

**ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК
ВО ФУНКЦИЈА НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ**

**ЗОРАН КЕКОВИЌ
ОЛИВЕР БАКРЕСКИ
СТЕВКО СТЕФАНОВСКИ
СЛАВИЦА ПАВЛОВИЌ**

ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК

**ВО ФУНКЦИЈА НА ЗАШТИТА
НА ЛИЦА, ИМОТ И РАБОТЕЊЕ**

**ЗОРАН КЕКОВИЌ ОЛИВЕР БАКРЕСКИ
СТЕВКО СТЕФАНОВСКИ СЛАВИЦА ПАВЛОВИЌ**



д-р ЗОРАН КЕКОВИЌ
д-р ОЛИВЕР БАКРЕСКИ
д-р СТЕВКО СТЕФАНOSКИ
м-р СЛАВИЦА ПАВЛОВИЌ

ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК
(ВО ФУНКЦИЈА НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ)

ЗОРАН КЕКОВИЌ
ОЛИВЕР БАКРЕСКИ
СТЕВКО СТЕФАНОВСКИ
СЛАВИЦА ПАВЛОВИЌ

ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК

**(ВО ФУНКЦИЈА НА ЗАШТИТА НА
ЛИЦА, ИМОТ И РАБОТЕЊЕ)**

СКОПЈЕ, 2016

**ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК
(ВО ФУНКЦИЈА НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ)**

Рецензенти:

д-р Желимир КЕШЕТОВИЌ
Факултет за безбедност – Белград
д-р Момчило МИЛОВАНОВИЌ
Машински факултет – Белград
д-р Драган МЛАЃАН
Криминалистичко-полициска академија – Белград

Издавач

Комора на Република Македонија
за приватно обезбедување – Скопје

За издавачот

Верица МИЛЕСКА СТЕФАНОВСКА

Лектор

м-р Лилјана ПАНДЕВА

Графички уредник

Билјана ИВАНОВА

Печати

Стеда графика – Скопје

Тираж

1000

CIP - Каталогизација во публикација

Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

351.759.5:061.231]:005.334

ПЛАНИРАЊЕ и проценка на ризик : (во функција на заштита на лица,
имот и работење) / Зоран Кековиќ ... [и др.]. - Скопје : Комора на
Република Македонија за приватно обезбедување, 2016. - 231 стр. :
граф. прикази ; 23 см

Автори: Зоран Кековиќ, Оливер Бакрески, Стевко Стефаноски, Славица
Павловиќ. - Библиографија: стр. 221-231

ISBN 978-608-65505-9-2

1. Кековиќ, Зоран [автор]

а) Приватно обезбедување - Управување со ризици

COBISS.MK-ID 100709130

СОДРЖИНА

Предговор	11
-----------------	----

ГЛАВА I

ПЛАНИРАЊЕ	13
-----------------	----

1. ОПШТО ЗА ПЛАНИРАЊЕТО	15
-------------------------------	----

2. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА ПОИМОТ ПЛАНИРАЊЕ	16
--	----

3. ЗНАЧЕЊЕ НА ПЛАНИРАЊЕТО	19
---------------------------------	----

4. ЗОШТО Е ПОТРЕБНО ПЛАНИРАЊЕТО	20
---------------------------------------	----

5. ЦЕЛИ И ЗАДАЧИ НА ПЛАНИРАЊЕТО	22
---------------------------------------	----

5.1. Цели на планирањето	23
--------------------------------	----

5.2. Задачи на планирањето	24
----------------------------------	----

6. ПРОЦЕС НА ПЛАНИРАЊЕ	25
------------------------------	----

7. УСЛОВИ ЗА УСПЕХ НА ПЛАНИРАЧКИОТ ПРОЦЕС	27
---	----

8. ПРЕДУСЛОВИ ЗА ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИЦИ	28
--	----

8.1. Предвидувањето како предуслов за ефикасно планирање и за процена на ризици	28
--	----

8.1.1. Фактори кои влијаат на предвидувањето	31
--	----

8.2. Информацијата како неопходен предуслов за планирање и за процена на ризици	32
--	----

8.2.1. Информации за планирање	36
--------------------------------------	----

8.2.2. Информациски систем на планирање	38
---	----

ГЛАВА II

СИСТЕМИ, РИЗИЦИ И СИСТЕМСКИ ПРИСТАП 41

1. ОПШТО ЗА СИСТЕМИТЕ 43

2. КЛАСИФИКАЦИЈА НА СИСТЕМИТЕ 44

3. ХИЕРАРХИСКО УРЕДУВАЊЕ НА СИСТЕМИТЕ 47

4. ТЕРМИНОЛОШКО ОДРЕДУВАЊЕ НА ЗАКАНИТЕ, РИЗИЦИТЕ И ЗАГРОЗУВАЊЕТО 49

4.1. Заканите по системите 50

4.2. Ризиците по системите 51

4.3. Загрозувањето по системите 54

5. СИСТЕМСКО ПОИМАЊЕ НА РИЗИКОТ 55

ГЛАВА III

УПРАВУВАЊЕ СО РИЗИЦИТЕ 61

1. ПОИМ ЗА РИЗИК И СИСТЕМСКИ РИЗИК 63

2. КЛАСИФИКАЦИЈА НА РИЗИЦИТЕ 68

3. КОМПОНЕНЕТИ (ЧИНИТЕЛИ) НА РИЗИКОТ 72

3.1. Опасност 73

3.2. Изложеност 73

3.3. Ранливост 74

3.4. Отпорност 76

4. УПРАВУВАЊЕ СО РИЗИК 76

4.1. Управување со ризик – теоретски аспекти 76

4.2. Управување со ризик – концептуални аспекти 81

4.3. Генеза на развојот на концептот за управување со ризик 85

4.4. Ранливоста во концептот на управување со ризик 89

4.5. Управување со ризик – мерки за намалување на ризикот 95

4.5.1. Собирање, анализа и мапирање на податоци за ризикот 95

4.5.2. Мониторинг на опасности и рано предупредување 97

5. ПОЛИТИКИ И РАМКА ЗА УПРАВУВАЊЕ СО РИЗИК	98
5.1. Политики за управување со ризик	98
5.2. Рамка на процесот за управување со ризик (ISO 31000:2009)	99
5.2.1. Генерална рамка на процесот на управување со ризик	101
5.2.2. Детаљна рамка на процесот на управување со ризик	102
6. МОНИТОРИНГ И КОНТРОЛА НА ПРОЦЕСОТ ЗА УПРАВУВАЊЕ СО РИЗИЦИ	104
6.1. Ажурирање на процените на ризик	104
6.2. Проверка на системот за управување со ризици	106
7. ПРИНЦИПИ ВО УПРАВУВАЊЕТО СО РИЗИК	107

ГЛАВА IV

УПРАВУВАЊЕ СО СИСТЕМОТ НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ	109
---	------------

1. СОВРЕМЕНИ ПОТРЕБИ ВО ЗАШТИТА НА ЛИЦАТА, ИМОТОТ И РАБОТЕЊЕТО И УПРАВУВАЊЕ СО РИЗИКОТ	111
2. ПОЛИТИКА НА ОСИГУРУВАЊЕ ПРИ ЗАШТИТАТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ	114
3. ОПКРУЖУВАЊЕТО И ВРЕДНОСТИТЕ НА ОРГАНИЗАЦИЈАТА ШТО СЕ ШТИТАТ	115
4. СТАНДАРДИ ОД ОБЛАСТА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ	118
4.1. Управување со ризик – теоретски аспекти	118
4.2. Меѓународни и европски стандарди во областа на заштитата лица, имот и работење	120
4.3. Национална и европска регулатива и пракса во областа на приватната безбедност	125
4.3.1. Значењето на приватната безбедност во заштитата на лица, имот и работење	125
4.3.2. Приватната безбедност во системот на националната безбедност	126

4.3.3. Регулирање на приватната безбедност во националните држави	132
4.3.4. Хармонизација на националните со европските стандарди во областа на приватната безбедност	135
4.4. Национални стандарди во областа на заштитата на лица, имот и работење	138
4.5. Корист од примена на стандардите	141

ГЛАВА V

ПРОЦЕНА И КОНТРОЛА НА РИЗИКОТ	145
--	-----

1. ТЕРМИНОЛОШКО ОДРЕДУВАЊЕ НА ПОИМОТ	147
---	-----

2. ОДГОВОРНОСТА И РЕСУРСИТЕ ЗА ПРОЦЕНА	147
---	-----

3. КОНТЕКСТ НА ПРОЦЕНАТА НА РИЗИКОТ	148
--	-----

3.1. Идентификација на потенцијални опасности	150
---	-----

3.2. Анализа на ризикот	152
-------------------------------	-----

3.3. Оцена на ризикот	153
-----------------------------	-----

4. ТРЕТМАН НА РИЗИЦИ	154
-----------------------------------	-----

4.1. Опции за контролирање или ублажување на ризиците	155
---	-----

4.2. Опции за изводливост	159
---------------------------------	-----

4.3. Анализа на цената-користа	159
--------------------------------------	-----

5. КОНТРОЛА, РЕВИЗИЈА И ДОКУМЕНТИРАЊЕ НА ПРОЦЕСОТ ЗА ПРОЦЕНА НА РИЗИЦИ	159
---	-----

6. ТЕХНИКИ ЗА ПРОЦЕНА НА РИЗИЦИ СПОРЕД СТАНДАРДОТ ISO/IEC 31010	161
--	-----

7. ПРАВНА ОСНОВА ЗА ПРОЦЕНА НА РИЗИЦИ И НОРМАТИВНИ АКТИ НА ОРГАНИЗАЦИЈАТА	162
--	-----

7.1. Внатрешни нормативни акти на организацијата како средство за проценка и контрола на ризиците	163
--	-----

8. КОРПОРАТИВНА БЕЗБЕДНОСТ И ПРОЦЕНА НА РИЗИЦИ	167
---	-----

ГЛАВА VI

МЕТОДОЛОГИИ ЗА ПРОЦЕНА НА РИЗИЦИ 177

1. ПРАВНА, ОРГАНИЗАЦИСКА И ИНСТИТУЦИОНАЛНА

РАМКА ЗА ПРОЦЕНАТА НА РИЗИЦИ

ВО РЕПУБЛИКА МАКЕДОНИЈА 179

- 1.1. Процена на загрозеност од ризици за природни непогоди
и други несреќи 180
- 1.2. Процена на загрозеност од ризици и опасности 181
- 1.3. Процена на штети од елементарни и од други непогоди 185
- 1.4. Безбедност и здравје при работа 187

2. МЕТОДОЛОГИЈА (ПОСТАПКИ) ЗА ПРОЦЕНА НА РИЗИЦИ

ВО СПРОВЕДУВАЊЕТО НА ЗАШТИТАТА НА ЛИЦА,

ИМОТ И РАБОТЕЊЕ 190

- 2.1. Идентификување на потенцијалните опасности 192
- 2.2. Процес на анализа на ризикот 194
- 2.3. Процес на евалуација на ризикот 195
- 2.4. Процес на третман на ризикот 196

