспект на тактика за дејствување, карактеристики и категории на терористите

Опасните материи и диверзантско терористичките дејствија се тесно поврзани, затоа што за извршување на диверзантско терористичките дејствија во голема мера се користат опасните материи. Кога опасното дејство на опасната метерија 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 која спаѓа во диверзантско терористичко дејство. За оваа цел можат да се употребат сите четири врсти на опасни материи.

- Експозивните материи претставуваат едни од најекспонираните опасни материи кои се применуваат за извршување на терористичките активности. Според Адам Долик 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 ги споменеме :

- Подметнувања на експлозиви на земја, такви примери се употребата на молотови коктели, импровизираните експлозивни направи, минирањата и сл.
- Подметнувања на експлозиви во: воздушниот(употреба на мали количини на експлозив за предизвикување на големи загуби), морски, патен и железнички сообраќај.
- Исфрлање на бомби од мали авиони врз дадени цели или пак употребата на воздухопловите како средство за масовно уништување, пример 11 Септември 2001г.[196]

Експлозивните материии се хемиски соединенија и хомогени односно хетерогени смеси на повеќе компоненти соединенија кои под влијание на одреден енергетски импулс, во многу кратко време, со своето хемиско разлагање ослободуваат голема количина на топлина и загреани гасови. Продуктите на разлагање, кои во голема мера

[194]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998
[195]Understanding Terrorist Innovation - Technology, tactics and global trends Adam Dolnik 2007
[196]Understanding Terrorist Innovation - Technology, tactics and global trends Adam Dolnik 2007

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 претвара 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 кои практично можат спонтано да детонираат без било какво 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 течни супстанции, соединенија и смеси[197].

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

- Тринитротолуен (TNT);
- Хексоген и неговите смеси како што е циклотол – В (смеса хексоген и TNT) и некои од пластичните експлозиви со ознаки С – 2, С – 3, С – 4, Н – 6, и Р – 4;
- Пентрит и неговите смеси како што е пентолит (смеса на пентритот со TNT) и пластичниот експлозив деташит – С и
- Октоген и неговата смеса октол (октоген и TNT).[198]

Во некои случаи за изведување на терористички цели се користат и стопанските експлозиви кои се карактеризираат со помала разорна моќ во однос на останатите. Фактот дека ваквите експлозиви се лесно достапни стануваат многу значајни за анализа кога се во прашање терористичките акции и употребата на импровизирани експлозивни направи. Прашкастите стопански експлозиви на база на амониум нитрат кои го носат трговскиот назив ,,амонекс" би ги издвоилеод причина што нивната употреба е присутна во градежнишвото, рударството и сл.

Експлозивните материи се карактеризираат со своите физичко хемиски особини, хемискиот состав и експлозивните својства. На основа на овие карактеристики може да се направи и соодветна поделба. Врз основа на агрегатната состојба како физички својства, експлозивните материи можат да бидат: цврсти, течни и гасовити.Концентрационата енергија е најмала кај гасовитите експлозиви, додека течните експлозиви се неприкладни и многу опасни за ракување, затоа во пракса најповеќе се користат експлозивите во цврста агрегатна состојба, кои покрај другото содржат и најголема концентрација на енергија.

---

[197]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998

[198]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998

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].

Иницијални или примарни експлозиви се супстанции кои служат за активирање на останатите експлозиви. Се карактеризираат со исклучителна осетливост на удар, триење, топлота, искрење и други надворешни влијанија. Вообичаен начин на хемиско разложување на оваа група на експлозивни материи е детонацијата без разлика на количината, со многу мал енергетски импулс. Се одликуваат со мала топлина на согорување и мал гасен волумен, но со доволна сила да предизвикаат детонација на бризантните експлозиви. Од причина што се многу осетливи на почетен енергетски импулс се вбројуваат во многу опасни експлозивни материи, па ракувањето со нив мора да се одвива во склад со исполнување на максимални безбедносни услови, како во фазата на производство и лаборација иницијални средства, така и при нивното складирање и чување[200].

Бризантните експлозиви претставуваат секундарни експлозивни материи-хемиски соединенија или смеси на повеќе компоненти, експлозивни и неекспозивни, кои под влијание на одреден енергетски импулс со својата детонација во поголема или помала мерка извршуваат рушење или кинење на матерјалите и елементите. За разлика од иницијалните експлозиви, бризантните експлозиви се карактеризираат со многу помала осетливост на иницијален енергетски импулс и потешко е да се донесат до режим на детонација по пат на удар, триење или други механички влијанија. Основен облик на нивното разлагање е детонација, но запалени во помали количини горат стабилно и полека, со одредена брзина без детонација. Бризантноста на оваа група на експлозиви се огледа на способноста за кинење на матерјалите во непосреден контакт во тек на детонаторскиот процес на разлагање. Од причина што процесот задетонаторско разлагање на бризантните експлозиви неопходен е силен енергетски импулс, кој се постигнува со употреба на примарни – иницијални експлозиви, па затоа овие се нарекуваат и секундарни експлозивни материи. Во групата на бризантни експлозиви, спаѓа голема група на експлозивни материи, кои

[199] Исто стр. 6
[200] Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998 год.

меѓусебно се разликуваат, по хемискиот состав, брзина на детонацијата, физичката состојба и начинот на употреба.

Во пракса еустановена поделбата на бризантните експлозиви, по однос на нивната примена, на две основни групи:

- Војни бризантни експлозиви, и
- Стопански бризантни експлозиви[201]

Во овој дел секако потребно е да ги споменеме Импровизираните Експлозивни Направи (ИЕН) ,,Improvised Explosive Devices" - ,,IEDs" , кои претставуваат една од основите во функција на извршување на терористичките активности. Модерните терористи често ги користат ИЕН како избор на оружје и често се многу креативни во дизајнирање, камуфлирање и поставување, односно, подметнување во функција на нивните цели.Составни делови на ИЕН се: експлозивот, изворот за напојување, иницијатор односно детонатор, прекидачот, жиците за поврзување и тајмерот. Што се однесува до техничките аспекти на градење на ИЕН, во терористичките напади евидентни се бомби направени од секојдневните предмети, па се до примена на високо софистицирани уреди користејќи дигитални компоненти и сл[202].

Запаливите материи во својство на терористички напади, пред се се користат за предизвикување на пожари во сите осетливи и делови на критичните инфраструктури. Предноста на запаливите материи во однос на останатите опасни материи се: лесна достапност, едноставна изработка на инпровизирани запаливи материи, големи ефекти на страв и паника, вештачењето за причинителите за настанокот на пожар е многу тешко. За намерно предизвикување на пожари најчесто се користат запаливи смеси со оксиданс (термит) или без оксиданс (напалм, легура,,електрон,, или бел фосфор), користени како темпирани или моментални дејства.

- 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 радиациони заболувања (опасни

[201]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998год.

[202]http://www.x-rayscreener.co.uk/?xray=improvised-explosive-devices преземено 11.12.2012 год.

и неизлечиви рани). Различните облици на радијација се разликуваат по енергијата и продорната моќ, па по основ на тоа и различното делување врз живите организми[203].

- Токсични / отровни материи претставуваат специфична безбедносна закана која што 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 поседуваат предности во однос на конвенционалните експлозивни средства:

- 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 кои се користат во биолошкото оружје, се наоѓаат во природното опкружувањен или можат лесно да се нарачаат од биолошките складови.[204]

Една од општоприфатените поделби на биолошките агенси, кои можат да се искористат како биолошко оружје е поделбата според Американскиот центар за контрола на заразни болесикој ги класифицира во три категории А, В, С:

А категоријата вклучува микроорганизми кои претставуваат голема опасност по националната безбедност, затоа што, лесно се шират или пренесуваат од лице на лице, предизвикуваат висок морталитет, имаат потенцијал за поширок круг на делување. Тука ќе ги вброиме: вариолата, антраксот, кугата, боулизам, тулатемија, ебола и ,,марбург" грозницата.

В категоријата вклучува агениси кои се релативно погодни за ширење а ги карактеризира низок морталитет, но тешко детектирање:

- Cohiella burnetti (Q грозница);
- Brucella типови (bruceloze);
- Burkholderia mallei;
- алфавируси;
- рицин, отрови добиени од рициново масло;

---

[203]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998, стр.8

[204]Ревија за безбедност 2/10 Центар за безбедносне студије - Биотероризам и употреба биолошког оружја – Далијела Милиќ

- Clostridium perfi ngens epsilon отрови;
- ентеротоксини В стафилокока.
- Подкатегорија на В агенсите, кои се опфатени патогените кои се пренесуваат по пат на вода и храна:
- Типови на салмонела,
- Шигела дизентерија (Shigella dysenteriae);
- Ешерихија коли (Escherichia coli);
- Колера (Vibrio cholerae);
- Cryptosporidium parvum[205].

С категоријата ги опфаќаат патогените во третата врста на приоритети, кои се карактеризираат со лесно производство и ширење, потенцијално висок степен на морталитет и удар врз здравјето на поголем број на луѓе. Се работи за патогени кои поради нивните карактеристики и расположливост погодни се за масовно уништување, па бараат постојано истражување поради откривање, дијагностика, третман и превенција. Во оваа група спаѓат:

- Нипа вируси
- Ханта вируси
- Вируси на хеморалгичните грозници
- Вируси енцефалитиси,
- Жолта грозница
- Туберколоза отпорна на повеќе врсти на лекови[206],

Тактиката на биотероризмот го опфаќа начинот на користење на биолошкото оружје, неговите карактеристики, специфики, начинот на употреба при терористичките дејства, но и одбраната. Концепирањето на успешните решенија за одбрана бара познавање на тактиките на напад.

Отровите и токсичните материи во функција на терористичките активности можат да се претстават од аспект на нивната особина на труење, кое 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 можат да се слабо, умерено, јако и екстремно токсични материи. Токсичните материи при терористичките активности во врска со труење на личностите можат да се внесат во организмот на следните начини: преку органите за варење, преку органите за дишење, кожно, директно во крвта. Токсичните материи се делат и на

[205]www.bt.cdc.gov/agent/agentlist-category.asp. Превземено на 12.12.2014год.
[206]Исто. Превземено на 12.12.2014год.

гасовити, лесно испарливи, минерални, растителни и синтетички и други поделби. Продирање на отров во организмот го нарекуваме тровање или интоксикација. Тоа има за последица пореметување 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)[207]

Отровите од природно потекло се делат на:

- Отрови од минерално потекло (солите на тешките метали: жива, олово, бакар, бариум, цинк, и др)
- Отрови од растително потекло (алкалоиди, гликозиди, естри, полипептиди, сексвипертени и др.)
- Отрови од животинско потекло (токсини): змиски отрови, шкорпиеви, пајакови, разни инсектиски отрови, бактериски токсинин и др.
- Отровите од вештачко потекло (синтетички) се: хербициди, дефолијанти, инсектициди, родентициди, фунгициди, бактерициди и сл[208].

Исто така, отровите можат да се поделат по нивната токсичност, во однос на количината потребна за предизвикување на средна смртна доза врз човек со просечна тежина од 70кг. Во токсикологијата, посебно во делот на воените отрови, поделбата се врши и според продирање на отровите во организмот, а можат да се поделат во три категории:

- Респираторна токсичност, продирање во организмот преку органите за дишење,
- Отрови кои продираат преку кожата,
- Опфаќаат отрови кои продираат во организмот преку отворени рани и кожни повреди[209].

Според начинот на кој делуваат, отровите може да се поделат на два начини:

- Физичко делување, нагласено е кај оние отрови кои имаат способност за растварање или создавање на емулзии на површинскиот дел на кожата, при што, после продолженото делување, создаваат на кожата ерозија, рани, отвори со помали или поголеми димензии и др. Овој ефект најчесто се јавува како последица на отстранување на мастите (липиди) од површината на кожата, или

[207]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998, стр.8
[208]Исто Стр.
[209]Исто

денатурација на кератинот илиоштетување на воденатa бариера на површината на кожата.

- Хемиското делување е последица на дејствувањето на отровите, и тука се јавуваат повеќе комбинации и начини на делување (директна или индиректна комбинација), делување на таканаречените хелатни материи (агенси) и др.

Од аспект на диверзанско терористичките акти сите отровни супстанции можеме да ги поделиме во две групи:

- Група во која спаѓаат материи кои наоѓаат примена во воени услови – бојни отрови.
- Група во која спаѓаат материи кои имаат специјална намена, заснована врз основа на нивното отровно дејство - се нарекуваат полициски отрови[210]

Во првата група или бојните отрови се опфатени следните материи:

- Загушливци – се отрови кои ги напаѓаат органите за дишење
- Пликавци – се отрови кои делуваат на кожата
- Општи отрови – имаат општо токсично дејство

Во втората група на бојните отрови опфатени се:

- Психохемиски отрови
- Надразливци

[210]Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998, стр.8

ГЛАВА VI

Имплементација на системите за обезбедување во функција на виталните објекти од акти на незаконско постапување

1.Организација на обезбедувањето

Една од примарните цели секако претставува безбедноста на компанијата, која претставува 'рбетот на функционалноста на компаниите. Традиционалните начини на обезбедување се повеќе се потиснуваат пред се понагласените закани кои ги носи глобализацијата. Физичката, оперативно техничката како и сајбер безбедноста стануваат се по доминантни во поглед на обезбедувањето на луѓето, инфраструктурите и податоците. Новите видови на закани бараат пред се организираност на обезбедувањето непрекинато 24 часа секој ден без исклучок, со вклучување на напредните безбедносни системи кои ја пратат технологијата и достигнувањата во функција на обезбедувањето.

Генералните мерки на кои се темели безбедноста на објектот кој е предмет на заштита можат да се групираат во:

- Градежно урбанистички мерки, кој ги опфаќаат градежно архитектонските карактеристики на објектот, уредување на околниот терен, функционалноста на поедини целини и бараните безбедносни потреби,
- Организациски мерки, ги опфаќаат организацијата на службите за обезбедување, распоредување на персоналот, обука и усовршување и др.
- Оперативни мерки, кои опфаќаат организација и собирање на информации, надзор над заштитените области и примена на репресивни постпки и
- Технички мерки, кои опфаќаат примена на средства и уреди за откривање, идентификација и сигнализација на несаканите случувања.[211]

Покарактеристични фактори кои влијаат на применливоста и спроведувањето на горе наведените мерки за заштита се:

- Макро и микро локацијата на објектот,
- Видот, значењето и вредноста на содржините во објектот,
- Активностите кои се извршуваат, организацијата на работа, технолошките процеси кои се извршуваат во објектите кои се предмет на заштита,
- Можностите и облиците на комуникација и движењето во и околу објектите,
- Климатските карактеристики и макролокацијата на објектите и др.[212]

Наведените, но и многу други фактори кои можат посредно или непосредно да влијаат на безбедноста на објектот, треба да послужат за поставување на,,темелот" врз кој се потпира функционирањето на системот за безбедност, а тоа се:

- Проценката на загрозеност,

[211]Милан Благојевиќ – Алармни системи Факултет за заштита при работа – Ниш 2011 Стр. 203
[212]Исто Стр.203

- Проектирање на техничките системи за заштита,
- Организација на службите за обезбедување,
- План / Програма за обезбедување[213]

Доколку постојат технички системи на заштита или други методи на обезбедување, тие се додаваат на наведените фактори и се вклучуваат во програмите или плановите за обезбедување врз основа на проценките на загрозеност.

Потребата од развивање и имплементираност на прописи, практики и процедури за да се заштитат критичните инфраструктури од дејствија на незаконско постапување, земајќи ги предвид безбедноста, уредноста и ефикасноста на компаниите, потребно е да бидат базирани и врз основа на меѓународните легислативи имлементирани преку националната регулатива.

Заштитата од дејствија на незаконско постапување, базирана по основ на проценката на ризик за безбедноста, потребно е да се врши од страна на релевантните институции со постојано следење на нивото на закана во рамките на компанијата и територијата која е предмет на заштита. Субјектите задолжени за обезбедување како на пример: агенции, државни безбедносни сили и други организации на државата, а кои се засегнати со одговорност за спроведување на различни аспекти на безбедност, најчесто треба да се концепираат според структура на просторот, дејноста која се врши во него, вредносната на висина на материјалните добра кои се обезбедуваат, проценката на загрозеноста, јавноста, задачите на организацијата и персоналот за обезбедување кој врши обезбедување.

Со оглед на фактот дека критичните инфраструктури претставуваат цел на дејствија на незаконско постапување и загрозување од различни форми, силната мотивираност на персоналот за обезбедување од дејствија на незаконско постапување, како и крајно совесно и професионално извршување на работните задачи, претставуваат битен елемент за успешно и професионално извршување на оваа многу одговорна и стресна професија.

2. Планирање како функција на безбедносниот менаџмент во објектите од витален интерес

Планирањето е примарна и суштинска фаза во процесот на менаџментот и тоа е одговорност на сите менаџерски нивоа. Планирањето претставува формулирање на цели и барање начин за решавање на остварување на целите, кое е во функција на креирање и прилагодување на организационите структури, стилот на раководење и

[213] Милан Благојевиќ – Алармни системи Факултет за заштита при работа – Ниш 2011 Стр. 203

моделот на контролата. Планирањето пред се претставува целосен начин на нивното остварување. Резултат на процесот на планирањето е донесување на плански одлуки. Главни плански одлуки се целите, додека останатите одлуки служат за постигнување на планираните цели. Прва фаза на планирањето е дефинирање на целите, потоа изработка на безбедносна проценка, проценка на ризикот, донесување на одлука и изработка на план на безбедност, после што се применуваат останатите функции во безбедносниот менаџмент[214]. Сето тоа се однесува и за критичните инфраструктури а се со цел :

- Создавање на адекватни безбедносни услови за непречено функционирање на државата.
- Обезбедување на заштита на критичните инфраструктури и нивните капацитети;
- Обезбедување на заштита на објектите, уредите и инсталациите од значење за безбедноста на критичните инфраструктури;
- Овозможување на преземање дополнителни мерки и активности во ситуации на зголемен степен на закана и вонредни ситуации.

Искуствата од минатото покажале задолжителна потреба за ставање акцент на безбедноста, како фактор за непречено одвивање на процесите за работа, додека пак, настаните од сегашноста имаат директен импакт врз создавањето на одредени безбедносни системи и процедури, кои до ден денес се усовршуваат и надополнуваат со цел да се елиминираат сите можни пропусти.

3.Тела задолжени за обезбедување

Критичните инфраструктури треба да имплементираат тело задолжено за безбедност кое треба да ја анализира ефикасноста на мерките за безбедност, врз основа на анализите и проценките на заканите, настаните и резултатите од контролите на квалитетот за безбедност. Исто така, треба да служи како форум за координирање на безбедносните активности, анализирајки оперативни прашања и проблеми во врска со спроведување на рутинските мерки за безбедност, како и оние големи вонредни настани.

Обрските на оваа тело во најмала рака потребно е да вклучуваат:

- координација со националните прописи кои ја регулираат областа;

[214]О. Бакрески,Основи на безбедносниот менаџмент, Аутопринт Т.А – Скопје, Филозофски факултет – Скопје 2012, стр.87.

- надзор и следење на компаниските програми за обезбедување, мерките за обезбедување на сите релевантни субјекти задолжени за обезбедување;
- сигурност дека безбедносните мерки и постапки се адекватни за справување со заканите и дека тие остануваат под постојана контрола и обезбедување во нормални и во непредвидени, но и при итни ситуации;
- препораки за подобрување на безбедносните мерки и процедури во развој на обезбедувањето на критичната инфраструктура;
- идентификација на чувствителните области, вклучувајќи опрема и објекти, како и преглед на безбедноста на областите на редовна основа;
- идентификација за потреба од специјализирана обука на персоналот;
- информирање на надлежното министерство за состојбите поврзани со безбедноста;
- согласност и анализи на сите планови на компанијата во поглед на инфраструктурни измени или дополнување и осовременување на капацитетите.[215]

Фреквенцијата на средбите треба да се прилагодат на потребите на компанијата.

4. Агенции за обезбедување

Под обезбедување на објекти (имот) се подразбира координирана активност на овластени лица (агенции за обезбедување) кои со помош на технички средства за надзор и детекција, механички средства за попречување и други средства за присилба, преземаат дејства, со цел оневозможување на неовластен пристап кон заштитуваниот објект, откривање, неутрализирање на криминална дејност и други видови на загрозувања, заштита на луѓето кои работат во него, предметите и документацијата и одржување на јавниот ред и мир[216].

Дејноста приватно обезбедување можат да ја вршат, правните лица кои имаат дозвола за приватно обезбедување преземаат мерки и активности заради спречување и откривање на штетни појави и противправни дејствија кои ги загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува. Приватното обезбедување под услови утврдени со Закон се врши:

1) во вид на давање на услуги и
2) за сопствени потреби.[217]

---

[215] ICAO Annex 17 http://www.theairlinepilots.com/forumarchive/quickref/icao/annex17.pdfПревземено на 10.10.2012година.
[216]Обезбедување – Практикум 2004 – З. Доревски стр.151
[217]Закон за приватно обезбедување Сл весник на РМ. Бр 166 од 2012 член 8

Генерално, приватното обезбедување се користи за да се заштитат четири подрачја (сфери):

Првото подрачје е насочено кон заштита на луѓето. Ова може да ги вклучи вработените и клиентите на една организација или граѓаните воопшто.

Второто подрачје вклучува заштита на имоти,

Трето подрачје на заштита е насочено кон заштита на информациите на една организација,

Четвртото подрачје на заштита е обезбедување на потребната репутација на индивидуата или на организацијата[218].

Според субјектот на заштита, разграничени се четири видови на обезбедување:

- Обезбедување на објекти,
- Обезбедување на личности,
- Обезбедување на манифестации,
- Обезбедување на транспорт[219]

Најголем дел од кадарот кој работи на задачи за обезбедување, денес е ангажиран на заштита на објекти со нешто помалку од 40% застапеност[220].

5. Програми и процедури за работа

Програмата за безбедност на критичната инфраструктура потребно е да ги обединува сите мерки за безбедност, кои се предвидени заради заштита и давање на насоки за имплементација на мерките за безбедност. Истата, потребно е да се раководи првенствено врз правните извори од Националното законодавство како и примена на насоките и мерките за безбедност, како што е барано во стандардите и препорачаните практики на меѓународните заедници.

Определувањето на овластувањата, обврските и одговорностите претставува првиот сегмент во изработката на програмата за безбедност, тоа се однесува на компаниискиот менаџмент, одговорните лица за безбедност, оперативните работници за техничко и физичко обезбедување, вклучувајќи ги и државните органи доколку се директно застапени, како и сите релевантни надворешни и внатрешни субјекти вклучени во процесите на работењето на критичната инфраструктура.

Описот на компаниските активности се важни од аспект на одредување и димензионирање на составните функционални капацитети на инфраструктурата, а

[218] Приватна безбедност – теорија и пракса (Бакрески.О , Даничиќ М, Кешетовиќ Ж, Митевски С – Скопје 2015 стр. 239

[219] Обезбедување – Практикум 2004 – Доревски З стр.41

[220] Исто.

пред се: физичките карактеристики, објектите, инсталациите, средствата, уредите, техничката и кадровската опременост, техничко технолошките процедури за работа на компанијата и сл.

Значењето на секоја критична инфраструктура лежи во неопходноста од прецизно дефинирање на сите мерки и активности, кои се во врска со безбедноста и обезбедувањето. Создавањето на внатрешен механизам помеѓу субјектите задолжени за безбедност на критичната инфраструктура и потребата за координација на активностите на сите субјекти, кои што се инволвирани во работењето,налага потребата од формирање на тело за безбедност, кое ќе претставува советодавен орган за сите активности во остварувањето на процесите за работа и примена на мерките за безбедност.

Важен сегмент при изработката на програмата претставува дефинирањето на превентивните безбедносни мерки на критичната инфраструктура. Во описот на овие мерки за безбедност, посебно место треба да заземаат определувањето на безбедносните зони на движење, контролата на движењето, пристапот и надгледување на лицата и возилата, дефинирање на критичните зони, идентификационите картички(бец), осветлувањето, заштитните препреки - периметарската ограда, безбедносните сили на критичние инфраструктури, како и имплементацијата на напредните системи и процедури за работа, документите кои се потребни за влез во компанијата, идентификацијата и проверка на вработените и посетителите од аспект на нивното криминално минато и сл. Во превентивните мерки секако потребно е да бидат разработени процедури за секој сегмент во работењето на пример: прием, складирање и испраќање на ресурсите, процедурата на прегледот на ресурсите и многу други процедури во зависност од спецификите на работењето.

Спроведувањето на превентивните мерки имаат за цел спречување на внесување на оружје, експлозивни или било кои други опасни направи, предмети и супстанци, а кои можат да бидат употребени за извршување на акт на незаконско дејство.

Во програмата треба да се предвидат постапките со кои се дејствува во вонредни случаи, а со цел ефикасно и правилно интервенирање и спречување на негативни последици кои можат да произлезат од вонредните ситуации, како и отстранување на последиците до колку настанат. Ваквите планови треба да бидат како посебни документи истренирани и практично симулирани.

Обуката на персоналот потребно е да го опфати: целокупниот персонал, вклучувајќи ја и обуката која што треба да биде спроведена и врз целокупниот персонал во критичните инфраструктури на полето на значението и свесноста за

безбедност. Тука би истакнале и еден друг сегмент, а тоа е психологијата на вработените лица, бидејќи при незаконско постапување или криминални дејствија, голема помош и придонес во општата безбедност може да даде секој еден вработен, без оглед на кое работно место е поставен според организационата поставеност. Развивањето на една ваква свест е процес кој трае, односно менување на свеста на персоналот во однос кон безбедноста и опасностите на кои може да биде изложен самиот персонал, како и компанијата во целина.

Праксата, истражувањата од студиите за безбедноста како и егзактните статистички податоци покажале дека во повеќето од 90% на случаеви на акти на незаконито постапување биле инволвирани лица кои биле вработени во самите компании. При анализирањето на актите на незаконско постапување, анализите покажале дека тие тоа го правеле свесно или несвесно. Како и да е, последиците односно штетите нанесени врз компаниите обично се многу тешки со губење на човечки животи како и големи материјални загуби.

За изведување на сите безбедносни мерки несомнено потребно е дефинирање на безбедносна опрема и карактеристиките на истата, која треба да ги задоволува бараните перформанси, а се однесува на рентген опремата, металдетекторските врати, рачните метал детектори, мониторинг центрите, системите за дојава на пожари, системите за детекција на провала, системите за детекција на опасни материи и испарливи гасови и сл. како и одржувањето на истата. Развојот на технологијата придонесе за софистицирање на нови модели на безбедносни уреди и системи, со чија помош полесно се утврдуваат, односно пронаоѓаат одредени недозволени супстанции или предмети кои што ја нарушуваат безбедноста на компаниите.

На крај, составен дел од програмата треба да бидат прилозите во поглед на шеми, дијаграми, карти, законски одредби, планови, процедури, податоци, кои во целост ќе ја дополнат програмата. Програмата за безбедност во компанијата треба да го регулира и финансирањето на безбедноста, во рамките на финансискиот план на компанијата потребно е да се предвидат и средства за процедурите поврзани за безбедноста и обуката на персоналот.

Наведените содржини претставуваат некој минимум за изработка на програма за безбедност, кој понатаму ќе служи како основа за извршување на конкретни работни задачи од областа на безбедноста.

6. Координација во функција на обезбедување на виталните објекти

Еден од клучните предуслови за правилно функционирање на безбедноста претставува потребата од дефинирање и распределбата на задачите, како и да се координираат активности меѓу различните институции, агенции и други субјекти засегнати со спроведувањето на различни аспекти на обезбедувањето, кои ја третираат одредената област.

Денес има се понагласената потреба од соработка помеѓу јавната и приватната безбедност, како и експликацијата на природата на соработката помеѓу овие сектори, покажува дека постои простор за зближување на овие два сегменти и дека е јасна потребата од нивна кохабитација за остварување на заедничките цели. Поради комплементарноста на задачите се заклучува дека полицијата и приватното обезбедување се предодредени заеднички да соработуваат[221].

По нападите од 11 Септември 2001 година, оваа соработка е многу изразена и интензивирана, посебно во делот на: заштита на критичните инфраструктури, сајбер безбедноста, заштита на пристаништата, заштита од тероризмот итн. Тука би се издвоиле неколку основни принципи во заштитата на ранливите категории изложени на терористички напади и тоа:

- без разлика на видот на јавното - приватно партнерство, политичарите треба да бидат свесни за важната улога што ја има овој вид на партнерства во справувањето со тероризмот,
- улогата на приватниот сектор не се ограничува само со вклучување во кризните ситуации. Мерките за превенција од тероризам со кои се зголемува нивото на целокупното водење на безбедноста треба да бидат истражени,
- треба да постои селекција на јасни насоки кој вид на информации јавните власти можат да ги споделат со приватниот безбедносен сектор и јавноста во однос на регулативите за заштита на податоци,
- јавните власти во ситуации кога се потребни информации на субјектите од приватниот сектор да им ги стават на располагање и обратно,
- заедничките вежби и тренинг за персоналот од јавниот и од приватниот сектор, може да придонесе во симнување на комуникациските бариери, со што ќе се

[221]Приватна безбедност – теорија и пракса (Бакрески.О , Даничиќ М, Кешетовиќ Ж, Митевски С – Скопје 2015 стр.164

промовира заедничкиот јазик и понатамошното зголемување на довербата помеѓу партнерите.[222]

Од аспект на функциите и надлежностите, најнапред треба да бидат делегирани од страна на соодветните министерства низ законски облигаторни насоки за потребата од обезбедување на критичната инфраструктура. Често пати се случува надлежностите за безбедност да се преклопуваат од страна на два или повеќе субјекти, што на некој начин претставува зголемување на безбедноста, но само под услов на добра координација на безбедносните институции. Но и покрај поделбата и/или преклопување на работите од областа на безбедноста, само еден орган потребно е да биде носител како на активностите,исто така и на евентуалната одговорност.

Со оглед на големиот број на институции и агенции, кои се вклучени во безбедноста на критичните инфраструктури, координацијата меѓу клучните носители на активностите потребно е да се воспостави низ тело кое ќе биде делегирано од страна на државата. Ова може да се постигне со формирање на Национални тела задолжени за координација и контрола во дадените области на критичните инфраструктури, а ќе бидат во надлежност на Владата или дефинираното Министерство, со преставници на високо ниво од сите субјекти задолжени за функционирање на инфраструктурата.

Овој орган односно тело ќе има мандат поврзан со:

- советување за мерките за безбедност во дадената критична инфраструктура по основ на заканите,
- контрола и давање на препораки за за безбедност, (технологии и техники на обезбедување, како и други фактори;
- обезбедува координација на мерките за безбедност помеѓу институциите, агенции и други субјекти,
- имплементација на националните програми за обезбедување како и нивна доследна примена.
- предлагање на политики и регулативи за безбедност или измени на постојните;
- промовирање на развојни концепти за безбедност;
- соработка со меѓународните организации и на други земји со цел да се постигне општи минимални стандарди за безбедност како целина.

Консензуалното донесување на одлуки на членовите ќе осигура дека се исполнети целите и барањата на државната политика.

[222]Приватна безбедност – теорија и пракса (Бакрески.О , Даничиќ М, Кешетовиќ Ж, Митевски С – Скопје 2015 стр.164

7.Разузнавањето во функција на заштитата на критичната инфраструктура

Широкиот спектар на ризици и закани кои ги пратат критичните инфраструктури, бара несомнено еден посебен системски пристап во насока на собирање и размена на информации и се позасилено делување на разузнавачките активности.

Разузнавачкиот безбедносен систем е задолжен за извршување на некои примарни функции од разузнавачката комплексност, што особено се однесува на придонесување на успешно функционирање на државниот апарат, како на внатрешен така и на надворешен план. Во основа, разузнавачкиот безбедносен систем, претставува со прописи дефинирана област на надлежности и меѓусебни права на сите разузнавачки и безбедносни служби и други државни органиили друг ентитет што одговара, кои се ангажирани да собираат, да проценуваат и да се дистрибуираат разузнавачки податоци, како и да извршуваат други надлежности кои им се ставени во надлежност[223].

Целта на формирањето и дејствувањето на разузнавачките служби е во функција на извршување на задачите кои се важни за зачувување на националната безбедност и заштита на националните интереси на државите во меѓународниот систем. Нивна првенствена задача е обезбедување вредни и прецизни податоци и информации, како и давање на тие податоци и информации на увид на крајните корисници[224].

Покрај големата лепеза на активности и обврски кои ја прати оваа безбедносна дисциплина, разузнавањето потребно е да осигура во рамките на ограничувањата на неговата моќ и заштита на економијата од криминални повреди, да спречи невољи при транспорт, во комуникациите и главните објекти на општествената подршка. Исто така, се бори против тероризмот, организираниот криминал, корупцијата кои влијат на интересите на националната безбедност и исто така, да ги идентификува, да ги спречи и елиминира другите злодела. Разузнавачките системи се клучна компонента на секоја држава, кои даваат анализа на информациите кои што се однесуваат на безбедноста на државата и на виталните интереси[225].

Со оглед на полето на дејствување и примарните задачи, службите кои влегуваат во рамките на разузнавачкиот систем можат да се поделат на:

- Разузнавачки служби
- Контраразузнавачки служби

---

[223]Бакрески О,Милошевиќ М., Современи безбедносни системи, компаративна анализа на земјите од југоисточна Европа, Аутопринт Т.А – Скопје2010, стр. 40

[224]О. Бакрески, Контрола на безбедносниот сектор, Филозофски факултет, Скопје 2008 стр.110

[225]Исто стр. 112

- Безбедносни служби[226]

Активностите на разузнавањето се темелат пред се во функција на навремен одговор на безбедносните закани, ризици и предизвици преку дефинирани стратешки цели, воспоставување и развој на соодветни ефикасни механизми за идентификација, превенција, предвидување, рано предупредување и информирање. Целите имаат големо значење во процесот на носење решенија и при креирањето на политиката за заштита на виталните и трајни национални интереси во насока на:

- Идентификација на заканите и оперативно-разузнавачко делување;
- Превенција на заканите;
- Информирање на државниот врв;
- Меѓународна билатерална и мултилатерална соработка;
- Меѓуинституционална соработка;
- Законитост и јавност во работата.[227]

Разузнавачките служби во основа преставуваат специјализирана организација која во рамките на своето делување, спроведуваат тајни разузнавачки, контраразузнавачкин и субверзивни активности, при тоа користејќи специфични методи и средства, со цел остварување на одредени политички интереси и заштита на внатрешната и надворешната безбедност.[228]

Од аспект на деловното разузнавање (Busines Intelligence),тоа преставува збир на методологии и концепти за прибирање, анализа и дистрибуција на информации со помош на различни софтверски алатки, или способност за разбирање и брзо снаоѓање на менаџментот на одредена компанијаво новите услови на работење.[229]

8. Развој и примена на напредната безбедносната опрема за заштита на критичната инфраструктура

Постојат голем број на опрема и уреди кои се користат во функција на обезбедувањето на критичните инфраструктури, но потребно е да се води сметка истата да се користи и одговара на спецификациите кои се барани во домашната и меѓународната регулатива како и во поглед на способноста и чуствителноста на опремата за откривање на забранетите предметиво зависност со објектите, дејностите и условите за работа.

---

[226]Таталовиќ С. Национална и меѓународна сигурност, Политичка култура, Загреб , 2006, стр 221
[227]http://ia.gov.mk/ превземено 17.02.2016 год.
[228] Андреа Савиќ , Увод у државну безбедност, Виша школа унутрашњих послова Београд, 2002 стр.42
[229] F.Dale, H Bonnie, Competitive Intelligence Ethics> Navigarion the Gray Zone, Competitive Inteligence Foundation, Aleksandria VA 2006.,p.115 Бакрески О. Триван Д. Митевски С.– Корпорорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот, Скопје 2012 стр стр.88

Безбедносните системи се во постојан развој со цел задоволување на барањата кои произлегуваат од праксата. Имплементацијата на современите системи зависи од повеќе фактори, но заначајно е тоа што безбедносната оправданост за инвестирање во опрема и средства несмее да биде предмет на економска оправданост. Потребно е само специфицирање на потребите во однос на загрозувањата и ризиците кои ја пратат секоја критична инфраструктура.

Развојот на технологијата несомнено придонесе за софистицирање на нови модели на безбедносни уреди со чија помош полесно се утврдуваат, односно, пронаоѓаат одредени недозволени супстанции или предмети кои што ја нарушуваат безбедноста на критичните инфраструктури.

8.1. X – ray технологија

Скенирањето на багаж, роба и сл. се врши со помош на уреди за детекција (х-зраци) или рачно во присуство на лицето на дискретен начин врз основа на ситуацијата која ја налага природата на работење.

Скенирањето е процес на испитување кој бара високо ниво на посветеност на човечкиот фактор и материјалните ресурси за да ја пронајдат опасноста во огромниот број на анализирани случаи. Скенерите кои се користат за контрола имаат заеднички својства, да помогнат да се донесе одлука дали да се внесе дадениот багаж, торби, предмети во контролираните зони. Безбедносните скенери и целокупната опрема што се користат мора да бидат во комплементарност со човечкиот фактор, кои треба да бидат професионално обучени и високо мотивирани. Проблемот во пронаоѓањето на опасни материјали е мошне комплициран од причина што спектарот на содржините во багажите, торбите и предметите што се контролираат е многу широк, а проблемот со лоцирањето на рачно направените експлозивни направи е сложен. Причината во тоа е што скенерите ја мерат специфичната густина на материјалот, а таа често пати е иста или слична со многу продукти и предмети кои не се опасни сами по себе, како на пример, органски материјали, пластика, кожа, гума, хартија, текстил, хранливи продукти, овие предмети рутински се пренесуваат во рачниот багаж и доколку се пренесува експлозивна направа во дадениот багаж може да помине незабележана поради сличноста на материјал односно специфична густина[230].

Треба да се спомене дека употребата на конвенционалните рентгенски системи постојано се унапредуваат, првите системи биле со флуороскопи, со лоша пенетрација, резолуција и динамички опсег и висока доза на радијација на багажот и

[230] http://www.x-rayscreener.com превземено 15.05.2015 год.

на лицата. Современите системи кои се унапредени, денес обезбедуваат скенирање со детални информации за композицијата и содржината на багажите, торбите и предметите. Најпознатите рентгени ги употребуваат методите на изготвување на слики со голем број на детали за да се зголеми претставата за третираниот предмет, а како последно, резултатот ќе зависи од самиот оператор на рентгенот кој ја донесува одлуката[231].

Најновите технолошки системи вклучуваат детекција на експлозиви, наркотици, оружје, и други забранети предмети и субстанции. На располгање се нудат широка палета на системи со најразлични димензии и перформанси, вклучувајќи и системи кои ги анализираат течностите и го одредуваат неговиот хемиски состав,со цел утврдување дали се работи за закана или не.

Во светот, во развој е CT (компјутерска томографија) технологија која овозможува 3 D слика и висока резолуција. Голем број на аеродроми и други критични инфраструктури користат технологии кои овозможуваат висока безбедносна контрола и целосно скенирање. Со цел зголемување на безбедноста, се повеќе се наметнува потребата од имплементација на CT технологиите.

8.2. Компјутерска томографија

Системот на компјутерска томографија (CT) ја испитува уникатната густина на супстанцијата кога електромагнетната радијација поминува низ неа. Математичките алгоритми кои се програмирани во софтверот на системот градат 3 – D слика на секој предмет. Информациите можат да бидат презентирани на дисплеј, користејќи томографија од секој предмет[232].

Многу вакви скенери имаат ротирачки диск или кружни отвори низ кои предметите мора да поминат, секој предмет, како на пример, парче багаж се движи низ тунел во внатрешноста каде што се наоѓа извор од x – зраци каде што типично е ротиран околу предметот. X зраците поминуваат низ скенираниот предмет од сите агли и се мерат од страна на детекторите кои се наоѓаат во тунелот. Системите за скенирање на багаж кои ја користат томографската технологија се користат на аеродромите од 1997 год., кога за прв пат бил доставен системот за скенирање на FAA направен од страна на GE Security со ознака CTX 5000, од тогаш па навака овој тип на скенери биле развивани од страна на повеќе производители. Најновите варијанти на овој модел, комбинираат проекција со висока резолуција на X зраци и компјутерска томографија, има подлога која ротира 2 резолуции во секунда. Подлогата е способна да внесе до 5

[231]Исто. превземено 15.05.2015 год.
[232]http://www.x-rayscreener.co.uk/x-ray/#other-tech превземено 15.05.2015 год.

детекторски прстени и може да направи 10 слики во секунда со проток од 542 парчиња на багаж на час. Исто така, во тек е имплементацијата на CTX 9800 DSi со висока резолуција и целосно скенирање со помош на 3D EDS (систем за детекција на експлозиви) со што се овозможува брз проток на багажи и попрецизна детекција[233].

Во овој дел ќе ги спомнеме и системите на examiners модел 1000, 3000, 6000 и 3DX кои користат (CT) технологија со двојна енергија за да престави две целосни 3D слики на багажот и неговата целосна содржина, овозможувајќи физичко мерење на густината и податоци на атомскиот број. 3DX поседува прецизност, сигурност и генерира целосни 3-Д слики со супериорна точност[234]. Флексибилни со можност за вмрежување, испитувачот може да се користи како целосно интегриран во линија систем, како дел од делумно интегриран систем или како самостојна единица.Тогаш, системот ги изолира и ги анализира сите работи во багажот споредувајќи ја базата на податоци со експлозивни материи. eXaminers модел 6000 може да процесира 675 парчиња на багаж на час. Ваков вид на скенери биле инсталирани во 26 земји од 1999. Најновиот 3DX бил неодамна инсталиран на аеродромите во Велика Британија. Неодамнешниот подобрен софтвер помогнал во намалување на лажните аларми за приближно 20%. Имплементирани се повеќе модели на скенери како на пример CT – 80, CT 80 XL со разни карактеристики и протоци. Најважно е да се спомене дека во иднина компанијата планира да ја спои ЦТ технологијата за препознавање на материи со автоматски детектор на експлозиви, скенери со висока 2 – D и 3 – D резолуцијата на сликата за препознавање на оружје и други видови на забранети предмети.

Компанијата Rapiscan во меѓувреме го развила системот томографија во реално време – четврта генерација на CT скенирачки машини, која ги задоволува стандардите и на TSA[235] и на Европските ECAC[236]. Ова е важно, затоа што, сите аеродроми во Европа од 2012год.ќе бидат задолжени да оперираат со CT инспекција на багаж. Системот за томографија во реално време RTT (real time tomography) се разликува од многуте други CT продукти во тоа што тој нема движечки делови. RTT е целосно уникатен.

---

[233]http://www.morpho.com/en/public-security/explosives-narcotics-detection/eds-explosives-detection-system/ctx-9800-dsi Превземено 15.06.2015 год.

[234]http://www.sds.l-3com.com/auto_explv_detect/examiner3DX.htmПревземено 15.06.2015 год.

[235] TSA : Transportation Security Administration – Сектор во рамките на американскиот оддел за национална безбедност. Таа ја има целокупната одговорност за сите транспортни модалитети на обезбедување ворамките на САД. Целта на TSA е да се заштитат сите транспортни системи од сите држави на САД (вклучувајќи го и воздухопловството) за да се обезбеди слободно движење на луѓе и трговија.

[236]ECAC : Европска коференција за цивилно воздухопловство. Покрај другото мисијата на ECAC е да обезбеди континуиран развој на безбеден, ефикасен и одржлив Европски воздушен транспортен систем.

Независно од производителите и моделите важно е да се спомене дека CT технологијата овозможува прецизни мерења на густината со многу висока резолуција. Системот може точно да ја мери густината во внатрешноста на шишето, а може дури да ја мери и густината на мешаните течности. Моделите од најновите генерации, покрај останатите можности ги задоволуваат и потребите во поглед на: целосните волуменски мерења, овозможување на операторите да гледаат 2 – D слика и 3 – D проекција, real time проекција, скенирања со едно поминување на торбата низ скенерот, намалување на лажните аларми, тридимензионална волуметрична слика која овозможува поглед од 360 степени на предметот, врзини на анализа на предметите и до 5 секунди по парче, и многу други предности.

8.3. Скенирање на рачниот багаж, торби и предмети

Процесот на скенирање бара висока посветеност и професионалност за дасе откријат заканиебидејки опасниот предмет може да биде добро скриен помеѓу големиот број на предмети[237].

На сите аеродроми кога се работи за рачниотбагаж конечната одлука за тоа дали еден предмет ќе биде ставен во авион почива во одлуката на операторите. Скенерите кои се користат за контрола, имаат заеднички својства, да помогнат да се донесе таа одлука односно дали да се внесе дадениот багаж, торби, предмети во контролираните зони или да се стопитаат активностите.

Во забранети предмети најчесто спаѓаат: огнено оружје, рачно оружје или предмети кои служат за напад, гранати, експлозиви, муниција, запаливи производи, отровни средства, компримиран и некомпримиран гас,сите предмети кои служат за напад и одбрана и др.

Системите за скенирање на рачниот багаж, торби и предмети се осврнува кон потребата за ненаметлива инспекција на мали до средни предмети. Скенирањето на рачниот багаж, торби и предмети е погоден за примена во голем број на критични инфраструктури како што се на пример: транспортните ифраструктури, државните институции, енергетските компании, хемиската индустрија и др. Најновите системи за ваков вид на заштита, овозможуваат многубројни енергетски слики, и широк опсег на процесирање на слики кои се клучни за квалитетот на сликата, функционалност на системот, високи перформанси, детекција на опасности со голем опсег на детектирање, со што на операторот му се олеснува можноста да го идентификуваат составот на скенираниот матерјал. Во голем број на вакви скенери инсталирани се и

[237] http://www.x-rayscreener.co.uk/?xray=cabin-baggage-screening Превземено на 15.06.2015 год.

опреми за тревога со прецизно детектирана закана, вклучувајќи ја и автоматската детекција на течности.

И покрај фактот дека, технологијата е се по прецизна, комплексноста на содржините на торбите, багажите, предметите кои се предмет на опсервација каде што во еден момент се присутни голем број на материи, уреди и средства го отежнува одредувањето помеѓу опасностите.

8.4. Скенирање на лица

Службите за обезбедување спроведуваат преглед на лицата со помош на металдетектор врати, рачни метал детектори и рачно. Сите лица не зависносно од критичната инфраструктура, кога влегуваат во контролираните зони потребно, е да им се спроведе контрола поради безбедноста на обезбедуваниот објект но и поради личната безбедност на вработениот или клиентот.

Првиот детектор за откривање на метал во шеесетите години од минатиот век најнапред се употребил во рударството за детектирање на метали. Во осумдесетите години од минатиот век се појавиле првите модерни детектори, кои како технологија користеле електромагнетна намотка која генерирала вкрстени магнетни полиња. Од 95 година па наваму компаниите за производство на метал детектори ги развиле посовремените модели од кога и почнува новата ера на металните детектори. Тие преставуваат програмирачки метал детектори кои генерираат електромагнетно поле за детектирање на метално оружје или орудие кое се наоѓа во лицето во моментот на контролата. При детекцијата метал дисплејот ја лоцира позицијата на сокриениот предмет. Овие модели вршат и евиденција на бројот на прегледани лица и овозможува статистичка операција за контрола[238]. Некои модели нудат и мулти димензионално скенирање со што се зголемува и бројот на прегледани лица.

Развојот на технологијата кое е забележано во последниве години, а по основ на потребите од се поголема заштита посебно на аеродромите, доведе до се поголем број на дополнителни иновативни системи за детекција.

Најдобро познат и најчесто применуван метод за контрола секако останува рачниот претрес. Овој начин е докажан како најдоверлив начин кој има резултирано со голем број на откривања на забранети предмети. Рачното пребарување сепак претставува не ,,популарен" метод на работа од повеќе аспекти, а како главни ќе ги споменеме човечкиот замор и големиот број на лица кои треба да се прегледаат во кратко време.

[238] https://www.google.com- metal detector doorПревземено на 15.06.2015 год.

Металниот детектор може да детектира електро магнетен попис на многу мала количина на метал, но поради тоа се зголемува и лажната детекција. Згора на тоа металдетекторите не се во можност да ги скенираат неметалните закани како што се керамичките оружја, пластичните или течните експлозивии сл.

Ограничувањето на ова технологија довела кон развој на детектори кои работат со помош на х- зраци, кои конвенционално биле користени кај контролата на рачниот багаж, торби и предмети. Ниско напојување на х - зраците се испуштат кон патникот, а потоа се формира слика од сенка на телото. Радијацијата лесно пробива преку секаков вид на облека, а резолуцијата која се добиваод овој систем скоро секогаш е со одличен квалитет.Ова овозможува дури и детекција на најмали предмети кои преставуваат закана и кои ги поседува лицето.

Овој вид на контрола предизвика силни реакции поради приватноста на лицата, но и поради спорото време на проток на лица и барањата кон патниците во текот на ваквата контрола, но и чувството на патниците за време на постапката.

Во развојот на друга технологија која има можност од траги на експлозивни направи на лицата, е потребен застој на лицата со вшмукување на воздух од околината на телото за анализа. Детекцијата може да се изврши многу брзо, но како слабост е покажано тоа што постои веројатност за контаминација на лицата со компоненти кои се слични но безопасни. Исто така, постојат и супстанции кои неможат да бидат препознаени од страна на софтверот. Овој систем за детекција на траги може да биде инсталиран за секундарно скенирање.

Милиметарско зрачење или MMW (Millimeter – Wave) со должина на зрачење помеѓу 1мм и 10мм (доволно за пробивање низ ткаенина и за овозможување на резолуција), развива два типа на детектори – активен и пасивен[239]. Активниот трансмитува и анализира приемни сигнали кои се рефлектирани од личноста на сличен начин со конвенционалниот радар, пасивниот систем не трансмитува само прима природни милиметарски бранови кои се емитирани и рефлектирани од личноста. Активни системи често постојат како портал кој е малку поголем од телефонска говорница. Група на трансмитери и ресивери се движат околу предметот, а собраните податоци се процесираат со цел да се формира 3D слика на личноста. Еден од поновите системи користи сензорно поле вградено во сид, каде што лицата стојат покрај него. Скенирањето се извршува по електронски пат, без движечки делови. Сликите добиени од активните системи можат да имаат многу висока резолуција, како што е случај со системите со Х – зраци кои, исто така, го имаат

[239] http://www.x-rayscreener.co.uk/?xray=screening-peopleПревземено на 15.06.2015 год.

проблемот со приватноста на лицата кои се скенираат. Исто така, се работи за скапа опрема и бара доплонително време за скенирање[240].

Пасивните MMW, исто така, вклучуваат механизми за скенирање, но работат на сличен начин со инфрацрвена термална камера со мерење на контраста – разликата на температурата или термалниот запис – помеѓу телото на лицето и предметот кој го носи со себе. Пасивните системи вообичаено користат повисоки фрекфенции во споредба со активните и поскапи компоненти кои го намалуваат бројот на корисници. Иако резолуцијата може да биде многу подобра, софтверот за процесирање на слика може полесно да ги детектира предметите со различна температура во пасивна слика. Овој систем нуди повеќе можности за автоматска детекција, со што може да се добие висока патничка проодност и откриваат помалку анатомски детали на објектот, и помалку проблеми со нарушување на приватноста[241].

На конвенционалната точка на детектирање со класичен метал детектор, патниците соработуваат, така што, стојат во мал простор помал од 2 метри квадратни.

Стоечката детекција одалечена 20 метри може да биде инсталирана пред шалтерите за регистрација или на други фрекфентни места. Во ова сценарио предметот на интерес може да биде засенат од други луѓе во метежот, но движењето на патниците може да биде менаџирано со повеќе стоечки системи, кои се конфигурирани да го скенираат предниот и задниот дел на лицето.

Многу сензитивни метал детектори се испробани на вакви отворени сценарија, но се пронајдени проблеми при одредување на заканите од големиот број на легални метални предмети кои ги носат луѓето. За разлика од рачно претресување и скернирање со X зраци, MMW се чини дека може да овозможи долгометражни способности, со што ќе стане многу користен во други аспекти на обезбедувањето кое не е поврзано со точките на проверка. На долг домет, на пример на 20 метри само големи предмети можат да бидат детектирани. Вакви системи веќе се користат на некои аеродроми, но и на манифестации каде учествуваат високи преставници. Балансирањето на трошоците, како и големината и перформансите на алтернативните системи, од различните видови на MMW системи, пасивните системи нудат најдобро долгорочно решение за брзо автоматско скенирање на голем проток на лица, како и ниска цена и ниски оперативни трошоци[242].

---

[240] https://en.wikipedia.org/wiki/Millimeter_wave_scanner Превземено на 15.06.2015 год.
[241] Ibid, 15.06.2015 год.
[242] https://en.wikipedia.org/wiki/Millimeter_wave_scanner Превземено на 15.06.2015 год.

8.5. Биомертиско скенирање

Фактот дека безбедносните барања се повеќе се зголемуваат, не само на аеродромите, после терористичките напади на 11 Септември, туку и врз сите критични инфраструктури. Една од централните грижи со кои се среќаваат практичарите и менаџерите за безбедност во компаниите, секако претставува контролата на пристап. Големиот број на физички системи за контрола на пристапот кои се користат денес, се засноваат врз безбројни клучеви, бројчаници, картички и сл. Сите овие методи овозможуваат само привидно чувствона безбедност, затоа што клучевите, картичките и сличните уреди можат да бидат загинати или украдени, додека пак системите на база на бројчаници или шифри зависат од меморијата на корисниците.

Биометриската верификациона технологија е единствениот вистински одговор, која е потребно да биде имплементирана како замена на физичките помагала. Денес, се повеќе аеродроми, но и компании со сериозни ризици се пренасочуваат кон позитивната идентификација со помош на биометриските модели за потврдување на идентитетот и точна престава кое лице пробува да добие пристап до одредена ограничена зона.Биометрика се однесува на параметри поврзани со човечки карактеристики[243].

Биометриските апликации вклучуваат земање на примерок од индивидуите кои потоа се дигитализираат, се автоматизираат и стануваат уникатни во базата на податоци. Користењето на биометриските податоци ја препознаваат личноста која добива пристап во ограничената зона. Пристап до ограничената зона можат да имаат само дел од персоналот, кои имаат конкретни работни задолженија. Овие системи можат да дадат одговор и на многу деликатни работи, поврзани со случаите за опасност, при евакуацијата точно ќе се знае бројот на лица и персонал кој биле присутни во загрозената област. Досегашните системи покажуваа само ограничувачки податоци без целосен преглед на комплетната ситуација.

Аеродромот во Сан Франциско и во Охајо Толедо користат читач на дланки за да овозможат целосна контрола на пристапот на пристанишната платформа и на другите сензитивни делови. Колку за пример, на ефикасноста на овие системи треба да се напомене дека во Сан Франциско 18 илјади вработени го користат читачот на дланки со повеќе од 25 илјади верификации на ден.

Геомертијата на дланката и отпечатоците на прстите се моментално најкористени биометриски технологии, а ирисот и детекцијата на лицето преставуваат методи во

[243]https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=biometric+security+tehnologyПревземено на 15.06.2015 год.

развој. Аеродромот во Манчестер поседува систем за препознавање на ирисот. Овој систем опслужува34000 корисници.[244]

Геометриските решенија денес почнуваат да влегуваат во масовна употреба поради нивната ниска цена и големата безбедност која ја даваат.

8.5.1. Видови на биомертиски скенирања

Секое човечко суштество поседува уникатни – единствени карактеристики кои го идентификуваат. Биомертиските се физички карактеристики кои се користат за идентификација на нечиј идентитет и вклучуваат:

Отпечатоци на прсти, претставуваат најкористените биометриски технологии, системот за препознавање на отпечатоците користи податоци кои ги зема од различните краеви на прстот. Автоматското препознавање на прстот започнало уште во 60 – тите години со напредокот на компјутерските технологии, додека во 1990 година е создаден автоматскиот систем за препознавање на отпечатоци. .

DNA- се наоѓа во нуклеусот на клетката, митохондритската – DNA се наоѓа во митохондрите. Користењето на - DNA произлегува од фактот дека нивото на прецизност како биометриски идентификувач, односно можноста за две индивидуи да делат иста DNA е често помалку од 1 спрема 100 милијарди. Денес, во САД учествуваат 183 лаборатории за собирање на DNA податоци.

Лице – Индивидуите се идентификуваат со анализана карактеристиките на нивното лице, кое неможе лесно да биде сменето и со анализите на растојанието помеѓу одредени точки на лицето. Слики на лицето се прават со помош на фотографии и видео, а потоа се споделуваат. Лицето претставува единствена биометриска технологија која се користи за верификација, идентификација и за надгледувачки цели.

Отпечаток од дланка – Оваа технологија ги мапира карактеристиките на дланкатана на лицето и ги мери сите линии на дланката.

Ирис – оваа технологија ги мери уникатните црти на ирисот, обоениот прстен кој се наоѓа околу зеницата кој содржи приближно неколку стотини различни карактеристики и претставуваат богат извор на биометриски податоци.

Глас – Системот за препознавање на глас фаќа делови од говорот на некоја личност, која мора да зборува на микрофон и да повторува делови од фрази. Примерок од нивниот глас се зачувува за идни споредби.

[244] http://us.allegion.com/irstdocs/article/106462.pdf Превземено на 15.06.2015 год.

8.5.2. Биометриски скенирања на контролните точки

Контролата на персоналот кој се движи во строго контролираните делови на критичната инфраструктура, вклучувајќи ги и аеродромите, посебно во делот на движење во airside (воздушната зоната) на аеродромот, моментално претставува најслаба алка во заштитата на безбедносниот кордон, затоа што голем број од идентификациите се состојат од пин кодови и радио фрекфентни идентификации.

Иако можат да се користат биомертиски системи, ефективноста може да варира. Пример со отпечатоците на прст кој зависи од повеќе фактори, носење на ракавици, чистината и контаминацијата на прстот и сл. кај системот со лице идентификуван е проблемот, односно, сериозноста на лицата во поглед на отвореност на очите или насмевкаи сл, но значајно е што овој вид на технологија е во постојан развој и ги мапира одредените точки налицето кои подоцна се користат за потврдување. Со вметнување на разни технолошки филтри, алгоритми за пронаоѓање на карактеристики на лицата и сл. ја зголемува ефикасноста на овој систем.
Моментално во развојна фаза е системот за скенирање на ирисот кој ќе може да изврши препознавање на растојание од 5 метри, а препознавањето да биде завршено за помалку од секунда.

Системот Glance and go кој е во развојна фаза небара од корисниците да застанат пред него, истото може да се направи во движење. Скенирањето е лесно, каде што лицето доволно е само да гледа во камерата, а системот прави слики од двете очи истовремено, 5 слики од секоја зеница се прават за помалку од 250 мили секунда. Потребни се две секунди да се скенираат две очи и повеќе од една секундада се препознае едно око.

Во овој поглед развивани се голем број на технологии кои ја развиваат оваа област, така што, разни производители презентирааат предности како што се на пример, скенирање без кооперативност на лицата, скенирања без амбиентални влијанија, услови од аспект на аглите на гледања, големо опслужно подрачје и др.

9. Сегменти во системот за обезбедување

Заканата од тероризмот претставува една од најпознатите вознемирувачки аспекти од модерниот живот. Дефинираните акти на тероризмот како и целите, огромниот број на потенцијално опасни предмети, вклучувајќи огнено оружје, IEDs, токсични хемикалии, високо запаливи супстанции, како и други заканувачки предмети бара високо ниво на посветеност на човечкиот фактор и материјалните ресурси за да ја

пронајдат, односно, откријат опасноста која се заканува на определената критична инфраструктура.

Системот за обезбедување треба да биде во можност да: попречи, одврати, открие, пренасочи, задржи, запре, фати сторители на кривични дела. Целокупниот безбедносен систем, генерално може да се класифицира во 4 групи:

- Физичко обезбедување,
- Електронско техничко обезбедување,
- Механичко обезбедување,
- Превентивно обезбедување.[245]

Физичко обезбедување е обезбедување на лица (живот, телесен интегритет) кое се врши заради нивна лична заштита и обезбедување на имот од пристап на неповикани лица, уништување, оштетување, противправно одземање и други форми на штетни дејства, што се врши од страна на работници за приватно обезбедување[246];

Механичко обезбедување Се темели на поставување и инсталирање на физички бариери, огради рампи, за попречување, пренасочување и контролирање на приодите и движењето во обезбедуваните објекти и простории. Механичката заштита, исто така, преставува и предуслов за функционирање на техничката заштита, алармните системи како и системите за контрола на пристап[247]. Безбедносните периметарски заштити од механички аспект можеме да третираме како постојни и привремени барикади. Од аспект на оградувањето треба да се заснова на објективните ризици и опасности, кои ја пратат компанијата со што се земаат во предвид: висината на оградата, материјалот од кој е изработена, тип на оградата, како и растојанието од оградата до заштитуваниот објект.

Од аспект на безбедносните капии, врати и слично постојат јасно дефинирани критериуми за заштита и технички карактеристики во зависност од намената.

Поимот **противдиверзиона заштита** претставува дејност која се занимава со проучување, планирање и спроведување на организациони и технички мерки за безбедност (кои предвидуваат примена на уреди), со цел за заштита на лицата и објектите кои можат да бидат мета на терорисички и разни диверзантски активностии претставуваат посебен превентивензначај во борбата против тероризмот.

Во текот на извршувањето на противдиверзионите прегледи, најчесто применуваната опрема можеме да ја поделиме на:

---

[245]З. Доревски, Обезбедување – Практикум 2004 Комора на република Македонија за обезбедување на лица и имот–Скопје, стр 120

[246]Закон за приватно обезбедување Сл весник на Р.М бр 166 од 2012год

[247]З. Доревски, Обезбедување – Практикум 2004 Комора на република Македонија за обезбедување на лица и имот–Скопје, стр 120.

- Уреди за детекција на иницијалните запалки (детектори за метал, детектори на механизми за активација, рентгенски уреди)
- Уреди за детекција на опасни материи (детектори за експлозиви, детектори за запаливи материи, детектори за радиоактивни материи, јонизирачки зрачења), детектори за токсични материи
- Заштитна и специјална опрема (различни уреди, алати и прибори кои овозможуваат ракување со сомнителни предмети (деактивирање, неутрализација, транспорт и др)[248]

Електронско техничка заштита и CCTV - Техничко обезбедување се врши со употреба на технички средства и уреди, заради спречување на противправни дејства насочени кон лица и имот, а особено за заштита од:

- недозволен пристап во објекти и простории што се обезбедуваат;
- неовластено користење и отуѓување на предмети што се обезбедуваат;
- неовластено внесување на огнено оружје, експлозивни, радиоактивни, запаливи и отровни материи;
- провалување, диверзија или насилен напад на објектот што се обезбедува;
- неовластен пристап до податоци и документација;
- напад на возила за транспорт на пари и други вредносни пратки и
- напад на работници за обезбедување кои вршат пренос на пари и други вредносни пратки.[249]

10. Воспоставување на современи безбедносни системи

10.1. Систем за обезбедување на критична инфраструктура

Концептот за обезбедување од аспект на заштита на критичната инфраструктура и безбедносно ограничените зони кои се детерминирани врз основа на проценките на ризик, претставени преку прстени – нивоа на заштита, а со цел спречување на неовластен пристап до контролираните зони на инфраструктурата и спречување на извршување на акти на незаконско постапување се состојат од:

- Дефинирани области,
- Системи за контрола на пристап,
- Физички мерки за безбедност (огради, брави, катанци и др.);
- Системи за откривање на оружје, експлозиви и опасни предмети.
- Безбедносно патролни активности,

[248]Основи противдиверзионе заштите – институт Безбедности – Београд 98 стр.295
[249]Закон за приватно обезбедување Сл весник на Р.М бр 166 од 2012год член 40

За да се заштитат сите делови на инфраструктурата, а пред се најранливите делови бара, имплементација на стандардни оперативни процедури, опрема, средства како и човечки ресурси.

Врз основа на веќе дефинираните потреби за обезбедување вклучувајќи ги и критичните делови на објектите, потребно е да се обезбеди физички и психолошки методи и техники за обезбедување, прекусистемоткој се состои од постигнување на 4 ефекти: одвраќање, одложување, откривање и одговор.[250]

Слика бр 8. Ефекти на обезбедување

Одвраќање

Претставува ефект кој ќе осигура дека некое дело на незаконско постапување против определената критична инфраструктура бара презентација на безбедносен профил, доволен да ги убедат потенцијалните сторители дека определената критична инфраструктура со нејзините составни делови преставува ,,тешка цел" и дека има висок ризик, односно, веројатност од неуспех во намерите, како и превземање на најстроги законски мерки против чинителите на незаконските дејствија .

Одвраќањето во основа се карактеризира со: јасно дефинирани граници на инфраструктурата, контроли, насоки прецизни смерници за движење, мониторинг системи, очигледо присуство на персонал за обезбедување и сл.

[250] ICAO - aviation security training package instructors - trainee reference book 2012

Во овој дел, потребно е да се води сметка на ,,Безбедносниот инжинеринг" кој претставува една посебна гранка во безбедноста која ги покрива минималните стандарди за детално проектирање и планирање на мерките за безбедност, посебно во текот на дизајнерскиот циклус која во најмала рака треба да опфаќа минимални антитерористички стандарди, безбедносни капацитети, планови упатства предвидени врз основа на нивото на загрозеност или ,,ранливост" на објектите од витално значење[251].

Минимум антитерористички стандарди за објекти опфаќа минимални растојанија на згради, воспоставувања стандарди кои обезбедуваат минимални нивоа на заштита од терористички напади. Финансиската конструкција за примена на овие мерки која може и треба да биде надвор од оние барани стандарди кои се однесуваат на конвенционалните градежни типови. Промените во градежништвото треба да направи паралела помеѓу трошоците и ризикот[252].

Одложување

Претставува метода со која лицето кое бара начин неовластено да влегува во критичната инфраструктураили во контролираните зони на истата, а со цел да изврши незаконско постапување, неговото дело може да биде одложено со присуството на физичките препреки, адекватна безбедносна ограда, уредите и алармните системи за контрола на пристап, и сл. вклучувајќи ги сите безбедносни, техничко технолошки и оперативни методи, кои ги користи обезбедувањето со јасни насоки дека веројатноста за приведување на ваквите лица е повеќе од очекуван. Со одложувањето на упадот му се овозможува на персоналот за безбедност да ги открие/ приведува натрапниците.

Откривање

Откривањето претставува метод на спречување на дејствија на незаконско постапување преку:

- Откривање на неовластен пристап
- Откривање на забранети предмети од лицата кои бараат пристап во контролираните зони
- Распоредување на персонал за безбедност на статични безбедносни пунктови или мобилни безбедносни патроли.

[251] ICAO - aviation security training package instructors - trainee reference book 2012

[252] Unified Facilities Criteria (UFC) Security Enginering: Energy Control: Energy Control Facilities/access Control Points Distribution Statement UFC 4-022-01 25 May 2005.

Одговор

Претставува ефикасен и брз одговор на секој безбедносен инцидент, по што за многу кратко време, сторителите на акти на незаконско постапување ќе бидат совладани.

Горе применуваните методи за обезбедување може да се надополнат и со мерки на обезбедување по примерот на главниот аеродром во Израел, Бен Гурион кој воедно претставува и мета на голем број на терористички напади. Мерките се состојат во спроведување на прецизни интервјуа со патниците и поставување на специфични прашања кои се дизајнирани од страна на психолози, со цел предизвикување на реакции кај потенцијалните сторители на актите на незаконско постапување. Исто така, аеродромот Бен Гурион се потпира на повеќе нивоа - прстени на заштита каде што првиот контакт веќе се остварува на еден километар до терминалната зграда, така што патниците поминуваат повеќе кругови на обезбедување пред да дојдат во терминалната зграда каде што има поголема концентрација на патници. Сето тоа поткрепено со разузнавачки информации кои непрекидно се реализираат помеѓу агенциите и аеродромите го зголемува успехот на еден од најбезбедните аеродроми во светот. Ваквиот начин на функционирање на безбедносниот систем бара доволна бројност на персонал но и специјални обуки на персоналот за обезбедување.[253]

Генерално, заштитата на критичните инфраструктури, со цел справување со заканите, можат да се квалификуваат како: законски, технички и физички мерки.

Од аспект на законските противмерки потребно е да бидат донесени од страна од областа на критичната инфраструктура во координација со меѓународните регулативи, кои ја третираат областа и одредбите содржани во регулативите преку стандарди и препорачани практики. Со цел да се опфатат овие меѓународни стандарди и препораки, државите потребно е да изготват Национални програми за обезбедување додека, пак операторите на критичните инфраструктури да изработат програми за обезбедување по насоки кои се усвоени и регулирани согласно националните програми.

Конвенциите, меѓународните стандарди, препорачани практики и процедури треба да се спроведат/толкуваат и да се вметнат во посебна национална легислатива со цел давање правно овластување и легитимитет. Државите потписнички на меѓународните

[253]http://www.jutarnji.hr/ovaj-je-aerodrom-glavna-meta-svih-terorista--ali-ne-mogu-mu-nista-tajna-najsigurnije-zracne-luke-na-svijetu-koju-sada-svi-zele-kopirati/1549848/, Превземено на 28.03.2016г.

договори се обврзани да воспостават и да одржуваат законска инфраструктура со цел поддршка на техничките и физичките контрамерки.

Без соодветна национална легислатива што дава правна сила на националната програма за обезбедување, регулаторниот систем не би можел да работи.

Тука пред се се мисли на:

- Развивање, имплементација и одржување на националната програма за безбедност за определената област,
- Определивање, специфицирање, дефинирање и распределување на задачи и координација на активноститепомеѓу различни оддели, агенции и други организации на Дражавата, лица/субјекти засегнати со имплементирњето на различни аспекти од програмата за безбедност на критичнаа инфраструктура,
- Мониторинг и контролни активности, во фирма на инспекции, контроли, истражувања, тестови и сл. и,
- Зголемување на безбедноста преку развој и ширење на прогресивни и проактивни административни и оперативни практики и процедури.

Како дополнување на Националната програма за безбедност потребен е развој и на одредени дополнителни Програми за безбедност како на пример:

- Национална програма за контрола на квалитетот на обезбедувањето на критичната инфраструктура,
- Национална програма за обука за обезбедување на определената критична инфраструктура,
- Програми за обезбдување на област критичната инфраструктура; и
- Програма за обезбедување на оператор од критичната инфраструктура,

Програмата за безбеднност на критичната инфраструктура е механизам преку кој целите на политиката на Националната програма на Државата се идентификувани и пропишани подетално. Опишува како барањата на Националната програма ќе бидат имплементирани.

За попрецизно разработување на Програмата за обезбедување на критичната инфраструктура, претставуваат стандардните оперативни процедури (СОП), кои претставуваат детални процедури на одреден или еден дел од целокупните операции за обезбедување. СОП се најчесто во форма на индивидуални пост налози/наредби или инструкции кои што наведуваат точно како безбедносните мерки детално наведени во Програмата да се имплементираат.

Целиот персонал за обезбедување треба да биде запознаен со СОП кои што се воспоставени за нивната конкретна работна средина, пред да бидат назначени. СОП треба во најмала рака да ги содржи следниве информации:

- Опрема и број на потребни лица. (Каква опрема иколку луѓе се потребни за да се изврши задачата);
- Каде и во кое време треба да се спроведе. (Каде и кога таа задача или безбедносна процедура треба да се изведе); и
- Комуникација, извештаи, итн. (До кого и како некој инцидент треба да се пријави и какви (доколку има) извештаи се потребни откако инцидентот или задачата ќе биде завршена).[254]

10.2. Применливост на системот за обезбедување од воздухопловството во останатите критични инфраструктури

Во основа гледано, концептуално за да се спроведе адекватно обезбедување на определена критична инфраструктура, добро е во целост или делови да се преземат од воздухопловството, како една од најрегулираните области во обезбедувањето. Овој концепт кој во голема мерка е пифатен и прилагоден за потребите на критичните инфраструктури кои не се регулирани со посебни меѓународни или домашни прописи би опфаќал:

- Листа на меѓународните легислативи (правни инструменти) на областа која се третира,
- Разбирање на барањето за националното законодавство, политики и програми за обезбедување,
- Опис на закани кон критичните инфраструктури,
- Разбирање на клучните одговорности на државниот надлежен орган; и
- Разбирање на концептот на противмерки на индустријата.[255]

Од аспект на физичките и техничките мерки може да се категоризираат како но не ограничено на следново:

- Контрола на пристап во безбедносно ограничените зони;
- Безбедносен преглед на персоналот;
- Безбедносен преглед на корисниците и посетителите
- Безбедносен преглед на добрата, матерјалите, торбите и сл;
- Заштита на критичната инфраструктура; и
- Заштита на објектите и зоните во рамките на критичната инфраструктура.

[254] ICAO - aviation security training package instructors - trainee reference book 2012
[255] ICAO Annex 17 Safeguarding International Civil Aviation Against Acts of Unlawful Interference.

Дефинирање на безбедносни граници во компаниите

Границите помеѓу јавните, безбедносно ограничените зони, критички делови и другите области треба да бидат јасно препознатливи на секоја критична инфраструктура, со цел имплементација на соодветни безбедносни мерки што треба да се преземат во секоја од овие области.

Границата помеѓу јавните и компаниските зони потребно е физички да биде одделена сојасно видлива заштитна ограда, која е наменета за спречување на неовластен пристап.

Безбедносно ограничените зони

Дефинираните безбедносно ограничени зони во критичните инфраструктури потребно е најмалку да бидат вклучени во областите каде што се одвива главниот технолошки процес, местата со најосетлива ранливост, складови и магацини каде што се чуваат опасните и запаливите материи и сл.

Кога се воспоставува безбедносно ограничените области, потребно е да се спроведуваат постојани безбедносни контроли на сите делови кои би можеле да се загрози критичната инфраструктура а воедно да се осигура дека во овие зони нема присуство на забранети предмети согласно листите кои ќе ги изработува компанијата во зависност од технолошкиот процес.

Во случај на присуство на неовластени лица во безбедносно ограничените зони, потребно е итно спроведување и пребарување на сите делови, со што ќе се осигура безбедноста.

Критични делови на безбедносно ограничените зони

Дефинирањето на критичните делови се основа за безбедност во секоја критична инфраструктура, посебно во компаниите каде што постојат поголем број на вработени и каде што нивното движење е регулирано согласно зонската поделба на критичната инфраструктура.

Критичните делови преставуваат точките со најголема осетливост во извршувањето на процесите за работа, тоа се точно специфицирани места каде што се забранува секакво движење на персонал без посебно одобрување согласно планот за зоните на движење. Кога ќе се утврди критичен дел, обезбедувањето и надзорот над ваквите зони е непрекинато 24 часа.

Контрола на пристап

Пристапот до ограничената зона ќе биде ограничен и ќе биде под постојана контрола со цел да се спречи неовластени лица и возила да влезат во овие зони

воедно, воедно дозволен присап ќе имаат само доколку ги исполнуваат потребните услови за безбедност регулирани со актите на компанијата.

Пристап до безбедните зони на критичната инфраструктура може да се одобри само во ситуации кога:

- лицата и возилата имаат легитимна причина да бидат таму,
- овластување од секторот за обезбедување согласно природата на работење во вид на идентификациона картичка и сл.
- возилото мора да има пропусница и ги поседува сите пропратни документи,

Со цел да се добие пристап до безбедносно ограничените зони, врз лицата потребно е да биде спроведено контрола на: личните документи и валидни пропусни документи, издадени од страна на органот задолжен за безбедност на критичната инфраструктура. Додека пак, за возилата треба да се прикаже валидна пропусница.

Со цел да се спречи неавторизиран пристап, потребно е да се примени:

- електронски или биометриски систем за идентификација со кој се ограничува пристапот;
- физичка и техничка контрола од овластени лица;
- пропусницата на возилото се проверува пред да е обезбеден пристапот до безбедносно ограничените зони за да се осигура дека таа е валидна и одговара на возилото.

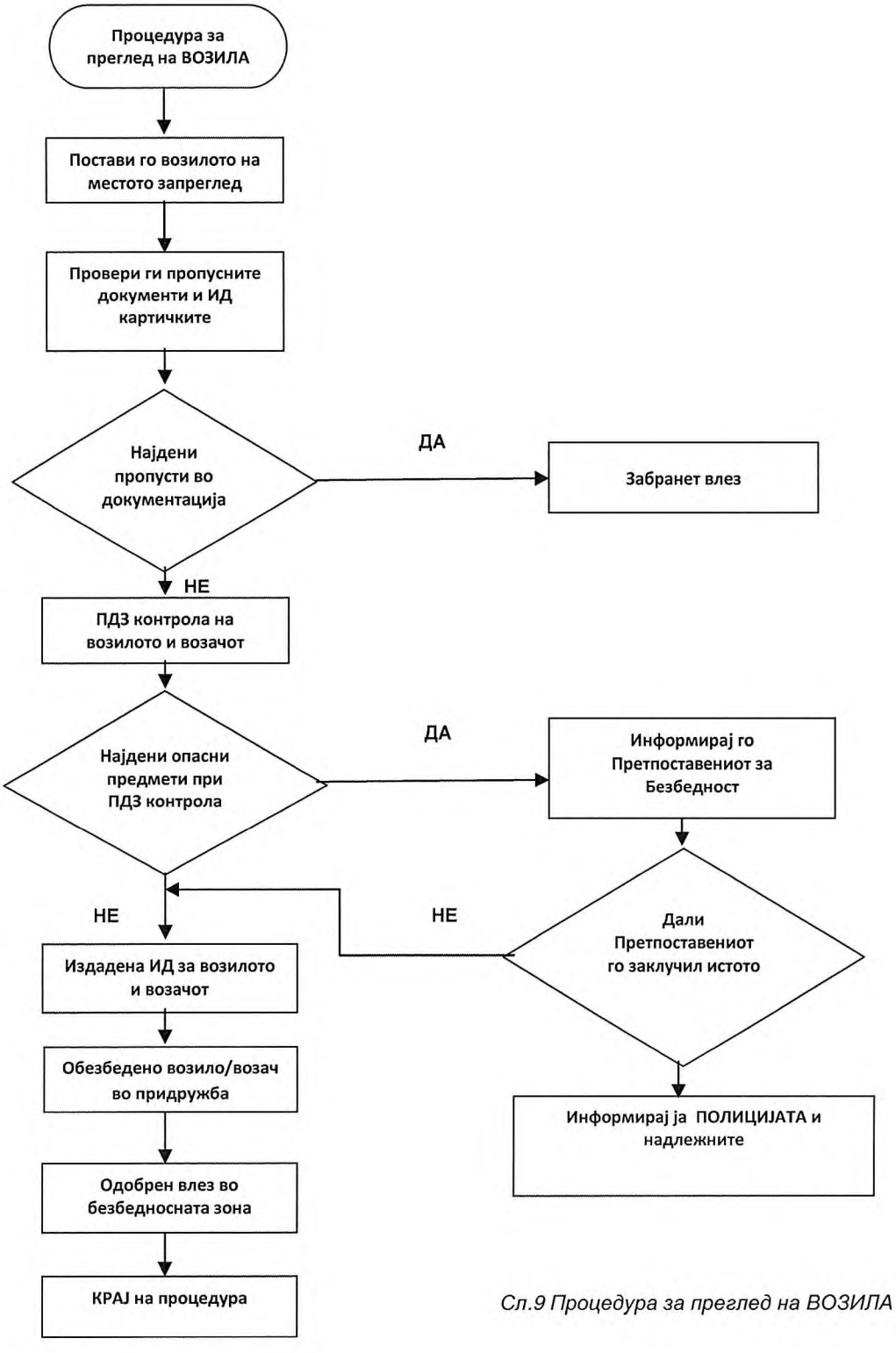
Пристапот до безбедносно ограничените зони, исто така, треба да биде предмет на дополнителни одредби утврдени со посебна одлука, како и начинот за поднесување на барања и издавање на идентификациони картички како за вработените, така и за посетителите на критичната инфраструктура.

Идентификационата карта може да се издаде само на лице кое има оперативни потреби за работење во одредените и строго дефинираните области во компанијата, согласно пропишаните стандарди за обезбедување.

Ваквите идентификациони картички ќе бидат издавани на определено време по што целокупната постапка се повторува на определен период согласно актите на компанијата. Исто така, важно е да се има во предвид позадинската безбедносна проверка на лицата т.е да се провери евентуалното криминално минато на барателот којќе работи во безбедносните зони на компанијата. Нивното криминално минато потребно е да биде ,,чисто", во спротивно издавањето на пропусни документи ќе биде забрането.

Начинот на издавање, носење и обврските поврзани со идентификационите картички, потребно е да бидат регулирани во секоја критична инфраструктура и

опишани во програмите за обезбедување, а контролирани и реализирани преку процедури за оваа активност.



Сл.9 Процедура за преглед на ВОЗИЛА

Придружуван пристап

Сите посетители на критичната инфраструктура, освен оние кои поседуваат важечка идентификациона картичка, ќе бидат придружувани кога се во безбедносно ограничените зони, но и покрај придружбата потребно е да бидат запазени сите формалности за издавање на идентификационата картичка.

Обезбедување на објекти - периметарска заштита

Периметарот, односно оградата која е поставена служи за да одврати, одложи и открие неовластен пристап. Типот, висината, материјалот како и дополнителните мерки,односно технички средства за заштита треба да бидат сразмерни со проценетиот ризик од неовластен упад. Секако физичките препреки потребно е да бидат јасно видливи со препорачани димензии, надополнети со бодликава или слична изведба на жица. Дното, односно, коренот на оградата потребно е да биде закопано во земјата или зацврстено во бетонска подлога. По должина од целокупната периметарска ограда потребно е да биде овозможено партолирање кое ќе овозможи моторизирано и пешадиско контролирање. Осветлувањето, видео надзорот и останатите системи за детекција потребно е да бидат компатибилни, со цел избегнивање на лажни аларми, но во исто време да бидат и надополнувања едни на други. Од двете страни на периметарот се препорачува да биде чисто, со цел полесна идентификација и прецизност на инструментите кои ја надополнуваат периметарската ограда. Ранливите точки и/или клучните инсталации, потребно е да бидат дополнително оградени и обезбедени со потребни технички средства. Ефективноста на секој периметар зависи во голема мера и од контролните точки за влез односно влезните капии. Капиите треба да се изградат по ист стандард, како и оградите со целосна физичка и техничка контрола.