3. ПРОЦЕНА НА ПОСТОЈНИОТ И ПОТРЕБНИОТ КАПАЦИТЕТ

НА ОДГОВОРНИОТ СУБЈЕКТ ЗА УПРАВУВАЊЕ СО РИЗИК 197

- 3.1. Процена на постојниот и потребниот капацитет –
општа рамка 197
- 3.2. Процена на постојниот и потребниот капацитет –
посебни чекори 199
 - 3.2.1. Процена на потенцијалните опасности 200
 - 3.2.2. Процена на можни последици 201
 - 3.2.3. Капацитет за справување со вонредни околности 204

ГЛАВА VII

МЕНАЏЕР НА РИЗИЦИ 211

1. МЕСТОТО НА МЕНАЏЕРОТ НА РИЗИЦИ

ВО УПРАВУВАЊЕТО СО ОРГАНИЗАЦИЈАТА 213

2. БАРАЊА ЗА КВАЛИФИКУВАНОСТ НА МЕНАЏЕРОТ

НА РИЗИЦИ 215

3. ОПИС НА РАБОТИТЕ	216
4. УПАТСТВО ЗА ПРИБИРАЊЕ НА ПОДАТОЦИ	218
БИБЛИОГРАФИЈА	221

ПРЕДГОВОР

Многу фирми/компаниии имаат искусено болни проблеми со нивните планирачки напори, а пред сè во нивното работење. Некои произлегуваат од самиот планирачки процес, некои од имплементирачката процедура, додека некои се резултат на лошата процена на ризиците. Оттука, идејата на авторите е во насока да укажат на сета општествена релевација, вредност и значење на планирањето и на процената на ризици кои се засноваат на широка платформа за реализација и конкретизација на одредени задачи за подобрување на работата.

Теоретската експликација во оваа книга е насочена кон укажувањето дека планирањето како активност во услови на динамични современи услови за живот и работа добива сè поголемо значење, а тоа го наметнуваат брзите техничко-технолошки промени, економските состојби, политичката ситуација и други фактори. Тоа значи дека колку социолошкото, економското, политичкото и технолошкото опкружување расте и станува покомплексно, сè поголемо внимание му се посветува на планирањето и процената на ризици како средства за креирање на извесната иднина, затоа што тие се камен-темелник од кој зависи успехот на правниот субјект.

Планирањето и процената на ризици низ призмата на безбедносната парадигма, односно анализата на овие динамични процеси упатуваат на заклучокот дека безбедносните закани треба соодветно да бидат согледани во нивниот тоталитет. Тоа подразбира примена на аналитички процеси и методи кои треба да помогнат во процесот на носење одлуки.

Оваа книга е во функција на точната интерпретација на поимите, но нуди и сигурност во аргументацијата на понудените решенија. Исто така, овој труд има непроценливо значење за конституирање на праксата на приватната безбедност во Република Македонија и претставува анализа на еден широк спектар на теоретски размислувања на авторите кои се предмет на нивната непрекината научна и творечка активност во сферата на безбедноста која во континуитет ја збогатуваат, ја продлабочуваат и непрекинато ја усовршуваат, следејќи ги новите тенденции и барања што се поставуваат пред овој мошне динамичен сегмент.

Авторите кои учествуваа во долгиот процес на пишување на книгата изразуваат благодарност на почитуваните рецензенти проф.д-р Лидија Георгиева, проф. д-р Момчило Миловановиќ, проф.д-р Жели-

мир Кешетовиќ и проф. д-р Драган Млаѓан за позитивните критики и поддршката за издавање на трудот. Најголемата благодарност ја упатуваме до издавачот „Комора на Република Македонија за приватно обезбедување“ што овозможи оваа книга да биде достапна до читателите.

Скопје, март 2016 година

Од авторите

I глава

ПЛАНИРАЊЕ

1. ОПШТО ЗА ПЛАНИРАЊЕТО

Уште од почетокот на развојот на цивилизацијата, луѓето планираат, односно си поставуваат своја цел, ги утврдуваат планските задачи што сакаат да ги постигнат, како и начините на кои тие цели и задачи би можеле да се постигнат. Меѓутоа основно прашање не е: „Дали треба да се планира?“, туку прашањето: „Како да се планира?“ и „Дали планираната активност ќе значи рационална претпоставка за остварување на планираните цели и задачи?“. Денес, не можеме да се обидеме да ја опфатиме целата сложеност на денешниот свет, појавите и процесите што се случуваат во него, сложеноста на системите што ги создал човекот, видот и бројот на информациите кои кружат низ него, а притоа да не се соочиме со потребата од нивно разбирање и планирање (Ѓорески В., 2005).

Планирањето се извршува секојдневно од речиси секој човек. Во личниот живот се размислува за определени работи кои треба да се извршат наредниот ден, наредната недела или наредниот месец. Личните активности многу често се планираат на неформален начин. Меѓутоа, институционалното планирање е посложено, формализирано и поодговорно. Основната намера на планирањето е да развие тек на акции за остварување на целите, односно тоа е процес на одлучување или антиципативно одлучување (Шуклев Б., 2004).

Почетоците и динамиката на развојот на планирањето како научна дисциплина се во економијата, каде што и перманентно се бараат методи и начини за реално планирање и намалување на трошоците на сметка на зголемување на профитот. Според теоријата на системите која е доминантно развиена во последните децении на минатиот век, нереалноста на планирањето доведува до пропаст на системите. Затоа е развиена и кибернетиката како наука за управување на сложените системи каде што најважна фаза е планирањето, а основни методи со кои се служи се моделирањето и системската анализа. Практично во голема зависност се теоријата на системите, моделирањето, планирањето и кибернетиката, бидејќи ги обединува иста цел, а тоа е подобрување на функционалноста и ефикасноста на сложените управувани системи (Ѓорески В., 2005).

Планирањето е многу тешка и комплексна активност што значи дека неговиот предмет го чинат сите облици на општествена активност, дејности и живот насочен кон постојан развој (Argenti J., 1989).

Планирањето како активност во време на динамични услови за живот и работа добива сè поголемо значење, а тоа го наметнуваат брзите техничко-технолошки промени, економските состојби, политичката ситуација и други фактори. Во вакви околности кога се изразени очекувањата и кога се соочуваме со непредвидливоста, комплексноста итн., планирањето претставува начин како да се држат очите отворени, како да се унапреди состојбата, како да се донесат подобри одлуки, како да се изберат најдобрите алтернативи и како да се создаде реален пристап кон остварување на задачите во иднина (William A., 1978). Со планирањето не се врши само пасивно приспособување на настаните, односно како ќе се случат тие, туку активно се влијае врз нив. Оттука, планскиот пристап во решавање на проблемите значи донесување соодветни одлуки врз основа на направена анализа на сите релевантни показатели, со цел да се подготви и да се избере соодветен начин на заштита и да се обезбеди навремено реагирање на идните настани.

2. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА ПОИМОТ ПЛАНИРАЊЕ

Планирањето е фаза на процесот на управување и претставува континуиран процес на донесување плански одлуки, и на избор на најповолни цели, политики, стратегии, програми и планови. Со планирањето ги одредуваме целите, силите и средствата и ги претвораме во плански задачи на одредени лица, органи и организациски единици. Исто така, планирањето претставува „целосно размислување однапред“ со кое се подобрува одлучувањето. Планирањето не се ограничува само на донесување плански одлуки, туку тоа е настојување тие одлуки да се реализираат. Всушност, планирањето е процес на одлучување, што и како нешто треба да се направи пред да се преземе акцијата, што значи со тоа да се влијае на работниот процес во целина или на неговите делови. Тоа укажува дека планирањето не е чин, туку процес што нема крајна точка. Тоа значи дека се приближува кон решението, но никогаш во потполност не стигнува до него, што е првенствено врзано за фактот дека во текот на планскиот процес се доаѓа до примена на системи за кои се планира во неговото опкружување (Стаменковски А., 2004).

Етимолошки, поимот планирање потекнува од латинскиот збор „planus“, што значи сплоснат или рамен. Подоцна опсегот на планирањето го опфаќа правењето скица или план (Čubra N., 1977).

Во литературата постојат голем број дефиниции кои поимот планирање го објаснуваат како функција, како процес, како содржина, како активност насочена кон перманентен развој итн.

Москов „ го дефинира планирањето како процес на одлучување што да се прави и како да се направи пред да се преземат определени акции, односно планирањето е одлучување однапред што да се направи, кога да се направи, кој да го направи и како да се направи (Moskow M., 1987).

За Хикс планирањето е умствена работа и тоа вклучува примена на логичко и корисно размислување за решавање на некој проблем, а успехот на организацијата зависи од успехот со кој функцијата на планирањето е извршувана на секое организациско ниво и доколку активностите не се планираат тие ќе бидат нерационални, неостварливи, ќе бидат случајни и нема да бидат ориентирани кон целите. Исто така, овој автор посочува дека планирањето води кон повисок степен на рационалност и тоа ги координира активностите во институцијата кон дефинираните цели. Алтернатива на планирањето е однесувањето препуштено на случајност (Hicks H., 1972).

Дармер смета дека планирањето му помага на менаџментот да ја антиципира иднината и да размислува за систем на меѓуодноси во кои тој дејствува. Со планирањето, менаџментот може да развие конзистентна ориентација кон непредвидливото опкружување на иднината на која се дејствува. Така, планирањето е средство на мислење на менаџментот за остварување на тоа што е сакано и како тоа треба да биде остварено. Конкретно, како умствена активност, планирањето охрабрува иновација, овозможува да има растегнување на умот и е истражување на повеќе алтернативи (Darmer J., 1977).

Британскиот економист Л.Робинс истакнува дека да се планира значи да се избере и да се дејствува кон определена цел, а изборот е суштината на економската активност и аналогно на тоа сиот живот вклучува планирање. Понатаму, овој автор посочува дека постоењето на повеќе од едно планирање (еден план) може да предизвика неусогласеност на различните планови. Во отсуство на координација еден план може да го оневозможи другиот. Во оваа насока шведскиот економист Ј.Свенилсон смета дека планирањето е координирање на акциите во различни идни периоди со користење на еден план.

Друкер планирањето го дефинира од аспект на неговата содржина и тоа како „формулирање цели, формулирање политики, програми и постапки за нивно остварување или планирањето опфаќа дефинирање на целите на организацијата, изработка на стратегија за остварување на тие цели и развивање сеопфатна хиерархија на планови која треба да ги активира и да ги координира активностите (Drucker P., 1997). Во аргументацијата на Станковиќ стои дека „планирањето е масовна активност која му помага на човекот, односно му овозможува да го постигне тоа што го сака со предвидување“ (Станковиќ Т., 2004).