CCTV (мониторинг систем – камери) за контрола на периметарот

Со цел зголемување на ефикасноста на периметарските заштитни опреми, потребно е да се користат електронски уреди за откривање на упади со генерирање на аларми. Со употребата на CCTV систем, во голема мера се зголемува процентот на откривање на упади, како и контролата врз автоматските системи за контрола на пристап, особено кога се користи за да се потврдат алармите од останатите системи за заштита. Сепак, ефективноста на системите пред се ќе зависат од изборот на соодветна опрема и методите на инсталација на опремата, која во најмала рака би обезбедиле:

- Превентивна заштита на периметарот и виталните делови на објектот,

- Заштита и безбедност од аспект на обезбедување и од аспект на справување со вонредни ситуации,
- Проверка на инсталациите, електричните уреди и енергетската ефикасност,
- Постојана 24 часовна опсервација и контрола на сите процеси на работењето и спречување на хаварии, пожари и сл.
- Употреба во сите временски услови и на сите дефинирани позиции,
- Автоматизација на определени технолошки процеси и др.

Капии за итна евакуација

Овие капии се инсталираат со цел да се овозможи брз пристап или излез на возилата од службите за итни случаи во случај на несреќи во критичната инфраструктура. Капиите за оваа намена, исто така, подлежат на мерките и процедурите за заштита и треба да бидат чувани согласно препораките кои гарантираат нивно безбедно користење.

Безбедносно осветлување

За да се обезбеди ефективен надзор над целокупниот периметар на критичната инфраструктура потребно е да се обезбеди соодветно осветлување кое ќе обезбеди безпрекорно функционирање на сите системи за безбедност.

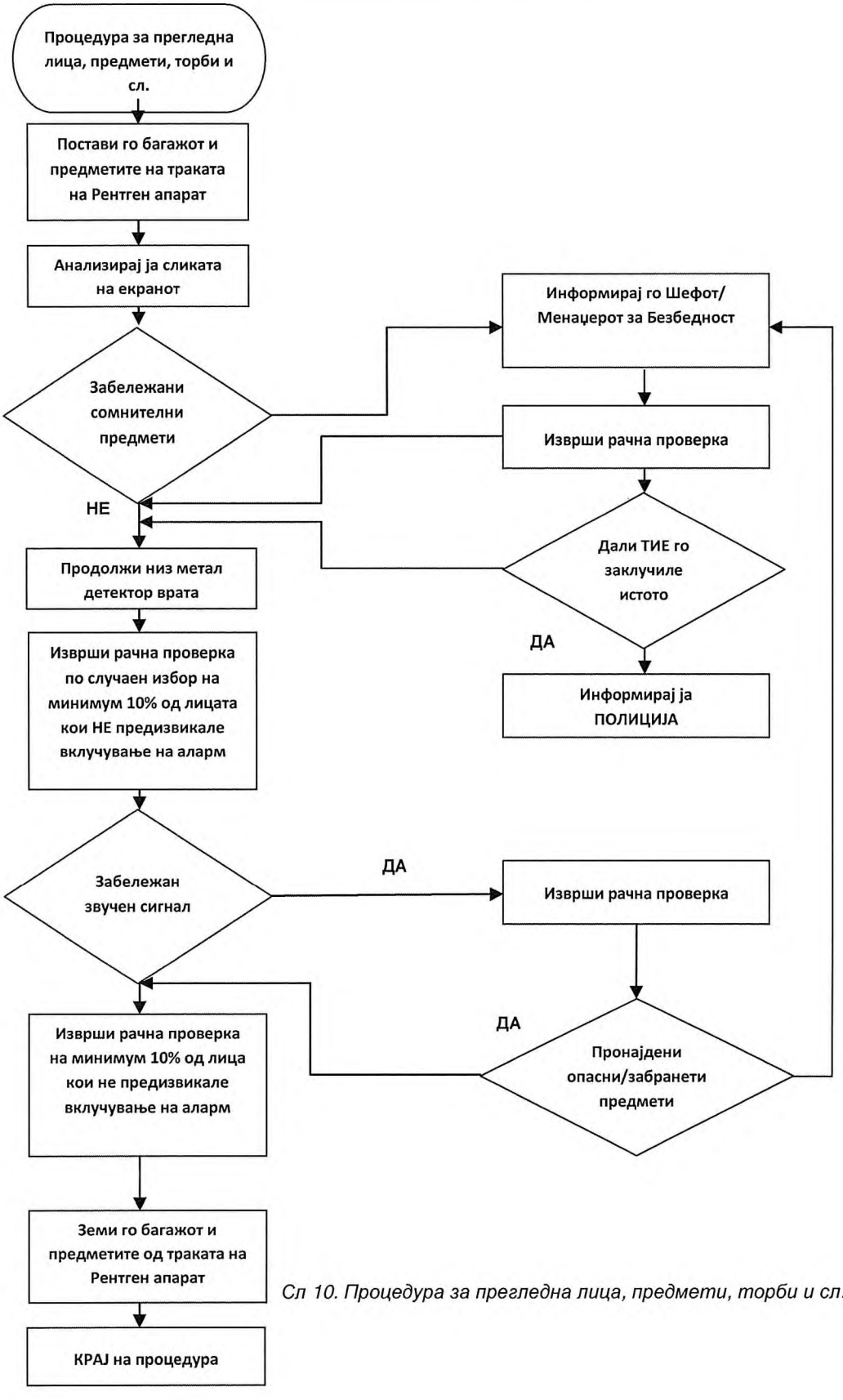
Ефектите кои треба да се постигнат со адекватното осветлување се:

- Ефект на заслепување на евентуалните напаѓачи;
- Ефект со кој се подобрува надзорот од страна на припадниците на обезбедувањето, без да се предизвика појава на сенки и рефлексии;
- Елиминирање на сите темни површини во подрачјето кое е предмет на заштита;
- Адекватна јачина на осветлување со цел прецизно определување на контурите;

Преглед на лица и нивните лични работи

Пред влез во зашитено ограничените зони силе лица и нивните предмети ќе бидат предмет на безбедносен преглед со цел да се спречи внесување на забранети предмети.[256]Примената на мерките за обезбедување вклучуваат, преглед со помош на технички средства или рачен преглед/претрес на лица и нивните лични работи, со цел попречување на внесување ,,забранети предметии" во безбедносно ограничените зони на компанијата. Мерките ќе бидат применувани од страна на персоналот кој што е соодветно селектиран и кој што е во доволна мера обучен и лиценциран за извршување на работни задачи согласно бараните стандарди и препораки.

[256]http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32008R0300&qid=1396879774275&from=EN Превземено 07.07.2015год.



Сл 10. Процедура за прегледна лица, предмети, торби и сл.

Во согласност Регулатива (ЕЗ) бр. 300/2008 во воздухопловството, дозволени се следниве методи на безбедносен преглед, поединечно или во комбинација, како во основно или секундарно значење и според дефинирани услови:

За безбедносен преглед на лица:

- рачен претрес;
- метал детекторски врати (WTMD);
- рачен метал детектор (HHMD);
- кучиња за откривање на експлозиви; и
- опрема за откривање на траги на експлозив (ETD).[257]

За безбедносен преглед на кабински багаж, предмети внесени од лица, освен оние од патници, пошта и материјали на авиопревозници, освен кога треба да се товараат во багажот на воздухопловот, резерви потребни во текот на летот и резерви на аеродромот:

- рачен претрес;
- визуелна проверка;
- рентгенска опрема;
- систем за детекција на експлозиви (EDS);
- кучиња за откривање на експлозиви; и
- опрема за откривање на траги на експлозив (ETD)[258].

За безбедносен преглед на течности, гелови и аеросоли:

- вкусување или тестирање на кожа;
- визуелна проверка;
- рентгенска опрема;
- систем за детекција на експлозиви (EDS);
- кучиња за откривање на експлозиви;
- опрема за откривање на траги на експлозив (ETD);
- тест траки за испитување на хемиски реакции; и
- скенери за течност во боци[259].

За безбедносен преглед на тежок багаж, карго и пошта како и пошта и материјали на авиопревозник кои треба да се утоварат во багажот на воздухопловот:

- рачен претрес;
- визуелна проверка;

[257] Регулатива (ЕЗ) бр. 300/2008 на Европскиот парламент.
[258] Регулатива (ЕЗ) бр. 300/2008 на Европскиот парламент.
[259] Регулатива (ЕЗ) бр. 300/2008 на Европскиот парламент

- рентгенска опрема;
- систем за детекција на експлозиви (EDS);
- кучиња за откривање на експлозиви;
- опрема за откривање на траги на експлозив (ETD); и
- симулациска комора[260].

Со цел да се оценат методите на безбедносен преглед, користејќи нови технологии кои не се предвидени во времето на донесувањето на регулативата, правилата за спроведување кои треба да се донесат може да дозволат употреба на други методи на пробна основа и за ограничен временски период, под услов таквите испитувања да не се на штета на целокупните нивоа на обезбедувањето .

Категории на предмети кои може да се забранети

Правилата за спроведување во согласност со Регулатива (ЕЗ) бр. 300/2008 може да забранат, под дефинирани услови, воведување на некои или сите од следниве категории на предмети во безбедносно ограничените зони и во воздухопловот :

- пиштоли, огнено оружје и други уреди за испуштање на проектили – уреди во состојба, или се чинат во состојба, да се користат за да се предизвикаат сериозни повреди со испуштање на проектил;
- уреди за зашеметување– уреди специјално дизајнирани за зашеметување или онеспособување;
- предмети со остра точка или остар раб – предмети со остра точка или остар раб во способни да се користат за да предизвикаат сериозни повреди;
- алатки за работниците – алатки кои може да се користат или за да предизвикаат сериозни повреди или за да ја загрози безбедноста на воздухопловите;
- тапи инструменти – предмети кои може да се користат за да предизвикаат сериозни повреди, кога се користат за погодување; и
- експлозивни и запаливи супстанции и уреди – експлозивни и запаливи супстанции и уреди во состојба, или се чинат во состојба, да се користат за да предизвикаат сериозни повреди или претставуваат закана за безбедноста на воздухопловот[261].

[260]Исто.
[261] Регулатива (ЕЗ) бр. 300/2008

Правила за спроведување употреба на следниве методи за проверка на возила, безбедносни прегледи и претреси на воздухоплови, поединечно или во комбинација, како во основно или секундарно значење и според дефинирани услови:

- рачен претрес;
- визуелна проверка;
- кучиња за откривање на експлозиви; и
- опрема за откривање на траги на експлозив (ETD)[262].

Како надополнување на веќе споменатата регулатива ќе ги споменеме следните регулативи кои ја третираат истата област, а тоа се:

- Регулатива (ЕУ) БР. 720/2011 на комисијата од 22 јули 2011 година за изменување на Регулатива (ЕЗ) бр. 272/2009 за дополнување на општите основни стандарди за обезбедување во цивилно воздухопловство во однос на безбедносен преглед на течности, аеросоли и гелови на аеродроми на ЕУ,
- Регулатива (ЕУ) БР. 1141/2011 на комисијата од 10 ноември 2011 година за изменување на Регулатива (ЕЗ) бр.272/2009 за дополнување на општите основни стандарди за обезбедување во цивилното воздухопловство во однос на употреба на скенери за обезбедување на аеродроми на ЕУ .
- Регулатива (ЕУ) бр. 1087/2011 на комисијата од 27 октомври 2011 година за изменување на Регулатива (ЕУ) бр. 185/2010 за утврдување на детални мерки за спроведување на заедничките основни стандарди за обезбедување во воздухопловството во врска со системи за откривање на експлозив
- Регулатива (ЕУ) бр. 1147/2011 на комисијата од 11 ноември 2011 година за изменување на Регулатива (ЕУ) бр. 185/2010 за спроведување на заеднички основни стандарди за обезбедување цивилното воздухопловство во врска со употребата на скенери за обезбедување на аеродромите во ЕУ,
- Регулатива (ЕУ) бр. 711/2012 од 3 август 2012 г. за изменување на Регулатива (ЕУ) бр. 185/2010 за утврдување на детални мерки за спроведување на заедничките основни стандарди за обезбедување во воздухопловството што се однесува до методите кои се користат за проверка на лица кои не се патници и за предмети кои тие ги носат
- Регулатива (ЕУ) бр. 104/2013 на комисијата од 4 февруари 2013 г. за изменување на Регулатива (ЕУ) бр. 185/2010 во врска со безбедносен преглед на патници и лица кои не се патници од страна на опрема за откривање на траги од експлозив (ЕТД) во комбинација со рачен детектор на метал (ХХМД)

[262]Исто.

- Регулатива (ЕУ) бр. 246/2013 на комисијата од 19 март 2013 година за изменување на Регулатива (ЕУ) бр. 185/2010 во врска со проверката на течности, аеросоли и гелови на аеродромите во ЕУ аеродромите,
- Регулатива (ЕУ) бр. 278/2014 на комисијата од 19 март 2014 година за изменување на Регулатива (ЕУ) бр. 185/2010 во однос на објаснување, усогласување и поедноставување на откривањето на траги од експлозиви,

Патниците се проверуваат барем со еден од следните методи:

- рачен претрес;
- поминување низ опремата за откривање на метал (WTMD);
- кучиња за откривање на експлозив;
- опрема за откривање на траги од експлозив (ETD);
- скенери за обезбедување кои не употребуваат јонизирачко зрачење;
- опрема за откривање на траги од експлозив (ETD) комбинирана со опрема со рачен детектор на метал (HHMD)[263].

Товарот и поштата се проверуваат барем со еден од следните методи:

- рачен претрес;
- рендген опрема;
- EDS опрема;
- кучиња за откривање на експлозив (EDD);
- ETD опрема;
- визуелна проверка;
- опрема за откривање на метал (MDE)[264].

Патролирање и патролни активности,

Физичките мерки на претпазливост потребно е да се надополнуваат со активно вклучување на персонал за обезбедување, со цел да се заштитат ранливите точки и да се спроведат безбедносни процедури.

Задачите за безбедносните патроли можат да вклучат:

- Заштита на објектите;
- Набљудување на движење на луѓе и возила;
- Проверка на конкретни објекти;
- Верификација на безбедноста на критичните области
- Патролирање низ конкретни ранливи области во периметарската ограда ;
- Проверка на областите за складирање на резервите ;

[263] Регулатива (ЕУ) бр. 185/2010год.
[264] Исто.

- Надгледување на процесот на работа и одвивање на технолошките процеси[265],

Обезбедувањето може да биде и врз основа на однапред дефинирани места за обезбедување (статични места), тука би се реализирале активности како на пример:

- Проверка на идентфикациони картички и дозволите за влез во зоните.
- Проверка на документацијата на лицата и возилата,
- Претрес на лицата и нивните торби
- Персоналот за безбедност може да биде задолжен да придружува товар со висока вредност за кои има висок ризик за напаѓање или кражба, опасен или штетен материјал, карго, разни возила кои имаат потреба од придружби и сл[266].

Во рамките на критичната инфраструктура постојат точки кои треба да се контролираат како такви би ги издвоиле:

- Местата каде природните препреки се користени како дел од заштита
- Водните инсталации и атмосферската канализација;
- Објектите кои се користени да бидат дел од границата.
- Линијата која ги дели небезбедносно ограничените зони од безбедносно ограничените зони мора јасно и физички да биде идентификувана, исцртана и заштитена со користење на мерки за физичка безбедност, соодветни на условите[267].

При спроведувањето на патролите на персоналот потребно е да бидат утврдени стандардни оперативни процедури, генерално земено, персоналот за обезбедување потребно е да се раководи по:

- Принципите на длабинска одбрана;
- Физичките препреки;
- Патролните активности да се вклопуваат во концептот за безбедност;
- Ранливите области во критичната инфраструктура;
- Стандардните Оперативни Процедури за спроведување на обезбедувањето
- Почитување на прописите и актите на компанијата кои го регулираат движењето на возилата во контролираните зони.

10.3. Употреба на дресирани кучиња

Повеќе од стотина години, кучињата се користат во функција на полициските, воените и други безбедносни служби во извршување на работни задачи, како што се, одржување на јавниот ред и мир, од 1970 за трагање по исчезнати лица, бегалци од

[265]Регулатива (ЕУ) бр. 185/2010год
[266]Исто.
[267]Исто.

затвор, а од 1980 и во откривање на наркотици, лешеви, експлозиви и сл. Полициските или војни кучиња, се посебно обучени кучиња кои уште од малечки (6 месеци) се навикнуваат на обука, а потоа се обучуваат во зависност од проценката на дресерот која врста на дресура ќе биде применета. Првите полициски кучиња се воведени во службата на Германската полиција во градот Hildesheim 1896 година во тој период 12 Германски овчари кои не биле дресирани, но се употребувале исклучиво за заплашување и демонстрација на сила[268]. Во повеќе држави во светот кучињата се нарекуваат К-9 единици. Тие единици се одвоени полициски одели кои служат за подршка на униформираните полицајци, инспектори и др. во пронаоѓање на наркотични средства, пронаоѓање на лица, експлозиви и сл., S.W.A.T тимовите во најголем број случаи поседуваат службени кучиња[269].

Употребата на дресирани кучиња во функција на обезбедувањето на виталните објекти станува се по нагласена потреба поради резултатите кои ги постигнуваат дресираните кучиња, во целокупниот систем на заштитни мерки регулирани со закон.Од аспект на воено полициските должности, кучињата се застапени во повеќе сегменти од секојдневното работење, во функција на претрага посебно, во граничното обезбедување кучињата се дресираат и употребуваат пред се за претрес, пребарување на поширок терен и откривање на лица и предмети. Како задачи поврзани со полициските активности на кучињата потребно е да ги споменеме:трагање од аспект на кривични дела, следење на траги, претреси вклучувајќи објекти и возила во функција на окривање на експлозивни направи, исчезнати луѓе, откривање на дроги и други психотропни супстанции и др.

Ако повлечеме паралела помеѓу техниката и употребата на кучињата во функција на отривање на забранети предмети вклучувајќи ги и експлозивите, кучињата со својот капацитет на запазување и позитивното насочување на осетот имаат постигнато значителна успешност во правилната детекција и лоцирањето на опасните предмети. Оттука, неминовно се наметнува нагласената потреба од примена на кучињата во функција на обезбедувањето на сите критични инфраструктури, а нивната примена би сестоела во:

- Преглед на простории и предмети за откривање на експлозивни средства,
- Патролни активности, како подршка на физичкото обезбедување,
- Периметарска заштита на дефинираната ограда,
- Подршка на работата на пункт за обезбедување, и др.

[268] http://www.specijalac.net/6077/sluzbeni-psi-policije-i-vojske.html, Превземено 11.12.2015год.
[269] Исто Превземено 11.12.2015год.

Согласно законот за приватна безбедност на Р.М дефинирани се условите за употреба на дресирано куче во функција на обезбедувањето. Согласно членот 56 од Законот:За вршење на работи на физичко обезбедување може да се употреби дресирано куче, доколку:

1. има потврда за успешно завршена дресура;
2. е под непосреден надзор на работник за обезбедување (водич на дресирано куче) кој има потврда за успешно завршена обука за употреба на дресирано куче.[270]

Со истиот Закон во вршењето приватно обезбедување, дресирано куче се употребува заради одбивање на непосреден напад над работникот за обезбедување, како и непосреден напад над лицето или имотот што се обезбедува.

Дресирано куче се употребува во случаите кога:

- се исполнети условите за примена на физичка сила или
- се исполнети условите за употреба на огнено оружје[271]

Делот кој го третира употребата на кучињата во функција на откривање на забранети предмети е во надлежност на Министерството за внатрешни работи.

Најпознати полициски видови на кучиња и нивната намена се:

- Германски овчар - напаѓачко куче
- Холандски овчар - напаѓачко куче
- Белгиски Малиноус - напаѓачко куче
- Германски боксер - напаѓачко куче
- Лабрадорски териер – откривање на експлозивни направи и наркотици
- Доберман пинчер - напаѓачко куче
- Блоодхоунт – куче трагач, откривање на експлозивни направи и наркотици,
- Беагле – откривање на човечки лешеви, откривање на експлозивни направи и наркотици
- Ротвајлер - напаѓачко куче[272]

Тимовите во кои вклучуваат високо обучени кучиња за трагање за различни експлозивни материјали во близина на зградата екстериери, паркинзи, канцеларии, возила, пакети и луѓе во и околу објектите. Овие тимови обезбедуваат силна видлива и психолошка пречка против криминалните и терористичките закани.[273] Овие тимови играат клучна улога во сеопфатни мерки за превентивна безбедност со поддршка на

[270] Закон за приватно обезбедување Сл весник на РМ. Бр 166 од 2012 член 56
[271] Закон за приватно обезбедување Сл весник на РМ. Бр 166 од 2012 член 56
[272] http://www.specijalac.net/6077/sluzbeni-psi-policije-i-vojske.html
[273] http://www.dhs.gov/explosive-detection-canine-teams

стратешките активности за откривање на експлозивните направи. Тие, исто така, обезбедуваат непосреден и специјализиран одговор на бомбашките закани како и контрола на торбите, пакетите и други предмети кои се оставени без надзор. Најчесто, овие активности за откривање им овозможуваат на тимовите да се открие или брзо да се исклучи присуството на опасни материјали, со што се овозможува непречено функционирање на работните текови како и избегнување на непотребни евакуации, блокирања на терен, како и прекин на процесот на работа и добивање на претстава на нестабилност или загрозеност на клиентите.

Од аспект на употреба на кучe во цели за откривање на експлозивни направи, треба да се спомене дека во воздухопловството претставува еден од прифатените методи за проверка на патниците, багажите, каргото како и целокупните средства и опрема кои влегуваат во стерилните зини на аеродромите. Сето тоа е дефинирано и регулирано согласно регулативата на ЕУ. Во оваа регулатива кучето за откривање на експлозив (ЕДД) може да открие и посочи специфични и високи поединечни количини на експлозивни материи. Откривањето е независно од обликот, местоположбата или ориентацијата на експлозивните материи. ЕДД дава аларм, во облик на пасивна реакција, кога открива експлозивни материи . ЕДД и неговиот водич можат да се употребуваат за безбедносен преглед доколку и двајцата се одобрени поединечно и како тим. ЕДД и неговиот водич подлежат на почетни и последователни обуки за да се обезбеди дека ги учат и одржуваат потребните компетенции и, онаму каде е соодветно, учат нови компетенции. По одобрението од страна на надлежниот орган, ЕДД тимот може да се употребува за безбедносен преглед со употреба на методи на слободно трчање или метод на трагање со оддалеченост по мирисот на експлозивот.[274] Тренингот на ЕДД тимот опфаќа теоретски и практични елементи и елементи на тренинг на работното место. Содржината на курсевите за тренинг се прецизира или одобрува од страна на надлежен орган. Кучињата кои треба да се дресираат за откривање на експлозив се кучиња единствено за таа наменапокрај другото со оваа регулатива се пропишуваат и:

- Стандардите кои треба да се исполнат во поглед на ЕДД
- Условите за тренинг
- Компетенциите во смисол на способностите и др.[275]

[274]Регулатива (ЕУ) БР. 573/2010 НА Комисијата од 30 јуни 2010 г.за изменување на Регулатива (ЕУ) бр. 185/2010 за утврдување на детални мерки за спроведување на заедничките основни стандарди за обезбедувањево воздухопловството.
[275]Исто. Регулатива (ЕУ) БР. 573/2010

10.4. Свесност за безбедност (безбедносна култура)

Покрај технологијата како дел на безбедносниот систем во критичните инфраструктури, потребно е да се спомене и еден друг сегмент, а тоа е психологијата на вработените лица, бидејќи при незаконско постапување или криминални дејствија, голема помош и придонес во општата безбедност може да даде секој еден вработен без оглед на кое работно место е поставен според организационата поставеност на критичната инфраструктура. Развивањето на една таква свест е процес кој трае, односно менување на свеста на персоналот во однос кон безбедноста и опасностите на кои може да биде изложен самиот персонал како и критичната инфраструктура во целина.

Свесноста за безбедноста е многу значаен фактор за целокупната безбедност на критичната инфраструктура, со крајна цел зачувување на човечките животи и материјалните добра. За да се постигне адекватна безбедносна политика на компанијата, секој еден вработен без разлика на работното место и профилот на струката, потребно е да поседува елементарно познавање за безбедност, посебно за времетраењето на неговите работни обврски. Работникот поребно е да биде внимателен и да информира за секоја сомнителна или абнормална состојба.

Сите ново вработени во компаниите третирани како критични инфраструктури, по теркот на воздухопловната безбедност, потребно е да бидат предмет на безбедносна проверка на нивното минато, но и да поминат обука за свесност за безбедност. Оваа обука треба да биде реализирана од страна на овластени инструктори по однапред дефинирани теми на обука. За персоналот кој влегува во контролираните делови на компанијата потребно е да се направи дополнителна безбедносна обука со специфики карактеристични за позицијата на работа. Персоналот потребно е да ја разбере потребата од мерките за обезбедување од дејствија на незаконско постапување, да биде свесен за постапките кои се преземаат од различните служби во компанијата со цел да укажат, односно, да помогнат во спроведувањето на заштитата на компанијата, посебно од тероризмот и други слични акти на незаконско постапување. Во текот на обуката на персоналот кој не спаѓа во групата на обезбедување, но треба да биде обучен за свесност за безбедност посебно во сегментите кои ја детерминираат потребата од обезбедување на конкретната инфраструктура, тероризмот како глобална закана и потенцијалната опасност врз критичната инфраструктура, правното регулирање на обезбедувањето, организационаа поставеност на компанијата, правилата за обезбедување, компаниската безбедност и др.

Многу битен фактор за свесноста за безбедноста е и почитување на безбедносните прописи кои важат за сите вработени во компанијата, со посебно залагање на раководителите, со мотивираност и личен пример во работењето да ги почитуваат правилата на компанијата кога е во прашање безбедноста.Свесноста за безбедност како фактор, исто така, подразбира и реагирање во одредени специфични состојби каде треба да се покаже одлучност и решителност, како одредена состојба коректно да се реши дали во нормани услови или во ситуации на вонредни состојби.

Последиците од немање на доволна свесност за безбедност и не адекватна примена на процедуриеили слабо односно површно извршување работни должности, босебно кога станува збор за безбедноста во компанијата, може да бидат катастрофални.

10.5. Трошоци за обезбедувањето

Во согласност со релевантните правила, секоја земја, може да определи во кои околности, и до кој степен, трошоците за безбедносните мерки за заштита на критичните инфраструктури од дејствија на незаконско постапување треба да бидат на товар на државата, субјектите, операторите, другите надлежни органи или корисниците. Доколку е соодветно, и во согласност со правото може да се применат и построги безбедносни мерки, така што, сите давачки или трансфер на трошоците за безбедност ќе бидат директно поврзани со трошоците за обезбедување на односните безбедносни служби и треба да бидат дизајнирани за да се опфатат не повеќе од релевантните трошоци кои се вклучени.

10.6. Селектирање на персонал и методи на обука

Еден од најважните сегменти во обезбедувањето, секако, претставува правилната селекција на персоналот за обезбедување. Селекцијата и критериумите потребно е да бидат сразмерни на специфичните потреби и задачи. Секој нововработен потребно е да биде подложен на безбедносни проверки како и ваквите проверки да бидат повторувани на одреден временски период. Безбедносните проверки на лицата кои работат или се вработуваат во КИ треба да вклучат проверки на идентитетот и предходното минато на лицето од аспект на било какво криминално минато и подоблоста за негово работно ангажирање во критичните инфраструктури. Сите лица вработени во оделите за обезбедување потребно е да поседуваат лиценца за

обезбедување согласно Законот за приватно обезбедување на Република Македонија.[276]

По завршувањето на генералните обврски, голем број на криични инфраструктури вклучувајќи го и воздухопловството организираат дополнителни обуки во зависност од потребите на компанијата, односно природата на работењето.

Како пример ќе го наведеме воздухопловството кое покрај основната обврска за поседување на лиценца за обезбедување, потребно е да биде реализирана обука по однос на спецификите на процесите за работа, како и употребата на средства и опрема за подобрување на обезбедувањето. Тука ќе ја споменеме потребата од воведување на лиценци за рентген оператори, инструктори за безбедност, супервизори за безбедност, како и физичко обезбедување, за кои постојат програми за обука со точно определени теми и предмети во форма на теоретско предавање, како и практична обука.

Оваа програма е наменета за определени позиции со цел вработените да се стекнат со знаења, способности и вештини да извршуваат работни задачи од областа на обезбедување од акти на незаконско постапување.

Со програмата ќе се направи имплементацијата на сите барања содржани во меѓународните и националните програми за обука за обезбедување од дејствија на незаконско постапување.

10.7. Контрола на квалитет

Со цел адекватно спроведување на сите барања од регулативите и нејзините акти, вклучувајќи и казнени одредби, а во врска со следење и откривање на недостатоците како и корегирање во рамки на одредени временски интервали, потребно е да се воспостави целосен и пропорционален пристап во однос на активностите за корекција.

Овој пристап се состои од прогресивни чекори кои треба да се следат додека не се постигне корекцијата, вклучувајќи:

- совет и препораки;
- формално предупредување;
- известување за спроведување;
- административни санкции и правни постапки.[277]

---

[276]Законот за приватно обезбедување ги опфаќа: Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 166/12) и Законот за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 164/13)

[277] Регулатива (ЕУ) БР. 185/2010 на комисијата од 8 јануари 2010 годиназа изменување на Регулатива (ЕЗ) бр. 300/2008 на Европскиот парламент и на Советот во однос на спецификации за националните програми за контрола на квалитет во областа на обезбедување во цивилно воздухопловство како што е засегнато.

Надлежниот орган може да направи еден или повеќе од овие чекори, особено кога недостатокот е сериозен или се повторува.

За да биде во целост реализирана контролата на квалитет, потребно е да се изработи Националната програма за контрола на квалитет со цел да се потврди дека мерките за обезбедување се ефикасно и соодветно спроведени и да се утврди степенот на усогласеност со одредбите од регулативите и националната програма за обезбедување, со помош на активности за следење на усогласеноста.

Сите инфраструктури, оператори и другите органи со одговорности за обезбедување, треба редовно да се следат за да се обезбеди брзо откривање, корекција и анализа на грешки. Следењето се врши во согласност со националната програма за контрола на квалитетот, земајќи ги предвид нивото на закана, видот и природата на операциите, стандардот на спроведување, резултатите од внатрешната контрола на квалитетот и други фактори и проценки кои ќе влијаат на зачестеноста на следење. Следењето вклучува спроведување и ефективност на мерките за внатрешна контрола на квалитет.

Управувањето, поставувањето на приоритетите и организација на програмата за контрола на квалитетот ќе се преземат независно од оперативното спроведување на мерките кои се преземаат во рамки на Националната програма за обезбедување. Активности за следење на усогласеност вклучуваат целосни инспекции, тестови, контроли поврзани со обезбедувањето.

Методологијата за спроведување на активностите за следење треба да го исполнуваат стандардизираниот пристап, кој вклучува барања, планирање, подготовка, активност на самото место, калсификација на наодите, комплетирање на извештајот и процесот на корекција. Активности за следење на сообразноста се вршат врз основа на систематско собирање на информации преку опсервации, интервјуа, преглед на документи и проверки. Следење на усогласеност вклучува најавени и ненајавени активности.

10.8. Процедури при вонредни ситуации

Во последните години, насилството и бројот на жртвите од дела врз неборбени цели постојано се зголемува. Терористичките и криминалните акти како и другите извори на загрозување кои во основа се состојат од: подметнување на експлозиви, запаливи и опасни материи, саботажи, срушување на авиони, грабнување, предизвикување на намерни несреќи; технички недостатоци кои можат да бидат предизвикани намерно или ненамерно; неуредност, неред, незнаење; неблаговремена, погрешна или непотполна проценкана на одредени фактори и др. се

едни од причините за случување на несреќите и катастрофите во критичните инфраструктури.

Поради тоа, припадниците на сите служби кои се инволвирани во одвивањето на процесите на работа, треба да бидат подготвени и стручно оспособени за навремено, ефикасно, безбедно и стручно реагирање и делување, при секаква евентуална појава која евентуалноби ја загрозила безбедноста.Тоа посебно се однесува на стручниот персонал, кој извршува работи што се директно поврзани со оперирањето и експлоатацијата на критичните инфраструктури. Заедничкиот именител на сите превземени активности и мерки претставува создавање на претпоставки и услови за највисоко можно ниво на безбедност.Од тие причини потребно е да бидат разработани постапки со кои генерално се опфатени активностите кои ги превземаат стручните службени лица во склоп на работите кои се од значење за безбедноста на критичната инфраструктура. Овие активности се превземаат со цел зачувување на животите на вработените, зачувување на објектите, имотите и други материјални добра, како и овозможување на нормалниот живот на граѓаните кои се зависни од критичната инфраструктура[278].

Причините за настанувањето на вонредните околности во критичните инфраструктури можат да бидат од најразлична природа, а крајните последици најчесто се непредвидливи и можат да бидат фатални по животите на луѓето или материјалните добра.

Од тие причини, согласно прописите секоја критична изработува План за заштита и спасување од природни непогоди и други несреќи, изготвен согласно Законот за заштита и спасување. При изготвување на Планот се користат планските документи во Република Македонија. Самиот план зависи од дејноста на работодавачот, опасностите, како и неговата големина[279].

Според препораките и на меѓународните организации, како и врз основа на домашната легислатива, секој субјект – компанија мора да изработи посебен план на мерки и активности, кои се превземаат во случај на вонредни околности. Во него треба да бидат прецизно дефинирани и наведени сите процедури, кои персоналот ги превзема во случај на опасност. Ваквиот план се изработува со цел да се минимизираат или анулираат евентуалните опасности по човечките животи или уништувањето на материјалните добра, при појава на било каква вонредна околност.

[278]Ѓ. Алчески Процедури при вонредни состојби- Скрипта Скопје 2010
[279]http://www.prorisk.mk/plan-za-zastita-i-spasuvanje Преземено 10.10.2015год.

Сите процедури, кои се разработени во плановите на различните субјекти, мора да бидат меѓусебно усогласени, истренирани, практично симулирани и да претставуваат дел од секојдневната обука на стручниот персонал. Независно од дефинираните сопствени процедури и постапки во случај на опасност, кои ги објавуваат поодделните субјекти, кои се инволвирани во работата на критичната инфраструктура преку разни форми на документи (прирачници, карти, проспекти, планови, брошури и сл.), при појава на вонредни ситуации, се постапува според утврдениот План.

Во зависност од ситуациајта можат да бидат вклучени голем број на субјекти како што се на пример: противпожарно спасувачките единици, полиција, обезбедувањето, компаниските служби, медицински служби, болници, владини преставници, комуникациски центри, транспортни власти, спасувачки координативни центри, цивилна заштита, војската, приобални единици, јавен информативен сервис, царина, психијатри - психолози, ветеринарни служби, спасувачки агенции од рамките на црвениот крст и др.Од тие причини, а со цел избегнување на било каква конфузија во дејствувањето на големиот број на субјекти, потребно е да се пропишат прецизни процедури за дејствување и истите да бидат составен дел на Планот.

Во овој дел потребно е да се споменат вонредните ситуации кои се предизвикани од акти на незаконско постапување, а се однесуваат на: нарушување на јавниот ред и мир од поголеми размери, киднапирања, вооружени напади, земање на заложници, анонимни најави за поставени експлозивни направи, откривање на сомнителни предмети за кои се смета дека преставуваат опасност, саботажите и сл. Со цел справување со наведените ситуации најнапред потребно е да се изработи План за вонредни ситуации од акти на незаконско постапување, кој би преставувал засебен План или да биде надополнување на постојните планови во критичните инфраструктури.Плановите завонредни ситуации имаат за цел да ги сведат во најмала можна мерка последиците од настанатата ситуација, создадат опкружување во кое се вклучени сите расположливи материјални и човечки ресурси, така да се осигура ефикасна реакција во било која ситуација.

Во поглед на управување со мерките, активностите и постапките во текот на разрешувањето со вонредните ситуации предизвикани од акти на незаконско постапување Планот ќе има две основни функции:

- Изолирање, локализација и спречување на понатамошната ескалација на вонредната ситуација,
- Планско преземање на сите мерки, активности и постапки заради разрешување на вонредната ситуација.

Во овој оперативен план кој го изработува компанијата носител на критичната инфраструктура треба да опфаќа најмалку:

- *дефинирање на надлежностите и одговорностите* при вонредни ситуации на сите инволвирани субјективо работата на критичната инфраструктура,
- *организациска структура* во вонредни ситуации од аспект на командување, воспоставување на оперативни центри, прифатни центри, области за третман на повредени и други центри во зависност од ситуацијата и видот на критичната инфраструктура,
- *пристап до критичната инфраструктура* во поглед на патишта, средства опрема и сл,
- *разработка на сите вонредни ситуации* со нивните специфики и карактеристики, тука пред се се мисли на: прием и пренесување на информации, преземање на мерки во зависност од ситуацијата,
- *организација на вежбовни активности*, по типови на вежби и обуки, зачестенот на вежбите, реализација на вежбовни активност.
- *Прилози во поглед на*: преглед на опремата за реагирање во вонредни ситуации, мапи и шеми на компанијата, органограми, списоци со систем за повикување и известување, опрема потребна за функционирање на центрите, упатства, извештаи и сл.

Планот како што споменавме го сочинуваат постапките и активностите на однапред утврдени и определени улоги и одговорности на секој поединец и субјект учесник во разрешувањето на вонредната ситуација.

ГЛАВА VII

Заштита на објектите од витално значење односно критична инфраструктура во САД, земјите од ЕУ и Австралија

1.Односот на САД спрема Критичната инфраструктура

Терминот ,,критична инфраструктура" во САД за прв пат е користен во документот насловен како: ,,Критични основи - Заштита на Американската инфраструктура" објавена од САД во 1997 год.

Извештајот содржи главно клучни дефиниции, анализи и насоки за заштита на критичната инфраструктура. Веднаш потоа, објавена е Одлука на Претседателот, код NSC – 63 потпишан од претседателот на САД. Оваа Директива е проследена до сите служби кои 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. Следен чекор во заштита на критичната инфраструктура е направен со донесување на Националниот акт за обезбедување од 2002, донесен од секторот за Национална безбедност на САД кој содржи насоки за координација на националните служби за заштита на критичната инфраструктура, вклучувајќи ја и ИТ и телекомуникациската технологија[280].

Од аспект на заокружување на соодветната докукументација, важно е да се истакне и внесувањето на ,,Национална Стратегија за заштита на сајбер простор" изготвен од белата куќа во 2003 година. Овој документ строго се однесува на информатичката критична технологија. Стратегискиот документ покажува дека сајбер системот е претставен како нервен систем на критичната инфраструктура, а претставува компонента на документот ,, Национална стратегија за заштита на државата" и е подршка на друг документ ,,Национална стратегија за физичка заштита на критичната инфраструктура"[281].

,,Национална стратегија за заштита на државата" е изготвен и издаден од страна на Белата куќа потпишан од претседателот и објавен 2002год. Овој формален документ содржи стратегија за заштита на критичната инфраструктура, како што се дадени на приватниот сектор, улогата на осигурувањето на критичната инфраструктура, спречувањето и оневозможувањето на терористички напади врз критичната инфраструктура, опоравувањето од инциденти и преземање на заштитни мерки.

Треба да се нагласи дека Белата куќа во Февруари, 2013 година публикуваше Претседателска Директива – за критичната инфраструктура - Безбедност и флексибилност за зајакнување и одржување на безбедна, функционална и

[280]https://www.dhs.gov/topic/critical-infrastructure-security, Преземено на 16.02.2015год.
[281] https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdfПреземено на 17.02.2015год.

флексибилна критичната инфраструктура.Оваа Директива ја утврдува националната политика за критичната инфраструктура во поглед на безбедноста и флексибилноста. Овој проект претставува заедничка одговорност меѓу федералните, државните, локалните и територијалните (SLTT) субјекти, и јавните и приватните сопственици и оператори на критичната инфраструктура. Директивата, ги појаснува критичните инфраструктурни функции поврзани со улогите и одговорностите во Сојузната влада, како и подобрување на целокупната координација и соработка.[282]

Основната политика на Соединетите Американски Држави е да се зајакне безбедноста и издржливоста на своите критични инфраструктури против физички и сајбер заканите. Сојузната влада работи со сопствениците на критичните инфраструктури и територјалните субјекти со цел да се преземат проактивни чекори за управување со ризик и да се зајакне безбедноста и издржливоста на критичната инфраструктура во државата, со оглед на сите опасности кои би можеле да имаат влијание врз националната безбедност, економската стабилност, јавното здравје и сигурноста, или било која комбинација. Овие напори бараат, како што се наведува во Директивата, да се намали ранливоста, минимизираат последиците и да се идентификуваат заканите како и забрзување на напорите за одговор и обновување[283]. Сојузната влада, со оваа Директива ги вклучува и меѓународните партнери за да се зајакне безбедноста и издржливоста на домашните критични инфраструктури, како и критичните инфраструктури кои се наоѓаат надвор од САД, а се во врска со државата.