Ланданер планирањето го дефинира како водење на стопански активности од страна на некој орган на заедницата, врз основа на некоја програма што ги опишува квантитативно и квалитативно потребните производствени процеси во некој иден период (Landaner C., 1947). Од друга страна, Месије смета дека „планирањето е процес преку кој се гледа во иднината и се откриваат нови алтернативни правци на акција“ (Massie L.J., 1987).

За Шуклев, планирањето е дел од процесот на управување, односно на менаџментот и тоа претставува прва фаза од процесот на управување и е примарна фаза на управувањето, која во себе ги опфаќа активностите поврзани со истражувањето, предвидувањето и донесувањето одлуки за основните цели, политиката, стратегијата и тактиката и поединечните планови со кои треба да се обезбеди остварувањето на зацртаните цели и политика“ (Шуклев Б., 2002).

Според Чепујноски, планирањето по својата суштина претставува инструмент на свесна организација и управување со општествено-економскиот развој во сообразност со научното спознание на економските законитости, (Чепујноски Ѓ. и Ќосев С., 2005) додека, пак, Стаменковски планирањето го дефинира како процес на одлучување што да се прави и како да се направи, пред да се преземат определени акции, односно „планирањето е селектирање на можни одлуки од многубројни алтернативи“ (Стаменковски А., 2004).

Оваа расправа можеме да ја заокружime со впечатливите ставови на реномираниот американски автор Стејнер кој планирањето го дефинира најкомплексно поаѓајќи од четири гледни точки важни за разбирање на суштината на планирањето, и тоа:

- планирањето како иднина на сегашните одлуки;
- планирањето како процес;
- планирањето како филозофија;
- планирањето како структура (Stejner G., 1997).

Планирањето како иднина на сегашните одлуки ја изразува комплексноста на планирањето во организационите нивоа и прави да се согледаат причините, но и ефектите од актуелните одлуки, како и нивните реперкусии во одредено време. Планирањето се однесува на развојот на експлицитните алтернативни цели и се фокусира на обликување на саканата иднина.

Планирањето како процес започнува со осознавање на целите и задачите кои станаа основен концепт и посакувана состојба што организацијата сака да ги оствари, потоа дефинирање на стратегијата и политиките, како и изработка на детални планови за постигнување на целта со кои се специфицираат неопходните алокации на ресурси за достигнување на саканите цели.

Планирањето како филозофија ја опишува потребата да се планира што е рационална претпоставка за определување на начинот на живеење. Планирањето симболизира легитимитет за континуирано спознавање на иднината.

Планирањето како структура опфаќа повеќе видови планови со кои се дефинираат организациските активности и алокациите на ресурсите во вид на луѓе, способности, простор, финансиски ресурси итн. Структурата се изразува преку ефективно дизајнирање на организационите цели, политиките и стратегиите, додека преку деталните планови се имплементираат политиките и стратегиите за постигнување на целите во одредени институции.

Изнесените констатации нè упатуваат на заклучокот дека е тешко да се дефинира планирањето како научна дисциплина, особено ако се знае дека се создаваат потешкотии за нивото на неговото теоретско вообличување, и ако се знае и фактот дека неговата практична дејност покажува приспособливост, виталност и флексибилност на различните општествено-политички и економски услови. Сепак, од изнесените дефиниции произлегува дека планирањето во основа е интелектуален процес, кој овозможува човекот да ги направи работите како што замислил на соодветен начин и при преземање акции да се раководи според фактите. Исто така, може да се каже дека планирањето треба да се заснова на рационална алокација на ресурсите, или гледано во најширока смисла на зборот планирањето опфаќа збир на активности и мерки со кои се предвидува одредена идна структура на конкретен систем.

3. ЗНАЧЕЊЕ НА ПЛАНИРАЊЕТО

Планирањето е системска подготовка и темел на решавачките цели за реализирање на плановите во иднина и како процес на апстракција на тие цели во основа е насочено кон селектирање од инфинитивната група на можни варијабли и врски, и тоа оние што најдобро ја карактеризираат активноста, а исто така, ги специфицира и резултатите остварени за одредено време. Според оваа традиционална секвенца за решавање на проблемите, планирањето е општ процес што вклучува неколку планирачки активности како што се политичка формулација, стратегиска детерминација, продукција и друго.

Планирањето е подеднакво значајно за сите институции, без разлика на нивната големина, на нивните цели и на нивните мисии кои ги објаснуваат организационите вредности, тежишта и причини за постоење. Сè повеќе се признава дека планирањето се темели на системска прогресија од надворешни и од внатрешни состојби и дека раководниот тим нема избор во однос на прашањето „Дали тој сака да планира или

не?“. Единствениот избор е дали планирањето треба да биде одраз на случајноста или да се изведува целосно, прагматично и систематично.

За значењето на планирањето треба да се истакнат следните укажувања: 1) идната неизвесност и промените го прават планирањето попотребно и во случаи кога постои извесна иднина, односно планирањето е потребно заради правење избор на оптимална алтернатива од повеќето алтернативи; 2) со планирањето се утврдуваат целите; 3) со планирањето се зголемува координацијата на активностите со кои се остваруваат целите; 4) со планирањето се зголемува ефикасноста. Покрај ова, значењето на планирањето се гледа и во следното: 1) со него се оневозможува парцијално одлучување; 2) се придонесува полесно да се совладаат промените; 3) претставува канал на комуницирање; 4) придонесува во унапредување на управувањето и раководењето; 5) со негова помош се овозможува да се донесат оптимални плански одлуки засновани врз претходно анализирање и предвидување; 6) се создаваат претпоставки за стабилен развој и друго (Стаменковски А., 2004).

Ако се согласуваме дека планирањето се карактеризира со секоја акција на донесувачите на одлуки, во тие рамки, значењето на планирањето се гледа во извршувањето на следниве работи:

1. Тоа би водело кон подобра позиција или положба во институцијата/органот. Планирањето не е само по себе крај, туку тоа е средство за остварување на крај.
2. Тоа би и помогнало на организацијата во развојот на начин на кој нејзиниот менаџмент размислува најкомплетно.
3. Тоа му помага на секое раководно лице да размислува, да одлучува и да постапува поефикасно за остварување на саканата цел.
4. Тоа помага да се одржи флексибилноста на организацијата.
5. Тоа стимулира интегративен и ентузијастички приод кон организационите проблеми. Постои природна тенденција во најголем број организации вниманието да се концентрира на моменталните проблеми, изолирајќи ги нив од другите проблеми.
6. Тоа му укажува на раководниот тим како да го оценува и да го проверува прогресот кон планските цели.
7. Тоа би водело кон општествени и корисни резултати (David W. Ewing, 1968).

4. ЗОШТО Е ПОТРЕБНО ПЛАНИРАЊЕТО

Често се поставува прашањето: „Зошто има потреба од планирање?“. Одговорот на ова прашање не е лесен, ниту е едноставен. Сепак, упатува на тоа дека тие коишто се вклучени во процесот на планирање треба да планираат затоа што „тоа овозможува да се согледаат развој-

ните потреби и можности, а со тоа се дава и можност да се истакнуваат билансно врз основа на единствен пристап и на утврдени показатели“.

Потребата за планирање зависи од можностите и од предизвиците со кои организацијата/институцијата се соочува и од комплексноста за креирање на посакуваната идна состојба. Специфицираните цели ја дефинираат идната состојба која организацијата посакува да се реализира. Празнината на планирањето содржи процена на разликата меѓу посакуваната идна состојба и состојбата која најверојатно ќе се случи ако не се преземат нови одлуки и акции. Заради тоа, планирањето се фокусира на идентификување на овие одлуки и акции кои мора да се превземат денес, утре или следниот месец со цел да се зголеми можноста за остварување на посакуваните цели на организацијата.

Потребата на самата организација за планирање се искажува преку нејзините потреби и за да се биде успешен во работата, треба да се најде начин да се капитализира можноста на организацијата. Можноста може да се наоѓа во екстерната околина или во способноста на организацијата да се диференцира самата себеси преку капитализирање на сопствените способности.

Генерално, идентификувани се повеќе причини од потребата за планирање. Прво, тоа е процес на комуникација и како таков ја унапредува координацијата. Второ, тоа мотивира што значи активно влијание на доброто планирање. Трето, планирањето води кон подобро одлучување, односно планирањето вклучува повеќе фактори во размислувањето, затоа што од донесувачите на одлуки се очекува да ги оценат идните импликации од сите донесени одлуки (Шуклев Б., 2004). Исто така, планирањето е потребно до степен до кој: 1) една организација/институција мора да ги антиципира промените од опкружувањето и да го намали временското заостанување содржано во процесот на приспособување; 2) раководниот тим во институцијата мора да бара општи рамки за да ги интегрира одлуките и целите; 3) комуникацијата мора да биде потпомогната, конфликтите разрешени, а координацијата и соработката остварени (Dermer J., 1977). Потребата од планирање, произлегува и од неопходноста: 1) да се одговори на брзите промени во околината; 2) подобро да се искористат расположливите ресурси; 3) да се заштитат интересите на работењето и да се остварат целите; 4) да се изврши поврзување на различните активности; 5) да се направи согледување на нови ситуации и реагирање и приспособување кон нив; 6) да се оствари подобар систем на контрола на работењето (Стаменковски А. 1996).

Потребата од планирање станува сè понагласена во услови на брзи промени на техничкото, технолошкото, економското, социолошкото, политичкото и безбедносно опкружување, бидејќи со него се градат инструменти за осознавање на неизвесната иднина и за приспособување

кон неа (Стаменковски А., 1996). Оттука, без планирање одлуките кои би се донесувале би биле „случајни“, а со тоа неизвесноста за успех од нивната примена би била далеку поголема.

5. ЦЕЛИ И ЗАДАЧИ НА ПЛАНИРАЊЕТО

Интересите и вредностите на една држава, во целина, се основен мотив за ангажирање во сите сфери на работата во насока на нивно постојано унапредување и развој. Секој потсистем во една држава (економски, политички, безбедносен, социјален итн.) има свои интереси кои се труди да ги оствари заради свое, најнапред, преживување, а потоа и за сопствен развој. Овие интереси се остваруваат низ развојни процеси или како што вели Клемен „преку перманентна, општоприсутна и сеопфатна акција на сите делови на државата и на разни нивоа на управување.“ Интересите кои се врзуваат со развојот обезбедуваат напредок на целиот систем, како и на другите делови. Од развојните интереси произлегува утврдувањето на целите и задачите кои sukcesивно треба да се реализираат во одредени планирани периоди (Ѓорески В., 2005).

5.1. Цели на планирањето

Целите им претходат на мисиите, односно на задачите. Мисијата опишува зошто постои организацијата, причината за постоење и класично дефинира што треба да се прави (Radosavljević Ž., 2001). Добро дефинирана мисија е основа за развој на сите следни цели и планови. Без јасна мисија, целите и плановите може да бидат развиени случајно и да не ја носат организацијата во правец во кој треба да оди како своевидна визија за тоа каде треба да се стигне. Силната мисија има, исто така, влијание врз вработените, овозможувајќи им да станат приврзани со организацијата зошто може да се идентификуваат со нејзината целосна цел и причина за постоење.

Целите можеме да ги дефинираме како одредена специфична состојба, ситуација или резултат, која организацијата посакува да го оствари. Тие претставуваат мерки според кои се мери идното дејствување (Mag. W. 1995). Целите се поставени во насока што ја дава целисходноста на акцијата која треба да се преземе, односно целите служат за насочување и за координација на сите активности, организациони делови и поединци. Кога еднаш ќе се формулираат, тие претставуваат критериуми за донесување рационални одлуки во изборот на алтернативните правци на акција, како и стандардна контрола за ефикасно и ефективно дејствување (Милисављевић М., 2002). На тој начин тие обезбедуваат единствен пристап во планирањето и претставуваат водич за организационата коегзистентност.

Целите на планирањето ја исполнуваат својата цел, кога се мерливи, кога се јасно дефинирани,¹ кога се усогласени, кога се предизвикувачки и реални и кога се временски детерминирани. Мерливоста на целите се изразува преку големата мотивациска сила за самите субјекти, додека дефинирањето на клучните цели е особено важно затоа што тоа овозможува да се прецизираат до ситни детали сите аспекти на однесување на субјектот во соодветната организација. Предизвикувачките цели секогаш не значи дека се и реални. Ако целите не се реални, тие негативно влијаат на човекот и на неговиот морал. Исто така, целите треба да се временски одредени, за да се знае во кој временски период треба да бидат реализирани (Станковиќ Т., 2004).

Во однос на одбраната, целите на планирањето се во корелација со утврдените развојни интереси и тие може да се категоризираат како цели на стратешко, на оперативно и на тактичко ниво. Во нивни рамки одделно се утврдени општите, посебните и поединечните цели.

Стратешките цели на планирањето на одбраната се утврдуваат на ниво на држава и врз нивна основа се насочуваат развојните активности на сите делови на системот на националната одбрана, односно на сите носители и учесници во планирањето. Во рамките на овие цели се утврдуваат општите, посебните и поединечните цели на развојот на одбраната, а кои се внесуваат во плановите за развој и во плановите на одбранбените активности. Практично, по нивното внесување и усвојување од надлежна институција (врховен командант, министер за одбрана и сл.) стануваат задолжителни за сите носители и извршители на планирањето, во согласност со нивната хиерархиска поставеност. Општите цели на стратешко ниво, имајќи ја предвид организациската и хиерархиска поставеност на системот за одбрана се единствени за целиот систем и неговите подсистеми. Со нив се насочува организацијата, подготвеноста и функционирањето на системот и неговите основни компоненти. Посебните цели на стратешко ниво произлегуваат од општите цели, а се однесуваат на развојот на потсистемите и нивните основни елементи² додека поединечните цели на стратешко ниво претставуваат конкретизација на општите и посебните цели, врз чијашто основа се утврдуваат конкретните задачи на

¹ Големината на целта може да се одреди во екстремни граници и тоа во својот максимален или минимален износ, во задоволувањето на горната или долната граница или преку фиксирање одредена вредност.

² Со нив се насочува подготовката и оспособувањето на потсистемите за спроведување специфични одбранбени активности (оние за кои се организирани и надлежни), работи во областа на одбраната, обуката, школувањето, подготовката за водење на вооружена борба и друго, што се заедно се остварува во мир и во воена состојба.

планирањето, со што до израз доаѓа нивната практична употребливост. Заради обезбедување единственост во планирањето и во развојот на одбраната, стратегиските цели натаму, се разработуваат и се конкретизираат во цели на планирањето на оперативно и на тактичко ниво (Ѓорески В., 2005).

На оперативно ниво, целите на планирањето се во функција на насочување на задачите, потребите и можностите за развој, на елементите на потсистемите на одбраната, односно на посебно организирани сили за одбрана на оперативно ниво. И овие цели во принцип, се разработуваат на општо, на посебно и на поединечно ниво. Оперативните цели мора да се усогласени со стратегиските, како и во нив да се содржи насоката, односно идејата за целите на тактичко ниво (Ѓорески В., 2005).

На тактичко ниво целите на планирањето служат за конкретизирање на развојот на одбранбениот систем и подготовките на извршителите во планирањето на одбраната и на силите и на средствата на посебно организирани сили за одбрана на тактичко ниво. Истите (тактичките цели) задолжително се во согласност со повисоките (оперативни) цели и тие можат, исто така, да бидат општи, посебни и поединечни (Ѓорески В., 2005).

5.2. Задачи на планирањето

Задачите на планирањето произлегуваат од утврдените цели и претставуваат нивна конкретизација. Задачите на планирањето се усогласени со објективните можности за реализација и се конкретни во однос на мерките и средствата за реализација. Тие конкретно се однесуваат на *кој, каде, што, како и кои* активности и акции треба да се преземат за да се остварат поставените цели (Станковиќ Т., 2004).

Планирањето има повеќе задачи кои сублимирано може да се изнесат во неколку елементи, и тоа:

- ◆ релативизација на конфликтноста на развојните цели во општеството во целина;
- ◆ намалување на неизвесноста во остварувањето на поставените цели на развојот;
- ◆ максимизирање на позитивните разлики од екстерните фактори и слично (Гоцевски Т. и Бакрески О., 2005).

Во основа, задачите се остваруваат преку одредени активности во утврден временски интервал.³ Во однос на нивото на планирањето, зада-

³ Целите можат да бидат формулирани во општи термини, додека задачите се дадени во точно утврден резултат кој мора да се оствари во одреден временски интервал.

чите може да бидат стратегиски, оперативни и тактички, а пак тие општи, посебни и поединечни (Станковиќ Т., 2004). Задачите на планирањето на највисокото ниво (стратегиско) се усогласуваат според централното ниво на хиерархија, додека, пак, задачите на планирањето на оперативно ниво се усогласуваат на различни нивоа во организационата структура, односно помеѓу организационите делови во рамките на сите нивоа на организирање во процесот на планирање. Остварувањето на задачите на стратегиско ниво треба да ги овозможи рационалните претпоставки за ефектуирање на планираните задачи кои се врзуваат со задоволување на потребите на организацијата.

Во областа на безбедноста треба да се напомне дека задачите на планирањето се утврдуваат и се спроведуваат со редица на детерминирачки претпоставки кои укажуваат на комплексното опкружување и влијание на одредени фактори кои се важни за реализирање на безбедносните цели.

6. ПРОЦЕС НА ПЛАНИРАЊЕ

Процесот на планирање во одредена институција, може да започне со многу прашања, дилеми и многу нејаснотии за тоа: „Што треба да се опфати со планирањето?“ и „Дали за тоа ќе се подготват соодветни одговори?“.

Со процесот на планирање се обидуваме да ги поставиме основните определби за насоките и за идентификуваните потреби. Исто така, во процесот при подготвување и при донесување плански одлуки треба да се направи потребната разлика меѓу доброто и лошото планирање, меѓу извршувањето и неизвршувањето на работите, како и да се обезбеди синхронизираност на одделните размислувања како и кога да се дејствува на вистински начин.

Процесот на планирање условно се состои од пет елементи. Секој од овие елементи се надополнува еден со друг, а најилустративно овој преглед е прикажан во моделот што следи:

1. *Поставување примарни цели и меѓуцели.* Личниот придонес на раководните луѓе влијае врз примарните цели. Поставувањето цели, на пример, во безбедносниот сектор се прави од страна на носителите на раководни функции во овој сектор. Меѓуцелите помагаат да се разјаснат примарните цели и најчесто се поставувани од пониските нивоа на управување.
2. *Истражување можности.* Истражувачкиот елемент е насочен кон собирање податоци и се фокусира кон откривање на можностите што ги нуди средината, а генерално се примарни за спроведување на понатамошните активности.

3. *Формулирање планови.* Тие што се задолжени за формулирање на плановите најчесто се квалификуваат себеси како планери без кои не може да се движат процесите, бидејќи тие имаат способност да ги претворат можностите откриени преку истражување, во соодветни стратегии и политики кои се насочени кон главните цели и кон меѓуцелите.
4. *Поставување на цели.* Добро поставените цели им помагаат на вработените себеси да се идентификуваат преку организацијата, ги мотивираат со редуцирање на несигурноста и им разјаснуваат што треба да постигнат. Недостатокот на чиста цел може да го оштети остварувањето. Целите најчесто ги поставуваат стручни и оспособени луѓе што ги предвидуваат активностите во пошироките планови преку конкретизирање и преку детализирање на конкретното време и многуте субјекти (одлучувачи и реализатори).
5. *Последица од планот.* Најчестата последица на планот се гледа во крајниот резултат. Ако постои механизам што може да потврди дека вистинската изведба како крајна секвенца во планирањето одговара на пресметаните активности, тогаш може да се каже дека планирањето ја остварило својата цел. Постојаните проверки на планот се во насока на утврдување дали планот навистина резултира со изведба во согласност со оригиналното, претходно размислување.

Генерално, фазите на процесот на планирање може да се групираат на следниот начин:



Извор: Гоцевски Т., *Образовен менаџмент*, Македонска ризница, Куманово, 2003, стр. 251

За да може планирањето да одговори на сложените предизвици кои му се поставуваат како задача, како што се: утврдувањето на целите, политиката, стратегијата и начините за остварување на поставените задачи, процесот на планирање мора да има определен логички редослед. Тој редослед би бил: (Стаменковски А., 2004)



7. УСЛОВИ ЗА УСПЕХ НА ПЛАНИРАЧКИОТ ПРОЦЕС

Во однос на условите од кои е детерминиран управувачкиот процес во литературата може да се идентификуваат следните критериуми за успех на планирачкиот процес, и тоа: партиципативен, континуиран, координативен, интегративен и експериментален.

Првиот критериум (партиципативен) се однесува на учеството во планирањето. Тоа значи дека во планирачкиот процес треба да учествуваат сите оние што на некаков начин може да придонесат кон остварување на целите на организацијата. Ефективното планирање не може да произлезе самото од себе или од самата организација, туку мора да биде резултат на ангажирањата во самата организација. Оттука, улогата на планерот не треба да се врзува за планирањето, туку тој треба да овозможи повеќе луѓе да се ангажира повеќе во процесот на планирање.

Вториот критериум посочува на тоа дека планирањето треба да биде *континуирано*. Заради амбиентот во кој се наоѓа самата институција и динамичноста на средината плановите мора да се дизајнирани да помогнат во извршување на главните стратегиски цели и задачи, а

тоа значи дека тие континуирано треба да се ажурираат и да се усогласуваат на новите околности.