1.1. Имплементација на Директивата за заштита на критичните инфраструктури во САД

Една од главните улоги во спроведувањето на Директивата ја има Секретарот за национална безбедност, кој треба да обезбеди стратешки насоки, промовирање на безбедноста и флексибилноста на критичната инфраструктура регулирани со националниот закон од 2002 година, а во врска со евалуацијата на националните капацитети за заштитата на критичната инфраструктура поврзана со анализата на заканите, ранливоста и последиците од сите видови на опасности, безбедноста и флексибилноста, а кои се неопходни за јавното и приватното ангажирање. Секретарот го развива националниот план во соработка со сите релевантни институции, вклучувајќи ја и Федералната служба за безбедност, ги идентификува

[282] Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013

[283] https://www.dhs.gov/topic/critical-infrastructure-security, Преземено на 16.02.2015год.

меѓузависностите на критичните инфраструктури и подготвува извештаи за ефикасноста на националните напори за зголемување на националната безбедност.

Како дополнителни одговорности на секретарот за национална безбедност се вклучуваат:

- Идентификување и давање на приоритет на критичната инфраструктура по основ на физичките, сајбер заканите и ранливоста;
- Одржување на национални центри за критични инфраструктури кои ќе обезбедат свесност и способност за прифаќање на информациите поврзани со заканите и статусот на состојбите, кои би можеле да влијаат на критичната инфраструктура;
- Во координација со ССА и останатите федерални сектори и агенции да обезбедат експертиза и техничка помош на сопствениците и операторите на критичните инфраструктури и да се олесни пристапот и размена на разузнавачки информации потребни за зајакнување на безбедноста и флексибилноста на критичната инфраструктура;
- Врши сеопфатна проценка на ранливоста на критичната инфраструктура на нацијата во меѓусебна координација на сите субјекти;
- Ја координира Федералната влада за одговорностите или физички инциденти кои влијаат на критичната инфраструктура во согласност со статутарните органи;
- Поддршка на јавниот обвинител и за спроведување на законот со своите обврски за истрага и прогон поврзани со закани и напади врз критичната инфраструктура;
- Координација и експертиза на соодветните оддели и агенции да ги мапира, анализира, со помош на комерцијалните сателитски и воздушни системи, постојните капацитети во рамките на други оддели и агенции; и
- Поднесува годишен извештај за состојбата на националните критични инфраструктури како што се бара во законот[284].

Секој сектор на критичната инфраструктура има уникатни карактеристики, оперативни модели, профил на ризик, институционално знаење и специјализирани експертизи.

Стратегијата на САД се води од три клучни императиви, а тоа се:

[284]https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilПреземено на 26.06.2014

- Прочистување на функционалните односи во федералната влада за унапредување на националното единство за зајакнување на безбедноста на критичните инфраструктури.

Ефективните национални напори за зајакнување на безбедноста на КИ мора да бидат водени од Национален План, кој ги одредува улогите и одговорностите и добива информаци преку експертизи искуства и одговорности на специфичните секторски агенции.Како дел на прочистените структури предвидени се два национални центри за КИ една за физичка инфраструктура и една за сајбер инфраструктурите. Истите треба да функционират како една целина во функција на обезбедување, свесност и информации за заштита на КИ.Успешноста на националните центри зависат од квалитетот и навременото доставување на информаци, кои се добиват од специфичните секторски агенци и другите федерални агенци и одели, како и од сопствениците и опреаторите на КИ.

- Потребно е обезбедување на ефикасна размена на информации за потребите на федералната влада,имплементирање на интеграциската и аналитичката функција заради донесување на одлуки, плански и оперативни, а кои се однесуват на КИ.

Безбедноста и функционалноста на КИ бара ефикасна размена на информации вклучувајќи и разузнавање, помеѓу сите нивоа на влади, сопственици и оператори на КИ. Ова вклучува и навремена размена на информаци на закана и ранливост што обезбедува развој на свесноста при инциденти.Поголемата размена на информации мора да се направи почитувајќи ја приватноста и цивилните слободи.

- Третиот стратегиски императив е изграден врз основа на првите два императива и се однесува на имплементацијата на интеграциската и аналитичката функција, заради донесување на одлуки, плански и оперативни, а кои се однесуват на КИ, и вклучува оперативни и стратешки анализи на инциденти закани и ризици:
  - Помош при приоритизација средства и објекти и менаџирање со ризици,
  - Одредување на меѓузависности
  - Препорачани безбедносни мерки
  - Менаџмент за подршка во инциденти и подршка при опоравување[285]

[285]https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilПревземено 29.07.2014

Оваа интеграциска и аналитичка функција треба да биде подржана како федерален сервис, со цел размена на информации околу заканите, ризиците и свесноста за инциденти на КИ.

Стратегијата уште обработува и Иновации истражувања и развој, иплементација на директиви, назначување на сектори и агенци на КИ, дефиници и др.

1.2. Специфични секторски агенции во САД

Препознавајќи ги постојните законски или регулаторни органи на специфики, се идентификуваат 16 критични сектори со следните одговорности:

- Хемиска индустрија / Секторот, специфични Агенција /Одделот за национална безбедност;
- Комерцијални објекти / Секторот, специфични Агенција / Одделот за национална безбедност;
- Комуникации / Секторот, специфични Агенција / Одделот за национална безбедност;
- Критично производство / на конкретен сектор Агенција / Одделот за национална безбедност;
- Брани / Секторот, специфични Агенција / Одделот за национална безбедност;
- Индустриска база одбрана / Специфични сектори Агенцијата / Министерство за одбрана;
- Службите за итни случаи / Секторот, специфични Агенција/ Одделот за национална безбедност;
- Енергија / Специфични сектори Агенцијата / Министерство за енергетика;
- Финансиски услуги / Специфични сектори Агенцијата / Министерство за финансии;
- Храна и земјоделство / Ко-специфични 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, специфични Агенција / Одделот за здравство и социјалните услуги;
- Информациска технологија / Секторот, специфични 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, специфични Агенција: Агенција за заштита на животната средина[286].

2. Односот на Европската унија кон Критичната инфраструктура

Безбедноста на критичната инфраструктура, генерално земено, се темели наДирективата 2008/114/ЕК - Council Directive 2008/114/EC од 08.12.2008, која опфаќа идентификација и одредување на Европската критична инфраструктура и оценката за потребата од подобрување на нејзината заштита. Советот на ЕУ го донесе овој документ врз основа на членот 308 од Договорот за создавање на европската заедница, попредлогот на Комисијата, мислењето на Европскиот Комитет и мислењето на Европската централна банка.

На оваа Директива и претходеа, најнапред во 2004 година Коминике за заштита на критичната инфраструктура во борбата со тероризмот, со предлози за подобрување на подготвеноста на ЕУ во превенцијата и справувањето со терористички акти. Во 2005 година Комисијата усвои ,,Зелена книга" за Европска програма за заштита на критичната инфрструктура, во која се понудени можните решенија за воспоставување на програма и вметнување на информациските мрежи за алармирање. Во 2005 година, исто така, Советот за правосудство и внатрешни работи има побарано од Комисијата изработка на Европска програма за заштита на критичната инфраструктура (EPCIP) со одлука да се базира на сите опасности, но предност да се даде на терористичките закани. Советот на ЕУ во 2007 година ги има усвоено и заклучоците на (EPCIP) во кој повторно се нагласува дека конечната одговорност за решенијата за заштита на критичните инфраструктури спаѓаат во рамките на државните граници на членките, но се поттикнуваат напори за развивање на Европска постапка за утврдување и означување на европски критични инфраструктури (ЕКИ). Од тие причини и Директивата 114 од 2008 година претставува прва насока во постапниот приод кон утврдување и означување на (ЕКИ) и проценките за нивна заштита.[287] Директивата се однесува на секторите енергетика и транспорт со напомена да се

[286]Presidential Policy Directive -- Critical Infrastructure Security and ResilienceFebruary 12, 2013
[287] COUNCIL DIRECTIVE 2008/114/ECof 8 December 2008 Whereas: (5)

преиспита, односно, да се надополни и примени и во останатите сектори, меѓу другите и секторот за информациски и комуникациски технологии.

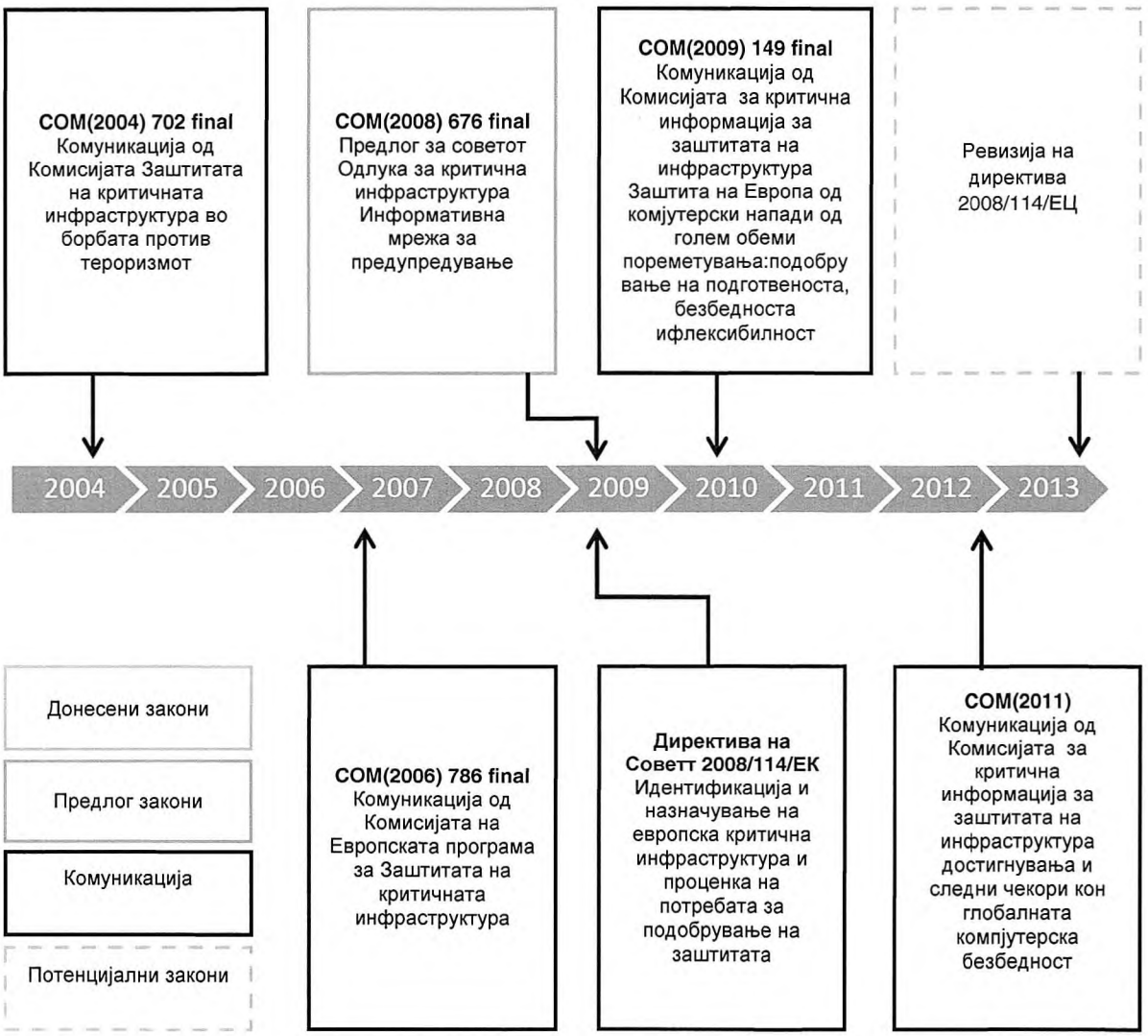
Како што е наведено во Директивата 114 /08 првенствена и конечна одговорност за заштита на (ЕКИ) имаат државите членки и сопствениците, односно, операторите на критичните инфраструктури.

Европската комисија ја има комплетирано индикативната листа за секторите од критичната инфраструктура, посветувајќи големо значење на заштита на критичната инфраструктура за многу функции на модерното општество. Додека пак, со Директивата на ЕУ 114 /2008 е претставена и методологијата, како критичната инфраструктура да се идентификува и дефинира како вообичаена процедура.

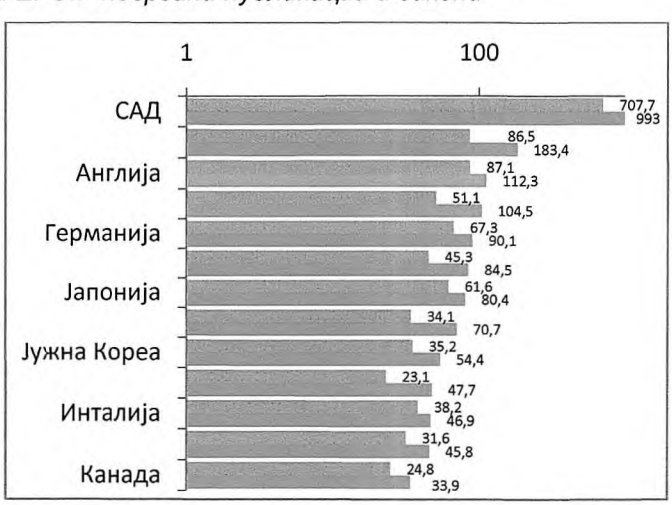
Проценката на безбедносните барања за ваквата инфраструктура како што е наведено во заклучоците, треба да се направат преку општ пристап. Европската унија во целост превзема конкретни чекори во развојот на политиките со кои во голема мерка ќе се влијае на подобрувањето и заштитата на Европската критична инфраструктура (ЕКИ), European Critical Infrastructure (ECI) во насока на редуцирање на ранливоста од разни закани, вклучувајќи и тероризам, криминални активности и природни катастрофи[288].

Како најзначаен напредок поврзан со CIP (critical infrastructure protection) е воведување на правна рамка наречена Европска програма за заштита на критична инфраструктура *(European Program for Critical Infrastructure Protection (EPCIP)*[289]. Првичната иницијатива беше дефинирана како одговор на закани од терористички закани врз критичната инфраструктура во ЕУ, но и покрај првичниот фокус на тероризмот, EPCIP ги содржи пристапите кон сите опасности вклучувајќи ги и природните катастрофи како и намерните опасности предизвикани од човекот.

[288] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[289] European Programme for Critical Infrastructure Protection (EPCIP) COM(2006) 786



Сл 11 Хронологија на EPCIP поврзани публикации и закони [290]



Сл.12 Истражувања кои се спроведени од страна на Corporation HSRC.[291]

[290] FOCUS Problem space report: Critical infrastructure & supply chain protection Cross-border Research Association (CBRA) January 2012 EU defined

Истражувања кои се спроведени од страна на Corporation HSRC. Прикажана е потрошувачката по основ на заштита на критичната инфраструктура со проекциите со 2018 год. (**$ B**)

2.1. Улогата наевропската програма за заштита на критичната инфраструктура EPCIP во развојот на безбедноста на европските критични инфраструктури

Главна цел на EPCIP е да се подобри заштитата на критичните инфраструктури во Европската Унија. Основата на EPCIP претставува, креирање на рамка која се однесува на заштитата на критичните инфраструктури, која е поставена во комуникето од комисијата . Иако, заканата од тероризам претставува приоритет на Програмата, заштитата на критичните инфраструктури се базира на пристап на заштита од сите опасности. Ако нивото на заштитни мерки во конкретен сектор на критичната инфраструктура е адекватен, сопствениците не треба да ги концентрират нивните напори кон заканите од кои се ранливи.

Следните принципи ја определуваат имплементацијата на EPCIP:

- *Субсидијарност* – напорите на комисијата во заштитата на КИ ќе се фокусираат на инфраструктурата која е критична од Европска перспектива, а не од национална или регионална. Иако, комисијата се фокусира на Европската КИ, може да побара да се земат во предвид земјите членки да ги имплементираат овие мерки во националните регулативи.
- *Комплементарност* – Комисијата ќе избегне дуплирање на постоечките напори, било да се на европско или на национално ниво кои се докажале како ефективни во заштита на Европската КИ, во тој случај EPCIP би ги содржале постоечките мерки.
- *Доверливост*– и на европско и на национално ниво, информациите за заштита на КИ (CIPI – critical infrastructure information protection) ќе се класифицираат соодветно и со одобрен пристап наречен ,,треба да се знае". Информациите кои треба да се споделуваат во поглед на КИ, треба да се во рамките на доверба и безбеднос.
- *Носители на активностите* – сите релевантни носители ќе бидат инволвирани колку што е можно повеќе во развојот и имплементацијата на EPCIP. Оваа ги вклучува сопствениците/ оператори на КИ како и јавните власти и други релевантни тела.

---

[291] Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljamaZdenko Kljaic, dipl.ing. Member, IEEE, Sadko Mandžuka, dr.sc. Member, IEEE, Pero Škorput, mr.sc. Member, IEEE 18. Telekomunikacioni forum TELFOR..

- *Пропорционалност*– мерките ќе бидат предложени само таму каде што ќе се идентификува потреба базирана на анализи на постоечките безбедносни празнини и ќе бидат пропорционални на степенот на ризик и типот на закана.
- *Сектор – по – сектор пристап* – со оглед на тоа дека различните сектори имаат одредено искуство, експертиза и барања во поглед на заштитата, EPCIP ќе се развива по принципот, сектор по сектор и ќе се имплементира според усвоена листа на сектори на КИ[292].

Според овој документ рамката на EPCIP ќе биде составена од:

- Процедура за идентификација и одредување на ЕКИ - ECI (European Critical Infrastructure), и пристап во одредување на потребите за подобрување на заштитата на тие структури.
- Мерките предвидени за обезбедување на имплементацијата на EPCIP, вклучувајќи го акциониот план и информациска мрежа за предупредување - critical infrastructure warning information network (CIWIN), користење на CIP (critical infrastructure protection) експертски групи на европско ниво, процес на споделување на информациии идентификација и анализа на меѓузависностите.
- Поддршка на земјите членки во поглед на националните критични инфраструктури кои би се користеле од одредени земји членки.
- План за делување (Contingency planning)
- Надворешна димензија
- Приклучување на финансиски мерки во предложената ЕУ програма за ,,превенција спремност и справување со последици од тероризам и други безбедносни ризици.[293]

Според овој документ ќе биде развиен механизам во вид на контакт група за координација и соработка во рамките на унијата. Претставен е и акциониот план со детерминирани рокови по основ на заштитата на критичните инфраструктури. Critical infrastructure warning information network (CIWIN) ќе се воспостави и ќе обезбеди платформа за размена на најдобри практики за размена на информации по безбеден пат[294]. Идентификацијата на меѓузависностите, претставува важен елемент во оваа програма од аспект на ранливостите, заканите и ризиците кои се однесуваат на критичните инфраструктури.

---

[292]COMMUNICATION FROM THE COMMISSIONon a European Programme for Critical Infrastructure Protection Brussels, 12.12.2006 COM(2006) 786 final

[293] COMMUNICATION FROM THE COMMISSIONon a European Programme for Critical Infrastructure Protection Brussels, 12.12.2006 COM(2006) 786 final

[294]http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260, Преземено на 14.05.2014год.

Одговорноста за заштитата на националните критични инфраструктури, според програмата паѓа на операторите на КИ на земјите членки, затоа во поглед на подобрување на заштитата, секоја земја членка е охрабрена да инсталира Национална програма за заштита на критичните инфраструктури. Целите на ваквите програми е да се одреди пристапот на секоја земја членка при заштитата на КИ лоцирани на нивна територија.

Ваквите програми, треба во најмала рака да се однесуваат на следните работи:

- Идентификација на критичните инфраструктури од страна на земјата членка според дефинирани национални критериуми,
- Област – онеспособувањето или уништувањето на одредена инфраструкрура, се одредува според распространетост на географската област која може да биде погодена со нејзино губење или онеспособување[295],

Последици – последиците од онеспособување или уништување на одредена КИ ќе се одредуваат врз база на:

- Граѓански ефект (број на загрозено население);
- Економски ефект (големина на економска загуба или деградација на продукти или услуги);
- Ефект врз животната средина;
- Политички ефекти;
- Психолошки ефекти;
- Последици по јавното здравје.[296]

Ако некој од овие критериуми не постои, комисијата ќе и асистира на земјата членка по нејзино барање во развој на истите, со обезбедување на релевантни методологии и тоа преку:

- Воспоставување на дијалог помеѓу КИ сопственици или оператори;
- Идентификација на географски и секторски меѓузависности;
- Донесување на оперативни планови поврзани со националните КИ;
- Секоја земја членка е советувана да ја базира националната програма за заштита на КИ врз основа на општа листа на КИ сектори кои се веќе етаблирани за Европската КИ[297].

[295] Ibid, Преземено на 14.05.2014год.
[296] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN Преземено на 12.03.2014год.
[297] Comunication from the Commision on a European Programme for Critical Infrastructure Protection Brussels, 12.12.2006 COM(2006) 786, p.7.

Според програмата, оперативното планирање е клучен елемент во процесот за заштита на критичните инфраструктури за да се минимизираат потенцијалните ефекти при онеспособување или уништување. Развојот на кохерентниот пристап при елаборација на оперативните планови, се однесуваат на учество на субјектите, соработката со националните авторитети и размена на информации со соседните земји, што ќе доведе до создавање на битен елемент во имплементирање на Европската програма за заштита.

Надворешна димензија поврзана со тероризмот, други криминални активности, природни катастрофи и останати причини не се заобиколени од интернационалните субјекти. Заканите не може да се гледаат само во национален контекст, надворешната димензија при заштита на критичните инфраструктури треба да има значајна улога при имплементацијата на Европската програма за заштита[298].

Поврзаноста и меѓузависноста на денешната економија и општество, значи дека и при нарушување, надвор од Европските граници може да има сериозни последици во ЕУ и земјите членки. Исто така, онеспособување или уништување на КИ внатре во ЕУ, може да има ефекти и на ЕУ партнерите. Дејствувањето за постигнување на зголемена заштита на КИ внатре во ЕУ ќе го минимизира ризикот од пореметување на европската економија, а со тоа ќе придонесе за европска глобална економска конкурентност.[299]

Исто така, подобрувањето на соработката во ЕУ преку специфични меморандуми на разбирање како на пр. (Менорандум за развој на општи стандарди, Заеднички студии на заштита, Идентификација на општи типови на закана, и сл.) и зголемување на стандардите за заштита надвор од ЕУ се битен елемент за Европската програма. Надворешната соработка примарно се фокусира на соседите на ЕУ. Глобалната поврзаност на одредени сектори и финансиските пазари бара и поглобален пристап, дијалогот и размена на најдобрите пракси кои треба да ги инволвираат сите ЕУ партнери и интернационални организации.

Што се однесува на надворешната димензија на EPCIP, а по основ на Заклучоците од Совет за 2011 година за развој на надворешната димензија на

[298] Comunication from the Commision on a European Programme for Critical Infrastructure Protection Brussels, 12.12.2006 COM (2006) 786, p.8

европската програма за критичната инфраструктуранагласена е потребата од соработка со релевантни трети земји[300].

Во поглед на општите цели и покриеност со финансиски инструменти, направена е програма која ќе стимулира, промовира и развива мерки на превенција, спремност и менаџирање со последиците, а има за цел спречување или редуцирање на сите безбедносни , поточно, ризиците поврзани со тероризмот, каде соодветно се базира на одредување на заканите и ризиците. Врз база на програмата по пат на грантови и постапки иницирани од комисијата треба да се обезбеди развој на инструментите стратегии, методологии, студии, активности и мерки на полето на ефективна заштита на КИ како во ЕУ така и во земјите членки[301].

Нов пристап кон EPCIP во првата фаза е да се направи пилот со четирите избрани критични инфраструктури на европска димензија, а тоа се Евроконтрол, Галилео, пренос на електрична енергија, мрежа и мрежата за пренос на гас, со цел да се оптимизира нивната заштита и еластичност.

Четирите сектори се одбрани врз основа на:

- нивната европска природата која се должи на нивната прекугранична димензија. Инфраструктурите се наоѓаат на територијата на повеќе од една земја-членка, така што нарушувањето на функцијата во една земја членка може да влијае на неколку други земји членки - домино ефект;
- нивната репрезентативност - избраните случаи покриваат транспорт, простор и енергетика; и
- нивните оператори / интерес на сопствениците е да учествуваат во овој пилот за споделување на најдобрите практики[302].

EUROCONTROL е определен Air Traffic Management (ATM) мрежен менаџер, системот за управување со воздушниот сообраќај на ЕУ, управување со протокот на голем број на летови во текот на денот.

Управувањето со воздушниот сообраќај е во врска со постапките, технологија и човечки ресурси кои се осигура дека:

- Авион се водени безбедно на небото и на земјата и
- Воздушниот простор се успеа да се прилагоди на променливите потреби на воздушниот сообраќај со текот на времето[303].

---

[300]COMMISSION STAFF WORKING DOCUMENT ON THE REVIEW OF THE EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP)Brussels, 22.6.2012 SWD(2012) 190 final, p16.

[301] COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection Brussels, 12.12.2006 COM(2006) 786 final - 8

[302]http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260Преземено на 12.03.2014год.

Целта, задачите и функциите на мрежата менаџер се уредени со Регулативата на Комисијата (ЕУ) бр 677/2011 на 7 јули, 2011 година за утврдување на детални правила за спроведување на АТМ мрежата.

GALILEO - Галилео е глобален навигациски сателитски систем (GNSS) кои во моментов се создадени од страна на Европската унија (ЕУ) и Европската вселенска агенција (ESA).[304]Со Европската програма за глобален сателитски систем за навигација, ќе се обезбедат услуги од витално значење за граѓаните и економијата во целост.

Во овој контекст потребно е да споменеме дека, електропреносот како и на европскиот пренос на гаспретставуваат мрежи без национални граници, што значи дека неуспехот на еден дел од мрежата би можеле да ги пренесат на други области и потенцијално би биле вклучени поголем број на држави.

Иако, Директивата е основа во сегашната европска регулатива, таа има доста празнини. Програмата EPCIP содржи многу повеќе елементи од Директивата 2008//114/ЕС и останува единствен пример на Европската легислатива.

2.2. Применливоста и имплементацијата на Директивата 2008/114/ЕС

Врз основа на Заклучоците од спроведувањето на Директивата 2008/114/ЕС која се однесува на заштитата на критичната инфраструктура се гледа дека безбедноста на КИ паѓа на повеќе сектори во индустријата, на сите земји членки, како и на земјите надвор од ЕУ.

Од тој аспект, Директивата претставува методологија како критичната инфраструктура да се идентификува и да се дефинира како средство за вообичаена процедура. Проценката на безбедносните барања за ваквата инфраструктура треба да се направат преку општ пристап, секоја земја членка треба да ја одреди потенцијалната критична инфраструктура која ги задоволува и меѓузависните и секторските критериуми. Процедурата е имплементирана од секоја земја членка според следните чекори:

Чекор 1 Секоја земја членка треба да имплементира секторски критериум со цел да се направи првична селекција на критична инфраструктура внатре во секторот.

Чекор 2 Секоја земја членка треба да дефинира критична инфраструктура како потенцијален дел од европската критична инфраструктура, а според критериумот од чекор еден.

---

[303]https://www.eurocontrol.int/articles/air-traffic-management-atm-explained Превземено 14.12.2015год.
[304]https://en.wikipedia.org/wiki/Galileo_(satellite_navigation), Превземено 14.12.2015год.

Чекор 3 Секоја земја членка треба да ги примени преку граничните елементи од дефиницијата на Европската критична инфраструктура кон дефинирање на потенцијалната критична инфраструктура.

Чекор 4 Секоја земја членка треба да примени вкрстени критериуми за поставување на потенцијална Европска критична инфраструктура.[305]

Сумирајќи ја Директивата 114 од 2008 поголемиот дел од земјите-членки ги спроведуваат одредбите на Директивата во инкорпорирање на насоките во рамките на нивната национална законодавна и регулаторна рамка прекуразлични пристапи, како што се:дополнувања на постоечките закони и прописи, нови закони, резолуции, процедурални промени на постоечките активности ЦИП поврзани, уредби и извршните наредби[306]

Голем број земји-членки, по оценка на нивните постоечки национални пристапи од аспект на Директивата, дојдоа до заклучок дека не се потребни законски измени за спроведување на Директивата, додека пак државите (Австрија, Естонија, Финска, Холандија, и Велика Британија) ќе ги исполнат неопходните процедурални промени во рамките на нивните постоечки национални рамки, а се со цел спроведување на Директивата.

Многу други европски секторски политики и законски рамки, ги содржат принципите на обезбедувањето, менаџментот со ризици, отпорност и подготвеност и подршка и ги делат истите цели со политиката на EPCIP. На пример, подолу наведените иницијативи и делови од европската регулатива содржат елементи од програмата и тоа:

- Регулативата на (ЕУ) (ЕС) No 300/2008 за општи правила во полето на безбедноста на цивилното воздухопловство
- Директивата 2005/65/ЕС подобрување на безбедноста на пристаништата
- Одлука на совет 2007/124/ЕС одредување на спецјални програми ,, Менаџмент за превенција, Подготовка и последици од тероризам и други безбедносни ризици,, и др.[307]

[305]Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection,Annex III

[306]Commission staff working document on the review of the European Programme for Stitical Infrastructure Protection (EPCIP) Brussels, 22.6.2012SWD(2012) 190 final.

[307]http://ec.europa.eu/dgs/home-affairs/news/intro/docs/sec_2010_911_en.pdf

3. Германска стратегија за заштита на критичната инфраструктура

Својот концепт на заштита на критичната инфраструктура Германската држава го темели на Националниот стратегиски план за заштита на критичната инфраструктура, издаден од страна на Министерството за внатрешни работи во 2009 год. Во овој документ заштитата на кртичната инфраструктура е претставена како централно прашање на безбедносната политика на земјата и се раководи по 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 развојот на анализи и заштитни концепти. Треба да се спомене дека, четири петтини на критичната инфраструктура во Германија се во приватен сектор[308].

Во оваа стратегија, снабдувањето со електрична енергија, е рангирано на врвот во споредба со другите земји. Овасе должи на фактот дека приватните компании се под законска обврска да работат со безбедна, сигурна мрежа за снабдување. Слична е состојбата и со телекомуникациските услуги, кој 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.

Сојузното министерство за внатрешни работи (Сојузна МВР) обезбедува секторски координации. Во име на Министерството за внатрешни работи, властите во рамките на нивна 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 во дер Informationstechnik - BSI), Сојузната кривична Полициска служба (Bundeskriminalamt - BKA) и Федералниот институт "Сервис за Техничка поддршка "(Bundesanstalt Technisches Hilfswerk,TXB) - развиваат проценка на заканите, анализи и заштита[309].

Како критичност и области на одговорност во документите на Германската стратегија се претставени во Табела бр.5, каде што се претставени значајните компоненти кои постојат помеѓу двата инфраструктурни сектори, бидејќи речиси сите социо-економски услуги во голема мера се потпираат на основната техничка инфраструктура. Основната техничка инфраструктура, пак, зависи од социо-економските услуги како стабилна правна служба или итна помош на медицински и спасувачки служби во случај на криза.

---

[308]National Strategy forCritical Infrastructure Protection(CIP Strategy), Federal Republic of Germany Federal Ministry of the Interior, Berlin, 17th June 2009

[309] Ibid, p.5

Техничка основна инфраструктура	Социо-економска инфраструктура
Снабдување со електрична енергија	Јавно здравје; храна
Информациски и комуникациски технологии	Спасувачки и сервиси за вонредни ситуации и катастрофи
Транспорт	Собранието; власт; јавната администрација; спроведување на законот
Вода за пиењеи одведување на отпадна вода	Финансии; осигурителниот бизнис
	Медиумите; и културни објекти (културно наследство)

Табела. 6 Критичните инфраструктури во Германската стратегија извор[310]

3.1. Закани, ризици, слабости и култура на ризик

Критичната инфраструктура може да биде изложена на разни закани кои мора да бидат вклучени како во анализи на ризик и закана, така и во изборот на опции за акција.

Природни настани	Техничка грешка / човечка грешка	Тероризам, криминал, војни
екстремни временски настани,меѓу другото: (бури, тешки врнежи, поплави,топлотни бранови и сл.)	оштетувања во системот, меѓу другото: неисправен хардвер или софтверски грешки	тероризмот
суши, пожари	небрежност	саботажа
сеизмички настани	несреќи и вонредни состојби	други форми на криминал
епидемии и пандемии, кај луѓето, животните и растенијата	неуспеси во организацијата,меѓу другото, недостатоците во ризик и управување со кризи, несоодветната координација,и соработка	граѓански војни и војни
космички настани,меѓу другото, метеорити и комети		

Табела бр.7: Спектар на закани преставена низ Германската стратегија[311]*:*

[310] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of Germany, p.6

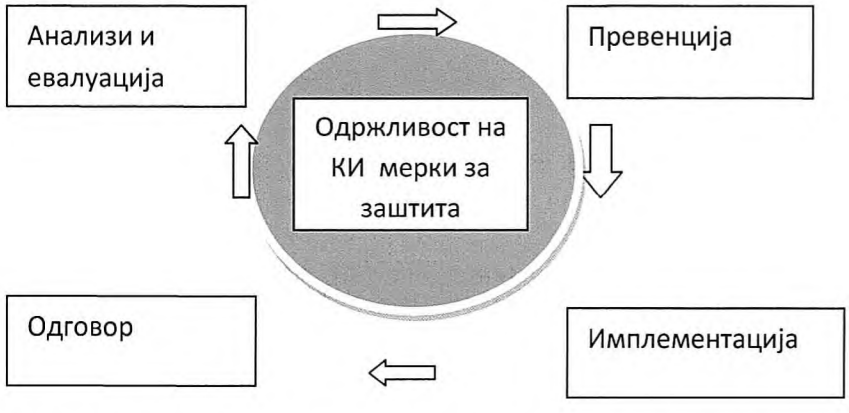
[311] National Strategy for Critical Infrastructure Protection (CIP Strategy) Federal Republic of Germany,p. 9

Тука се потенцира дека вниманието на државата и на општеството мора да биде насочено кон терористичките закани и природните непогоди, но од големо значење преставуваат и ризиците и заканите за информатичката инфраструктура.

Мора да се истакне дека, непостои целосна, односно, потполна заштита на инфраструктурата и нејзината оперативна ефикасност, штоможе да се обезбеди од страна или на државата или операторите. Концептот кој го прокламира Стратегијата е наречен ,,култура на ризик". Таа култура се базира, меѓу другото, на:

- отворена комуникација меѓу државата, компаниите, граѓаните и општата јавност, земајќи ја предвид чувствителноста на одредени информации;
- соработка помеѓу сите засегнати страни во спречување и управување со инциденти;
- поголема самозаложба од страна на операторите во врска со инцидентот спречување и управување;
- поголема и независна самозаштита и самопомош на поединци или институции, погодени од прекин или загрозување на критични нфраструктурни услуги[312].

Водечките принципи за заштитата на критичната инфраструктура ги наведува како: доверлива соработка помеѓу државата и бизнис индустријата на сите нивоа



Сл. бр.13 Принципи на заштита преставена преку германската стратегија

Со цел да се зајакне заштитата на критичната инфраструктура, потребна е интензивна соработка, координација и информации помеѓу релевантните партнери и актери, вклучувајќи ги особено:

- федералната администрација: Сојузните министерства и нивните специјализирани, агенции;

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

- сојузните држави (Länder) и нивните органи,
- административните области, општините и локалната власт,
- инфраструктурни оператори;
- различните организации за помош и итни случаи;
- релевантни индустриски асоцијации и секторски / професионалниздруженија,
- на научната и истражувачката заедница;
- безбедносната индустрија;
- јавноста воопшто (популација, медиуми);
- меѓународни и наднационалните институции;и
- други институции по потреба[313].

Доколку се идентификуваат значителни безбедносни недостатоци во критичните сектори на инфраструктурата и не се исправат врз основа на доброволни заложби од страна на давателите на услуги и операторите или ако, поради појавата на новите закани и ризици, постојните законски одредби не понудат соодветна заштита или не важат во поглед на сигурноста и безбедноста, мрежната безбедност, безбедноста на операторот и корисниците, Федерацијата самата го задржува правото, во рамките на својата надлежност, да се оптимизира за заштита на соодветните инфраструктури со измена на постоечкото законодавство или донесување на нови законски прописи.
Федерацијата и локалните власти во Република Германија се обврзани заеднички за подобрување 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, кои се спроведуваат паралелно, и е врз основа на кооперативен пристап усвоен од страна на Федералната администрација со вклучување на други големи ,,играчи,, односно оператори и соодветни здруженија:

1. дефинирање на општите цели на заштита;
2. анализа на закани, слабости и менаџмент;
3. процена на заканите;
4. спецификација на цели, земајќи ги предвид постоечки заштитни мерки; анализа на постојните прописи, применливоста, идентификација на дополнителни мерки кои 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.

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

Имплементација на мерки за постигнување на целите според:

- специфични решенија и внатрешна регулатива,
- договори за подршка на бизнисот и индустријата,
- развој на заштитните концепти од страна на компаните,
- постојан процес на комуникација за ризиците (дијалог за наодите од анализите, проценките, заштитни цели и акциони планови).[314]

За имплементација на стратегијата за заштитата постојат голем број на инструменти во форма на:

- програми и планови (пр. Национален план за заштита на информатичка инфраструктура и односните имплементациски планови како стратешки концепт за заштита на ИТ),
- специфични препораки за делување (пр. Основен Национален концепт за заштита како основно упатство за физичка заштита на КИ, Упатство за менаџмент на ризици и кризи за операторите на КИ или Национални концепти со препораки за делување при заштита на индивидуални сектори на КИ),
- стандарди норми и регулативи (пр. Стандарди за информатичка безбедност, како основна препорака за делување на операторите, или регулативи на Германската асоцијација на снабдувачи со гас и вода, за справување со ризици на полето на снабдување со вода за пиење).[315]

Со оглед на давање на приоритет во соработката се организираат соодветни платформи кои ги вклучуваат државните и јавните авторитети како и компаниите и асоцијациите, со цел да се имплементира политичко стратегиска рамка.

Платформите за партнерство во безбедноста може да се организираат како:

- тркалезни маси;
- федерално ниво;
- ниво на сојузни држави;
- ниво на локална власт;
- заеднички тркалезни маси помеѓу горе наведените;[316].

Овие сегменти, организираат активности врз основа на меѓусебно прифатени процедури, во согласност со националната стратегија, политика, процедуралните чекори и механизмите.

---

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

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

[316] Ibid.

3.2. Меѓународна соработка

Катастрофите кои влијаат на оперативноста на критичните инфрструктури не запираат во националните граници на државата, оттука една од поважните интернационални компоненти, особено во делот на информатичките и комуникациските технологии, енергијата и транспортот, се однесува на меѓународната соработка и истата е опишана во национална стратегија а како поважни меѓународни партнери се:

- директните соседи
- Европската Унија
- земјите од Г8
- НАТО[317]

Во рамките на меѓународната соработка Германската држава ги подржува сите напори и мерки за идентификување и минимизирање на ранливоста, особено во инфраструктурата со меѓународно значење. Централната важност се однесува на порастот на постоечката и новата билатерална соработка за размена на податоци и најдобрите практики како и координацијата на мерките за заштита на прекуграничните КИ.

Активностите на Европско ниво поврзани со билатералните и мултилатералните активности имаат за цел заштита на КИ, во делот на размена на информаци и методи, примена на проверени и тестирани процедури, како и соодветен пристап во поглед на непречено спроведување на заштитата на критичните инфраструктури во ЕУ стремејќи се кон принципот на солидарност.

4. Односот на Република Хрватска кон заштитата на критичната инфраструктура

Во Република Хрватска управувањето и заштитата на критичната инфраструктура е регулирано со закон донесен во 2013 год, а е изготвен врз основа на Директивата 114 од 2008 на ЕУ.

Со овој Закон Р.Хрватска ги има уредено националните и европските критични инфраструктури, секторите на националните критични инфраструктури, управувањето со критичните инфраструктури, изработката на анализата на ризик, безбедносниот план на сопствениците, безбедносниот координатор за критични инфраструктури,

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

постапки со осетливи и класифицирани податоци, како и надзорниот механизам над спроведување на законот[318].

Во Законот на Р.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 (патничкиот, железничкиот, воздушниот, поморскиот и внатрешната пловна инфраструктура)
- Здравството (здравствената заштита, производството, трговијата и надзорот над лековите),
- Водата (регулација и заштита на снабдителните системи за вода и комуналните постројки),
- Храна (производството и снабдување со храна и безбедноста на храната, залихите),
- Финансиите (банкарството, берзите, инвестициите, осигурувањето)
- Производство, складирање и превоз на опсните материи (хемиски, биолошки, радиолошки и нуклеарни материјали) ,
- Јавните служби (обезбедување на јавниот ред и мир, заштитата и спасувањето, итна медицинска помош),
- Националните и културните вредности[319]

Покрај овие сектори со Одлука на владата на Република Хрватска, можат да се одредат и критични инфраструктури од други области.

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

[318]Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, Преземено на 14.11.2015год.
[319] Закон о критичним инфраструктурама NN56 13, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, Преземено на 14.11.2015год.