Третиот критериум во основа е координативен. Овој критериум претпоставува дека активностите во одредена институција/организација треба да се планираат независно во рамките на одделни организациони единици, но сепак ниту една активност не треба да биде планирана во целосна независност од другите активности. За да се оствари оваа претпоставка потребен е одреден степен на координација на потребните активности. Координирањето се случува во временска димензија, бидејќи еден вид работа треба да се изврши пред следната да може да биде извршена.

Четвртиот критериум е интегративен и зависи од степенот на меѓузависност на луѓето во самата институција или орган. Кога е потребен повисок степен на реализација на задачите тогаш е потребен висок степен на интеграција за да може поефикасно да се реализираат задачите со помали интеракции.

Петтиот критериум е експерименталниот. Тој добива на значење во услови на забрзан техничко-технолошки развој кога динамиката и начинот на живеење се детерминирани од современите услови за работа, а праксата покажува дека искуството повеќе не е најдобриот учител. Според тоа, искуството треба да биде надополнето со експериментирањето, односно со дизајнирани и контролирани експерименти. Тоа ќе предизвика брз, целосен, флексибилен и релевантен фидбек.

8. ПРЕДУСЛОВИ ЗА ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИЦИ

8.1. Предвидувањето како предуслов за ефикасно планирање и за процена на ризици

Предвидувањето претставува мошне сложена и тешка задача, а истовремено и извонредно одговорна, бидејќи квалитетот на претпоставките на идниот амбиент зависи од квалитетот и успешноста на поставените цели, политика и плански акции. Ова дотолку повеќе што во современите услови за живеење и работа промените се мошне брзи и сè повеќе се непредвидливи. Затоа предвидувањето мора да се заснова на истражување на минатото и сегашноста (Стаменковски А., 2004).

Етимолошки, терминот предвидување потекнува од грчкиот збор (gnosis) знае, со значење дека треба однапред да се добие претстава за нешто за што се претпоставува дека ќе се случи.

Во литературата се среќаваат бројни дефиниции за тоа што претставува предвидувањето. Од нив ќе бидат презентирани некои за кои се смета дека се покарактеристични.

Под поимот предвидување се подразбира „логички и психолошки процес за изведување на синтетички искази за можната, но сè уште неизвесна состојба создадена од конјуктура на изрази за почетните и граничните услови“ (Ристиќ Ж., 1983).

Дефиницијата што ја објаснува потребата од предвидување, а не ги обработува суштинските, содржинските и методолошките аспекти на предвидувањето истото го дефинира како „сервис чија намера е да понуди најдобра корисна основа за управување со иднината“ (Milne E.T., 1975), или под предвидувањето се подразбира антиципативно согледување на функционирањето и развојот на некоја разгледувана појава која се базира на рутинско познавање на нејзиното функционирање и развој во некој изминат период, како и на интуицијата во врска со можностите и условите за нејзиното функционирање во иднина (Периќ Ж., 1980).

Некои автори поимот предвидување го дефинираат како истражување на иднината со цел да се дојде до позначајни претпоставки, односно ставови за релативноста и природните дејства (екстерните и интерните фактори на идните работни потфати), (Милисављевиќ М. и Тодоровиќ Ј., 1987).

Во литературата се среќава и компромисна дефиниција во која „предвидувањето вклучува подготвување извештај, однесувајќи се на несигурните и непознати случаи, а главната намена на предвидувањето е да прибави знаење за несигурните настани кои се важни за нашето сегашно одлучување“ (Sullivan G. William-Wayne W. 1977).

Предвидувањето, исто така, се дефинира како збир на акции што се преземаат за определување на идните состојби и идните настани во системот и околината во која системот егзистира, (Михајлов К., 1971)⁴ или пак, предвидувањето се дефинира како „активност што ја проценува вредноста на непознатите варијабли во иднината со вредноста на варијаблите, кои се сега познати“, а пак, од аспект на системот на информации предвидувањето се дефинира како „обид за создавање мост меѓу податоците што би сакале да ги имаме, но не можеме да ги добиеме директно“.

Значи, предвидувањето претставува една од најважните задачи на истражувањето бидејќи со него, со примена на научни методи, се врши проценка, односно се прави прогноза⁴ за идните настани (Стамен-

⁴ Некои автори поимот предвидување го поистоветуваат со изразот прогноза, па поимот предвидување го користат како синоним за прогноза. Поимот прогноза потекнува од грчкиот збор *prognosis* (претходно знаење, сознание) и се објаснува како „одредување на исходот од некоја состојба која е веќе во тек или се очекува однапред прескажување и донесување заклучок, или како

ковски А., 2004). Тоа претставува умствен процес и свесно заснована стручна дејност на прогнозирање на идното дејство на факторите на работење и на исходот на саканата акција со цел да се намали неизвесноста и ризикот при подготвување и донесување одлуки.

Врз основа на презентираниите дефиниции за предвидувањето, во литературата се формулираат следните констатации:

1. Иако предвидувањето како процес и дејност веќе подолго време се практикува во економските истражувања, сè уште не е дефинитивно расчистено прашањето за тоа што тоа претставува. Во прилог на оваа констатација зборува многубројноста и разновидноста на дефинициите што се однесуваат на разгледуваното прашање.

2. Во одредени случаи предвидувањето се дефинира како сервис, како извештај за непознатите настани, како активност за проценување на непознатите променливи, како анализа на различно поставени податоци и информации, или дека се прави во форма на извештај.

3. Како издиференциран став што доминира кај најголем дел автори е дефинирањето на предвидувањето од аспект на намената за која служи. Според концепцискиот приод, целта за која служи предвидувањето претставува основа за квалитетно и рационално подготвување и донесување одлуки, средство за управување со иднината или намената е да се намалат ризиците при подготвувањето и донесувањето на стратешки и тактички одлуки.

4. Независно од кој аспект се дефинира и се детерминира предвидувањето, изнесените дефиниции се парцијални зашто опфаќаат само одделни компоненти од структурата на предвидувањето. Во некој од нив, предвидувањето се дефинира во потесна смисла на зборот.

5. Во литературата преовладува содржински или концепциски приод при детерминирање на предвидувањето (со забелешка кон тие дефиниции дека им недостасува уште една компонента, а тоа е исходот на саканиот тек на акции во така предвидениот тек), а помалку е застапен методолошкиот приод. Содржинскиот приод кон предвидувањето ги објаснува прашањата во поглед на тоа што се предвидува и зошто се предвидува. За разликата од концепцискиот период, во теоријата е разработен и методолошкиот период, кој за појдовни основи ги има објаснувањата за начинот на предвидување, односно како треба да се предвидува за да се оствари поставената цел и со што се предвидува.

„предвидување на траењето и исходот од некој одреден процес или активност што е засновано на утврдени податоци“. Произлегува дека прогнозата е повеќе неутрален и пасивен напор на полето на истражувањето на иднината, додека предвидувањето е насочено кон подготовка на базата за планирање.

6. Не е прифатливо стојалиштето според кое предвидувањето е резултат на наднормални способности на некои луѓе, односно засновано врз рутина и интуиција. Авторите при дефинирањето на предвидувањето не поаѓаат од определување на суштината (поимот, содржината и значењето), туку појдовна основа е техниката на предвидувањето и лицата што го спроведуваат. Исто така, не е прифатливо презентираниот дефинирање на поимот прогнозирање, според кое промените на проучуваната појава се условени од дејството на внатрешните фактори, а индиректно неговото разликување од поимот предвидување.

7. Во последно време, секако под влијание на теоријата на системите, иако многу ретко, забележливи се почетните чекори во дефинирањето на предвидувањето од системски аспект. Исто така, забележливо е дефинирање на предвидувањето од аспект на теоријата на информации (од аспект на местото, улогата и значењето на предвидувањето за информативниот систем, како мост меѓу сегашноста и иднината, односно како мост меѓу сегашните и идните податоци што би сакале да ги имаме).

8. Поаѓајќи од изнесените дефиниции и детерминирање на предвидувањето се прави обид да се даде покомплексна, посуштинска и посодржајна дефиниција. Дефиницијата на предвидувањето, од аспект на суштината, би требало да ги опфати следните елементи: а) поим, дека предвидувањето е мисловен процес, а едновременно и стручна дејност; б) содржина, тоа се факторите на работење, кои по својата природа и место на локација, може да бидат внатрешни и надворешни и исходот на саканиот тек на акции во така предвидениот иден амбиент на работење; в) значење, за намалување на неизвесноста и ризикот при подготвување и донесување одлуки, т.е. систем и средство за управување со иднината (Шуклев Б., 2002).

8.1.1. Фактори кои влијаат на предвидувањето

Тргувајќи од фактот дека предвидувањето мора да се темели на располагањето сознанија за минатото и сегашноста, тоа никогаш не може да ја покаже точно иднината. Точноста на предвидувањето зависи од временскиот период за кој се изработува прогнозата. Постојат повеќе фактори кои го определуваат степенот на точноста, и тоа: неадекватен базен приод од причини што предвидувањето се заснова на историски околности; неочекувани настани, како што се меѓународните кризи, елементарните непогоди и сл.; опфатноста на предвидувањето, односно колку предвидувањето опфаќа поголем број појави или подрачја, постои поголема точност и обратно; должината на предвидувањето што

значи колку подолг период на предвидување, толку грешката може да биде поголема итн. (Стаменковски А., 2004).

Сепак, целта на предвидувањето не е одредување апсолутна точност на однесувањето на истражуваните појави во иднина, туку на точноста и прецизноста на предвидувањето влијаат голем број фактори. Основни се:

1. Временски период на предвидување. Временската димензија на планирањето е особено значајна, бидејќи со поставените цели се одредува иднината, а средствата со кои тоа се остварува се разликуваат во моментот на планирањето (моментот на започнување на планската акција) и во целиот плански период до моментот на остварување на целите. Во основа, ако се предвидува за подолг временски период тогаш е дозволено недоволно прецизно предвидување, но не е дозволено задоцнето предвидување, ниту е прифатливо да се воочат пропусти во процесот на предвидување. Од наведените прилози може да се заклучи дека од степенот на успешното предвидување зависи и успешното планирање и реализација на планските одлуки во иднина.

2. Стабилност на факторите и условите во опкружувањето. Ова значајно ја зголемува извесноста на предвидувањето за однесување на одреден систем во иднина. Наспроти тоа, во услови на чести промени во политиката на земјата, се намалува и извесноста на предвидувањето, воопшто.

3. Степен на можното влијание на работниот систем во опкружувањето и методите кои се користат во предвидувањето. Познато е дека поголемите работни системи по правило имаат поголемо влијание на однесувањето на факторите на опкружувањето, па според тоа имаат поголема можност за извесни предвидувања за иднината и обратно. Од друга страна, изборот на адекватните научни методи за предвидување значајно го зголемува бројот на добиените резултати од предвидувањата за иднината (Станковиќ Т., 2004).

8.2. Информациската како неопходен предуслов за планирање и за проценка на ризици

Информацијата несомнено е синоним на знаењето и таа е пошироката основа на организираноста, среденоста и поврзаноста на деловите во системот т.е. таа се идентификува со знаењето што некој го употребува за да оствари одредена цел.

Располагањето со навремена, точна и издржана информација значи остварување на зацртаната цел, односно ако вистинската информација се искористи во вистинско време и на вистински начин

тогаш таа може да биде најсилно оружје во рацете на тој што ќе ја поседува. Со други зборови, постоењето вистинска и брза информација значи дека планираните задачи ќе се реализираат во целост и дека информацијата како своевиден податок за одредена состојба, селектирана, анализирана и интерпретирана ќе го има главниот збор при донесување одредени одлуки. Значи, од информираноста, односно од неинформираноста во голема мера зависи ефикасноста на процесот на планирање. Оттука, не е сеедно каква информација ќе добие одредена институција, ниту е небитен одговорот како соодветната институција откако ќе ја добие потребната информација ќе се однесува и како ќе ја искористи, затоа што од овие претпоставки во голема мера зависи и одлуката за функционирањето на самата институција.

Информациите се предуслов и резултат на одлучувањето. Без потребните сознанија, податоци, параметри, невозможно е да се донесе одлука. Од друга страна, резултатот на одлучувањето – одлуката како предуслов за акција, исто така, е информација (Кралев Т., Скопје, 2007, стр. 86). Оттука, секој систем, пред сè човекот, се бори за точни, квалитетни, комплетни, навремени и корисни информации. Информацијата со вакви карактеристики ја намалува неизвесноста. Ако ја зголемува неизвесноста, тогаш таа е лоша, некорисна информација. Но постојат различни комбинации за карактеристиките на информациите. На пример, информациите може да бидат точни, но некомплетни со што ќе го дезориентираат корисникот. Може да бидат точни, но ненавремени со што нема да ја имаат очекуваната вредност за корисникот. Можат да бидат точни, но некорисни, доколку се претставени во поголем обем или пак на начин неприфатлив за корисникот итн. (Поповска З., 2006, стр. 113).

За да го разбереме значењето на информацијата најнапред започнуваме со поширока елаборација на термините кои најчесто се користат како синоними. Тоа се термините: симболи, податоци, информации и знаење.⁵ Симболите ги користиме најшироко како букви, бројки, кодови и други знаци. Потоа, следат податоците кои според некое правило претставуваат комбинација на симболите. Од семантички аспект, податок е сè она што е меморирано (чувано, регистрирано), но не е искористено, меѓутоа постои веројатност да се искористи. Кога

⁵ Се смета дека најсоодветен хиерархиски редослед на термините е следниот: податоци на најниското ниво, следат информациите, потоа интелигенцијата (правила), знаењето (комбинација на податоците и информациите) и мудроста на највисоко ниво, во Barraba V., and Zaltman G., *Hearing the Voice of the Market*, Harvard Business School Press, 1990.

податокот ќе се искористи, станува информација.⁶ Доколку податокот има карактеристика на новост, тогаш се зборува за вест. По податоците следат информациите. На прашањето: „Што се информациите?“, се добиваат многубројни одговори. И покрај разликите во дефинициите, како суштествени за поимањето на информациите најчесто се вклучуваат новоста, корисноста и релевантноста. Доколку некој каже „економските науки не се исто со безбедносните науки, студентот по економија нема да прими информација, туку само сознание за апсурдноста на исказот“. Но, ако некој му каже за правците на развојот на економската наука, тој ќе прими информација, бидејќи исказот содржи новост. Од друга страна, сè што се прима како новост, не се користи веднаш, бидејќи корисноста е поврзана со одредена промена, задача, цел. Информацијата е релевантна вест само кога носи знаење на корисникот за да може да го промени неговото однесување, став, мислење и да реши некоја задача (Поповска З., 2006, стр. 111-112). Во однос на знаењето, особено човековото знаење, тоа се создава низ перманентниот процес на креирање, пренесување, обработка, чување и користење на информациите. Знаењето се состои од преносливи, но и од непреносливи информации, како и од кодифицирани, но и од тие кои не можат да се кодифицираат, бидејќи се резултат на високата експертска и имагинативна творечка сила на човекот. Затоа најшироката дефиниција за знаењето која е и најсоодветна потенцира дека „знаење е она што служи за да биде искористено при одлучувањето“ (Поповска З., 2006. Во литературата постојат различни дефиниции за поимот информација. Сите тие во основа го имаат феноменот на осознавачки процес од кој произлегува поимно одредување на информацијата најчесто како „капацитет за зголемување на знаењето“ (Лазаревиќ В., 2002). Ќе наведеме неколку често користени дефиниции:

- Информација е процес и своевидна активност на комуницирање, информирање, значи да се пренесе знаењето некому. Во потрага по информација се задоволува потребата да се пополни знаењето. Доколку некој податок, или мноштво податоци кои сме ги примиле не го зголемат нивото на нашето знаење, тогаш тие податоци не претставуваат информација.⁷
- Информацијата е значење и таа е поврзана со формата. Буквално, „да се информира“ значи „да се даде форма на

⁶ Податокот се дефинира како неанализиран факт или настан врз кој се развива самата информација. Врз основа на оваа рационална претпоставка податоците се средство за изразување на информациите.

⁷ <http://www.poslovnaznanja.com/objavljeni-autorski-tekstovi/e-magazin/11-sta-je-informacija-definicija-informacionog-dizajna.htm>

нешто“. Најпрво, информацијата мора да биде содржана во некаква форма и да се пренесува или во материјален систем (пр. печатена страница) или во некоја енергија (радиобран). Воопшто, чиста форма сама по себе не постои, туку мора да е во опстанок на некаков вид материјална или енергетска база; поради ова информацијата мора да биде пренесена на некаква база (Бохм Д., 1989).

- Информацијата е резултат на поседување на знаење и им е потребна на тие што ја немаат. Информациите кои на никому не им се потребни тие се беспредметни и немаат никаква вредност (Урош С., 2006, стр. 107).
- Информација е ново знаење кое влијае на корисникот за да го промени своето однесување или му користи за да оствари некоја цел или за да реши некоја задача (Поповска З., 2006, стр. 112).
- Информација е збир на податоци, знаење или претстави за еден систем што го прима друг систем, односно информацијата е ново знаење за некој настан, процес, појава или објект што му овозможува на примателот да преземе целнонасочна акција (Поповска З., 2006, стр. 112);
- Информацијата претставува интерпретирани податоци кои го менуваат разбирањето на примачот, односно информацијата е наменски насочено знаење, при што намерата е да се подготви однесувањето дека информација се оние делови од веста кои за примачот имаат вредност на новост/новитет (Шуклев Б., 2002, стр. 264);
- Информацијата значи собирање на знаење (податоци) и пренесување на знаење (Кралев Т., 2007, стр. 87);
- Информацијата е содржината на она што го разменуваме со надворешниот свет, додека му се приспособувањето и додека влијаеме на него со своето приспособување (Винер Н., 1964, стр. 3-15);
- Информацијата е дел од знаењето со кое се намалува или се отстранува неодреденоста на системот и неизвесноста на промените (Поповска З., 2006, стр. 113).

Од наведените дефиниции може да се констатира дека информацијата е врвна општествена употребна вредност, Основен стратегиски ресурс, главен инпут на секоја човекова дејност и главен развоен фактор, кој е поважен дури и од материјалниот фактор (Стојановиќ П., 1964, стр. 3-15). Како таква таа се прима заради некоја цел, односно таа е основа за донесување одлука која е во функција на дадената цел. Донесувањето на одлуката и целта се одредени во

време. Доколку информацијата се прима за време на случување на некој настан т.е. во време на донесување одлука, тогаш таа има константно реална вредност, бидејќи овозможува реализација на целта во тоа време. Доколку информацијата се прима порано, пред да се случи настанот, пред да се донесе одлуката, таа има максимална вредност, и обратно, ако информацијата се прима подоцна, по случувањето на настанот, по донесувањето одлука, таа има минимална вредност т.е. нема практична вредност. Треба особено да се истакне дека информацијата, покрај директната вредност, може да се анализира и како ресурс што го олеснува управувањето со останатите ресурси и тоа само ако е доставена на вистинска личност во вистинско време и во вистински облик. Кратко речено, информацијата има вредност само ако го надополнува постојното знаење, инаку во спротивно таа е неважен податок (Jakson J., 1986). Значи, информацијата да биде корисна, таа треба да биде новост, односно да се приспособува на околината.

Значењето на информацијата расте со сè поголемите промени во окружувањето како и со техничко-технолошкиот развој. Информациите денес претставуваат еден од важните извори на моќ. (Joseph L. Massie, 1987, pp.126-130). Со растењето на бројот на информациите и нивните извори, доаѓа до нивно испреплетување на сите нивоа. Силните системи реализирани во комбинација на силни сметачки техники и телекомуникациски технологии, постоење електронска размена, употребата на сателитите и оптичките влакна овозможува раст на информатичкиот сектор до невидени размери. Според тоа, слободно може да се каже дека гледано од аспект на структурните промени секторот за обработка на податоците спаѓа во најбрзорастечките сектори и има најголеми екстерни ефекти (Миличевиќ В., 2002, стр. 92).

8.2.1. Информации за планирање

Праксата укажува на логичната меѓузависност на процесот планирање и информирање. Планирањето не може да биде ефикасно ако не се заснова на добар систем на информирање. Имено, ако планирањето се сфати како антиципативно одлучување, тогаш важно е да се знае дека преку информациите кои носат пораки за сегашноста и иднината се намалува ризикот и неизвесноста при донесувањето плански одлуки. Со планирањето во основа се предвидува какво ќе биде однесувањето на системот во иднина, па според тоа и потребата за информации за неговата состојба е поголема ако и предвидувањата се подолгорочни, а квалитетот на бараните информации поригорозни заради неизвесноста која постои секогаш во предвидувањето. Квалитетот на планските одлуки е определен од квалитетот на информациите врз основа на кои се донесени. За планските одлуки потребни се покрај информации за идните настани и информации во врска со

реализацијата на планските одлуки. Планската одлука е поквалитетна кога информациите се навистина релевантни за решавање на проблемот за кој се донесува одлуката. Многу е поедноставно да се обезбеди информација за оперативно и тековно планирање, отколку за среднорочно и долгорочно планирање, односно лесно е да обезбедиш информација за она што било и за она што се случува, а потешко за она што ќе се случи (Станковиќ Т., 2004, стр. 82-83).

Имајќи предвид дека добар дел од информациите за планирање се однесуваат на многу долги временски интервали, често не е ниту можно, ниту неопходно инсистирањето на одредени детали. Носителите на планските одлуки во поголем број случаи ќе мора да се задоволат со трендовите. Тоа е поважно за навремено донесување планска одлука од детални податоци кои ќе доведат до задоцнето донесување на планската одлука (Станковиќ Т., 2004, стр. 83).