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 Р. Хрватска се базира на утврдување на севкупните причинители по следниот редослед:

- Човечки губитоци (се проценува бројот на можните човечки загуби или повреди од причина на престанок на работа на определена критична инфраструктура)
- Стопански губитоци (проценката се врши врз основа на важноста на стопанските губитоци и или можните влијанија на околината)
- Влијанието врз јавноста (оваа проценка се однесува на довербата на јавноста, загриженост и пореметување на секојдневното функционирање на животот, вклучувајки и загуба на основните јавни услуги)[320]

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 проценката 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 делување на сите утврдени критични делови или објекти, мрежи или состави со примена на следните мерки:

[320] Закон о критичним инфраструктурама NN56 13 член 9http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, Преземено на 14.11.2015год.

- Постојани сигурносни мерки и постапки (технички, организациски, комуникациски мерки и мерките и постапките за навремено предупредување и зголемување на свеста)
- Степенување на безбедносните мерки кои се активираат во зависност од јачината на заканата.
- Преиспитување на безбедносните планови (временска рамка)[321]

Безбедносен координатор за критичната инфраструктура се именува за секој сектор на критичната инфраструктура, а го определуваат сопствениците на критичната инфраструктура, кој е задолжен за комуникација помеѓу сопствениците на критичните инфраструктури и државното тело.Исто така, со овој закон во делот Европска Критична инфраструктура се дефинираат условите, како и обврските на Р. Хрватска во поглед на одредување на европската критична инфраструктура која се наоѓа на подрачјето на Р. Хрватска, како и критичната инфраструктура која е од заначење за Хрватска, а се наоѓа на подрачјето на друга држава од ЕУ.

5. Односот на Република Чешка кон 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 создавање на амандман430/2010 на актот 240/2000 (Критички Акт) и одредува нови обврски кога се работи за заштита на критичната инфраструктура. Во смисла на овој амандман, во тек е постапката за идентификација и 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 произлегуваат од директивата[322].

Сл.14 Постапката за идентификација и означување на ЕКИ во Р Чешка Извор:

[321] Закон о критичним инфраструктурама NN56 13 член 13 http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, Преземено на 14.11.2015год.

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

Во правниот кодекс на Чешка Република, прашањата за критична инфраструктура не биле регулирани до Декември 2010 година. Постапка за идентификација и означување на критичната инфраструктура е во процес во Република Чешка. Како што е прикажано на слика бр.12, постапката произлегува од законската регулатива, а се состои од четири чекори:

- **Избор на критична инфраструктура во рамките на одделни сектори.**Овој чекор е во тек во Чешката Република и субјектите кои 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 КИ, според критериуми дефинирани од страна на законодавството.
- **Примена на дефиницијата на критична инфраструктура.**Овој чекор е директно испреплетен со претходниот. Суштината на овој чекор е дека потенцијалната КИ мора да е во согласност со дефиницијата за КИ која е дадена од законодавството (директива). Овој чекор се врши од страна на истите лица како и во претходниот чекор.
- **Примена на дефиницијата за Европска критична инфраструктура (ЕКИ).** Дефиницијата за ЕКИ ќе се примени на КИ како што е дефинирано со критериумите на секторот и во согласност со дефиницијата за КИ. Критичните инфраструктури што ја задоволуваат дефиницијата за транс-граничен елемент ќе го следат следниот чекор од процедурата. Критичните инфраструктури што не го задоволуваат транс-граничниот елемент на дефиницијата на ЕКИ, можат да бидат назначени како национална КИ на Чешка Република. Овој чекор се врши од страна на истите лица како и во претходните два чекори.
- **Примена на сеопфатни (вкрстени) критериуми**. Секоја земја-членка ќе ги применува вкрстените критериуми со останатите потенцијални ЕКИ. 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 ЕКИ што не ги задоволува вкрстените критериуми нема да се смета за ЕКИ. Овој чекор е покриен од страна на Министерството за внатрешни работи - Генерален директорат на Противпожарната

служба како највисок администратор и субјект за контакт во Чешка Република, во смисла на ЕКИ[323].

Критичните инфраструктури што поминале низ сите чекори на оваа постапка се смета за потенцијална 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 КИ, елементи и назначувањето, активни субјекти на заштита на КИ во Чешка Република, сега се Министерствата и другите централни органи на управата, во чија сфера спаѓаат некои сектори на КИ и индивидуални сопственици на КИ или операторите на КИ.

5.1. Субјекти на заштита на критичната инфраструктура во Република Чешка

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 КИ субјекти, индивидуални администратори и ко-администратори, кои се вклучени во сегашната постапка на идентификација на елементи и означување на КИ во Република Чешка се:

Министерствата и другите централни административни органи на Чешка

Министерствата и другите централни административни власти се администратори или ко-администратори за поединечни сектори за КИ и нивната главна задача е координација и изнаоѓање консензус со субјектите на КИ при спроведувањето на заштитата на КИ. Овие Министерствата се: Министерството за надворешни работи, Министерство за одбрана, Министерство за финансии, Министерство за труд и социјална политика, Министерство за внатрешни работи, Министерство за животна средина, Министерство за индустрија и трговија, Министерство за транспорт и врски, Министерство за земјоделство, Министерство за здравство, Министерство за правда. Министерството за внатрешни работи е контакт точка за работи за ЕКИ и ги извршува задачите во секторот на заштита на КИ кои следуваат од членството на Чешка Република во Европската Унија (предлага вкрстени критериуми; ја процесира листата која е основа за определување на КИ и ЕКИ елементите; комуницира и ја информира Европската комисија во врска со ЕКИ; и др.) Централни административни канцеларии во својство на администтартори и ко-администратори за оделни КИ сектори се: Регулаторна канцеларија за енергетика, Управа на државните материјални резерви,

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

Чешка управа за телекомуникации, Чешка народна банка, Државен завод за нуклеарна безбедност, Чешката управа за рударство, Национална безбедносна управа, Завод за статистика на Чешка Република, Безбедносно информативна служба.Во сегашно време, ангажирани се воглавно администартори и ко-администратори од сектори во кои се врши постапката на идентификација и означување на КИ (енергетика и транспорт).[324]

Субјекти на КИ - сопственици / оператори на КИ

Според законската регулатива, субјекти на КИ се поединечните сопственици или оператори на КИ. Постапката за идентификација и означување на КИ елементи се уште не е завршена, така што индивидуалните субјекти сеуште 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 КИ од самиот почеток, поголемиот број на субјекти во постапката на идентификација и означување на КИ активно учествуваат. Согласно законската регулатива, основната и крајна одговорност за заштита на ЕКИ 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 КИ. Финансиската одговорност во врска со мерките за зголемување на безбедноста на елементите на ЕКИ е на сопственикот / операторот на елементите на ЕКИ[325].

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 потенцијалниот КИ сектор. Со тоа се поврзани економските влијанија на овие субјекти од имплементацијата на заштитата на КИ. 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 отстранување на дуплирањето во системот, правичност на мерките итн.

---

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

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

Јавност

Претходната категорија може да се сфати и како јавен субјект. Исто така, јавните интереси се примарно претставени, пред се, од централно административните органи на Чешка. Причина е појавата на заштитата на КИ како систем за граѓаните - зголемување на јавната безбедност. Оттука, и јавните субјекти треба да се разгледуваат поединечно. Начините на кои системот на заштита може да влијае врз јавноста се повеќекратни.

Примарно, на индиректен начин, е преку државните структури - централните административни органи на дадената земја-членка. Овие органи ги води избрано јавно претставништво или тоа претставништво избира раководство на одредени централно административни органи. Друг начин е преку здружение на граѓани, чија цел ќе биде одбрана на специфичните интереси на одреден дел од јавноста во системот на заштита на КИ. На јавните интереси може да се влијае, исто така, од страна на поединец. На пример, Министерството за внатрешни работи во Чешка Република има воспоставено база на податоци на експерти во истражување на безбедносниот сектор, кои, меѓу другото, се занимаваат со истражување на сектори кои се однесуваат на прашањата за заштита на КИ. Меѓутоа, потребно е одредено ниво на стручни квалификации за оваа активност.

Други субјект

Последна група на субјекти претставува институции и организации кои се занимаваат со прашања на заштита на КИ. 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 КИ, воглавно, во однос на професионален аспект[326].

6. Односот на Австралија кон безбедноста на критичните инфраструктури

Безбедноста на критичните инфраструктури разгледуван низ Националните насоки за заштита на критичната инфраструктура од тероризам, донесен од страна на Комитетот за борба против тероризмот, наменет за Австралија и НовЗеланд, обезбедува рамка за национален конзистентен пристап на заштита на критичните инфраструктури, државата, владата и бизнисот. Стратегијата е дизајнирана да им помогне на сопствениците и операторите на критичните инфраструктури во нивните дискусии со надлежните органи (вклучувајки ја и Владата) при заштита на критичната

[326]International jurnal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal.

инфраструктура од тероризам. Во неа, исто така, е дефинирано дека третирањето на индивидуалните критични нфраструктурни капацитети ќе зависат од одредување на критичноста на објектот, природата на безбедносното опкружување и профили, односно, видови на ризик за објектот или релевантниот сектор.Како што се наведува во документот, заканата од тероризам бара постојани напори за заштита, вклучувајќи и разузнавачки информации заради развој на соодветни нивоа на заштита на критичните инфраструктури во Австралија и постапки за брзо опоравување. Иако, владите имаат значителна улога во заштитата на критичните инфраструктури, сепак одговорноста паѓа на сопствениците или операторите. Операторите треба да го разберат тероризмот, како опасност во рамките на менаџментот на ризици и од сите опасности. На национално ниво критичната инфраструктура е дефинирана како ,,оние капацитети, ланци на снабдување, информациски технологии и комиуникациски мрежи со чие уништување или оштетување би имале значително влијание на социјалната и економската благосостојба или би ја нарушила способноста на Австралија да обезбеди национална одбрана и безбедност".[327].

На национално ниво, терминот заштита на критична инфраструктура CIP (critical infrastructure protection) се користи за да се опишат активностите и мерките за справување со одредена закана од тероризам. CIR (critical infrastructure resilience) еластичност/ флексибилност на критичната инфраструктура е термин кој се користи во стратегијата 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 го подржува CIR преку TISN (trusted information sharing network) мрежа за споделување на доверливи информации и CIAC (critical infrastructure advisory council) – советодавен совет на критичната инфраструктура.

Националните насоки за заштита на критичната инфраструктура од тероризам ги подржува и препознава следните активности:

- Клучна одговорност на операторите во заштита на критичните инфраструктури,
- Рамка за менаџмент со ризици при заштита во однос на идентификација и приоритизација на критичните инфраструктури,
- Национален антитеристички План,
- Национален Прирачник за заштита на критичните инфраструктури,

[327]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година

- Владина стратегија за еластичност на критичните инфраструктури,
- Релевантни Австралиски стандарди,
- Релевантна легислатива и меѓународни обврски кои се применуваат во специфични индустрии како што се транспортот или производство на нафта и гас надвор од државата.[328]

Од аспект на секторирање на критичните инфраструктури, односно, идентификување на критичните инфраструктури по области, застапени се: економијата, транспортот, енергијата, водите, здравјето, храната и комуникациите, но исто така, ги вклучува 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 идентификува критичните инфраструктури во рамките на нивните надлежности кои се критични или битни 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 - одредени услуги или капацитети, неможат да бидат обезбедени на национално или регионално ниво,
- Главно - ако услугите или капацитетите се потешко оштетени би се применила 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 - незначителна штета на процесите[329].

Во однос на пристапот кон контратеристичките мерки врз основа на информации и разузнавање, Австралија се потпира на силна разузнавачка активност, при

[328]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година
[329]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година

превенција и спремност во антитерористичките подготовки. Овој пристап вклучува мерки базирани на принципите на менаџментот со ризици и обезбедување на капацитети за справување со различни видови на терористички напади и справување со нивните последици. Овие разузнавачки и криминални истраги се изведуваат од страна на ASIO Australian security intelligence organization - Австралиска служба за разузнавање и слични агенции со цел спречување и истражување на заканите од клучните елементи при проценка на ризик а тоа се:

- идентификација на клучните елементи во критичните инфраструктури капацитетите,
- земање во предвид дали критичните инфраструктури е производител на продукти кои можат да се искористат од терористите,
- идентификација на можните закани,
- определување на ризици кои бараат или не бараат третирање,
- средства со кои би се извршил нападот,
- проценка на ранливост,
- последици,
- надворешни меѓузависности[330]

Битен елемент во оваа насока, секако претставува функционирањето на Национален советодавен систем при терористички закани. Исто така, превенција 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.

[330]https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf Превземено 11.11.2015година

ГЛАВА VIII

Критична инфраструктура во Република Македонија

1. Регулирање на Критичната инфраструктура во Република Македонија

Терминот критична инфраструктура, се уште не е прифатен во рамките на Националната регулатива на Република Македонија, меѓутоа тоа незначи дека не се определени или дефинирани објектите од посебно значење или виталните објекти во Република Македонија.

Република Македонија има континуитет во насока на дефинирање на овие објекти, предвидени се мерките за безбедност, делегирани се задолженијата и одговорностите, меѓутоа, не се усогласени, односно, детерминирани во согласност со насоките на Европската Унија. Во оваа насока, не постои јасно конкретизирање на поимите, односно, не се опфатени критичните инфраструктури во согласост препораките на унијата.

Најнапред ќе ја наведеме Одлуката од 1996 годиназа определување на личностите и објектите што се заштитуваат, а се однесуваат на мерките и активностите кои ги преземаат Министерствата за внатрешни работи и одбрана со општи и посебни мерки на заштита, вклучувајќи ги и општите мерки на заштита кои се преземаат од страна на самите органи, организации, претпријатија и другите правни лица. Во оваа Одлука покрај објектите кои се во целосна надлежност на обезбедувањето од страна на Министерството за одбрана и Министерството за внатрешни работи, се наведени и објектите кои се од интерес на безбедноста на државата. Оваа Одлука за определување на личностите и објектите што се заштитуваат е донесена врз основа на Законот за внатрешни работи од 1995 година, покрај останатото во еден дел се наведени и објектите од интерес за безбедноста на Република Македонија, а тука се преставени: објектите од радио и телевизијата, објектите од ПТТ сообраќајот, електростопанството, железниците, аеродромите, водоводите.

Еден од позначајните чекори во оваа насока е направен со донесувањето на Одлуката за определување на правните лица кои се должни да имаат приватно обезбедување. Оваа Одлука е донесена од страна на Владата на Р.М во 2013 година, а врз основа на член 44 од Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 166/12) и Законот за изменување и дополнување на Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 164/13) во кој е означено времето на нивното влегување во сила. Според членот 44 од овој Закон, Владата на Република Македонија определува кои правни лица се должни да имаат приватно обезбедување, ако вршењето на нивната дејност е поврзано со ракување со радиоактивни материи или други по луѓето и околината опасни материи, предмети и објекти од особено културно и историско значење, како и во други случаи

кога е тоа во интерес на безбедноста, односно одбраната на Република Македонија.Во ставот (1) на овој член го дефинира правното лице да може да го врши обезбедувањето како:

1) обезбедување за сопствени потреби врз основа на издадена дозвола за обезбедување за сопствени потреби и
2) обезбедување со користење на услуги од правни лица што вршат приватно обезбедување во вид на давање на услуги, согласно со овој закон, врз основа на склучен договор[331]

Со Одлуката се наложува задолжително обезбедување на правните лица чија дејност е поврзана со ракување со:

- радиоактивни материи или други по луѓето и околината опасни материи. Тука, пред се опфатени правните лица кои се регистрирани за вршење на дејност согласно Законот за заштита од јонизирачко зрачење и радијациона сигурност;
- правните субјекти регистрирани за производство и промет на големо со лекови и медицински помагала согласно Законот за лековите и медицинските помагала како и други прописи од областа на лековите;
- правните субјекти регистрирани за производство и промет со запаливи течности и запаливи гасови, правните субјекти за вршење на превоз на опасни материи;
- правните лица на територијата на Република Македонија регистрирани за вршење на превоз на опасни материи, во кој покрај обврските предвидени со Законот за превоз на опасни материи во патниот и железничкиот сообраќај.[332]

Треба да се истакне дека, со истата Одлука опфатени се и правните лица чија дејност е поврзана со ракување со предмети и објекти од особено културно и историско значење. Задолжително физичко и техничко обезбедување е предвидено и за јавните установи и приватните музеи основани согласно Законот за музеите и јавните установи основани, согласно Законот за заштита на културното наслаедство, чија дејност е поврзана со ракување со предмети од особено културно и историско значење како и археолошките локалитети и другото недвижно културно наследство[333].Во делот IV од оваа Одлука дефинирано е задолжителното приватно обезбедување на правните лица кога е тоа во интерес за безбедноста и одбраната на Р.М. Тука пред се, се наведени дејностите:

---

[331] Законот за приватно обезбедување („Службен весник на Република Македонија“ бр. 166/12) член 44

[332] Одлуката за определување на правните лица кои се должни да имаат приватно обезбедување, Службен весник на Р.М бр. 106 на 29.07.2013Год. член 2

[333] Исто член 3

- од областа на енергетиката согласно одредбите од законот за енергетика, производство, пренос и дистрибуција на енергија.
- дејностите од областа на водоснабдувањето на населението со вода за пиење и технолошки потреби согласно Законот заводостопанства.
- дејностите за заштита и управување со повеќенаменски подрачја, заштита и унапредување на животната средина, заштита на природата и природното наследство согласно законот за животната средина, Законот за заштита природата и согласно други прописи од областа на заштитата и унапредување на животната средина, човековата околина, природата и националните паркови.
- Македонската радиотелевизија и другите правни лица кои се регистрирани за вршење на дејност од јавен интерес, електронски и печатени медиуми согласно законските прописи кои ја регулираат оваа област.
- Народната банка на Р.М. и правните лица регистрирани за вршење на банкарски работи согласно Законот за Народна банка на Република Македонија и согласно Законот за банките[334].

Во доменот на обезбедување на објектите од посебен интерес, засегнати се повеќе субјекти како и надлежностите, во рамките на обезбедувањето на овие објекти кое спаѓа во категоријата на обезбедување третирано од повеќе институции, вклучувајќи го и Министерството за внатрешни работи кое има разработено и евидентен е континуитетот во развојот на обезбедувањето на објектите од посебен интерес. Во рамките на МВР оваа проблематика од секогаш била застапена и била предмет на обработка и регулирана согласно разни акти.

Мора да се истакне дека во рамките на прописите кои ги третираат критичните инфраструктури навлегуваат и законските прописи кои ја регулираат заштитата и спасувањето, како и областа за управување со кризи. Во тој контекст ќе го издвоиме Законот за управување со кризи со кој се уредува системот за управување со кризи во Република Македонија и тоа во поглед на организацијата и функционирањето, одлучувањето и употребата на ресурсите, комуникацијата, соработката, проценката на загрозеноста на безбедноста, планирањето и финансирањето, како и други прашања поврзани со системот за управување со кризи. Системот се остварува и организира поради превенција, рано предупредување и справување со кризи кои претставуваат ризик за добрата, здравјето и животот на луѓето и животните, а се настанати од природни непогоди и епидеми или други ризици и опасности кои директно го

[334] Исто член 4

загрозуваат уставниот поредок и безбедноста на Република Македонија или дел од неа, а за кои не постојат услови за прогласување на воена состојба. Системот за управување со кризи опфаќа и прибирање на информации, процена, анализа на состојбата, утврдување на целите и задачите, развој и спроведување на потребните дејства за превенција, рано предупредување и справување со кризи[335]. Анализирајќи го овој Закон во поглед на превенцијата и справување со кризните состојби, предвидени се и јавните претпријатија, јавните установи и служби, како и трговските друштва кои се од посебно значење за работа во кризна состојба.

Во овој Закон, со посебни одредби се утврдуваат Министерствата и другите органи на државната управа да учествуваат во превенцијата, раното предупредување и справување со кризи, во согласност со закони кои се уредуваат нивните надлежности.
Во рамките на овој Закон заради предлагање на Одлуки и обезбедување на постојани консултации, координација, навремена реакција, ефикасност и соодветно искористување на расположливите ресурси во случај на кризна состојба како и обезбедување на навремена, квалитетна и реална проценка на загрозеноста на безбедноста на Република Македонија од ризици и опасности како што е наведено во членот 12 од Законот се формираат Управувачки комитет и Група за проценка кои се основа на Дирекцијата за управување со кризи и кои имаат јасно дефинирани надлежности и задолженија[336].

Без да се навлезе во целосна елаборација на законското решение, сепак важен сегмент поврзан со критичната инфраструктура се и одредени одредби од Законот за класифицирани информации посебно во членот 30 (Сл.весник на РМ бр. 09/2004), врз кој Владата на Република Македонија во 2004 година, има донесено ,,Уредба за физичка безбедност на класифицирани информации" со која поблиску се пропишуваат мерките и активностите за физичка безбедност за заштита на класифицирани информации кои ќе се спроведат од стана на државните органи, организациите, институциите и другите правни и физички лица.
Проценката за можното нарушување на безбедноста на класифицираните информации се врши од аспект на:

- бројност, степен, форма и проток на класифицираните информации;
- непосредната околина на објектот во кој се наоѓаат класифицирани
- информации и поставеноста на безбедносниот појас околу објектот;
- безбедносните и административните зони во објектот; физичката градба;

[335]Закон за управување со кризи Сл. Весник на Р.Македонија бр.29/05 од 04.05.2005 година
[336]Исто, член 12.

- ѕидовите, вратите и прозорците на објектот;
- состојбата на поширокаta околина на објектот;
- лицата кои работат во објектот;
- заканата од разузнавачки активности, саботажа, терористички, или други криминални активности насочени кон класифицираните информации;
- постапките за работа со класифицираните информации и нивното чување во објектот[337].

Во членот 3 од истата уредба стои дека врз основа на проценката на органот се изготвуваат планови за физичка заштита за секој објект посебно.

Несомнено безбедноста на критичните инфраструктури во современи услови стана безбедносна функција која го прати современото живеење, оттука и Република Македонија низ еден сеопфатен сет на мерки и активности поддржани со законски регулативи потребно е што поитно да се приклучи кон европските текови на обезбедување на критични инфраструктури.

2. Обезбедување на некои критични инфраструктури во Република Македонија

2.1. Енергетски сектор во Република Македонија

Во Република Македонија оваа област е регулирана согласно Законот за Енергетика кој покрај другото има за цел:

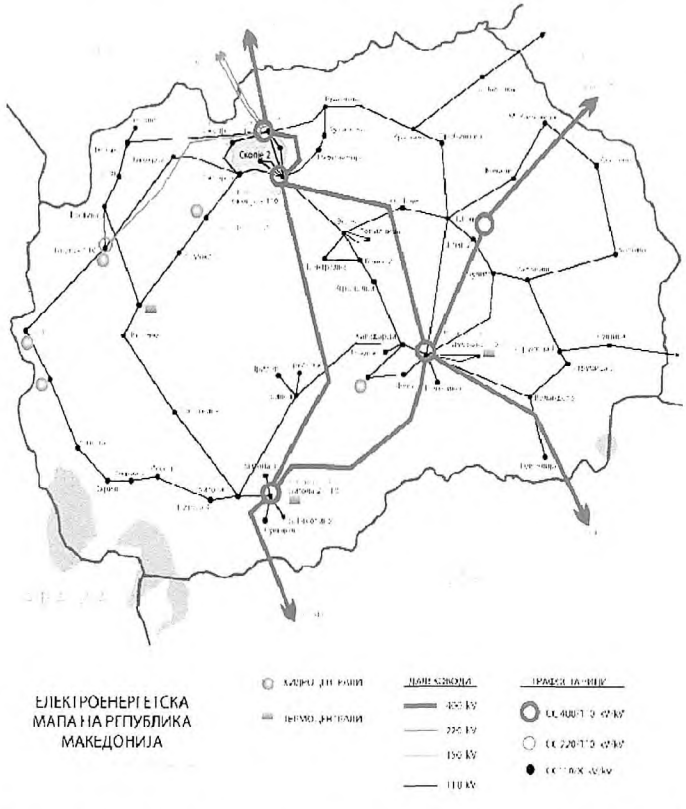
- Сигурно, безбедно и квалитетно снабдување на потрошувачите со енергија и енергенти;
- Создавање на ефикасен, конкурентен и финансиски одржлив енергетски сектор;
- Потикнување на конкуренцијата на енергетските пазари со почитување на начелата на недискриминација, објективност и транспарентност;
- Интегрирање на енергетските пазари на Република Македонија во регионалните и меѓународните енергетски пазари во согласност со обврските преземени со ратификување меѓународни договори;
- Зголемување на енергетската ефикасност и поттикнување на искористувањето на обновливите извори на енергија и
- Заштита на животната средина од негативните влијанија при вршењето на одделни дејности од областа на енергетиката[338].

[337] Уредба за физичка безбедност на класифицирани информации („Службен весник на РМ“, бр. 82/2004)

Во делот на обезбедувањето, енергетскиот сектор спаѓа во групата на значајна инфраструктура за безбедноста и одбраната. Од тука, сите правни лица кои се регистрирани за вршење на дејности од областа на енергетиката, согласно одредбите од Законот за енергетика, за производство, пренос и дистрибуција на енергијата, покрај другите безбедносни мерки утврдени со закони пропишани со подзаконски прописи, поради заштита на здравјето и животот на луѓето и заради заштита на животната средина, природата и растенијата имаат физичко и техничко обезбедување[339].

2.1.1. Преглед на енергетските капацитети во Република Македонија

Капацитетите на ELEM произведува околу 96% од вкупното домашно производство.Од термоелектраните со инсталиран капацитет од 825 MW произведува 5.000 GW/h електрична енергија годишно, додека од хидроелектраните со инсталиран капацитет од 538 MW, произведува 1.200 GW/h годишно електрична енергија. Само рударско-енергетските комбинати Битола и Осломеј даваат околу 80 отсто, додека хидроелектраните на АД ЕЛЕМ произведуваат околу 16 отсто од вкупната електрична енергија од домашните капацитети. Од сопствениот енергетски потенцијал на јаглен, Република Македонија поседува околу 7 милиони тони годишно. Оттука, несомнено АД ЕЛЕМ важи за стратегиски најважна компанија - стожер на македонскиот електроенергетски систем.[340]



Слика 15. ЕЛЕМ – електро енергетска мапа на Р.М[258]

[338] Закон за енергетика, Службен весник на Р.М, бр. 16 од 10.02.2011год

[339] Одлука за определување на правни лица кои се должни да имаат приватно обезбедување - Службен весник на РМ, бр.106 од 29.07.2013

[340] http://www.elem.com.mk

Од аспект на хидроенергија, Водата е еден од најисплатливите извори на енергија и претставува најзначаен обновлив енергетски извор во Македонија. Хидропроизводството претставува 15% од вкупното производство на електрична енергија во АД ЕЛЕМ. Хидроелектраните работат на принципот на конверзија на механичка во електрична енергија, при што основен двигател се водените текови, односно проточните води во земјата[341].Вкупниот волумен на акумулациите е 891000000 м3 со вкупно годишно производство од 1000 GWh. Вкупната инсталираност на хидрокапацитетите изнесува 504MW, односно 39% од вкупните капацитетите на АД ЕЛЕМ.Хидроенергијата е најзначајниот обновлив извор на енергија познат досега.Неговото искористување е поврзано со изградба на значајни градежни објекти, пред се брани и акумулации, односно долги доводни тунели или цевоводи, кои објектите ги прават од една страна скапи за изградба, но од друга страна допринесуваат за целокупниот развој на економијата во земјата. Наспроти големата цена на изградбата, годишната експлоатација на објектите и производството на електрична енергија од истите е многу ниско. Со оглед на ограниченоста на природните ресурси во Република Македонија, искористувањето на хидропотенцијалот е од витално значење за развојот на електроенергетскиот сектор и државата во целост. Хидро-производството учествува со 15% во вкупното производство на електрична енергија во АД ЕЛЕМ и тоа пред сè за задоволување на дневните варијации на потрошувачката на електрична енергија, со што се постигнува поголема флексибилност и расположивост на електроенергетскиот систем, како и соодветен процент на производство од обновливи извори на енергија.Термокапацитетите даваат константна енергија. Термопроизводството има растечка тенденција. На Пелагонискиот и Кичевскиот басен изградени се двете наши термоцентрали на лигнит, кои претставуваат стожер на електроенергетскиот систем на Македонија со учество во вкупно произведената електрична енергија од 80-85% Најголем производен капацитет е Рударско-енергетскиот комбинат "Битола" со своите три блока од по 225 MW и нето производство од околу 1.434 GWh по блок[342]. Комбинатот е целосно заокружена производна целина со повеќе единици. Оваа термоелектрана како основно гориво користи јаглен кој е со просечна калоричност од 7.900 kJ/kg. Другиот термокапацитет во составот на електроенергетскиот систем е Рударско - енергетскиот комбинат "Осломеј" кај Кичево, со инсталирана моќност на блокот од 125 MW и нето годишно

[341] http://www.elem.com.mk – хидроенергија Преземено на 16.01.2016
[342] http://www.elem.com.mk превземено на 18.12.2015 год.

производство од околу 700 GWh[343]. И овој термокапацитет како основно гориво користи јаглен со просечна калоричност од 7.660 kJ/kg. Овие термоелектрани имаат важна улога во покривањето на базниот дел од дијаграмот на конзумот на Р.Македонија[344].Покрај производството на електрична енергија, важна алка во процесот е Дистрибуција.Во Р.М. овој сегмент му е препуштен во моментов на (Македонски електропреносен систем оператор)МЕПСО е непречен пренос на електричната енергија низ високонапонската мрежа, управување со електроенергетскиот систем и редовен и навремен ток на електрична енергија до своите клиенти: директните потрошувачи (Бучим, ОКТА, Макстил, Арчелор Митал, Усје, Југохром-Фероалојс, Скопски Легури, Фени Индустри, Македонски Железници) и до дистрибутивната мрежа на ЕВН Македонија[345]. Оператор на преносна мрежа (ОПМ) се грижи за оперативноста ифункционалноста на повеќе од 2.000 километри преносна мрежа и за 148 енергетски трансформатори со инсталирана моќност од 6.417 (MVA) инсталирани во повеќе од 50 трансформаторски станици. Оператор на електропреносен систем во структурата на МЕПСО е систематизиран како подружница чија основна функција и обврска е оперативно управување со електропреносниот систем на Република Македонија. Оваа функција ОЕЕС ја врши преку Одделот за управување и со користење на уредите и опремата за оперативно управување. За логистиката, одржувањето и за развојот на управувањето со електро-енергетскиот систем се грижи Одделот за техничка Информатика. АД МЕПСО за остварување на надзор, заштита и управување со електроенергетскиот систем обезбедува ефикасна комуникација и размена на податоци помеѓу НДЦ (Национален диспечерски центар)и електроенергетските постројки[346].

Нафтената инфраструктура се состои од пет компоненти:

- Производство на сурова нафта
- Превоз на сурова нафта
- Рафинирање
- Транспорт и дистрибуција на продуктите
- Контрола и други пропратни системи

ОКТА АД Скопје има водечка улога во продажбата, снабдувањето и дистрибуцијата на нафтени деривати во земјата, но и пошироко на Балканот.

[343]Исто, превземено на 18.12.2015 год.
[344]http://www.elem.com.mk превземено на 18.12.2015 год.
[345]http://www.mepso.com.mkпревземено на 18.12.2015година.
[346]http://www.mepso.com.mkпревземено на 18.12.2015година.

ОКТА АД Скопје е главниот гарант за снабдување со гориво во земјата. Компанијата поседува капацитети за рафинирање односно за преработување на сурова нафта со номинален капацитет од 2,5 милиони тони. Инсталациите се поврзани преку 210км долг нафтовод со HELPE Рафинеријата во Thessaloniki. ОКТА снабдува повеќе од половина од потребите за гориво во земјата со производи со висок квалитет и е значителен извозник за пазарот во Косово. Нејзината мрежа за извоз, исто така, ги покрива и потребите на другите соседни[347].

На крај би потенцирале дека, одредена улога во енергетиката, а може да се каже во одредени држави дури и клучна улога, има индустријата за производствона природен гас.Таа се состои од три компоненти:

- Експлоатација и производство
- Пренос и
- Локална дистрибуција

3. IT Безбедност во Република Македонија

Агресивното воведување и масовното ефикасно користење на електронските комуникации и информатичките технологии, со што се придонесува за вклучување на Република Македонија во глобалната вмрежена економија и остварување на значаен скок во економијата, предвидени се со националната стратегија за развој на електронските комуникации со информатички технологии - информатичко општество.

Република Македонија има релативно скромно искуство во доменот на сајбер-безбедноста. Официјален датум за почеток на историјата на интернетот во Р. Македонија е 20 април 1995 г. Во овие 20-тина години од користење на сајбер-просторот можеме да истакнеме неколку карактеристични случаи кои се однесуваат на напади на веб-страници на државните институции, оддавање на класифицирани информации и заштита на личните податоци. Досега Р. Македонија немала искуство од сајбер-напади врз нејзината критична инфраструктура[348].

Посебен акцент е ставен на мерките кои се однесуваат на развојот на комуникациската инфраструктура, како единствена технолошка платформа на развој на информациското општество, како предуслов за воведување и масовно користење на сите услуги на информатичко општество и дигитални содржини што како крајна цел го има подобрувањето на квалитетот на животот во Македонија. Во делот на програмата е разработена и информациската безбедност, како и потребата од

[347] http://www.okta-elpe.com/Main.aspx?lan=1 Превземено на 27.12.2015.
[348] http://morm.gov.mkПредизвик на современите општества – С. Славески, 30.05.2015год.

воведување на примена на мерки за заштита од појавата на информациска ,,не – безбедност". Меѓутоа, мора да знаеме дека,сајбертероризмот се развива паралелно со информациско-комуникациската технологија и се наоѓа во фаза на брз развој и динамички промени и од таа причина е не возможно да се согледаат и предвидат сите можни правци на развојот, големината, динамиката и содржините на тие процеси и самата комплексност на компјутерските мрежи расте побрзо одколку способноста да се разбере и да се заштити, така што од квалитетот и сигурноста на расположивите информациски системи ќе зависи и одбраната и голем број на безбедносни структури на голем број на држави .

Со оглед на фактот дека стратегиската определба на Република Македонија и на нејзината концепција за национална безбедност и одбрана е својата иднина да ја остварува како дел од европското семејство и членка на НАТО и ЕУ, како и градење на взаемно кооперативни односи и взаемно координирани активности од областа на безбедноста, одржавањето на стабилноста, превенцијата и решавањето на кризи и др., насочени најмногу преку водечката улога на НАТО во креирањето на безбедносната политика, и е активен партипициент во Евроатланските безбедносни структури, како држава аспирант за членство во НАТО и ЕУ ни дава за право, се посериозно да се размислува во поглед на зголемување на мерките на заштита од сајбертероризмот, затоа што Евроатланските организации претставуваат главна мета на радикалните групи. Потенцијалот на терористичките организации и поединци во иднина постојано ќе се зголемува заедно со промените во информатичко – комуникационите технологии.

Во овој дел ќе го издвоиме операторот Македонски Телеком кој нуди говорни и податочни услуги на фиксна и мобилна мрежа и воведува меѓународна експертиза, иновативни решенија и најсовремени технолошки трендови. Компанијата нуди портфолио на услуги за приватни и деловни корисници, кои се обезбедуваат од едно место и се фокусира на Cloud и ИКТ решенија, со цел да обезбеди најдобро корисничко искуство. За таа цел, во согласност со најновите телекомуникациски трендови, Македонски Телеком постојано се фокусира на современите потреби и барања на корисниците[349].

Исто така, ќе ги споменеме и ОНЕ и ВИП, кој е исто така, приватен мобилен оператор во Република Македонија и член на Групацијата Телеком Австрија, оне.Вип е основан во 2015 г., по спојувањето на двата оператора, ОНЕ и ВИП оператор, кои работат на територијата на Македонија. оне.Вип опслужува околу 1.3 милиони

[349] http://www.telekom.mk/ Преземено 11.02.2016

корисници во Македонија. Во моментов, портфолиото на услуги е поделено на услуги од следните брендови: Вип и ОНЕ (вклучувајќи ги и Џабест и BoomTV)[350].

4. Обезбедување на водните системи во Република Македонија

Прашањата поврзани со водите во Р.М се регулирани со Законот за Води со кој се уредуваат прашањата кои што се однесуваат на површинските води, вклучувајќи ги и постојаните водотеци или водотеците во кои што повремено тече вода, езерата, акумулациите и изворите, подземните води крајбрежното земјиште и водните живеалишта и нивното управување, вклучувајќи ги и распределбата на водите, заштитата и зачувувањето на водите, како и заштитата од штетното дејство на водите; водостопанските објекти и услуги; организационата поставеност и финансирањето на управувањето со водите, како и условите, начинот и постапките под кои можат да се користат или испуштаат водите.[351]

Денес, пристап до безбедна вода имаат 97 проценти од населението. Тоа покажува дека Република Македонија е во групата земји во светот со многу висок пристап до безбедна вода за пиење[352].Од Извештајот за вода за пиење за 2014 година година е регистрирано дека 1.301.646 жители т.е 63,1% од популацијата во Републиката се снабдува со вода за пиење од централни водоснабдителни системи, управувани од јавни комунални претпријатија кои ги исполнуваат законските обврски во однос на обезбедување и контрола на здравствената исправност на водата за пиење (Извештај за вода за пиење за 2014 година. Институт за јавно здравје на РМ; 2015). Останатите се снабдуваат на следните начини: 422 жители (10,34%) се приклучени на градски водоводи, 471 жители (22,7%) во селските населби се снабдуваат од локални јавни водоснабдителни системи, со кои не стопанисува секогаш јавно претпријатие (во најголем број на овие објекти водата не се дезинфицира, а доколку и се врши вообичаено со хлорни препарати, тоа се врши нерамномерно и нередовно), 703 жители (3,86%) се снабдуваат со вода за пиење од локални водоснабдителни објекти (јавни чешми, бунари, извори, пумпи и други индивидуални водоснабдителни објекти)[353].

Пристапот до безбедна вода за пиење изнесува 97% и ја категоризира Република Македонија во групата земји во светот со многу висок пристап.

---

[350] http://onevip.mk/mk/za-nas/za-one-vip/ Преземено 11.02.2016
[351] Закон за водите, Службен весник на РМ, бр. 87 од 15.07.2008 година
[352] http://www.iph.mk/svetski-den-na-vodata-2015/ Превземено 11.11.2015година
[353] Истио, Превземено 11.11.2015година

Покрај другото во законот се дефинирани и целите кои се:

- достапност до доволно количество квалитетна вода, во согласност со начелата за одржливо управување со водите за пиење и за производство на храна, за потребите на земјоделството, индустријата, хидроенергетските потреби, за потребите на парковите и други јавни површини, туризмот, пловидбата и за други потреби,
- заштита, зачувување и постојано подобрување на расположливите водни ресурси, подобрување на состојбата на крајбрежното земјиште, водните екосистеми и на екосистемите зависни од водата, заштита и унапредувањето на водната средина преку рационално и одржливо користење на водите, како и прогресивно намалување на штетните испуштања и постепено елиминирање на емисиите на опасни материи и супстанции во водите,
- ублажување на последиците од штетното дејство на водите и од недостигот на вода и
- заштита и унапредување на животната средина и природата, на водните еко системи и на биолошката разновидност и заштита на здравјето на луѓето[354].

Од аспект на снабдувањето со вода за пиење, е зафаќање, обработка и дистрибуција на водата преку водоснабдителниот систем. Вода за пиење претставува секоја вода, во својата првобитна состојба или по третман, наменета за консумирање од страна на човекот, готвење, подготовка на храна или за други домашни намени, без оглед на тоа од каде потекнува и дали се снабдува од водоводната мрежа или од цистерна и водата што се користи за производство на храна за производство, обработка, конзервирање или за продажба на производи или на материи наменети за консумирање од страна на човекот. Додека пак, водоснабдителен систем е збир на хидротехнички објекти за снабдување со вода за пиење и тоа: водозафат (места каде давателот на услугата зафаќа површинска и/или подземна вода), резервоар, објект за обработка на вода, пумпна и хлоринаторска станица, главен довод, магистрален вод, улична водоводна мрежа и водоводен приклучок заедно со придружните објекти и опремата за довод на вода од водозафатот до приклучокот на главниот водомер на корисникот на услугата[355]

Обврските кои произлегуваат од Законот ги дефинираат и целите кои во најмала рака треба да обезбедат:

---

[354]Исто член 2

[355]Закон за снабдување со вода за пиење и одведување на урбани отпадни води С. Весник на Р.Македонија, Бр. 07-3750/1од 2004 г.

- достапност на доволни количества здравствено исправна и чиста вода за пиење за потребите на корисниците на услугата, согласно со барањата, стандардите и вредностите за квалитет на водата;
- снабдување со здравствено исправна вода за пиење, а во случај на нејзина контаминираност, забрана или ограничување на користењето;
- соодветно информирање на корисниците на услугата за квалитетот на водата за пиење и преземање мерки за обезбедување на квалитет на водата за пиење;

Поради неговата критичност, безбедната вода за пиење и соодветното третирање на отпадните води се критични од повеќе аспекти најнапред за јавното здравје, животната средина, економијата, но и од зависноста на останатите категории на критични инфраструктури. Од тој аспект потребно е да се посвети посебно внимание во поглед на превенција, детектирање на заканите во смисол на што побрзо откривање на опасностите како и брз одговор на заканите и опасностите кои ја пратат оваа област.