За добро планирање не е доволно да се задоволи основниот предуслов, а тоа е постоење соодветна информација. Покрај поседувањето бројни информации, особено е важно како тие ќе циркулираат, односно како ќе се пренесуваат т.е. какво ќе биде меѓусебното информирање. Меѓусебното информирање е особено значајно затоа што многу е важно како ќе биде пренесена информацијата и како таа ќе биде разбрана. Постојат повеќе начини на меѓусебно информирање, и тоа:

1. внатрешно и надворешно;
2. итно, дневно и периодично;
3. текстуално, усно и комбинирано.

Внатрешното информирање е од особено значење. Доброто планирање и ефикасната работа во самиот орган/институција се невозможни без квалитетно внатрешно информирање. Врз основа на квалитетни информации и извештаи се донесуваат вистински одлуки, а врз основа на реализација на одлуките се менува безбедносната состојба, појавите и случувањата на кои се однесуваат информациите и извештаите. Според тоа, ако нема безбедносни известувања, нема да има ниту безбедносни мерки и дејности, или тие нема да се преземаат таму каде што се потребни и тогаш кога се потребни (Савиќ Ј., 1991, стр.15). Внатрешното информирање од една страна, подразбира информирање внатре во самата институција и тоа во соодветниот орган се уредува со посебни прописи, со кои се утврдува самата постапка околу тоа кој, како, кога и кому му се дистрибуираат потребните информации, додека од друга страна, надворешното информирање подразбира размена на информации меѓу организационите единици на одреден орган, а опфаќа и информирање на јавноста за активностите и за работата на органот (Стевановиќ О., 1999, стр.146).

Итното информирање се обезбедува со доставување итни информации (по телефон, со радиоврска, или на друг начин), со податоци за случувања или појави со кои се располага веднаш по сознанието за нивното настанување и со податоци за преземените мерки. По правило, итните информации се доставуваат преку дежурните служби, заедно со паралелно информирање на функционалните раководители на повисоко ниво на раководење (Стевановиќ О., 1999, стр.146-147). За разлика од итното информирање, дневното информирање се сведува на изработка и доставување дневни извештаи или билтени за одредени случувања кои можат да бидат прикажани и квантифицирано низ бројки, додека периодичното информирање опфаќа одредени секвенци или периоди за кои се прави и соодветен приказ на случувања и појави.

Планирањето може да биде текстуално, усно и комбинирано, а тоа е условено од моменталната ситуација која укажува на поголемо испреплетување на проблемите. Исто така, треба да се потенцира дека овие форми на информирање може да се реализираат и преку средствата за врски со што се олеснува и самото проследување на информациите.

8.2.2. Информациски систем на планирање

Информацискиот систем и работењето се во непосредна врска и зависност од опкружувањето. Поврзаноста со опкружувањето е двојна и се изразува преку информациите што влегуваат (тоа е влијание на околината како систем врз внатрешниот систем на информации како потсистем или т.н. центрипетално движење на информациите) и преку информациите што излегуваат (влијание на потсистемот врз системот-опкружување или т.н. центрифугално движење на информациите) (Шуклев Б., 2002, стр. 262).

Во основа, информацискиот систем за планирање во организацијата претставува формален и во поново време компјутеризиран систем за обезбедување неопходни информации кои се користат во процесот на планирање и донесување одлуки. Тој вклучува повеќе елементи: пишувани документи, архива, дописи, записи, извештаи, билтени итн. На ова се надоврзуваат и техничките системи: компјутерот, факсови, електронска пошта, електронски информации, телеконференции итн. Според структурата и карактерот тој претставува комплексен организациски систем, при што таа комплексност се однесува како на составот на елементите, така и на нивната врска внатре во системот и со опкружувањето (Станковиќ Т., 2004, стр. 91).

Во рамките на информацискиот систем може да се направи поделба на информацискиот систем на три дела, и тоа:

- информативна база како збир на сите текови на информации и комуникации;
- квантитативни и други модели, методи и постапки и
- сметачки и други машини и уреди (Кралев Т., 2007, стр. 88).

Основната цел на информацискиот систем е насочена кон создавање предуслови за подобро функционирање на одреден систем. Врз основа на тоа може да се дефинираат редица задачи на информацискиот систем од кои поважни се следните:

- 1) создавање адекватна база на податоци и информации за потребите на оптималното информирање на субјектот на одлучување;
- 2) развој на методите на научно одлучување и создавање поддршка на процесот на планирање и одлучување; и
- 3) воспоставување оптимална организација на извршување на информациски дејности (Станковиќ Т., 2004, стр. 92-93).

Информацискиот систем кој е приспособен на потребите на планирањето го зголемува степенот на благовремено реагирање на промени. При неговото проектирање за потребите на планирањето треба да се води сметка за специфичностите на информациските барања, природата на одделни извори на информации, како и дали користа од предложениот систем ги оправдува направените трошоци. Генерално гледано, во планирањето, управувачкиот информациски систем помага во чување, интеграција и издвојување на податоците кои се собираат од интерното и екстерното опкружување и од кои се изведуваат плански претпоставки и се развиваат сценарија. Нивната предност се гледа и во тоа што овозможуваат меморирање на големи количини на податоци кои лесно можат да се ажурираат и на кои може лесно и брзо да им се пристапи за да може да се донесуваат навремени одлуки со помалку неизвесност. Исто така, значајно ја зголемува брзината на работата и комуницирањето, дејствувајќи позитивно на квалитетот на донесените одлуки и ја подобруваат продуктивноста и вкупната ефикасност на управувањето (Станковиќ Т., 2004, стр. 92-93).

III глава

СИСТЕМИ, РИЗИЦИ И СИСТЕМСКИ ПРИСТАП

1. ОПШТО ЗА СИСТЕМИТЕ

Во секојдневниот живот, многу често, свесно или несвесно, во различни контексти и за различни потреби го употребуваме поимот „систем“, кога зборуваме на пример, за општествен систем, економски систем, правен систем, социјален систем, образовен систем, информациски систем, безбедносен систем, систем за кризен менаџмент, систем за заштита на граѓаните, материјалните добра, и слично, но најчесто тој поим се користи без да се обрне особено внимание на неговото етимолошко значење и што под тој поим попрецизно се подразбира.

Употребата на поимот систем не е новина ниту во теоријата ниту во праксата. Неговото изворно значење доаѓа од грчкиот збор „система“ што значи, составено од делови, целина или збир на елементи. Можеби и затоа во различни научни дисциплини со поимот систем се означуваат најразлични зборови на делови и компоненти на некоја целина. Во досегашната научна теорија, а во зависност од потесната цел и намена, постојат многу толкувања и определувања на поимот систем, меѓутоа некоја општо прифатена дефиниција не се издвојува.

Така за познатиот кибернетичар и основоположник на општата теорија на системите Рос Ешби, системот претставува „листа на променливи кои треба да се земат предвид“. Според Т. Гоцевски, системот може да се дефинира „како целина (множество) на елементи од материјален, општествен, информациски или друг карактер, кои се наоѓаат во постојана интеракција, односно целина која е единствена според својата структура и функција“ (Гоцевски Т., 2006). Од денешен аспект на гледање интересно е дефинирањето на поимот систем што го дава Герхард Маер во шеесеттите години на минатиот век, според кој „системот ја опфаќа вкупноста или комплексноста на елементите или поединечните делови. Тој има структура, реализира функции, пренесува или обработува информации и претставува збир на елементи кои се во взаемна поврзаност.“ Системите имаат одредени свои карактеристики или специфики, кои генерално се однесуваат на следното:

- Заедничка карактеристика на сите системи е дека имаат одредена структура, односно се составени од одредени елементи и дека структурната поставеност на елементите е во согласност со одредени природни закони или други однапред логички утврдени норми и критериуми.
- Елементите или деловите на системот се наоѓаат во одредена меѓусебна корелација, односно заемно си дејствуваат. Тоа за-

емно дејство во науката за управувањето со системите (кибернетиката) се нарекува интеракција. Според тоа системите не се прости збирови на различни компоненти (составни делови), туку збирови кои се наоѓаат во меѓусебни постојани врски и како такви извршуваат одредени функции, кои ги немаат или не се својствени за нивните компоненти кога се јавуваат надвор од системот и дејствуваат засебно.

- За еден систем, покрај важноста од какви елементи е составен и во какви врски се тие, исто толку е важно и во каква врска е со она што не претставува негов составен дел. Тоа што не е органски состав на системот претставува надворешна средина или опкружување на системот. Тоа значи дека системите имаат карактеристика да бидат во интеракција со своето опкружување и да трпат влијанија од надворешноста. Овие врски на системот со опкружувањето се определуваат како влез (input) и излез (output) на системот.
- Еднаш определената и поставена структура и функција на одреден систем, не е статична, односно тој е подложен на постојани промени со цел да постигне поголема ефикасност и ефективност во извршувањето на своите цели.
- Поголемите системи се карактеризираат со постоење на помали сегменти или потсистеми во нивни рамки. Основните карактеристики на ваквите големи или повеќесистемски целини се однесуваат на следното: целта на функционирањето на потсистеми е определена со општата цел на системот, сите потсистеми подлежат на единствен систем на управување кој има хиерархиска структура, постоење на разгранета информатиска мрежа за потребите на управувањето и др. Овие карактеристики особено се важни кога станува збор за безбедносен систем или систем кој целно е насочен кон заштита на животот и здравјето на луѓето, нивниот имот и останатите процеси во потесното и поширокото опкружување, бидејќи во рамките на овие системи дејствуваат мноштво субјекти кои реализираат голем број мерки, активности и задачи во определен простор и во определено време.

2. КЛАСИФИКАЦИЈА НА СИСТЕМИТЕ

Системите можат да се поделат во различни групи, видови и типови. Нивната класификација зависи од бројот и од групирањето на елементите внатре во системот, потоа од интеракциските односи и од однесувањето на посебните елементи, како и на системот во целина.

Со цел да се потенцираат некои својства кои се блиски до општите карактеристики на безбедносните и заштитните системи, во овој контекст би ја споменале следната класификација на системите: според обликот во кој постојат, според начинот на настанување, според поврзаноста со опкружувањето, според степенет на сложеност, според однесувањето, според стабилноста, според активноста и според својствата.