Поради неговата критичност безбедната вода за пиење и соодветното третирање на отпадните води се критични од повеќе аспекти, најнапред за јавното здравје, животната средина, економијата, но и од зависноста на останатите категории на критични инфраструктури. Од тој аспект потребно е да се посвети посебно внимание во поглед на превенција, детектирање на заканите во смисол на што побрзо откривање на опасностите како и брз одговор на заканите и опасностите кои ја пратат оваа област.

Во Република Македонија со Закон се уредуваат условите за обезбедување на безбедноста на храната и на производите и материјалите што доаѓаат во контакт со храната, производството и прометот, правата и обврските на физичките и правните лица кои произведуваат или вршат промет, со цел да се заштити здравјето на луѓето, да се заштитат потрошувачите од заблуда и да се овозможи слободен промет на внатрешниот и надворешен пазар[356].

Согласно Одлуката за задолжително обезбедување, обезбедувањето заштитата и унапредувањето на животната средина, заштитата на природата и природното наследство во заштитените подрачја и надвор од заштитените подрачја согласно Законот за животна средина, Законот за заштита на природата и согласно други прописи од областа на заштитата и унапредување на животната средина, човековата

[356]Закон за безбедност на храната и на производите и матерјалите што доаѓаат во контакт со храната Сл. весник на Р Македонија, бр.54 од 15.07.2002 год.

околина, природата и и националните паркови потребно е да имаат физичко и техничко обезбедување на просторите и објектите со кои стопанисуваат.[357]

5. Воздушниот сообраќај како критична инфраструктура во Република Македонија

Република Македонија е членка на Организацијата на обединетите нации од 1993година, а во доменот на меѓународното цивилно воздухопловство, истата е членка на ICAO (International civil aviation organization) од 09.10.1993година и на ECAC (European civil aviation coference) од 03.07.1997година[358]. Како држава која е рамноправна членка на горе споменатите меѓународни организации, а истовремено и како земја која ја има прифатено Конвенцијата за меѓународното цивилно воздухопловсво од 1944 година (Чикашка конвенција), Република Македонија е обврзана да ги почитува и имплементира меѓународните стандарди кои се однесуваат на безбедноста на цивилната воздушна пловидба, следејќи ги практиките и обврските кои произлегуваат од домашната и меѓународната регулатива во функција на сузбивањето на незаконските дејствија насочени против безбедноста на цивилното воздухопловсво преку регулативи, практики и постапки.

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)[359]

Министерството за транспорт и врски е надлежно за работите од областа на воздухопловсвото и тоа: ја подготвува Националната стратегија за развој на воздухопловството, ја реализира политиката на Владата во областа на воздухопловсвото, ја спроведува политиката на владата при доделување на концесии од областа на воздухопловството, предлага закони, врши надзор врз работата на АЦВ, спроведува постапка за привремено ставање на концесија под привремена принудна управа (секвестар), именување на независен слот координатор за алокација за слотови за полетување и слетување, формира комисија за испитување на несреќи и сериозни инциденти и др[360].

---

[357] Одлука за определување на правни лица кои се должни да имаат приватно обезбедување - Службен весник на РМ, бр.106 од 29.07.2013

[358] Т. Тунтев, Аеродромски Прирачник за Прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год. Охрид, стр.13

[359] Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013 член 5

[360] Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013 член 6

Агенцијата за цивилно воздухопловство - АЦВ е организирана како воздухопловна власт на Република Македонија чија организациона структура обезбедува квалитетно и навремено извршување на безбедносните регулаторни функции опишани во ICAO Annex 19 и Doc.9734 (Safety Oversight System) како и останатите функции поврзани со надзор на обезбедувањето (Security), економски надзор, права на летање итн.[361] Исто така, врши инспекциски надзор над примената на одредбите од Законот за за воздухопловсво и прописите донесени врз основа на законот. Подготвува предлог на закони и донесува подзаконски акти од областа на воздухопловсвото согласно со ЕУ, ICAO, ECAC, EUROCONTROL, JAA/EASA. Одобрува зборник на воздухопловни информации, водење на управна постапка за издавање, продолжување, промена суспендирање и повлекување на дозволи, овластувања, уверенија, одобренија и др. утврдено со Законот за воздухопловство, Регистрација на воздухоплови, аеродроми, летилишта и евиденција на терени, предлага мерки за развој и примена нанови технологии во воздухопловсвото, организирање и координирање на активности поврзани со потрага и спасување на воздухоплови, како и други работи во согласност со Законот за воздухопловство[362].

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,
- Авиопревозниците.[363]

Ефикасна сигурност на цивилната авијација може да се постигне низ развојот, примена и одржување на сеопфатни флексибилни и ефикасни законски прописи, програми, мерки и процедури на национално ниво. Насоките за развојот на националните програми за безбедност на цивилното воздухопловсво треба да бидат во склад со меѓународната регулатива.

За да се постигне стандардизирано рамниште за безбедност на воздушната пловидба, секоја држава мора низ телото кое е задолжено за безбедност (обично низ агенцијата за цивилно воздухопловство), да усвои сеопфатна политика, поддржана со законски прописи, кои ќе ги спроведуваат сите субјекти вклучени во која било безбедносна структура во цивилното воздухопловство. Секој од споменатите субјекти, аеродроми, полициски служби, авио оператори, разузнавачките служби и др. мораат

[361] http://www.caa.gov.mk/3/Za_nas.html
[362] Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013 член 7
[363] Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013

да имаат јасно дефинирана политика, процедури, стандарди за делување и методи за примена во согласно со насоките на државата. За да се постигнат ефикасни и конзистентни цели, државата потписничка мора да воспостави стандарди и да ги надгледува спроведените постапки и процедури кои се применуваат за да се осигура спроведувањето на политиката за наведените стандарди. Државата, исто така, треба да формира национален комитет за безбедност, како и комитети за аеродромска безбедност, т.е и други ефикасни тела со кои координирано ќе се спроведува политиката и стандардите. Политиката и стандардите за спроведување на мерките за безбедност мораат да ги исполнуваат препорачаните постапки формулирани пред се во Анексот 17 на ICAO[364].

Согласно Анексот 17,,Секоја договорна земја ќе воспостави и имплементира пишана национална програма за воздухопловна безбедност заради заштита на цивилното воздухопловство од незаконски дејствија преку регулативи практики и постапки, во кои ќе се води сметка за безбедноста, уредноста и ефективноста на летовите"[365] Националниот програм за цивилната авијација, која го формулира државата потписничка, мора да биде во согласно со меѓународните стандарди и препорачаните практики и да се усвојат законските прописи и обврзувачката регулатива која и дава на државата овластување за превземање на одговорност за формулирање и спроведување на политиката, како и плановите поврзани со безбедноста во авијацијата. Воспоставување на блиска соработка помеѓу голем број на различни организации вклучени во успешноста на спроведувањето на програмата за безбедност на цивилното воздухопловство. Организации кои треба да бидат вклучени во овие напори треба да бидат: Агенцијата за цивилното воздухопловство, Полиција, Царина, Силите за безбедност, Управата на аеродромот, авио операторите и др компании кои се присутни на аеродромот[366].

6. Резултати од спроведеното тереснско истражување врз објектите од витален интерес за Р. М

За потребите на оваа дисертација спроведено е истражување, кое имаше за цел да ги провери и анализира безбедносните капацитети на компаниите. Беше спроведено низ два елемента: прво, се направи согледување на критичната инфраструктура од аспект на нејзиното значење врз националната безбедност и второ, анализата е направена за да се согледа како е регулирана безбедноста и какви

[364]Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013 Година.
[365]ICAO Annex 17 to the convention on International Civil Aviation Ninth Edition March 2011.
[366]Закон за воздухопловство Сл. весник на Р.Македонија бр.63 од 13.05.2013 Година.

чекори се прават или треба да се направат за да се обезбеди нејзина соодветна заштита.

По однос на сложеноста на истражувачкиот проблем, акцент беше ставен на деталната проценка на факторите кои што доведуваат до неефикасност на самото планирање на безбедноста, мерките за обезбедување, условите, имплементацијата на напредните системи и процедури како и клучните фактори кои предходеле на неефикасноста на системот за обезбедување.

Менаџирањето со обезбедувањето посебно во делот на приватното обезбедување, беше насочено кон анализи на теоретските и практичните решенија во областа како и согледување, изнаоѓање и дефинирање на можностите и условите за применливоста на напредните процедури и системи во развојот на обезбедувањето.

За градење на ефикасен безбедносен систем и создавање на услови за примена односно, целосна имплементација на меѓународните стандарди и процедури во обезбедувањето, потребни се трансформации на безбедносните капацитети во делот на обезбедување на критичните инфраструктури. Во тој контекст, истражувањата за состојбите во обезбедувањето на критичните инфраструктури, беа насочени кон согледување на сите аспекти (организациони, регулаторни, структурни, суштински, технички и др.) секако со тенденција на понудување на одредени решенија со кои би се подобрило обезбедувањето и примена на одредени практични решенија кои добро функционираат во некои критични инфраструктури.

При реализација на истражувањето кое беше направено за потребите на оваа дисертација, главната цел беше насочена кон откривање и согледување на релевантните фактори кои ги третираат прашањата поврзани со обезбедувањето на критичните инфраструктури во Република Македонија, односно, 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 обезбедување, да се утврди дали развојот на обезбедувањето е во вистинска насока, да се види вклучувањето на обезбедувањето во целокупниот безбедносен систем на Р.М. да се истестира ефикасноста на применетите мерки и активности на обезбедувањата, да се согледаат факторите кои придонесуваат за зголемување на ефикасноста на обезбедувањето, да се согледа модернизацијата и осовременувањето на техничко технолошките иновации во функција на обезбедувањето и сл.

Генералната цел на истражувањето беше да се соберат објективни, прецизни, потполни, проверливи и искуствени податоци, кои понатаму ќе бидат применети во истражувачкиот процес во целост.

Интервјуирањето имаше примена во насока на добивање на податоци од конкретните носители на функции, особено од оние кои директно раководат со обезбедувањето во критичните инфраструктури. Беа реализирани повеќе од 30 интервјуа, во временски период од 01.05.2014 до 01.05.2015 во голем број на компании кои се од витален интерес за Република Македонија, а врз основа на однапред изготвена чек листа, односно прашалник, додека како техника за прибирање на податоци беше користено интервјуирање, на повеќе теми и области.

Најголем дел од прашањата беа идентични за сите компании, и беа обработувани само теми кои имаа општа индикативна вредност. Анализата на одговорите поради карактерот на доверливост беа анализирани внимателно, со цел да се запази дискретност и препознавање на слабостите кои ги пратат критичните инфраструктури во Република Македонија.

За успешно и објективно спроведување на интервјуто претходеше подготвителна фаза во поглед на добивање на дозволи за посета на компаниите, како и план за работа по целни групи. За селекцијата на прашањата кои беа користени во прашалникот, беше користена чек листа за извршување на инспекциски надзор кој се спроведува во делот на воздухопловството, која беше изменета и модифицирана за потребите на оваа дисертација и структурата на обезбедување на критичните инфраструктури за да се овозможи со предвидените прашања да се добијат конкретни одговори, а да се запази анонимноста во целост.

Покрај спроведувањето на интервјуто, за потребите на оваа дисертација беше направена и теренска опсервација на функционалноста на обезбедувањето со анализа на одредени пунктови, односно, проверка на практичното работење на службите за обезбедување.

По добивањето на податоците од спроведеното интервју, како и врз основа на теренската опсервација на компаниите, се пристапи кон обработка на податоците селектирани по основ на нивната јасност концизност и прецизност.

Истражувањето, исто така, беше насочено кон утврдување на ставовите и мислењата на испитаниците во врска со: потребата од воведување на современи безбедносни системи и процедури, координација на сите инволвирани субјети во критичната инфраструктура, поставеност на службата за обезбедување во рамките на компаниите, функционалноста на постоечките системи и процедури, потреба од

специјализирани обуки на персоналот за обезбедување, како и начин на зголемување на свесноста за безбедност за сите вработени во критичната инфраструктура, влијанието на политичките текови врз обезбедувањето на критичните инфраструктури итн.

Врз основа на исказите од страна на релевантните авторитети, компарирајќи ги сличностите како и разликите на нивните видувања во поглед на обезбедувањето, добиена е слика за потреба од унапредување на обезбедувањето во секој сегмент на функционирање на оваа специфична гранка.

6.1. Презентација на спроведеното истражување врз објектите од витален интерес – критична инфраструктура

Од истражувањето кое беше реализирано и изнесените констатации на испитаниците во однос на имплементацијата на напредните системи и процедури во развој на објектите од витален интерес за Република Македонија, како и придонесот во поглед на поголема ефикасност на обезбедувањето, констатирано е следното:

6.1.1. Регулирање на обезбедувањето на критичната инфраструктура

Во делот на правната поставеност, воглавно сите компании обезбедувањето го темелат согласно правилници за работа на службата за обезбедување донесени од страна на управувачкиот одбор на компаниите, врз основа на кој се изработени планови за обезбедување како и процедури за работа. Во сите акти запазен е Законот за приватно обезбедување со кој се уредуваат условите за вршење на приватно обезбедување; приватното обезбедување за сопствени потреби; задолжителното приватно обезбедување; овластувањата на работниците за приватно обезбедување; работната облека и ознаката на работниците за приватно обезбедување; формирањето, овластувањата и финансирањето на Комората на Република Македонија за приватно обезбедување; евиденциите, заштитата на податоците и информациите;надзорот; овластувањето за подзаконски прописи и прекршочните одредби, а се со целправните лица кои имаат дозвола за приватно обезбедување преземаат мерки и активности утврдени со овој закон заради спречување и откривање на штетни појави и противправни дејствија кои ги загрозуваат телесниот интегритет и достоинството на личноста и имотот што се обезбедува. [367]

Покрај целосната примена на Законот, голем број на компании имаат изработено и интерни планови, правилници, процедури за обезбедување во кои генерално е опишана заштитата на објектите, критичните места за обезбедување, обрските и

[367] Службен весник на Р.М бр.166 од 26.12.2012 год член 1

правата на персоналот за обезбедување, техничките средства и опреми и др. заради давање на насоки за имплементација на мерките за обезбедување, како што е барано согласно домашните прописи, со исклучок на аеродромското обезбедување, каде што во целост се применуваат и меѓународните стандарди и препорачани практики, земајќи ја во 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 кои се инволвирани во одвивањето на обезбедувањето на цивилното воздухопловство од дејствија 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 се 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, отклонување 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, која е дефинирана согласно меѓународните и домашните прописи.

Во овој контекст важна компонента во обезбедувањето на критичните инфраструктури преставува потребата од попрецизно регулирање на критичните инфраструктури по теркот 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, кој подразбира најнапред донесување на документи кои се неопходни за дефинирање на обезбедување на 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 потребно е 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 кои ги носи обезбедувањето на критичните инфраструктури, способност за детекција на заканите, ризиците и опасностите кои ги прати секоја критична инфраструктура, и изработка на адекватни планови и процедури во функција на севкупните безбедносни проценки.

Улогата на националните институции во насока на подобрување на обезбедувањето потребно е да се издигне на едно повисоко ниво по теркот на 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 на правни документи за регулација на дејноста и преставува на некој начин национален координатор во делот на обезбедување на воздухопловството, воедно, претставува и тело кое е одговорно за имплементирање на домашните и меѓународните стандарди и давање на насоки за постапување по истите.

Во Република Македонија до сега се направени голем број на чекори во насока на подобрување на обезбедувањето, а како покарактеристичен чекор е направен со Одликата за правните лица кои се должни да имаат приватно обезбедување, но потребно е нејзино надополнување со сите критични сектори кои би биле дефинирани согласно Закон или друг правен документ кој ќе ги дефинира критичните инфраструктури во Република Македонија.

Значи, најнапред потребно е изготвување на Закон па сите останати подзаконски прописи кои ќе го дефинираат обезбедувањето на критичните инфраструктури, како посебен сегмент во рамките на приватната безбедност во Република Македонија. Фактот дека Република Македонија треба да ги почитува насоките и директивите на Европската Унија на оваа проблематика треба да и се даде посебен осврт со целосно имплементирање на Директивата 114 од 2008 на ЕУ.

Податоците од резултатите на испитаниците покажаа дека со цел да се разгледа состојбата во Р.М и какво е размислувањето во оваа насока потребно е да се организира тело или работна група составена од сите релевантни чинители на обезбедувањето на критичните инфраструктури, вклучувајќи ја и Комората за приватно обезбедување на Република Македонија за да се придонесе во регулирање

на областа, која и тоа како, влијае на целокупната безбедност на Република Македонија.

Интресно е да се спомене дека сите интервјуирани експерти во нивните области на обезбедување се сложни за потребата од посебно дефинирање и регулирање на објектите од витален интерес – критична инфраструктура, и на прашањето: зошто е потребно дефинирање, односно, регулирање на објектите како критичниа инфраструктура беа дадени следните одговори:

- 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,
- да се зголеми значението на обезбедувањето како служба,
- полесно да се стигнува до пософистицирани средства и опрема,
- зголемување на моралот кај обезбедувањето,
- специјализирани обуки и др.

Генерално земено, сите испитаници се сложуваат со фактот дека е потребна правна регулација на критичните инфраструктури со сите свои елементи и специфики како посебен сегмент во рамките на безбедносниот систем на Република Македонија. Генералниот заклучок од овој сет на прашања и добиените податоци 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.

6.1.2. Координација и дефинирање на тела за обезбедување

Во однос на прашањето дали компанијата – оператор, има дефинирано тело за обезбедување и кои се членови во истото, беше констатирано дека од аспект на поставеност на службите за обезбедување, сите служби за обезбедување се поставени во рамките на одредени сектори кои имаат и дополнителни ангажмани од областа на заштитата и спасувањето. Координирањето меѓу различните институции, агенции и други субјекти засегнати со спроведувањето на различни аспекти на обезбедувањето кои ја третираат одредената област, беше евидентна на аеродромите, додека во останатите институции генерално се сведува на внатрешна координација и соработка со МВР.

Координацијата има големо значење за успешно функционирање на обезбедувањето во сите институции. Од причина што обезбедувањето поради своите специфики посебно во критичните инфраструктури потребно е да има целосно оделување од останатите сектори за да се избегне било каква импровизација. Менаџерот за обезбедување потребно е да одговара директно под менаџерот на компанијата и носењето на клучните одлуки во целост ќе биде на ниво кое обезбедува решавање на секакви сложени безбедносни ситуации. Кординацијата, како во внатрешноста на инфраструктурите, така и со надворешните субјекти претставува значајна вариабла 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.

Во областа на аеродромите, обезбедувањето преставува 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 координација на активностите на сите субјекти во обезбедувањето кои се инволвирани во одвивањето на воздушниот сообраќај утврдо е тело – Национален комитет за обезбедување на цивилното воздухопловство со свој постојан состав дефиниран со Законот за воздухопловство. Во основа, 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.

Од исказите на поголемиот број на испитаници, следи заклучокот дека соработката и координацијата на безбедносниот сектор во Република Македонија треба да се издигне на повисоко ниво со посебно вклучување на претставници од критичните инфраструктури во сите тела кои ја третираат безбедноста на државата. Потребни се што повеќе експертски дебати, вежби, научни конференции, со цел да се зголеми комуникацијата помеѓу клучните ресори, а сето тоа да биде поткрепено со правна рамка.

6.1.3. Закани и безбедносни ризици по критичните инфраструктури

Анализата на безбедносните закани, загрозувања и ризици, претставува проценка на секоја реална и потенцијална закана, која може да предизвика повреда или смрт на лица или уништување (губење на имотот на компанијата и или смалување на профитот, односно финансиски загуби без разлика на неговата големина). Се

однесува на постепена или системска анализа на работата и постапки кои 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 корпорацијата.[368]

Ако се земе во предвид значењето на критичната инфраструктура во поглед на останатите ефекти кои би се предизвикале врз националната економија, националната безбедност, здравство и сл., соочувањето со ризиците и опасностите потребен е повнимателен приод поради последиците за општеството и државата.

Во поглед на природата на заканите ризиците и опасностите кои ги пратат критичните инфраструктури во Република Македонија, може да се каже дека нужно е да се изградат и да се развиваат модерни служби за обезбедување кои ќе одговораат адекватно на современите закани кои ја пратат денешницата. На прашањето поврзано со евентуални закани, безбедносен ризик, како и настани кои влијаеле на безбедноста и нормално функционирање на компанијата,добиени се одговори дека присутни но и се соочиле со сите видови на загрозувања, од незаконско отуѓување на имот, саботажи во работењето поради материјална корист на поединци, анонимни закани за подметнувања на експлозивни направи, нарушувања на јавен ред и мир од поголеми размери, шверцување на стоки и предмети кои можат да ја загрозат безбедноста и др.

Евидентно беше дека проценките на ризици и опасности кои ги прават компаниите, во основа се однесуваат на обврските кои произлегувааат од Законот за управување со кризи во кој се третита и областа на тероризмот и другите акти на незаконско постапување. Во воздухопловството, проценката на опсност и соодветно преземење на мерките ја прави Агенцијата за цивилно воздухопловство, Министерството за внатрешни работи и другите надлежни субјекти. Понатака во доменот на проценката на нивото на закана се организираат зачестни контроли и воведување на дополнителни мерки на заштита.

Безбедносните ситуации кои владеат во земјата и регионот, но и пошироко може да имаат силен инпакт во функционирањето на критичните инфраструктури, поради лошите безбедносни проценки од страна на релевантните субјекти. Исто така, доколку лошата проценка се надополни со лоша координација на сите инволвирани субјекти ангажирани во извршувањето на безбедносни задачи, или пак недостаток од

[368] Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – Скопје 2012 стр67 - , Даничиќ М, Сајиќ Љ, оп. цит.стр.47

навремени и точни информации за постоење на опасност надополнета со неспремноста на безбедносните капацитети да се справат со современите ризици кои ја пратат денешницата, потенцијалната опасност која ја демнее државата ќе биде и тоа како опасна по целокупната безбедност, не само на критичната инфраструктура туку и на целата држава па и пошироко.

6.1.4. Посебни безбедносни процедури кои се применуваат во критичните инфраструктури

Во основа, сите опсервирани компании имаат поставено систем на обезбедување воден од домашните прописи, со исклучок на аеродромската безбедност која во целост ги има имплементирано меѓународните стандарди регулирани согласно ICAO, ECAC и EU.

Генерално земено во согласност со доктрината и практиката на европските земји со високоразвиена пазарна економија и стабилна демократија функциите на корпорациската безбедност опфаќаат:

- административна безбедност (administrative Security) – процедури и политика во областна на информатичката заштита,
- физичка и техничка безбедност (outsource/Proprietary) – машини, постројки и објекти,
- безбедност на имотот и 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 работисо 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)[369].

Од горе споменатото може да се каже дека, компаниите кои беа предмет на опсервација делумно ги имаат воведено функциите на корпорациската безбедност.

[369] 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., pp.161-162/ Корпорациски безбедносен систем О. Бакрески Д. Триван, С. Митевски – Скопје 2012 стр117

Сетот на прашања кои беа поставени во поглед на физичката заштита се однесуваа на условите за планирање на безбедноста од самото почнување со градба на критична инфраструктура или измени на постојните објекти, како и во поглед на дефинирање на границите на критичните инфраструктури, односно, зонирањето 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 подржан со електронски системи и уреди. Висините на оградите се дефинирани со актите на компаниите, а постои и дополнително оградување на местата кои се дефинирани како критични.

Од аспект на определување на зоните на движење констатирано е дека 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 истите според важноста, функционалната улога и техничко технолошката поставеност на одредени објекти, површини, инсталации, уреди, средства и опрема во аеродромскиот комплекс. Согласно зонската поставеност: јавна, ограничена, безбедносно ограничена и 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 обезбеди адекватна проверка на лицата и предметите кои 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 возачите.

Во делот на идентификационите картички,освен на аеродромите, во сите останати 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 на барање за издавање,

носење и враќање на идентификационите картички, евиденцијата како и надзорот над носење и поседување на идентификационите картички. Контролата на документите и идентификационите картички потребно е да се спроведуваат на сите контролни пунктови при влез во ограничените зони на компанијата и истото би можело да се реализира со помош на електронски системи кој го ограничува пристапот или пак од овластено лице кое врши контрола на пристап. Во основа сите компании издаваат пропусници и водат евиденции за движење на возилата, но не се прави детална проверка по основ на процедура или упатство за оваа намена од аспект на против диверзиона контрола. На аеродромите ова е прецизно регулирана постапка со посебни процедури за работа и специјална опрема за контрола на возилата. Сите возила кои имаат пристап во безбедносните зони на аеродромот подлежат на проверки и спроведување на постапки, мерки и дејствија кои ги преземаат работниците за обезбедување согласно нивните надлежности.

Пристапот до ограничените зони во сите компании е регулиран и се применува техничка опрема врз основа на моменталните потреби на компаниите. На аеродромите постои јасно дефинирана опрема (специјална опрема) која се користи и треба да биде поставена во определени простори и кои карактеристики е потребно да ги задоволува истата. 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, сите компании се темелат на мониторинг системите кои не се доволни за откривање на прикриени предмети.

При опсервација на движењето на персоналот и другите лица кои своите должности ги извршуваат во безбедносно ограничените зони во компаниите кои беа предмет на опсервација, минуваа низ премини кои 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 се со цел остварување на стандардизиран, квалитетен и одржлив систем на мерки и техники на обезбедување кои 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 на експлозиви, системи за откривање на траги од експлозиви (ETD), скенери за обезбедување кај кои не се употребува

јонизирачка радијација и систем за откривање на 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.

Во текот на интервјуата водени со експертите од областа на обезбедувањето, како и врз основа на извршените тестови во реални ситуации, констатирани се слабости во примената на некои од применуваните техники и опреми во реализацијата на откривање на експлозиви и опасни материи.Од тестовите кои се направени за потребите на трудот, врз опремата и начинот на спроведување на процедурите за работа со доследно почитување безбедносните услови, и правила за оваа намена односно активност, констатирана е ранливост во поедини сегменти во обезбедувањето која останува како деловна тајна и не е предмет на публикување.

Низ имплементацијата на напредните системи и процедури кои се опишани во овој труд ќе се извлечат многу позитивни заклучоци кои во најмала рака ќе се намали ранливоста на виталните објекти од акти на незаконско постапување.

Исто така, при осервација на контролните места за проверка на возилата со исклучок на аеродромите, во останатите критични инфраструктури, овие контроли се сведуваат 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.

Физичката контрола која се реализира во компаниите, во основа се остварува со работење на службата за обезбедување, со определен број на извршители. Физичките контроли се реализираат воглавно во сите коппании со цел откривање на сомнително однесување на лицата, откривање на неовластени упади во компаниите и оневозможување на преземање на дејсвија 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 кои се имплементирани во некои компании.

6.1.5. Обука на персоналот

Обуката на персоналот за обезбедување, генерално е засновано врз основа на Законот за приватно обезбедување и обврските кои произлегуваат од истиот. Не постои посебна пр. спецјалистичка обука или надоградување на знаењата во областа на обезбедување за виталниот објект. Не постојат посебни програми за обуки како за

стекнување и за продолжување на дозволите за работа. На аеродромите покрај обврските кои произлегуваат од Законот за приватната безбедност постојат и дополнителни обуки на персоналот, согласно одобрени програми за обука, регулирани според меѓународната и домашната регулатива од областа на воздухопловството, каде што главен акцент се става на: селекција на персоналот, минималните квалификации за одредени овластувања како и обврските кои произлегуваат од домашната и 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 кои се предмет на посебна контрола, контролата на пристап до ограничените зони на критичните инфраструктури, издавање на идентификациони картички и пропусни документи т.е. персоналот кој е директно вклучен во примената на специјалните мерки за обезбедување, потребно е да мине низ специјализирана обука во однос на прашањата кои ги третираат: одговорностите и селекција на персоналот за обезбедување, имплементација и спроведување на 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. Одговорностите за спроведување на програмите за специјализирани обуки потребно е да бидат во надлежност на државните институции кои спроведуваат покрај останатото и координација и следење на заедничките основни стандарди утвреди со правен акт. По примерот на цивилното воздухопловство, како надлежен орган е Агенцијата за цивилно воздухопловство и оваа организација е одговорна за развој, одржување, координација и оценување на степенот на имплементација на програмата за обука и осигурува: имплементираност на програмата, селекција и обука на персоналот, примена на стандардите, и сл.

Важен момент во делот на човечките ресурси, секако потребно е да биде споменат моментот на селекција на персонал, кој треба да биде сразмерен на специфичните потреби и задачи. Во голем број на компании кои беа предмет на истражување при процесот на селекција, не се спроведува безбедносни проверки на лицата, ниту пак, проверките се повторувани во одреден временски период по 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 предходното однесување вклучувајќи било какво криминално поведение како критериум за негова подобност.

Во сите компании како основен критериум е кандидатите да поседуваат лиценца за обезбедување, согласно законот за приватна безбедност и можеме да кажеме дека овој услов во целост е исполнет.

Од аспект на потребниот број на персонал сите компании го поседуваат неопходниот број на персонал согласно систематизациите и персоналната поставеност. Не постои конкретена статистичка или изработена анализа на загрозување, врз основа на која би биле дефинирани и димензионирани безбедносните капацитети на службите за обезбедување

Важно е да се напомене дека, со исклучок на аеродромите во ниту една компанија не се спроведува обука на небезбедносниот non-security персоналот. Генерално, вработените во виталните објекти не ја познаваат свесноста и потребата од обезбедување, како и нивните обврски во делот на обезбедувањето, ниту се запознаени од страна на овластени инструктори со заканите и опасностите кои ја пратат компанијата од аспект на актите на незаконско постапување, вклучувајќи го и тероризмот. На аеродромите тоа е регулирано согласно правни акти со кој компанијата е обврзана да реализира основна обука - свесност за безбедност за сите вработени кои работат во безбедносните зони на аеродромот, додека пак, небезбедносниот персонал кој има директна поврзаност со безбедноста на летовите, подлежат на дополнителни обуки од областа на обезбедувањето.

6.1.6. Контрола на квалитет во делот на обезбедувањето

Во делот на контролата на квалитетот на обезбедувањето од спроведената опсервација на документацијата забележано е дека, во мал дел од компаниите се применува програма или план за контрола на квалитет, која има за цел константна контрола над мерките за обезбедување регулирани со правни акти, преку активности за контрола и надзор над сите инволвирани субјекти задолжени за обезбедување на виталните објекти. Аеродромите за разлика од останатите витални објекти се под постојани контроли, инспекции, тестирања, со посебна методологија за вршење на контрола над обезбедувањето регулирана со правни акти, а спроведени од страна на домашни, но и од меѓународни експерти и организации кои ги следат постојано мерките за обезбедување.

Од тие причини по примерот на воздухопловната безбедност, а со цел квалитетно спроведување на мерките за обезбедување, потребно е да се имплементира Национална програма за контрола на квалитетот од определената област, која во основа ќе има улога да: провери дали сите субјекти ефективно ги спроведуваат мерките за обезбедување, утврдување на нивото за обезбедување преку активности

за контрола и надзор, како и проверка насоодветноста на програмите за обезбедување. Покрај Националната програма за контрола на квалитет, потребна е и имплементација на компаниска програма за контрола на квалитет. Овие програми ќе обезбедат почитување на меѓународните и домашните стандарди, организација и обврски во доменот на контролата на квалитет, квалификации и задачи на инспекторите, активности за контрола и надзор, комуникација и поднесување на извештаи и информации и сл.

6.1.7. Планови за вонредни ситуации

Во основа сите компании имаат планови за дејствување во вонредни ситуации, кои генерално се базират врз основа на законот за управување со кризи и заштита и спасување. Но, како посебни планови кој ја третираат само областа од обезбедување и кои 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. Аеродромите поседуваат повеќе планови за постапување во вонредни ситуации како и план за постаување при акти од незаконско постапување, кои се одобрени од релевантните институции, усогласени, истренирани и практично симулирани.

Од тие причини по примерот на воздухопловната безбедност, критичните инфраструктури потребно е да изработат компаниски планови за вонреди ситуации предизвикани од акти на незаконско постапување, коиќе имаат оперативен карактер со цел управување со мерките, активностите и постапките, со цел справување со вонредните состојби, спречување на понатамошна ескалација и намалување на ефектите од незаконските дејствија 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.

6.1.8. Трошоци и финансирање на обезбедувањето

Во делот на покривање на трошоците за нормално функционирање на обезбедувањето на виталните објекти, освен аеродромите, сите останати финансирањето го обезбедуваат од буџетите на своите компании. Генерално, не постои начин на прибирање на средства кои би биле наменети експлицитно за осовременување, обука и други потреби на обезбедувањето.

Поради современите ризици и опасности кои ги пратат критичните инфраструктури,потребно е да се изградат и функционираат модерни служби за обезбедување, кои ќе одговорат на сите безбедносни предизвици кои го пратат нивното работење. Само по себе, се наметнува и прашањето за одобрување на средства кои ќе бидат насочени кон осовременување на техниката, како и континуирани обуки на безбедносниот персонал. Се добива впечаток дека во поголем дел од инфраструктурите, финансирањето на обезбедувањето е недоволна и неконтинуирана. Генерално се пратат основните – елементарни потреби кои се регулирани со некаков правен акт, без желба за дополнителни финансирања во обезбедувањето.

ГЛАВА IX

Можен модел за подобрување на безбедноста и намалување на последиците од актите на незаконско постапување врз објектите од витален интерес во Република Македонија

Креирањето на развојната безбедносна политика врз ,,критичната инфраструктура" треба да ги обликуваат идните развојни стратегии, инвестиции и едукации, а се со цел навремено, безбедно и ефикасно одвивање на технолошките процеси од една страна и заштитата на,,критичната инфраструктура,, како национален интерес од друга.

Во таа насока потребно е првичниот приод да биде фокусиран на:

- дефинирње на критичната инфраструктура, како нов термин во рамките на безбедносниот систем во Република Македонија.
- 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 после кризно закрепнување,
- поддржување и развивање на меѓународна соработка и др.

Ако се водиме по примерот на Германската стратегија за заштита на критичната инфраструктура, може заштитата да биде втемелена врз Национален стратегиски План[370] или како многу европски држави низ законска регулатива, која би се раководела по принципот на задничка инволвираност на државата, општеството, бизнисот и индустријата.

Во стратегијата или друг правен акт кој треба да биде донесен на највисоко државно ниво ќе бидат селектирани критичните инфраструктури според видот и проценатa на критичност од аспект на обезбедување на општествено важни стоки и услуги базирани на социоекономски и инфраструктурно технички аспект.

Што се однесува до заканите, ризиците врз критичната инфраструктура, потребна е сеопфатна анализа на три основни фактори а тоа се:

- Природните непогоди
- Техничко технолошки причини
- Актите на незаконско постапување вклучувајќи го и тероризмот

Во однос на инволвираните субјекти кои треба да бидат носители на ваквите активности потребно е вклучување на:

[370] National Strategy for Critical Infrastructure Protection Berlin, 17th June 2009 .

- Министерствата, агенциите и дирекциите кои функционираат во рамките на државата,
- Локалните власти,
- Инфраструктурните оператори,
- Организациите за пружање на помош и итни случаеви,
- Релевантните индустриски и општествени организации кои ги третираат засегнатите критични инфраструктури,
- Научната и истражувачката заедница,
- Сите безбедносни капацитети на државата вклучувајќи ја и приватната безбедност,
- Јавноста посебно делот на медиуми,
- Меѓународниот фактор и др.[371]

Од аспект на анализата на ризикот за идентификација на критичната инфраструктура, потребно е да биде базирана врз основа на :

- Човечки губитоци,
- Стопански губитоци,
- Влијанието врз јавноста.[372]

Проценката 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.

Водејќи се по Европските стратегии за заштита на критичната инфраструктура, како на Европско, така и на Национално ниво, одговорноста за заштитата на критичната инфраструктура паѓа на операторите на критичните инфраструктури на земјите членки. Според ова, во поглед на подобрување на заштитата, секоја земја членка е охрабрена да изработи Национална програма за заштита на критичната инфраструктура. Целите на ваквите програми е да се одреди пристапот на секоја земја членка при заштитата на критичните инфраструктури лоцирани на нивна територија.[373]

Важен сегмент во критичната инфраструктура во Република Македонија е имплементација на регулативи и насоки во подобрување на обезбедувањето на ,,критичната инфраструктура".

---

[371] National Strategy for Critical Infrastructure Protection Berlin, 17th June 2009 .

[372] Закон о критичним инфраструктурама http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama, Преземено на 14.12.2015год.

[373] (COMMISSION OF THE EUROPEAN COMMUNITIES Brussels, 12.12.2006 COM(2006) 786 final COMMUNICATION FROM THE COMMISSION on a European Programme for Critical Infrastructure Protection)

Обезбедувањето на критичните инфраструктури или безбедноста на објектите од посебен интерес потребно е да биде засновано на една прецизна основа, која во најмала рака би требало да се раководи по следната хиерархија:

- Законска регулатива, вклучувајќи ги и меѓународните прописи
- Национални програми за обезбедување на критичната инфраструктура
- Програми за обезбедување на критичната инфраструктура
- Стандардни оперативни процедури.

Слика бр.16 Хиерархија на безбедносно регулирање на критични инфраструктура

Национална законска регулатива како и меѓународните прописи поддржани од конвенциите, потребно е во најмала рака да воведат и дефинираат правни инструменти, како пример Закон за заштита на критичните инфраструктури во кој покрај другото ќе бидат предвидени и кривичните дела од акти врз критичните инфраструктури.

Законодавството треба да ги утврди параметрите на одговорност и отчетност својствени на еден безбедносен систем со цел:

- дефинирање на критичните инфраструктури
- зајакнување на надлежниот орган за развој, имплементација, одржување и преглед на Националните програми во согласност со одредбите и препораките

на меѓународните организации во кои членува државата и брзо да одговори на било каква закана за безбедноста.

- анализа на ризиците по критичните инфраструктури,
- имплементација на програма, вклучувајќи го и акциониот план, информациска мрежа, формирање на експертски групи и систем за споделување на информации, идентификација и анализи на меѓузависностите.
- дефинирање обврски на субјектите кои се чинители на обезбедувањето да извршат усогласување на националните програми кои ја регулираат областа на критичната инфраструктура.
- раелизирање инспекции, истражувања, ревизии и проверки од страна на надлежниот орган за да се утврди усогласување со релевантното законодавство и за следење на ефикасноста преку контролата на квалитет.
- одбивање на соработка со лицата и компаниите кои се сметаат за закана на инфраструктурата.
- обезбедување на едукација и тренинзи на сите органи вклучени во обезбедувањето на критичната инфраструктура.
- распределба на одговорностите помеѓу релевантните субјекти за обезбедување на критичните инфраструктури.
- обезбедување на овластувања за извршување на специфични работи поврзани со обезбедувањето,
- обезбедување на финансиски мерки, за менаџмент, превенција, припрема и последици од тероризам и други безбедносни опасности, а обезбедува основа за мерки за заштита на критичната инфраструктура.
- надворешна соработка на полето на обезбедување на ,,критичната инфраструктура"

Националната програма за обезбедување на критичната инфраструктура ќе преставува документ со креираната безбедносна политика врз основа на донесените прописи, дефинирани низ националната законска регулатива во дадената област на критичната инфраструктура на државата, така што, секој субјект вклучен во обезбедување на критичната инфраструктура ќе има јасно дефинирани безбедносни насоки, кои понатаму ќе бидат имплементирани во рамките на безбедноста на критичната инфраструктура. Тоа пред се преставува збир на меѓународни и домашни правила кои ја регулираат областа.

Во поглед на подобрување на заштитата на критичната инфраструктура, согласно препораките на Европската комисија, секоја земја е охрабрена да инсталира

Национална програма за заштита на критичната инфраструктура. Така што и Република Македонија треба да го одреди пристапот кон заштита на критичните инфраструктури лоцирани на територија на Р.Македонија.

Идентификација на критичностите ќе бидат реализирани според дефинирани национални и меѓународни критериуми. Овие критериуми треба да се развиваат врз основа на квалитативни и квантитативни ефекти во случај на онеспособување или уништување на конкретната инфраструктура во поглед на обласно - територијално загрозување и последиците како директен или индиректен ефект врз: граѓаните, економијата, политиката животната средина и др.

Програмата за обезбедување на критичната инфраструктура би опфаќала и:

- Идентификацијата на важните инфраструктурни делови во рамките на дефинираната област,
- Идентификација, одбирање и одредување на сите потребни мерки и постапки за смалување на ранливоста и обезбедување на делување на сите утврдени критични делови или објекти мрежи или состави со примена на сигурносни мерки и постапки како што се техничките, организациските, комуникациските и мерките за навремено предупредување и зголемување на свеста,
- Анализа на ризикот втемелена на сценарија на големи закани, ранливоста на објект, состав, мрежа и функционалноста, можните последици во редовна работа и во случај на престанок со работа вклучувајќи и ризик од напуштање на локацијата,
- Финансиска покриеност, која ќе стимулира, промовира и развива мерки на превенција, спремност и менаџирање со последиците,
- Преиспитување на безбедносните планови (временска рамка),
- Спречување или редуцирање на сите безбедносни ризици, поточно ризиците поврзани со тероризмот, каде соодветно се базира на одредување на заканите и ризиците.

Конзистентноста и координацијата на сите субјекти вклучени во обезбедувањето на критичната инфраструктура, 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.

За да се обезбеди одржливост на националната програма неопходна е имплементацијата на национална програма за контрола на квалитет.

Програми за обезбедување на критичната инфраструктура подразбира дека секоја компанија носител на ,,звање" критична инфраструктура потребно е да ја развие безбедноста низ документ кој ќе биде определен со прецизни и специфицирани насоки кои понатаму треба да бидат опишани и содржани во стандардни оперативни процедури.

Овие Програми потребно е:

- Да ги исполнуваат или надминуваат барањата од законските регулативи, а посебно барањата пропишани во Националната програма за дадената област на критичната инфраструктура,
- Да се делегираат задолженија и одговорности на лицата и субјектите задолжени за спроведување на безбедносните мерки,
- Потребни критериуми на персоналот за обезбедување, вклучувајќи и обуки.
- Да се обезбедат стандардизирани мерки на безбедност,
- Адекватни инфраструктурни и архитектонски решенија со цел реализирање на безбедносните мерки
- Подготовка и имплементација на компанискиот безбедносен документ и др.

Од оперативен аспект ваквата програма потребно е да ги имплементира најнапред, Националните прописи кои произлегуваат од законските акти, меѓународните обврски кои произлегуваат од телата во кои членува државата, како и обврските кои произлегуваат од Националната програма дефинирана во областа на критичната инфраструктура.

Физичките карактеристики и капацитетите се неминовен дел на програмата, пред се во поглед на распоредот на објектите, ограничените зони на движење со детерминација на критичност на деловите во технолошкиот процес.

Во Програмата потребно е да се содржат и мерките за контрола на пристап во зоните на компанијата, стандардите кои треба да се запазат при контролите, проверка на минатото на сите работници кои работат во компанијата, пропусни и идентификациони документи, прегледите на возилата и сл.

Програмата ќе стави посебен акцент на надзорот на компанијата од аспект на инфраструктурното оградување, патролниот концепт, осветлувањето, мониторинг системите, заштитата на околината.

Надзорот над движењето, особено во деловите кои компанијата ќе ги дефинира како критични,ќе биде реализирана и врз вработените на компанијата и врз посетителите, односно, корисниците на услугите кои се наоѓаат во дефинираниот круг

на критичната инфраструктура, надзор над коминтентите и робата со која се снабдува критичната инфраструктура.

Дополнителните мерки за безбедност ќе бидат предвидени и пропишани согласно зголемениот ризик, врз основа на проценките, а квалитетот на програмата во секој случај ќе зависи од контролата на квалитетот низ адекватни прегледи, испитувања и тестови.

Обуката, покрај стандардната дефинирана со закон,ќе биде потребно да се надградува во поглед на секоја критична инфраструктура, а согласно препораките на националните прописи и меѓународните регулативи.

Како еден од позначајните делови при изработката на овие програми, потребно е да се стави нагласок на планирањето при вонредни ситуации дефинирани согласно природата на работата на критичната инфраструктура, тука пред се, се мисли на заканите од акти на незаконско постапување (пр. киднапирања, подметнувања на експлозиви, вооружени напади и сл.)

Во делот на Стандардните оперативни процедури потребно е да бидат изработени на начин кој ќе обезбеди ефикасно реализирање на мерките со прецизно дефиниран персонал, опрема и средства. Тука, потребно е да се нагласи и степенот на заштита кој се имплементира во нормални услови на функционирање на критичната инфраструктура, како и во услови на зголемено ниво на закана или вонредна ситуација.

Оперативното планирање е клучен елемент во процесот за заштита со цел за да се минимизираат потенцијалните ефекти при онеспособување или уништување на критичната инфраструктура. Развојот на кохерентниот пристап при елаборација на оперативните планови, се однесуваат на учество на субјектите, соработката со сите чинители на безбедносниот систем во функција за непречено одвивање на процесите на работа.

Анализата упатува и на потреба од воведување на напредни уреди, опреми и системи во развој на обезбедувањето на критичните инфраструктури. Од извршените истражувања, реализирани низ објектите од витален интерес во Република Македоника, како и анализите кои се направени во поглед на опремата и средствата кои се користат во функција на обезбедувањето, потребно е да се даде еден нов приод кон примената на напредните технологии. Исто така, врз основа на тестовите кои се направени врз работењето на службите во поглед на способноста и чуствителноста на опремата за откривање на забранетите предмети, како и по однос на контролата на движења и упади во контролираните зони, детектирана е ранливоста

од одредени дејства, а од тука и евидентна е потребата од имлементација на посовремени системи во зависност од загрозувањата и ризиците кои ја пратат определената критична инфраструктура.Големиот број на опрема, уреди и системи кои служат во рамките на обезбедувањето на критичните инфраструктури, потребно е да се компатибилни со потребите и да одговарат на спецификациите во поглед на способноста и чуствителноста на опремата за откривање на забранетите предмети, недозволени упади и сл.

Безбедносната опрема, вклучувајќи ги и системите за обезбедување, се во постојан развој во зависност од задоволување на барањата кои произлегуваат од праксата. Имплементацијата на современите системи зависи од повеќе фактори, но заначајно е тоа што безбедносната оправданост за инвестирање во опрема и средства, посебно во критичните инфраструктури несмее да биде предмет на економски заштеди.

Од аспект на аеродромското обезбедување, а во врска со примената на напредната технологија за откривање на забранети предмети во багажите, патниците како и робата, треба да се спомене дека,голем број на аеродроми користат конвенционални рентген уреди, како и стандардни метал детектори или уреди кои се со софтверски иновации во поглед на детекција на експлозиви, делови од експлозивни направи, како и автоматска детекција на опасни и забранети предмети.

Согледувајќи ги пропустите кои можат да настанат за време на безбедносните контроли низ аеродромите, како и спроведените тестови врз процедурите и опремата, при симулации, подметнувања, вешто камуфлирање на опасните материи, можеме да кажеме дека, постојните системи потребно е да бидат надоградени, заменети со посовремени системи, уреди нормално надополнети со мерки и процедури на заштита како комбинација и подршка на импементираните технологии.

Од аспект на *скенирање на багажите*, стандардната процедура, која се користи на голем број на аеродроми, се врши со помош на апарати за детекција (X – зраци) или рачно во присуство на патникот, како и одобрените методи согласно меѓународните регулативи. Со цел да се зголеми безбедноста, неопходна станува потребата од примена на CT технологијата, независно од производителите и моделите, таа овозможува прецизни мерења на густината со многу висока резолуција. Системот може точно да ја мери густината во внатрешноста на шишето, а може дури да ја мери и густината на мешаните течности. Моделите од најновите генерации, покрај останатите можности, ги задоволуваат и потребите во поглед на: целосните волуменски мерења, овозможување на операторите да гледаат 2 - D слика и 3 - D

проекција, во реално време, проекција, скенирања со едно поминување на торбата низ скенерот, намалување на лажните аларми, тридимензионална волуметрична слика која овозможува поглед од 360 степени на предметот, врзина на анализа на предметите и до 5 секунди по парче, и многу други предности.

Во поглед на применливоста на уредите и *системите за скенирање на рачниот багаж, торби и предмети* се осврнува кон потребата за ненаметлива инспекција на мали до средни предмети во сите критични инфраструктури во Република Македонија, особено при влегување во контролираните и строго контролираните зони во дадената критична инфрструктура. Скенирањето на рачниот багаж, торби и предмети е погоден за примена во голем број на критични инфраструктури, како што се на пример: транспортните ифраструктури, државните институции, енергетските компании, хемиската индустрија и др. Најновите системи за ваков вид на заштита овозможуваат многубројни енергетски слики, и широк опсег на процесирање на слики, кои се клучни за квалитетот на сликата, функционалност на системот, високи перформанси, детекција на опасности со голем опсег на детектирање, со што на операторот му се олеснува можноста да го идентификува составот на скенираниот материјал. Во голем број на ваквите скенери инсталирани се и опреми за тревога со прецизно детектирана закана, вклучувајќи ја и автоматската детекција на течности. Најновите технолошки системи вклучуваат детекција на експлозиви, наркотици, оружје и други забранети предмети и супстанции. Денешните производители нудат широка палета на системи кои се со најразлични димензии на тунелот и можат лесно да се пренесуваат од едно на друго место. Исто така, со цел намалување на рестрикцијата за пренесување на течности поголеми од 100мл. во рачниот багаж, потребна е имплементација на системи кои можат успешно да го одредат хемискиот состав на течностите и да утврдат дали се работи за закана. Воздухопловните пристаништа во Република Македонија, со цел да се во чекор со другите аеродроми, во делот на прегледот на течностите, а во поглед на удобноста на патниците како и намалување на преземање на непопуларни мерки на одземање и ограничување на превозот на течностите, потребно е да воведе вакви системи кои нудат високи перформанси и детекција на опасностите.

Службите за обезбедување спроведуваат *преглед на лицата* со помош на металдетектор врати, рачни метал детектори и рачно. Сите лица, не зависносно од критичната инфраструктура, кога влегуваат во контролираните зони потребно е да им се спроведе контрола. Детекторите кои се користат во моментов најчесто, како технологија користат електромагнетна намотка која генерира вкрстени магнетни

полиња, како и посовремените модели кои преставуваат програмирачки метал детектори кои генерираат електромагнетно поле за детектирање на метално оружје или орудие кое се наоѓа во лицето во моментот на контролата. При детекцијата на метал, дисплејот ја лоцира позицијата на скриениот предмет. Овие модели вршат и евиденција на бројот на прегледани лица и овозможува статистичка операција за контрола. Некои модели нудат и мулти димензионално скенирање, со што се зголемува и бројот на прегледани лица. Потребата која се наметнува од недостатоците за детектирање на експлозивите и опасните материи кои не се изработени од метал пример: графитни ножеви, керамички опасни средства, како и експлозивите кои по состав спаѓаат во органски материи, се наметнува потребата од развој на технологијата во поглед на детектирање на сите видови на опасности. Металниот детектор може да детектира електро магнетен попис на многу мала количина на метал, но поради тоа се зголемува и лажната детекција. Згора на тоа металдетекторите не се во можност да ги скенираат неметалните закани како што се керамичките оружја, пластичните или течните експлозивин и сл. Ограничувањето на оваа технологија ја наметнува потребата од воведување на детектори кои работат со помош на X зраци, кои конвенционално биле користени кај контролата на рачниот багаж, торби и предмети. Ниско напојување на X зраци се испушта кон патникот, а потоа се формира слика од сенка на телото. Радијацијата лесно пробива преку секаков вид на облека, а резолуцијата која се добива од овој систем скоро секогаш е со одличен квалитет. Ова овозможува дури и детекција на најмали предмети кои претставуваат закана и кои ги поседува лицето. Како недостаток претставува приватноста на лицата, но и поради спорото време на проток на лица и барањата кон патниците во текот на ваквата контрола, но и чувството на патниците за време на постапката. Од тие причини, како најадекватна е примената на милиметарско зрачење или MMW (Millimeter – Wave) со должина на зрачење помеѓу 1мм и 10мм (доволно за пробивање низ ткаенина и за овозможување на резолуција). Од различните видови на MMW системите, пасивните системи нудат најдобро долгорочно решение со брзо автоматско скенирање и голем проток на патници, како и ниска цена и ниски оперативни трошоци.

Како надополнување на системите за контрола на лицата секако најдобро познат и најчесто применуван метод за контрола останува рачниот претрес. Овој начин е докажан како најдоверлив, кој има резултирано со голем број на откривања на забранети предмети. Рачното пребарување, сепак претставува непопуларен метод на

работа од повеќе аспекти, а како главени ќе ги споменеме човечкиот замор и големиот број на лица кои треба да се прегледаат во кратко време.

Од аспект на биометриското скенирање и фактот дека безбедносните барања се повеќе се зголемуваат, не само на аеродромите после терористичките напади на 11Септември 2001година, туку и врз сите критични инфраструктури. Една од централните грижи со кои се среќаваат практичарите и менаџерите за безбедност во компаниите секако претставува контролата на пристап. Големиот број на физички системи за контрола на пристапот кои се користат денес,полека стануваат неприменливи во зависност од напредокот на терористичките тактики и оружја. Застарените методи овозможуваат само привидно чувствона безбедност. Биометриската верификациона технологија е единствениот вистински одговор, која е потребно да биде имплементирана како замена на физичките помагала. Денес, се повеќе аеродроми, но и компании со сериозни ризици се повеќе се пренасочуваат кон позитивната идентификација со помош на биометриските модели за потврдување на идентитетот и точна претстава кое лице пробува да добие пристап до одредена ограничена зона. Биометриските апликации вклучуваат земање на примерок од индивидуите кои потоа се дигитализираат и се автоматизираат и стануваат уникатни во базата на податоци. Користењето на биометриските податоци ја препознаваат личноста која добива пристап во ограничената зона. Пристап до ограничената зона можат да имаат само дел од персоналот кои имаат конкретни работни задолженија. Овие системи можат да дадат одговор и на многуте деликатни работи поврзани со случаите за опасност, при евакуацијата точно ќе се знае бројот на лица и персонал кој биле присутни во загрозената област. Досегашните системи покажуваа само ограничувачки податоци без целосен преглед на комплетната ситуација.

Алармите системи во функција на обезбедувањето претставуваат незаобиколен дел од системот за обезбедување кој треба да биде инсталиран во сите критични инфраструктури како облик на систематко поставена заштита. Системите имаат за цел заштита на лицата, имотот, информациите, технологијата, опремата и др. од намерно или случајно дејствување на одредени негативни појави. Сложените и софистицирани системи кои треба да се применат во обезбедувањето на критичната инфраструктура, генерално, треба да ги опфаќаат минимум следните врсти на системи кои мора да се инсталираат во критичните инфраструктури, а тоа се:

- Алармните системи,
- Системите за контрола на пристап
- Мониторинг системите – видео надзор,

- Останати системи на заштита како што се: системите за детекција на опасни супстанции и гасови, детекција на води, кражби упади и сл.

Целта на овие системи е во најраната, односно, почетната фаза да откријат и сигнализираат појава на опасност врз објектите кои се предмет на заштита. Структурата на системите директно зависат од тоа што се штити: луѓе, приватноста, објектите – опремата – информациите, работниот и технолошкиот процес и од што се штити. Фактот што, настанатите штети како последица на негативните влијанија експоненционално расте со времето кое е потребно за дојава, откривање,значи дека времето на заштита е зависно од времето на детекција, времето на пренос на информацијата и од времето на интервенција. Со оглед на фактот дека времињата за откривање, пренос и интервенција во областа на заштитата на критичните инфраструктури се мали поради значењето на дејностите, со сигурност се наметнува потребата од имплементација на ваквите современи системи во развој на безбедноста.

Употребата на дресирани кучиња во функција на обезбедувањето на виталните објекти, станува се по нагласена, поради резултатите кои ги постигнуваат дресираните кучиња, во целокупниот систем на заштитни мерки регулирани со закон.

Кучињата се застапени во повеќе сегменти од секојдневното работење:

- Трагање по сторители на кривични дела,
- Трагање по исчезнати лица
- Следење на траги,
- Претреси на простории, багажи, лица за откривање на експлозивни направи
- Претреси за откривање на наркотици и други психотропни супстанции, и др.

Во рамките на приватната безбедност потребно е измена во Законот за приватната безбедност. Согласно Законот за приватно обезбедување сл. весник на РМ. Бр 166 од 2012 член 56 став 7, во кој употребата на дресирано куче е ограничена само на одбивање на непосреден напад над работникот за обезбедување, како и непосреден напад над лицето или имотот што се обезбедува. Со истиот закон би се регулирал и тренингот на ваквите кучиња.

Ако повлечеме паралела помеѓу техниката и употребата на кучињата во функција на откривање на забранети предмети, вклучувајќи ги и експлозивите, кучињата со својот капацитет на запазување и позитивното насочување на осетот имаат постигнато значителна успешност во правилната детекција и лоцирањето на опасните предмети. Оттука, неминовно се наметнува се по нагласената потреба од примена на кучињата

во функција на обезбедувањето на сите критични инфраструктури, а нивната примена би се состоела во:

- Патролирање и контролни активности во рамките на физичкото обезбедување,
- Контрола, преглед и претрес врз возила простории, багажи и останата опрема и добра во рамките на обезбедуваната критична инфраструктура, со цел откривање на опасни материи и експлозиви,
- Заштита на целокупниот периметар на критичната инфраструктура,
- Подршка на работата на пункт за обезбедување, и др.

Тимовите во кои ќе бидат вклучени високо обучени кучиња за трагање за различни експлозивни материјали во близина на зградата екстериери, паркинзи, канцеларии, возила, пакети и луѓе во и околу објектите, исто така, овие тимови ќе обезбедат силна видлива и психолошка пречка против криминалните и терористичките закани. Ваквите тимови ќе играат клучна улога во сеопфатните мерки за превентивна безбедност со поддршка на стратешките активности за откривање на експлозивните направи. Тие, исто така, ќе обезбедат непосреден и специјализиран одговор на бомбашките закани како и контрола на торбите, пакетите и други предмети кои се оставени без надзор. Активности за откривање ќе им овозможуваат на тимовите да се открие или брзо да се исклучи присуството на опасни материјали, со што се овозможува непречено функционирање на работните текови, како и избегнување на непотребни евакуации, блокирања на терен, како и прекин на процесот на работа и добивање на претстава на нестабилност или загрозеност на клиентите[374].

Од аспект на употреба на куче, во цели за откривање на експлозивни направи, треба да се спомене дека во воздухопловството претставува еден од прифатените методи за проверка на патниците, багажите, каргото како и целокупните средства и опрема кои влегуваат во стерилните зони на аеродромите. Сето тоа е дефинирано и регулирано согласно регулативата на ЕУ. Во оваа регулатива, кучето за откривање на експлозив може да открие и посочи специфични и високи поединечни количини на експлозивни материи. Откривањето е независно од обликот, местоположбата или ориентацијата на експлозивните материи. Кучето дава аларм, во облик на пасивна реакција, кога открива експлозивни материи . Кучето и неговиот водич можат да се употребуваат за безбедносен преглед доколку и двајцата се одобрени поединечно и како тим. Кучето и неговиот водич подлежат на почетни и последователни обуки. По одобрението од страна на надлежниот орган, тимот може да се употребува за безбедносен преглед со употреба на методи на слободно трчање или метод на

[374] http://www.dhs.gov/explosive-detection-canine-teams Превземено на 29.11.2015год.

трагање со оддалеченост по мирисот на експлозивот. Тренингот опфаќа теоретски и практични елементи, како и елементи на тренинг на работното место. Содржината на курсевите за тренинг треба да биде прецизирано или одобрено од страна на надлежен орган. Кучињата кои треба да се дресираат за откривање на експлозив се кучиња единствено за таа намена со строго дефинирани стандарди.

Свесноста за безбедноста е многу значаен фактор за целокупната безбедност на критичната инфраструктура со крајна цел зачувување на човечките животи и материјалните добра. За да се постигне адекватна безбедносна политика на компанијата, секој еден вработен без разлика на работното место и профилот на струката, потребно е да поседува елементарно познавање за безбедност, посебно за времетраењето на неговите работни обврски. Работникот потребно е да биде внимателен и да информира за секоја сомнителна или абнормална состојба.

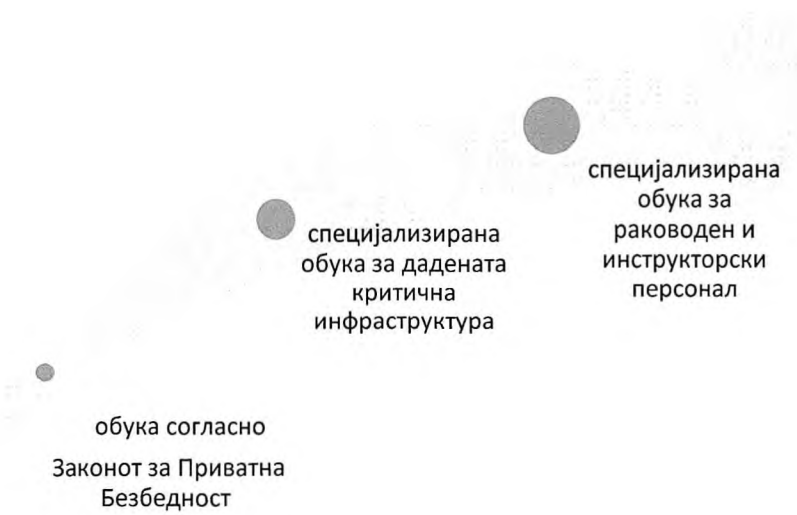
Финансирање на обезбедувањето, по примерот на финансирањето на обезбедувањето во воздухопловството, со воведување на дополнителни давачки во услугите применет и прифатен во многу европски држави, како резултат на зголемување на мерките за обезбедување, поради степенот на закана потребно е да се размисли и за останатите критични инфраструктури кои ќе бидат дефинирани и регулирани со пропис. Во согласност со релевантните правила секоја земја, може да определи во кои околности, и до кој степен, трошоците за безбедносните мерки за заштита на критичните инфраструктури од дејствија на незаконско постапување, треба да бидат на товар на државата, субјекти, операторите, другите надлежни органи или корисниците. Доколку е соодветно, и во согласност со правото може да се примени и механизам за финансирање на активностите од обезбедувањето преку процент кој ќе се издвојува од секоја реализирана наплата на услуга или продажба. Во овој случај, компаниите оператори на КИ,ќе бидат независни од останатите сегменти во компанијата и средствата,ќе бидат користени само за опремување и имплементација на современи системи, техника и средства во развојот на обезбедувањето на критичната инфраструктура, исто така, средствата ќе бидат користени и за континуирани обуки и усовршување на персоналот кој работи на дадената проблематика.

Обука на персоналот, по примерот на аеродромското обезбедување се препорачува бидат реализирани како: основна и повторна обука со прецизна оценка, сертификација и евиденција на целокупниот персонал[375].

[375] ICAO – Annex 17

Поради спецификите на обезбедување на критичните инфраструктури и употребата на средства и опреми кои се нестандардни во обезбедувањето на останатите корпорации, по примерот на воздухопловната безбедност, потребно е да се допрецизираат, односно, да се специјализираат работниците, но и раководниот кадар во поглед на: обука заради преземање на мерки и примена на технички средства кои ги карактеризираат некои специфични работни позиции, дефинирање на минимум квалификации на раководителите на службите за обезбедување како и поседување на неопходно ниво на знаење и искуство во доменот на обезбедување на определената критична инфраструктура, дефинирање на минимум квалификации за инструкторите за безбедност кои се задолжени за развој и спроведување на обуките.

Целокупниот персонал за обезбедување потребно е да биде обучуван на теми во врска со обезбедување од акти на незаконско постапување, со цел да можат да ги извршуваат нивните работни задачи согласно бараните стандарди.



Сл.17 Категории на обуки

Контролата на квалитет потебно е да биде спроведена во сите критични инфраструктури, а се со цел адекватно спроведување на сите барања од регулативите и нејзините акти, вклучувајќи и казнени одредби, а во врска со следење и откривање на недостатоците, корегирање во рамките на одредени временски интервали и да се да се воспостави целосен и пропорционаленпристап во однос на активностите за корекција. За да биде реализирана во целост контролата на квалитет, потребно е да се изработи Националната програма за контрола на квалитет за сите области дефинирани како критични инфраструктури за да се потврди дека мерките за обезбедување се ефикасно и соодветно спроведени и да се утврди степенот на

усогласеност со одредбите од регулативите и програмите за обезбедување, со помош на активности за следење на усогласеноста.

1. Модел на Програм/План за обезбедување на критична инфраструктура (ПОКИ)

Компаниите кои се подведуваат под називот,,критични инфраструктури" од аспект на обезбедувањето, детерминирани врз основа на потребите, потребно е да развијат сопствена Програма за обезбедување како еден основен концепт, кој во најмала рака би содржел барања, мерки и постапки за обезбедување со детали опишани низ стандардни оперативни процедури. По моделот на аеродромската Програма дефинирана со документ на (ICAO, ECAC, ACI) која за потребите на оваа дисертација е прилагодена за да може да се употреби во голем број на критични инфраструктури(ПОКИ) ги опфаќа следните теми:

- Извори на законодавство, регулативи, организациона поставеност на критичната инфраструктура,
- Тела задолжени за обезбедување на критичната инфраструктура,
- Опис на критичната инфраструктура и комуникациите,
- Мерки и активностиво функција на безбедноста на критичната инфраструктура,
- Опрема и средствата кои се во функција на обезбедувањето,
- Одговор на дејствија од незаконско постапување
- Обука за обезбедување,
- Контрола на квалитетот.
- Додатоци во функција на Програмата[376].

Слика бр.18 Концепт за изработка на ПОКИ

[376]http://clacsec.lima.icao.int/Reuniones/2007/Seminario-Chile/Presentaciones/PR13.pdf Превземено 12.12.2015год.

При изготвувањето на ПОКИ,најнапред низ дефинирани национални законски и подзаконски акти потребно е да се формулира правната рамка на која се темели обезбедувањето, секако вклучувајќи ги и меѓународните прописи дефинирани за определената критична инфраструктура. Во тој поглед внимателно треба да се разгледаат сите детали кои треба да бидат опфатени во документот, особено чувствителните информации. ПОКИ обично ќе има широка дистрибуција и доверливоста на податоците потребно е да биде селекивен. Соодветно на тоа, чувствителните информации кои ќе бидат содржани во процедурите или одредени документи на програмата, ќе имаат ограничена дистрибуција и прецизно насочени кон корисниците, тоа значи дека ПОКИ ќе претставува класифициран компаниски документ.

Целите на Програмата треба да содржат, но не се ограничени на:

- барањата на националното законодавство
- дефинирање на компаниските одговорности, поврзани со безбедноста на различни засегнати страни;
- опис на процесот за изработка на процедури, поврзани со безбедноста кои се потребни за заштита на критичната инфраструктура,
- опис на организациската поставеност за управување и координирање на обезбедувањето на критичната инфраструктура;
- дефинирање на минималните стандарди;
- разгледување и ажурирање на програмата за да се обезбеди неговата континуирана ефективност и др[377].

Програмата за безбедност на критичната инфраструктура потребно е да ги обединува сите мерки за безбедност кои се предвидени заради заштита, инфраструктурата и давање на насоки за имплементација на мерките за безбедност. Определувањето на овластувањата, обврските и одговорностите претставува првиот сегмент во изработката на програмата за безбедност а тоа се однесува на компаниѕкиот менаџмент, одговорните лица за безбедност, оперативните работници за техничко и физичко обезбедување, вклучувајќи ги и државните органи, доколку се директно застапени, како и сите релевантни надворешни и внатрешни субјекти вклучени во процесите на работење на критичната инфраструктура.

[377] http://www.airsafety.aero/getattachment/Requirements-and-Policy/OTACs/OTAR-Part-178-Aviation-Security/Airport-Security-Programmes/Example-Airport-Security-Programme/OTAC-_178_1_Attachment_Example_ASP_Issue1.pdf.aspx Превземено на 12.12.2015год.

Описот на компаниските активности е важен од аспект на одредување и димензионирање на составните функционални капацитети на инфраструктурата, а пред се: физичките карактеристики, објектите, инсталациите, средствата, уредите, техничката и кадровската опременост, техничко технолошките процедури за работа на компанијата и сл.

Во делот на одговорности, потребно е да бидат идентификувани сите релевантни чинители во критичната инфраструктура и дефинирање на нивните специфични обврски според ПОКИ, вклучувајќи, но не ограничувајќи се на:

- надлежниот орган за безбедност на критичната инфраструктура;
- операторот на критичната инфраструктура;
- орган за спроведување на законот;
- менаџерот за безбедност на критичната инфраструктура;
- даватели на услуги во однос на обезбедувањето на критичната инфраструктура;
- националните вооружени сили;
- владини агенции;
- единици за одговор при катастрофи
- операторите во критичната инфраструктура;
- закупци на простори во критичната инфраструктура;
- телекомуникациски агенции;
- гранични контролни органи како што е царината и имиграцијата;
- општински власти;
- регулаторни компании;
- агенции или компании кои ракуваат со одредени сегменти во компанијата;
- оператори од угостителството;
- компани за чистење;
- даватели на услуги во критичната инфраструктура и др.

За попрецизно следење како и евидентирање во рамките на критичната инфраструктура низ шема која покажува соодветните одговорности на овие чинители ќе биде пожелно да стои како додаток во ПОКИ.

Во овој сегмент, како важен дел треба да се нагласи потребата од идентификување и функционирање на тело за безбедност (комитет, совет или сл.) во критичната инфраструктура, кое ќе имаулуга да:

(А) го советува операторот за развој на контроли и процеси кои се потребни на критичната инфрструктура, со цел да се усогласат со одредбите од законот и регулаторните барања кои се однесуваат на работата поврзана со безбедноста;

(Б) помага во координацијата на спроведувањето на контролата и процесите кои се потребни, со цел да се усогласат со одредбите на законот и регулаторните барања кои се однесуваат на работата; и

(В) ја промовира размената на информации и почитување на програма за безбедност на критичната инфраструктура.[378]

Овој орган во критичната инфраструктура би претстравувал советодавен орган на сите правни лица кои се присутни со значајни надлежности за безбедноста на критичната инфраструктура. Ако има голем број на организации или компании во категорија на засегнатите страни, може да се направат аранжмани за колективно претставување. Слично на тоа, членството може да се прошири со претставници од вработените на критичната инфраструктура. Во овој оддел, исто така, треба да се именува претседател и секретар. Обично, операторот на критичната инфраструктура ќе назначи виш претставник или член на висок менаџерски тим да дејствува како претседател, поддржан од страна на директорот, односно, менаџерот за безбедност на критичната инфраструктура.

Во прилог на редовното членство во оваа тело, може да биде предвидено номинирање на други претставници или да се формираат ад хок поткомитети за решавање на конкретни прашања. Деталите за таквите аранжмани, исто така, треба да бидат вклучени во ПОКИ. Ова тело низ акт на критичната инфраструктура би требало да ја дефинира периодичноста на седниците, подготвување и свикување на седнисците, одржување на седниците заклучоци од истите и сл.

Во делот на кореспонденција потребно е да се опишат различните начини на кои надлежниот орган ја соопштува својата безбедносна политика, како и класификацијата на документите, изјавите, заштитата на доверливите документи и ограничувањата при нивната дистрибуција. Потребно е да се наведат и ограничувања за комуникација со медиумите за прашања поврзани со безбедноста на критичните инфраструктури.

Опис на критичната инфраструктура

Описот на критичната инфраструктура ја третира содржината на критичната инфраструктура која со цел да се обезбеди доволно податоции да се објасни објасни оперативниот контекст во кој функционираат мерките на безбедност. Тука се содржани општи информации за критичната инфраструктура, вклучувајќи го и кодот за

[378]http://gazette.gc.ca/rp-pr/p1/2013/2013-04-27/html/reg8-eng.html Превземено на 12.11.2015год.

идентификација и локација, името на операторот на критичната инфраструктура, податоците за контакт како што се адресите и телефонските броеви. Во вој дел се опишуваат и надворешните и внатрешните ограничувања на критичната инфраструктура.

Во овој дел, исто така, треба да биде опишано следново:

- компаниското имот и објектите;
- зградите, терминалите и сл;
- јавните површини;
- пристапни патишта и паркинг места;
- ограничените зони и нивните граници;
- магацините, комуникациските системи и угостителските објекти;
- објектите на критичната инфраструктура, како што се пожарни станици и инсталации од значење на одвивање на технолошките процеси,
- патничките, товарните како и зоните за одржување и платформите;
- услугите во критичната инфраструктура,
- комерцијални или закупени контролирани области;
- пунктови за безбедност и контрола;
- зони за граничната контрола, царина и имиграција (доколку се работи за граничен појас);
- компаниски организации и др.

Тука можат да се вклучат и планови во вид на додатоци како на пример:

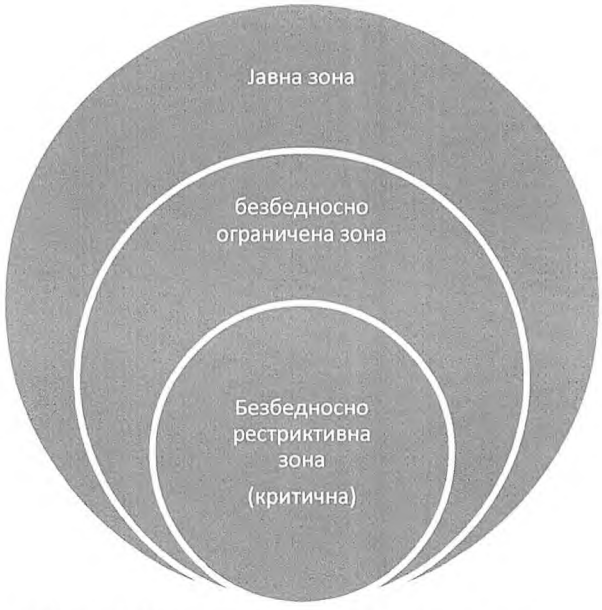
План во размер на критичната инфраструктура кој ги покажува погоре наведените локации,усогласување и дефинирање на јавните и контролираните зони, разграничување на безбедносно ограничените зони и др.

Исто така, потребно е да се опише времето на оперативност на критичната инфраструктура, различните видови на операции и обемот на работа.

Мерки за безбедност на критичната инфраструктура

Фактот дека секоја критична инфраструктура со сите сопствени објекти, површини инсталации, уреди, средства и опрема спаѓаат во редот на посебен интерес за државата и од посебен стратешки интерес од аспект на одбраната, во прегледот на мерките за безбедност во критичните инфраструктури, потребно е да бидат опишани начините на кој безбедносните мерки се дизајнирани и имплементирани во критичната инфраструктура. Според важноста, функционалната улога и техничко технолошката посавеност на содржините на критичната инфраструктура пожелно е да се воспостават концентрични кругови, каде надворешниот круг ја претставува јавната

зоната претставена со сродните мерки за безбедност, вториот круг претставува безбедносно ограничена зона и границата или ограничена област со целокупните мерки за безбедност,и третиот круг го претставува безбедносно рестриктивна зона или зона со највисока заштита, во која лица, предмети и возила може да бидат предмет на дополнителна проверка или други безбедносниконтроли.



Сл.19. Дефинирање на зони во Критичните инфраструктури

Неавторизираниот пристап е дефиниран со физички бариери за безбедност, како што се огради и порти, системи за надзор како и мерки за контрола на пристапот на овластени лица, возила и предмети.

Безбедност во јавната зона, во основа ги претставува инфраструктурните делови каде што е дозволен пристап на сите посетители но каде што е предвидена физичка безбедност со рутински оперативни мерки за безбедност, кои се спроведуваат за заштита на јавните површини на критичната инфраструктура. Тие обично вклучуваат мерки со кои се намалува ризикот од напад со возила во кои има експлозивни и други опасни материи, имплементација на соодветни техничко технолошки решенија во кој се следат сомнителните активности, патролни активности, заштита во форма на предупредувања и информации за присутните и останата адекватна заштита на компаниските маерјали и вработените.

Ограничената зона, ги опфаќа инфраструктурните елементи на комплексот од критичната инфраструктура кои се директно поврзани со процесите за работа вклучувајќи ги сите објекти, површини инсталации, уреди, средсва опрема кои служат и директно придонесуваат за нормално функционирање на структурните сегменти.

Тука ќе ја споменеме потребата од периметарската заштита и контролата на пристап,која треба да биде назначена со правен акт, кој ќе овозможи најнапред ограничување на пристап само на овластени лица. Потребно е да се опишат правните акти со кои ограничената зона е обележена и одговорностите и овластувањата кои им се дадени на операторот на критичната инфраструктура. Овие правни норми генерално ќе го формализираат системот за идентификација и издавање на дозволи - идентификациони картички за движење во критичната инфраструктура. Тука пред се се мисли на процесот кој вклучува: далежност, видови на идентификациони картички, поделба на идентификационите картички, изглед, технологија на изработка но и контрола, процедурите за работа во функција на работењето со идентификационите картички и др.

Процедурите за придружните лица во контролираните зони, исто така, потребно е да бидат јасно дефинирани во ПОКИ, низ адекватни бедносни причини за движење.

Во делот на периметарската заштита потребно е во ПОКИ да се опише физичката заштита на ограничената зона и периметарот, вклучувајќи спецификации за: Осветлувањето (јачина, агол на осветлување, правец, вид на светлина и сл.), оградување (висина, ширина, должина, материјал и сл), видео надзор (видови на камери, технички карактеристики на камерите и сл), системи за откривање на упад и др. Исто така тука се опишува како ќе се спречи неавторизиран пристап со применетите мерки, средства и техники, како и број, локација и часови на работа на безбедносни пунктови за контрола на пристап, како и локацијата на излези во случај на опасност.

Контролата на пристап како еден од значајните форми на обезбедување, бара, да се опише процесот за контрола на пристап на лица, стоки и возила. За лицата, таквите процеси обично ќе вклучуваат проверка на лицето кое ја поседува дозволата, идентификацијата, важоста како и зоната на движење. За оваа намена може да се користат технологии или биометриски апликации.Истото се однесува и за возилата и лицата кои управуваат со нив. На крајот од овој дел во ПОКИ, треба да се опише контролата на безбедноста и процесот на проверка на лица, стоки и возила, доколку е применливо.

Во поглед на патролите и позициите на обезбедување треба да биде дефиниран, видот на патролата (моторизирана или пешадиска) или пак статично обезбедување со распоред на лица, заради физичката безбедност и спроведување на мерки на заштита и контрола на пристап со целосна евиденција на активностите.

Како важен сегмент во овој вид на заштита потребно е да се дефинира и контролата на ,,клуч" системот, односно, да се опише спецификација за заклучувања и контрола над заклучените области, кои се користат во функција на обезбедувањето на критичната инфраструктура.

Заштита на Безбедносно ограничените зони

Најнапредтреба да се спомене дека овие зони во основа претставуваат објекти, површини, инсталации, уреди, средства и опрема, кои се од витално значење за безбедно, сигурно и ефикасно одвивање на основната дејност на критичната инфраструктура во било кое време, но исто така и за несметано функционирање на сите структурни сегменти (сектори, служби, оделенија, единици, испостави и др.) а кои се инволвирани во одвивањето на основната дејност на критичната инфраструктура. Несметаното функционирање на критичната инфраструктура е поткрепено со правна основа, според која безбедносно ограничените области се назначени и преставуваат посебни области во рамките на ограничената зона. Областите кои треба да бидат содржани во овие зони најчесто се:

- деловите за клучните активности на критичната инфраструктура;
- областа после спроведената безбедносна проверка;
- зоните на складираната роба која се користи во функција на процесите за работа,
- телекомуникациските и информатички центри на критичната инфраструктура
- зоната на движење на прегледаните лица, возила и роби,
- системите за електрично напојување,
- и други делови на критичната инфраструктура според спецификите на дефинираните критични сегменти во работењето.

При контролата на пристап до безбедносно ограничените зони се применуваат и дополнителни мерки за контрола на пристап за да се спречи неавторизиран пристап и треба да биде опишана во детали. Доколку се бара скрининг на лица и предмети или прегледи на возила, потребно е да бидат наведени во овој дел на ПОКИ во детали за тоа каде и како се спроведува скрининг или употреба на друга адекватна и одобрена опрема и средства за оваа намена.

Одговорноста за одржување на интегритетот на безбедносно ограничените зони паѓа на операторот на критичната инфраструктура и потребно е да се опише со какви методи, средства и техники се реализира истото, секако низ оперативни процедури и применети безбедносни стандарди.

Проекција на персоналот за реализација на контролите при влез во безбедносно ограничените зони во ПОКИ обезбедува детали за:

- бројот и локацијата на контролни пунктови,
- скрининг процесот;
- исклучоци од скрининг, (доколку ги има);
- предмети кои се забранети или ограничени;
- процесот за прием на алати и др.

Во овој дел потребно е да биде разработена и постапка во случај на откривање на сомнителни или забранети педмети.

Прегледот на возила при влез на безбедносно ограничените површини е неизбежна во процесот на работење и во голема мерка се применуваат адекватни методи споменати погоре.

Треба да се напомене дека само проверени лица, возила, предмети, торби и роба можат да се пуштат во контролираните зони на критичната инфраструктура, скрининг процедурите треба да содржат општ опис на процесот на проверка кој опфаќа: цел, постапки и / или стандарди за скрининг и рачно пребарување, список на лица ослободени од скрининг и претреси (доколку има); процедури и/или стандарди за скрининг и пребарување, податоци за операторот и / или давателот на услуги; третман на сомнителни лица и роби; контрола на движењето на прегледаните лица; мерки за посебна категорија на лица; постапки при одбивање на рачен претрес, постапување по откривањето на забранети предмети; ракување со одземените предмети; постапка при откривањето на непријавени опасни материи; мерки за електронски и електрични предмети и сл.

Оперативните процедури, во овој дел, треба да содржат општ опис на опремата која се користи во провека, чувствителни информации во врска со калибрација, оперативни проверки и одржување на таквата опрема, сервисирање и др. Во врска со безбедносниот персонал, потребно е да бидат опишани и задачите, позициите, ротациите при работа и сл.

Во контекст на ова, потребно е да се изработи листа на забранети предмети која ќе биде секогаш при рака на операторите.

Контролата на огнено оружје потребно е да биде базирано врз одредбите од Законот, кој ја регулира оваа област и треба да ја опише политика и барања во врска со оружјето.

Карактеристиките кои се дефинираат во различните критични инфраструктури ќе бидат опишани по основ на природата на работа на определената инфраструктура,

секако, поткрепени за нормативни акти кои се донесени или ќе бидат донесени во иднина. Чувствителни информации во врска со скрининг процедури можат да бидат содржани во стандардни оперативни процедури.

Одговор на дејствија на незаконско постапување

Во овој дел од ПОКИ треба да бидат разработени условите за планирање кои се однесуваат на планот на критичната инфраструктура за непредвидени (вонредни) ситуации, кои можат или да се дел или да бидат како составен дел, односно, прилог на ПОКИ. Планот за постапување на операторот на критичната инфраструктура, е со цел справување со вонредните ситуации предизвикани од акти на незаконско постапување, локализација и изолирање со планско првземање на активности за спречување од понатамошна ескалација и намалување на ефектите од таквите дејствија.Оперативниот план кој ќе биде разработен од страна на сртучните лица во компанијата за секој вид на незаконско постапување со прецизна евиденција на ажурирање на податоците, одговорностите, надлежностите, организациска поставеност во вонреднис ситуации, вклучувајќи и вежбовни активности.

Обука

Во ПОКИ потребно е да биде дефинирана и потребата за обука која може да биде опишана и во посебна програма, но да ги содржи во најмала рака, следниве три категории:

- Обука за свесност за безбедност - обезбедување за општи информации, вклучувајќи: одговорности за одржување на обука; условите на вработените да присуствуваат на почетна обука; времетраење и зачестеност односно периодичност на повторни обуки; методи за одржување на обуката, програми; и евиденција за присуство. Оваа обука ќе биде задолжителна за сите вработени во К.И.

Сл.20. Обуки за безбедност повид на персонал

- Обука на не безбедносен персонал - non security personnel, оваа обука ќе се реализира за категорија на персонал кој не е во рамките на обезбедувањето, но со неговата работна позиција може директно да биде засегната безбедноста. И за оваа категорија на персонал потребни се посебни програми за обука по модули и целни групи.
- Обуката за обезбедување (security), која е наменета за безбедносниот персонал, прилагодена за критичната инфраструктура по категории на персонал, како што е: раководниот персонал, физичкото обезбедување и рентген операторите – скринерите (доколку се употребува ваква опрема) и да се определи точна програма за извршување на овие активности.

Ваквиот вид на обука ќе овозможи адекватно спроведување на мерките за обезбедување од страна на целокупниот персонал вработен во критичната инфраструктура а кој е предходно селектиран согласно стандардите а кој во голема мерка ке биде во можност да да применува мерки за обезбедување како во нормални услови така и во услови на зголемено ниво на закана.

Надзор и контрола на квалитет

Во основа претставува следење на ефикасноста на ПОКИ како и другите мерки и активности кои ја дефинират безбедноста на критичната инфраструктура. Најчесто, контролата на квалитет е претставена како засебна програма, која има за цел: дали сите инволвирани субјекти правилно ги спроведуваат мерките, активности за контрола и надзор на усогласеноста, потврдување на ефикасноста на обезбедувањето и програмите кои ја третираат оваа област, но и да се увидат слабостите на процедурите и делотворноста на човечкиот фактор.

Прилози

На крај, ПОКИ потребно е да биде надополнет содокументи кои не можат да бидат вклучени во содржината на главниот документ, а тука се мисли на:

- мапи и планови;
- копии од закони и прописи;
- постапки;
- технички информации;
- подредени програми; и
- примероци на дозволи за идентификација на критичната инфраструктура, како и други релевантни документи.

Заклучок:

Новите безбедносни предизвици и нивното влијание врз виталните објекти – ,,критичните инфраструктури", претставени низ зависноста на националната безбедност, националната економија, здравство, како и ефикасното функционирање на системите на државата, пред се бара примена на мерки за безбедност кои ќе гарантираат стандардизирано ниво на безбедност преку градење на сеопфатна безбедносна политика, поддржана со законски прописи и имплементација на современи безбедносни системи и процедури во развој на обезбедувањето на критичните инфраструктури. Неопходноста во препознавање, спротивставување и послекризно опоравување од сите видови на закани, кои ја пратат денешницата е обврска на сите инволвирани субјекти во безбедноста и обезбедувањето и треба да функционираат беспрекорно во утврден и воспоставен систем на секоја држава.

Анализирајќи ги применетите практики од западните држави, воедно и Република Македонија како држава аспирант за членство во Европската унија, недвосмислено се наметнува потребата од се поопсежно елаборирање на оваа проблематика и нејзино имплементирање во законска или подзаконската регулатива во безбедносниот сегмент, кој е значаен за современо функционирање на државата. По примерот на современите држави, Р. Македонија, најнапред потребно е во догледно време да пристапи кон дефинирање на поимот ,,критичната инфраструктура", а потоа и кон прилагодување според европските стандарди и препораки како и подготовка за активно учество во сите тела на ЕУ, кои ја третираат оваа област. Како што споменавме, прв чекор во дефинирање и регулирање на оваа област претставува изработка на соодветни документи (Закон за заштита на критичната инфраструктура, Национална програма за заштита на КИ, Национален План за заштита на КИ, Национална стратегија за безбедност на КИ) или сличен документ, во кој јасно ќе бидат регулирани прашањата поврзани со заштитата (безбедноста) на критичната инфраструктура, како и појмовно креирање на терминот ,,критична инфраструктура" во Република Македонија. Базирана врз основа на општите и теоретските постулати за обезбедувањето на ,,критичната инфраструктура", потребно е да се воспостави методолошки пристап во имплементацијата на еден нов сегмент во националниот систем за безбедност на Република Македонија.

Концептот на заштита на критичната инфраструктура во Република Македонија, треба да се темели врз законска или друг вид правна регулација, во која централно

прашање ќе биде безбедносната политика на земјата, соработката и дефинирањето на надлежностите помеѓу државата, општеството, бизнисот и индустријата. Важноста ќе произлезе директно од имплементацијата на терминот ,,критична инфраструктура", кој ке биде еден нов дефиниционен елемент, втемелен во безбедносниот систем на Република Македонија. Од тие причини и политиката на Националната безбедност која, претставува сложен и меѓузависен збир на мерки, планови, активности и програми, уште повеќе ќе придонесе во одржување и унапредување на безбедноста, со посебен акцент на критичните инфраструктури.

Вниманието треба да биде насочено кон доградба на досегашните регулативи и практики, во функција на безбедноста, согледувањето, изнаоѓање и дефинирање на можностите и условите за применливоста на напредните практики, процедури и системи и нивна имплементација во развојот на обезбедувањето.

Врз основа на истражувањето направено за потребите на оваа докторска дисертација, како и врз основа на анализата на голем број на литература, законски, подзаконски акти, прирачници, упатства и сл., кои ја третираат заштитата на критичната инфраструктура и изнесените согледувања на практичарите, направена е можност да се обликуваат и практично да се применат определени стандарди и процедури, кои произлегуваат од крајната операционализација на понудените решенија во оваа докторска дисертација. Во таа насока, недвосмислено се наметнува потребата од имплементирање на рамка врз која треба да се темелат идните развојни стратегии во поглед на обезбедувањето на ,,критичната инфраструктура" од акти на незаконско постапување која директно влијае врз безбедноста на државата.

Со цел критичните инфраструктури квалитетно да се дефинираат и развиваат, потребен е најнапред институционален приод, потребна е стратегиска рамка во поглед на дефинирање, а аналогно на тоа, потребно е поприфатлива методологија на безбедност за намалување на ризици од негативните последици врз критичните инфраструктури, што претставува услов за стабилно општество, и сигурно одвивање на стратешките функции на земјата.

Управувањето со критичните инфраструктури, потребно е да биде составен дел на сите развојни програми, а посебно во делот на безбедност и превенција од ризици, непогоди и катастрофи и истите потребно да се интегрираат во сите релевантни документи на државата.

Анализата потврди дека сериозноста на последиците од загрозувањата на критичните инфраструктури и општиот впечаток, кој се добива на полето на обезбедувањето на критичните инфраструктури, е доста значаен и суштински,пред се,

поради констатацијата дека безбедноста на инфраструктурите е фокусирана на процесите и состојбите во државата и пошироко, значи носењето на релевантните одлуки стануваат пред се државен интерес.

Одговорноста за заштитата на националните критични инфраструктури, во најголем дел паѓа на операторите на критичните инфраструктури, оттука, најнапред потребно е да се направи индикативната листа за критичната инфраструктура врз основа на значењето. Со понудените методологии за идентификување и дефинирање на критичните инфраструктури, овој докторски труд дава преглед на пристапот кој го имаат напредните држави кон безбедноста и какви мерки и активности се преземаат за развивање на заштитата на критичние инфраструктури.

Разработените тези од областа на актите на незаконско постапување, како извор на закана на критичната инфраструктура и тероризмот како најекспониран елемент претставен низ примената на опасните материи во функција на терористичките дејствија, недвосмислено говори за сериозниот пристап кој треба да биде применет од сите нивоа на заштита и во сите дефинирани критични инфраструктури.

Зависноста на општествата од безбедноста на компаниите, во ситуација кога традиционалните начини на обезбедување се повеќе се потиснуваат, пред се понагласените закани кои ги носи глобализацијата бара еден нов пристап на физичка, оперативно техничка и сајбер безбедност. Новите видови на закани бараат пред се, организираност на обезбедувањето непрекинато 24часа со вклучување на напредните безбедносни системи кои ја пратат технологијата и достигнувањата во функција на обезбедувањето.

Анализата појаснува дека имплементацијата на современите системи и процедури во развој на обезбедувањето на критичните инфраструктури, претставува неопходност и процес кој треба да има свој континуитет кон создавање на посакуваната безбедносна клима.

Денешните програми и процедури за работа, особено во делот на критичните инфраструктури, потребно е да ги обединуваат сите мерки за безбедност кои се предвидени заради заштита и давање на насоки за имплементација на мерките за безбедност. Од исклучителна важност е процесот на обезбедување на критичните инфраструктури да биде детерминиран и дизајниран за справување со новите ризици и опасности како еден од клучните предуслови за правилно функционирање на безбедноста.

Синтезата на одговори потврди дека постои потреба од дефинирање и распределба на задачите, но и суштинско прашање како да се координираат

активности меѓу различните институции, агенции и други субјекти, засегнати со спроведувањето на различни аспекти на обезбедувањето кои ја третираат одредената област. Анализата покажува дека координацијата помеѓу релевантните субјекти овозможува поефикасно реализирање на безбедносните цели, како и намалување на ризиците и справување со непредвидените ситуации. Соработката со државните институции треба да биде насочена кон интензивирање во преземање на чекори за зајакнување на партнерските односи, како во делот на зголемување на безбедносниот потенцијал, дефинирање на надлежностите и заедничка позиција на дејствување и воспоставување на проактивен дијалог за прашања поврзани со обезбедувањето на критичните инфраструктури.

По примерот на воздухопловството и аеродромското обезбедување, како една одпорегулираните области кога е во прашање заштитата и обезбедувањето, во овој труд е направена една симбиоза на применливост на определени методи, техники и опреми и во останатите критични инфраструктури кои не се и / или недоволно се регулирани во делот на обезбедувањето. Во таа насока, понудена е методологијата на обезбедување на аеродромите да биде применета и адаптирана во обезбедување на останатите области, со крајна цел создавање на модерен, ефикасен и сеопфатен безбедносен систем во Република Македонија. Стручното, професионалното и перманентното водење на развојни безбедносни политики, опфаќа широк спектар на мерки, постапки и процедури на полето на превентивната безбедност, но и на полето на справување со кризни ситуации и опоравување од истите.

Безбедносните системи кои се во постојан развој, а со цел задоволување на барањата кои произлегуваат од праксата, имплементацијата на современите системи треба да зависи од повеќе фактори, но заначајно е тоа што безбедносната оправданост за инвестирање во опрема и средства треба да биде константна и во зависност од потребите. Нема дилема дека опремувањето на службите за обезбедување во согласност со современите достигнувања од оваа област подразбира можност за несметано извршување на поставените задачи, адекватни на ризиците и опасностите кои ја пратат денешницата. Во овој докторски труд, покрај другото понуден е концепт за обезбедување на крирична инфраструктура, со детерминирани основи, претставени преку нивоа на заштита, а со цел спречување на неовластен пристап до контролираните зони на инфраструктурата и спречување на извршување на акти на незаконско постапување. Врз основа на согледувањата наметната е потребата за развивање на стратегија поврзана со свесност за безбедност кај сите вработени во критичната инфраструктура, со цел да се постигне

адекватна безбедносна политика на компанијата со која секој еден вработен без разлика на работното место и профилот на струката, потребно е да поседува елементарно познавање за безбедност, сразмерни на специфичните потреби и обврски. Исто така, секој нововработен потребно е да биде подложен на безбедносни проверки, а проверките да бидат повторувани на одреден временски период, вклучувајќи проверки на идентитетот и предходното евентуално криминално минато.

Секоја држава во својата национална безбедносна агенда потребно е да вклучијасно дефинирани интереси и задачи, вклучувајќи ги и националните инфраструктури низ јасна сеопфатна безбедносна политика. Затоа,со цел адекватно спроведување на сите барања од регулативите и нејзините акти, вклучувајќи и казнени одредби, а во врска со следење и откривање на недостатоците како и корегирање во рамки на одредени временски интервали, потребно е да се воспостави целосен и пропорционален пристап во однос на активностите за корекција преку имплементација на контрола на квалитет, која ќе обезбеди пред се правилно, безбедно и квалитетно функционирање на критичните инфраструктури во Република Македонија.

Суштинската карактеристика на ризиците и изворите на загрозување од актите на незаконското постапување, се повеќе стануваат непредвидливи, асимертрични и имаат транснационален карактер. Оттука неминовно се наметна потребата за воведување на проценки, како и имплементација на методологии низ модели прилагодени и адаптирани за конкретни критични инфраструктури.

Актите на незаконско постапување како извор на закана, претставени низ облиците на загрозување и тероризмот како еден од најекспонираните опасности на денешницата, бара поголема заинтересираност на државата и компаниите оператори со критичните инфраструктури во елиминацијата на актите насочени кон безбедноста на државата преку ранливоста на овие капацитети.

Прашањата поврзани со имплементација на мерките за обезбедување во функција на виталните објекти од акти на незаконско постапување во сегментите на планирањето, службите за обезбедување, координацијата, разузнавачките функции, напредните технологии и превенцијата, беа насочени кон создавање на стабилен безбедносен систем и јакнење на безбедносните капацитети на критичните инфраструктури.

Преземените практики од современите држави низ спецификите на раководење со безбедносните служби како и применливоста и имплементирањето на директивите и стратегиите на современите држави, дадоа целосен императив во насока на поддршка на регулирањето на оваа релативно ,,нова" дисциплина.

Прилог бр 1: Чек листа за истражувачка дејност

Нестандардизирано интервју

р.бр	Област / Прашања	Наод	Референтен документ	Опис
1	**Регулирање на обезбедувањето на критичната инфраструктура.** - Дали компанијата – оператор, поседува одобрена програма за безбедност/ процедури, планови, интерни акти со кои се регулира обезбедувањето? (меѓународни акти и домашна регулатива)			
2	**Кординација и дефинирање на тела за обезбедување.** - Дали компанијата - оператор, има дефинирано тело за обезбедување, како функционира и кои се членови ?			
3	**Закани и безбедносни ризици по критичните инфраструктури.** - Податоци за евентуални закани, безбедносен ризик, настани кои влијаеле на безбедноста и нормалното функционирање на кпомпанијата.			
4	**Трошоци и финансирање на обезбедувањето**. - Дали компанијата - оператор има соодветна процедура или др.документ кој го регулира начинот на покривање на трошоците поврзани со обезбедувањето? и колку средства се користат за таа намена?			

5	**Посебни безбедносни процедури кои се применуваат во критичните инфраструктури.** - Дали постои определување на зоните со ограничено движење? - Дали постои оградување со периметарска ограда со ограничен број на влезно-излезни капии за пристап на возила под надзор? - Реализација на обиколки на периметарската ограда, во неправилни временски интервали и др. мерки за контрола на пристап? (Кои системи на тех.заштита се користат) - Дали операторот издава идентификациони картички за сите лица кои своите должности ги извршуваат во контролираните подрачја. - Дали персоналот и др.лица кој своите должности ги извршува во безбедносно ограничените зони минуваат единствено на службените влезови по извршен безбедносен преглед? (со која опрема располага сл. влез) - Дали операторот обезбедува пристапот до контролираните зони да биде ограничен само на овластени лица? - (кои се техниките и опремата која се користи) - Дали операторот издава пропусници за возилата кои мора да се движат и дали се проверувани на сите пунктови за контрола на пристапот? (со која опрема и средства располага пунктот)			

	- Дали операторот има пропишано и применува процедури за постапување со т.н "забранети предмети? - Дали операторот има ангажирано доволен број на извршители за обезбедување? - Дали операторот има изработена соодветна програма за обука на персоналот во доменот на обезбедувањето? - Дали операторот има предвидено мерки за постапување во случај на потреба од зајакнати мерки на безбедност заради зголемено ниво на закана? - ЦЦТВ системи и останата опрема и средства кои се во употреба на обезбедувањето (Тех. Спецификација)			
6	**Обука на персоналот** - Дали персоналот кој своите должности ги извршува во безбедносно ограничените зони има редовна обука поврзана со обезбедување - Дали персоналот задолжен за обезбедување поседува соодветни уверенија за стручна оспособеност? - Дали операторот има обезбедено обука за обезбедување за non-security персоналот и согласно кои акти?			
7	**Контрола на квалитет во делот на обезбедувањето**. - Дали операторот има изработена соодветна програма за интерна контрола на квалитетот во доменот на обезбедувањето и дали истата се применува ?			

8	**Планови за вонредни ситуации.** - Дали постои План за постапување во вонредни околности во кој се предвидени постапките во случај на терористички и други слични акти на незаконито постапување? - Дали во наведениот план се усогласени мерките и активностите на различните државни органи и други субјекти задолжени за безбедноста ? - Дали во последните години е организирана и реализирана вежба (целосна или делумна) заради проверка на ефективноста на планот? (каква вежба е организирана – опис на вежбата)			
9	**Прашање кое не е поставено, но соговорникот смета дека треба да биде разгледано а е од значај за трудот и природата на објектот.**			

Дополнителни забелешки:

Работна библиографија:

1. Aleksandro Iazari European Critical infrastructure protection University of Florence Firence Italy, Springer 2014,
2. A.V. Gheorghe, M. Masera, M.P.C Weijnen, Critical Infrastructures at Risk Securing the European Electric Power System, Springer 2006,
3. Aviation safety plan, International Civil Aviation Organisation, Montreal, Kanada, 2007,
4. Airport Cooperative Research Program; Safety Management Systems for Airport, Washington D.C 2009,
5. Аеродромска тренинг програма за заштита на цивилното воздухопловство група автори, Скопје 2008,
6. Андреа Савиќ , Увод у државну безбедност, Виша школа унутрашњих послова Београд, 2002,
7. Antunovic B., I. Varga, Gordana Kralik, Mirjana Baban, V.Poljak, B.Njari, Z. Pavlovic,S.Mackic: Racunalna simulacija kao alat za procjenu rizika od teroristickih napada u lancu proizvodnje hrane – Krmiva 53 Zagreb 2011,
8. Алчески П. Постапки во случај на опасност, Скрипта за стручна обука на персоналот на ППСС на Аеродромите, Охрид 1998,
9. Алчески Ѓ, Процедури при вонредни состојби- Скрипта Скопје 2010,
10. Бакрески. О, Драган.Т, Митевски, Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот – Скопје 2012,
11. Бакрески О., Основи на безбедносниот менаџмент, Аутопринт Т.А – Скопје, Филозофски факултет - Скопје 2012,
12. Бакрески О., Контрола на безбедносниот сектор, Филозофски факултет, Скопје 2008,
13. Бакрески О, М. Даничиќ, Ж. Кешетовиќ, С. Митевски – Приватна безбедност – теорија и концепт Комора на Република македонија за приватна безбедност, Скопје 2015,
14. Бакрески О,Милошевиќ М., Современи безбедносни системи, компаративна анализа на земјите од југоисточна Европа, Аутопринт Т.А – Скопје 2010,
15. Brigrs R, Edwards C., The Buseness of Resilience: Corporate Security for the 21 st Century, Demos, London, 2006,
16. Ванковска Б. Меѓународна Безбедност, Филозофски Факултет, Скопје 2011,
17. В. Водинелиќ, Криминалистика, Савремена Администрација Београд 1984,

18. Група автори: Основи противдиверзионе заштите, Министерство за унутрашњих послова република Србије - Институт Безбедности, Београд 1998,
19. Гоцевски Т., Бакрески О., Драгичиќ Ж., Авторизирани предавања, Менаџмент во безбедноста,
20. Георгиева Л, Менаџирање на ризиците Филозофски Факултет Скопје 2006,
21. Green Paper on a European Programme for Critical Infrastructure Protection Brussels, 17.11.2005 COM(2005) 576 final,
22. Гоцевски Т. Бакрески О., Славевски С., Европската Унија низ призмата на Европската Безбедност Филозофски факултет Скопје, 2007,
23. Department of State Office of Antiterrorism Assistance, Vital Installation Security Course - 2003,
24. D. Caleta, P. Shemella, Counter terrorism challenges, regarding the process of Critical infrastructure protection, Ljubljana 2011,
25. D. Kulisic, F. Magusic, O aktualnim općim pristupima i elementima za raščlambe opasnosti od zlonamjernih ugroza sigurnosti prometnih tokova, Strucni clanak: 343.9:323.285, 2006.
26. D. Caleta, Corporate security in dynamic global environment – challenges and risk, Ljubljana 2012,
27. Доревски З., Практикум - Обезбедување, Комора на Република Македонија за обезбедување на лица и имот Скопје, Јуни 2004,
28. Dorfman S. Mark, Introduction to Risk management and insurance , Prentice Hall, Englewood Cliffs NJ.
29. Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan Homeland Security – United States Department of Energy 2010;
30. European Programme for Critical Infrastructure Protection (EPCIP) COM(2006) 786,
31. EPA Water Security & Resiliency Highlights, Office of Water (4608-T) EPA 817-F-12-012 United States, Enviromental Protection Agency EPA, December 2012,
32. Z. Klaic, S. Mandžuka, P. Škorput, Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama, 18. Telekomunikacioni forum TELFOR Beograd, 2010,
33. Z. Radmilovic, Biometriska identifikacija, Strucni clanak UDK: 57.08:343.982, 2008,
34. Zastita kriticne infrastructure I osnovni elementi uskladivanja sa direktivom saveta Evrope 2008/114/ES Mirko Škero Bezbedno-informativna agencija Vladimir Ateljević

Vlada Republike Srbije, Kancelarija za evropske integracije - Visoke studije bezbednosti i odbrana

35. Z. Brincka, S. Raguz, Procjena kao stadij obavještajnog procesa, Strucni clanak, UDK, 343. 98. 06, 2009,
36. Ibrahim Jusufranić, Osnove drumskog saobracaja , Tehnologija – Organizacija – Ekonomika – Logistika – Upravljanje. – Травник 2007,
37. International jurnal of mathematical models and methods in applied sciences Measures for critical infrastructure protection, Ludek Lucas, Lubos Necesal Issue 2011,
38. ICAO, Aviation Security Manual 8973
39. ICAO,Aviation security training package instructors - trainee reference book 2012,
40. ICAO, Annex 17 Safeguarding International Civil Aviation Against Acts of Unlawful Interference,
41. ICAO Annex 17 to the convention on International Civil Aviation Ninth Edition March 2011.
42. ICAO Airport services manual – Airport Emergency planing doc. 9137 –an /898 part 7. 1991g.
43. ICAO Annex 12 Sarch and rescue. Annual edition, ICAO, Montreal, Canada 1990.
44. ICAO Annex 13, Aircraft Accident Investigation. Annual edition, ICAO, Montreal, Canada 1990,
45. IIEA European Security and Defence Series: European Security in the 21st Century" Institute of International and European Affairs 2012,
46. International journal of mathematical models and methods in applied sciences - Measures for critical infrastructure protection – Ludek Lucas, Lubos Necesal , 2011;
47. Jakovljević V., Gačić J. Zastita kriticne infrastructure u kriznim situacijama - Medunarodna naucna konferencija Menadzment Mladenovac, Srbija, 2012.
48. Klemen Groselj Critical Infrastructure Protection and the Energy Sector Counter – Terrorism Challenges regarding the Processes of Critical Infrastructure: Ljubljana : Septrember 2011,
49. Critical Infrastructure Protection: Threats, Attacks and Countermeasures, Editors Luca Montanari, Leonardo Querzoni, Tenace March 2014,
50. Кековиќ З. Системи Безбедности, Факултет Безбедности, Београд 2009
51. Critical Infrastructure Security and Protection The Public-Private Opportunity- White Paper and Guidelines by CoESS And its Working Committee Critical Infrastructure December 2010.

52. Commission staff working document on the review of the European Programme for critical infrastructure protection (EPCIP) Brussels, 22.6.2012,
53. Конвенција за престапи и други дејствија извршени во воздухоплови во тек на лет Токио 1963 (Dok 8364).
54. Конвенција за спречување на незаконско грабнување на воздухоплови Хаг 1970(Dok 8920).
55. Конвенција за спречување на незаконски дејствија против безбедноста на цивилното воздухопловство Монтреал 1971(Dok 8966)
56. Костеска Миљковиќ Е. Опасни материи (Dangerous Goods Manual) Аеродром Александар Велики Скопје, 2007,
57. Котовчески М.. национална Безбедност на Република Македонија I, II, III kniga, Makedonska civilizacija, Skopje 2000,
58. Котовчески М., Современ тероризам, Македонска цивилизација, Скопје 2002,
59. Kostic. V. Zapalive I druge opsne materije, Udruzenje publicista Beograd, 1980,
60. Кешетовиќ.Ж. Кризни Менаџмент, Факултет безбедности Београд 2008,
61. Љубо Пејановиќ Тероризам и противтерористичка дејства у ваздушном саобрачају – Војно издавачки завод Београд 2003
62. Matka D. Energetska sigurnost i kritčna infrastruktura – pregled rezultata istraživanja Zbornik radova: Krajcar, S, Energetska sigurnost i kri čna infrastruktura, Sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb 2009.
63. М. Мијалковски, Одговор тероризму, Београд 2005,
64. М. Митревска, Кризем Менаџмент Филозофски Факултет Скопје 2008,
65. Милан Благојевиќ – Алармни системи Факултет за заштита при работа – Ниш 2011,
66. М.Даничиќ, Љ. Стаиќ, Приватна безбедност, Висока Школа Унутрашњих послова Бања Лука 2008,
67. Milan Vrsec: 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 201
68. Михајло Басара, приказ од книгата на Јонатан Вајт, Тероризам, војно дело 4/2004,
69. Marlin S. Darvey M. ,, Disaster – Recovery Spending on the Rise" Information Week, Manhasset NY, August 2004;

70. Методологија избора критичне информатичке инфраструктуре – Министарство за информационо друштво и телекомуникације Црне Горе, 2014,
71. 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,
72. 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;
73. National Guidelines for Protecting Critical Infrastructure from Terorism, Australia – New Zealand Counter – Terorism Commite, Commonwealth of Australia 2015,
74. National critical infrastructure protection – regional perspective, Belgrade, 2013,
75. National critical infrastructure protection – regional perspective - UDC726.9:75.041.5 ID176374796, M. Marjanović I. Nađ: Assesment of threats to critical infrastructure facilities from serious and organized crime, Belgrade, December 2013.
76. NIPP 2013 Partnering for Critical Infrastructure Security and Resilience – Homeland security USA NIPP 2013,
77. N. Milosevic, S. Milojevic, Osnovi metodologije bezbednosnih nauka, Policiska Akademija, Beograd 2001
78. Нацев З., Теориски основи на доктрината и стратегијатана национална одбрана Скопје 2006
79. Пајкович Д – Обезбеѓење одредзених личности и објеката, МУП Републике Србије, Београд 2003
80. Problem space report: Critical infrastructure & supply chain protection Cross-border Research Association (CBRA) January, 2012.
81. Pozari I eksplozije, Savremena Administracija, Beograd, 1983,
82. P. Auerswald, L.M. Branscomb, T.M. La Porte, E.Michel – Kerjan – The Chalenge of Protecting Critical Infrastructure – issues in science and tehnology FALL 2005;
83. Partnering for Critical Infrastructure Security and Resilience homeland security NIPP 2013;
84. Prezelj, I., Konceptualna opredelitev kritične infrastrukture, FDV, Ljubljana, 2008,
85. Primjena ICT-a u upravljanju kriticnom infrastrukturom u tranzicijskim zemljama Zdenko Kljaic, dipl.ing. Member, IEEE, Sadko Mandžuka, dr.sc. Member, IEEE, Pero Škorput, mr.sc. Member, IEEE 18. Telekomunikacioni forum TELFOR.

86. Presidential Policy Directive -- Critical Infrastructure Security and Resilience The White House Office of the Press Secretary February 12, 2013,
87. Протокол за спречување на незаконски насилни дејствија на аеродромите кои опслужуваат меѓународна цивилна авијација Монтреал 1988. (Dok 9518)
88. Р. Гачиновиќ Антитероризам – Библиотека на тргу Београд 2006,
89. Радослав Гачиновиќ Савремени тероризам Графомарк, Београд 1998,
90. Регулатива (ЕУ) БР. 720/201, 272/2009,1141/2011,1087/2011, 185/2010, 1147/2011, 711/2012, 104/2013, бр. 246/2013, 278/2014,
91. Регулатива (ЕЗ) бр. 300/2008 на Европскиот парламент
92. Спасиќ Д. Економика заштите на раду Ниш 2003,
93. Славески С. Безбедносен систем, Европски универзитет Скопје 2009,
94. Steiner, S.: Elementi sigurnosti zračnog prometa, Fakultet prometnih znanosti, Zagreb, 1999,
95. Source: Bundesverband deutscher Banken (Federal association of German banks), Management von Kritischen Infrastrukturen, Protection of Critical Infrastructures – Baseline Protection Concept Recommendation for Companies – Federal ministry of internal. 2004,
96. Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analysing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001,
97. Stallings William, Network and Internetwork Security – Principles and practices, Prentice Hall, Englewood Cllifs, New Jersey 1995.,
98. Таталовиќ С. Национална и меѓународна сигурност, Политичка култура, Загреб2006,
99. Tatalović S. - Energetska sigurnost i zastita kriticne infrastrukture: uticaj na politike i nacionalne bezbednosti - Zbornik radova: Krajcar, S., Energetska sigurnost i kritčna infrastruktura, sveučiliše u Zagrebu, Fakultet elektrotehnike i računarstva, Zagreb 2009;
100. Тунтев Т. Историја на воздухопловството охрид 2003,
101. Т. Тунтев, Аеродромски Прирачник за прифат и отпрема на воздухоплови, патници и предмети, трето изменето и дополнето издание Февруари 2004 год
102. Тунтев Т., Аеродроми, Технички факултет, Битола, 2005,
103. Таталовиќ С. Биландзиќ М. Основе националне сигурности, полициска академија, Загреб 2009,

104. The National Security Strategy states that "the danger from climate change is real, urgent, and severe." National Security Strategy, 2010,
105. Transportation Systems, Sector-Specific Plan, An Annex to the National Infrastructure Protection Plan, Homeland Security United States Department of Transport, 2010,
106. Управување со вонредни ситуации предизвикани од тероризам во воздушниот сообраќај во Р.М - Институт за безбедност, одбрана и мир, Филозофски факултет УКИМ Скопје- Магистерски труд 2009,
107. U.S. Department of Homeland Security, Strategic National Risk Assessment, December 2011,
108. Understanding Terrorist Innovation - Technology, tactics and global trends Adam Dolnik 2007,
109. Unified Facilities Criteria (UFC) Security Enginering: Energy Control: Energy Control Facilities/access Control Points Distribution Statement UFC 4-022-01 25 May 2005.
110. Food and Agriculture Sector-Specific Plan An Annex to the National Infrastructure Protection Plan, Homeland Security United States Department of Agriculture, 2010,
111. F.Dale, H Bonnie, Competitive Intelligence Ethics> Navigarion the Gray Zone, Competitive Inteligence Foundation, Aleksandria VA 2006,
112. Harland Onsrud Research and Theory in Advancing Spatial Data Infrastructure Concepts ESRI Press California 2007,
113. Water Sector-Specific Plan An Annex to the National Infrastructure Protection Plan United States Environmental Protection Agency – Homeland security 2010
114. Walsh B.C, Farrington D.P , Public area CCTV and crime prevention: An udated systematic review and meta – analysis. Justice Qarterly London 2009,

Списанија

1. Airport wrld volume 13 5 October – November 2008,
2. Безбедност, бр.4/2008, МУП Републике Србије, Београд, 2008,
3. European Buisiness Air News, issue 225 may 2012,
4. International airport review – issue 3 2013,
5. Jane s airport review – volume 21 – issue 1 – February 2009,
6. Jane s airport review – volume 21 – issue 2 – March 2009,
7. Jane s airport review – volume 21 – issue 4 – May 2009,
8. Jane s airport review – volume 21 – issue 6 – July - August 2009,

9. Jane s airport review – volume 21 – issue 9 – May 2009,
10. Jane s airport review – volume 25 – issue 4 – May 2013,
11. Jane s airport review – volume 25 – issue 5 – June 2013,
12. Jane s airport review – volume 25 – issue 7 – September 2013,
13. Jane s airport review – volume 25 – issue 8 – October 2013,
14. Critical infrastructure E – newsletter, issue 2 2010,
15. Ревија за безбедност, стручни часопис о корупции и организованом криминалу бр.5 Мај 2009
16. Ревија за безбедност 2/10 Центар за безбедносне студије - Биотероризам и употреба биолошког оружја – Далијела Милиќ,
17. Ревија за безбедност, стручни часопис о корупции и организованом криминалу бр.3 Март2009
18. Ревија за безбедност, стручни часопис о корупции и организованом криминалу бр.3 Мај 2010
19. Ревија за безбедност, струцни часопис о корупции и организованом криминалу 1/10
20. Ревија за безбедност, струцни часопис о корупции и организованом криминалу 3/10
21. Rješenje softverske integracije sustava tehničke zaštite po mjeri, a b system DCI alarm automatika,
22. Современа Македонска одбрана, XII, бр.12, 2005,

Регулативи и други правни акти

1. Закон за приватно обезбедување Сл весник на РМ. Бр 166 од 2012
2. Закон за управување со кризи Сл. Весник на Р.Македонија бр.29/05, 36/11,
3. Закон за заштита и спасување – Прочистен текст, Службен весник на Р.М. бр.93/12,
4. Закон за безбедност и здравје при работа, Службен весник на РМ, бр92/07, 136/12,
5. Законот за внатрешни работи Службен весник на РМ, бр. 42 од 03.03.2014,
6. Закон за Одбрана – Прочистен текст, Службен весник на РМ, бр185/11,
7. Закон за енергетика, Службен весник на Р.М, бр. 16 од 10.02.2011год
8. Закон за водите, Службен весник на РМ, бр. 87 од 15.07.2008
9. Закон за безбедност на храната и на производите и материјалите што доаѓаат во контакт со храната Сл. весник на Р Македонија, бр.54 од 15.07.2002 год.

10. Закон за воздухопловство, Сл. весник на Р.Македонија бр.63 од 13.05.2013,
11. Закон за класифицирани информации, Сл. весник на Р.Македонија бр.9/04, 113/07,
12. Закон за личните податоци, Сл. весник на Р.Македонија бр.7/05,, 103/08, 124/10, 135/11,
13. Кривичен законик, Службен весник на Република Македонија, број 37/96, 80/99, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008 и 114/2009),
14. Национална стратегија за заштита и спасување (Службен весник на Р.М бр. 23/09),
15. Одлуката за определување на правните лица кои се должни да имаат приватно обезбедување, Службен весник на Р.М бр. 106 на 29.07.2013,
16. Стратегија на одбраната на Република Македонија (Службен весник на Р.М. бр 30/2010,
17. Уредба за физичка безбедност на класифицирани информации, Службен весник на РМ, бр. 82/2004)

Матерјали од Интернет

http://www.airports.com.mk
http://www.mvr.gov.mk
http://morm.gov.mk/
http://zastita.info/hr/clanak/2013/2/denis-caleta-(ics)-slovenska-iskustva,311,10204.html;
http://www.dhs.gov/what-critical-infrastructure;
https://erncip-project.jrc.ec.europa.eu/download-area/viewcategory/24-erncip-office-reports)
http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0013_en.htm)
http://www.irsd.be/website/media/Files/Focus%20Paper/FP15.pdf
http://www.caa.gov.mk/
http://www.morm.gov.mk;
http://ec.europa.eu/dgs/home affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf
http://www.asadria.com/index.php/teme/kolumne/276-kriticna-infrastruktura-i-znacaj-osiguravanja-njenog-neprekidnog-djelovanja
https://ciwin.europa.eu/Pages/Membership.aspx

www.epa.gov/watersecurity
http://www.bmi.bund.de/EN/Topics/Civil-Protection/Critical-Infrastructure-Protection/critical-infrastructure-protection_node.htm
http://www.dhs.gov/energy-sector
http://mio.gov.mk/files/pdf/dokumenti/zakoni/ 15 10 2015.pdf
http://www.icao.int/Pages/default.aspx
http://www.iata.org
http://www.aci.aero
https://www.ecac-ceac.org/about-ecac
https://www.eurocontrol.int/articles/who-we-are
https://en.wikipedia.org/wiki/Joint_Aviation_Authorities
http://www.airserbia.com/magazin/vuk/terorizam_u_vazduhu/terorizam.htm
http://en.wikipedia.org/wiki/Pan_Am_Flight_103,
http://en.wikipedia.org/wiki/Dawson's_Field_hijackings,
http://en.wikipedia.org/wiki/Air_India_Flight_182
http://www.planecrashinfo.com/2015/2015-16.htm
https://en.wikipedia.org/wiki/Metrojet_Flight_9268
http://en.wikipedia.org/wiki/List_of_accidents_and_incidents_involving_commercial_aircraft,
http://en.wikipedia.org/wiki/List_of_accidents_and_incidents_involving_commercial_aircraft
http://www.aerospaceweb.org/question/planes/q0283.shtm
https://en.wikipedia.org/wiki/2012_Burgas_bus_bombing
https://en.wikipedia.org/wiki/2016_Brussels_bombings
http://www.dhs.gov/water-and-wastewater-systems-sector
http://www.dhs.gov/xlibrary/assets/nipp-ssp-food-ag-2010.pdf
http://www.dhs.gov/xlibrary/assets/rma-strategic-national-riskassessment-ppd8.pdf
https://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010
, www.bmi.bund.de
https://www.fer.unizg.hr/_download/repository/Davor_Sinka_kvalif_ispit.pdf,
https://www.fer.unizg.hr/_download/repository/Davor_Sinka_kvalif_ispit.pdf
http: www.ebizmags.com
http://www.x-rayscreener.co.uk/?xray=improvised-explosive-devices
www. bt.cdc.gov/agent/agentlist-category.asp.
http://ia.gov.mk

http://www.x-rayscreener.com
http://www.specijalac.net/6077/sluzbeni-psi-policije-i-vojske.html,
http://www.dhs.gov/explosive-detection-canine-teams
http://www.prorisk.mk/plan-za-zastita-i-spasuvanje
https://www.dhs.gov/topic/critical-infrastructure-security
https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33260
http://ec.europa.eu/dgs/home-affairs/news/intro/docs/sec_2010_911_en.pdf
, http://www.zakon.hr/z/591/Zakon-o-kriti%C4%8Dnim-infrastrukturama,
https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
http://www.elem.com.mk
http://www.mepso.com.mk
http://www.okta-elpe.com/Main.aspx?lan=1
http://www.telekom.mk/
http://onevip.mk/mk/za-nas/za-one-vip/
http://ec.europa.eu/enlargement/pdf/croatia/screening_reports/screening_report_24_hr_internet_en.pdf
http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/hr_analytical_2012_en.pdf,
http://ec.europa.eu/commission_2010-2014/fule/docs/news/20120424_report_final.pdf
http://www.mvep.hr/custompages/static/hrv/files/pregovori/ZSEUEN/24.pdf
http://clacsec.lima.icao.int/Reuniones/2007/Seminario-Chile/Presentaciones/PR13.pdf
http://www.airsafety.aero/getattachment/Requirements-and-Policy/OTACs/OTAR-Part-178-Aviation-Security/Airport-Security-Programmes/Example-Airport-Security-Programme/OTAC-_178_1_Attachment_Example_ASP_Issue1.pdf.aspx