- *Според обликот на постоење*, ситемите можат да се поделат на реални и апстрактни системи. Реалните системи се материјално објективни, тие физички постојат и за нив може да се даде реален опис, додека апстрактните системи немаат непосредна основа во постојната реалност, тие се формални или замислени системи во човековата свест. Нивното значење е во тоа што тие претставуваат концепција за воспоставување на реалните системи, впрочем и безбедносно-заштитните системи првенствено се конципираат, потоа се обезбедува нормативно, организациско и друго уредување и се продолжува со надградба на неговата структура и компоненти.⁸
- *Според начинот на настанување*, главно системите се категоризираат како природни и вештачки системи. Природни системи се оние што настанале под влијание на природните закони, без посредство и влијание на човекот, а вештачките системи се оние што ги создал човекот со своето влијание со цел да задоволи одредена своја потреба. Во оваа група спаѓаат безбедносните и заштитните системи кои се создадени со цел за остварување на посебни интереси на поединци и заедницата.
- *Според поврзаноста со опкружувањето (околината)*, системите се делат на затворени и отворени. Затворените системи се такви во кои врските помеѓу елементите во нив прават затворена целина, без влез или излез. Отворени системи се оние што примаат влијание од опкружувањето и пренесуваат влијание на опкружувањето. Ваквите системи се во постојани интеракциски односи со околината. Системите за заштита на лица, имот и работење се отворени по својот карактер, се наоѓаат под силно влијание на опкружувањето, а исто така можат да предизвикаат силно влијание на опкружувањето.

⁸ Кога се во прашање работите поврзани со заштитата на лица, имот и работење, секако дека станува збор за организиран систем, кој во основа го препознаваме преку концепциски и нормативно-правни компоненти, институционално-организациски чинители, како и потребните човечки, финансиски и материјално-технички и други ресурси за остварување на основните и посебните цели на системот.

- *Според степенот на сложеност*, системите се делат на прости, сложени и комплексни системи. Простите системи се системи кои имаат мал број елементи и проста структура на меѓусебни врски, а сложени системи се оние системи што имаат поголем број елементи и сложена структура на врски, додека комплексни или многу сложени системи се такви системи што се составени од голем број различни потсистеми и елементи поврзани со многу сложена структура на меѓусебни врски. Од аспект на оваа тема, потенцираме дека системите за заштита на лица и имот ги имаат сите карактеристики на еден комплексен или многу сложен систем.
- *Според однесувањето*, системите се делат на детерминистички и стохастички системи. Детерминистички системи се такви системи чие однесување во текот на времето може сосема точно да се предвиди, додека стохастички системи се тие системи чие однесување не може однапред да се предвиди, туку само да се процени и да се планира неговото однесување во зависност од влијанието на промените кои дејствуваат врз него. Системите за заштита на лица и имот спаѓаат во оваа група и нивните функции се проектираат врз основа на квалитетна процена и антиципирање на состојбите на кои треба да се одговори, врз основа на однапред подготвени планови за преземање конкретни мерки, активности и задачи.
- *Според стабилноста на однесувањето*, системите можат да бидат стабилни, нестабилни и индиферентни. Стабилни системи се оние системи што имаат изградено механизми за побрзо враќање во состојба на рамнотежа од која ги извадила некоја надворешна сила на влијание, а нестабилни системи се такви системи кои немаат доволно механизми сами да се вратат во состојба на рамнотежа, туку за нивно враќање во функција потребно е преземање дополнителни активности, додека индиферентните системи се системи кои се карактеризираат по тоа што немаат постојана положба на рамнотежа. За ваквите системи секоја положба е положба на рамнотежа. Ако некое надворешно влијание ги исфрли од постојната положба тие продолжуваат во новонастанатата положба. Според оваа класификација, безбедносните и заштитините системи за да можат да ја исполнат својата функција се стремат да се најдат во првата група на стабилни системи, бидејќи секоја друга состојба доведува до дисфункција на истиот.
- *Според активноста*, системите се делат на неактивни или статички и динамички системи. Неактивни или статички

системи се оние чија состојба не се менува во текот на одреден временски период, бидејќи тие можат долго да опстанат во иста положба, додека состојбата кај динамичките или активните системи се менува со текот на времето и тие имаат цврсто поставени односи помеѓу составните елементи кои функционираат по однапред предвидени процедури, претставуваат организирани системи со одредена автономија на структурите (потсистемите), но сите активности се насочени кон исполнување на целта за која постојат. Овие карактеристики се неопходни за функционирањето на системите за заштита на лица и имот.

- *Според својствата*, системите може да се групираат во неколку видови, и тоа: саморегулативни, адаптивни, хиерархиски, неодредени, системи кои сами учат и др. Од аспект на тоа кои од овие својства би требало да ги поседуваат безбедносните системи во продолжение ќе изнесеме неколку констатации за адаптивните и хиерархиските системи. Адаптивните системи се такви системи кои можат динамички да ја менуваат својата состојба во зависност од менувањето на околностите што ги опкружуваат и нивното влијание. Ваквите системи имаат способност на флексибилност и еластичност што им овозможува да амортизираат силни влијанија врз нив и да продолжат да ја исполнуваат својата функција во изменети услови на постоење. Исто така, хиерархиските поставените системи се такви системи кај кои органите кои управуваат со неговото функционирање се распоредени во повеќе нивоа. Кај овие системи елементите кои управуваат се наоѓаат во односи кои можат да бидат подредени и надредени.

3. ХИЕРАРХИСКО УРЕДУВАЊЕ НА СИСТЕМИТЕ

Секој систем е во хиерархиски однос со некои други системи коишто се надредени или подредени во однос на него. Секој систем припаѓа на втор, а тој на трет, на четврт итн.

Хиерархијата е карактеристика на сите организирани системи. Категоријата „хиерархија“ е универзална. Затоа хиерархиски може да се третираат како материјалните така и нематеријалните нешта. Да започнеме со пример. Наутро кога ќе станете правите распоред на нештата што тој ден треба да ги направите. Имате повеќе обврски. Определуваат што ви е најважно, па помалку важно и најмалку важно. Без да сте свесни за тоа вие правите хиерархија на нештата. Потребата да ги подредувате во хиерархиски ред е услов за да се организирате. Колку повеќе нешто

треба да се заврши, толку повеќе ви е потребно хиерархиски да ги подредите и да ги поврзете (Поповска З., 2006).

Од системски аспект, хиерархијата може да се претстави како „систем во систем“ сè до она ниво каде што води влијанието на растечката комплексност. Секое ниво е пододредено од некое друго ниво (Поповска З., 2006). Според тоа, хиерархијата е организација на компоненти уредени по нивоа започнувајќи од највисокото кон најниското ниво. Значи, сите интегративни процеси започнуваат на некоја точка над нултото ниво и продолжуваат до највисокото ниво на системот. Системот на активности е заснован на поделба на работата, односно на организациски потсистеми кои треба да ги остварат поставените цели. Тоа всушност се раководителите⁹ кои се вертикално распоредени и структурно поврзани и во суштина ја претставуваат хиерархиската структура или субординациските односи. Ниту еден систем или одредена организација (полициска, воена итн.) не може да опстои без односот на субординацијата. Секоја организациона структура е во облик на пирамида, поради што е неопходно постоење на субординација, а самото тоа наложува, кога ќе се гради организационата структура да се воспостават и хиерархиски односи т.е. вертикална димензија на односи.¹⁰

Во основа, хиерархијата на системите не претставува ригидна структура, туку напротив таа е подложна на промени. Нивоата на хиерархијата се менливи и деливи. На пример, врските помеѓу две постојани нивоа може да продуцираат одреден ентитет - ново ниво помеѓу нив. Или, пак, може две хиерархиско подредени нивоа да се спојат и да се добие помал број нивоа во структурата. Хиерархиски уреден систем функционира преку мрежа на вертикални и хоризонтални врски помеѓу потсистемите на различни нивоа. Повратноста може да се остварува низ врските со различен интезитет. Ако се поврзани сите нивоа (и најдолните нивоа), значи постои хиерархија која се нарекува „мрежна хиерархија“. Таа е од интерес за управување со процесите. Доколку не мора да се вклучени најниските нивоа, таа хиерархија е немрежна хиерархија. Мрежата на врски го овозможува одлучувањето, односно управувањето што е резултат на поделбата на должностите и

⁹ Рбетот на еден хиерархиски уреден систем на раководење ја претставува структурата од различни положби, кои се пополнети со соодветен кадар од раководители. Во хиерархиската структура на организацијата главна положба има раководителот.

¹⁰ Хиерархиското уредување дава претстава за организирана структура во вид на пирамида. Пирамидата може некогаш да го асоцира на централизиција и на децентрализиција. Затоа потенцираме дека хиерархијата е пред сè ниво на сложеност на структурата (систем во систем) па затоа може да еволуира во мрежна структура.

на работата (Поповска З., 2006). Значи, таа хиерархија во структурата не е хиерархија на личности, туку, хиерархија на должности.

Хиерархиската структура е иманентна на секој организиран систем. Во хиерархиската структура потсистемите влегуваат со свои независни особини што е услов за релативна автономност. Истовремено, тие ги поседуваат и особините на системот што е услов за нивна меѓусебна координација. Обликот на хиерархијата не зависи само од бројот на нивоата, туку и од капацитетот и од способноста за одлучување на потсистемите и од квалитетот на поврзување т.е. комуникацијата помеѓу потсистемите во рамките на системот.

4. ТЕРМИНОЛОШКО ОДРЕДУВАЊЕ НА ЗАКАНИТЕ, РИЗИЦИТЕ И ЗАГРОЗУВАЊЕТО

Теориите за безбедноста, особено тие, кои безбедноста ја сфаќаат преку концептот за национална безбедност, како основен начин преку кој може во целост да се осознае природата на безбедноста го поставуваат следниот пристап:

- целосно идентификување на заканите и ризиците и природата на загрозувањето кои тие можат да ги предизвикаат и
- проценување на ранливоста, односно отпорноста на објектот кон кој се насочени заканите и ризиците.

Водејќи се од претходно изнесеното, несигурноста, односно небезбедноста на објектот (државата, заедницата, поединецот, системот итн.) претставува причинско-последична врска помеѓу безбедносните закани и ризици, од една страна и ранливоста (чувствителноста) на безбедносниот објект, од друга страна¹¹.

Вака поставениот пристап на концептот за безбедност кој е насочен кон двата битни елементи на безбедноста, а тоа се: изворот на несигурност (закани и ризици) и последиците (загрозување – вид, степен итн.), овозможува преземање на целно ориентирани активности на системите за безбедност и заштита, преку примена на политики за:

- рано откривање и проценување на актуелните закани и ризици и предвидување на потенцијалниот објект кон кој се насочени, со цел превенирање и намалување на очекуваните загрозувања и
- зголемување на отпорноста, односно намалување на ранливоста на објектите/објектот кој е изложен на конкретни закани и ризици.

¹¹ Во современиот концепт на "Risk Management", Ранливоста, како посебен елемент на ризикот има примарно значење.

Постојано поставуваното прашање во рамките на теоријата за безбедност и дефинирањето на концептот за безбедност претставува проблемот како и на кој начин да се препознае и утврди нивото на ранливост/отпорност на објектот на безбедност и како да се препознаат и да се утврдат потенцијалните закани и ризици. Приврзаниците на неореализмот го поддржуваат концептот дека ранливоста како елемент на безбедноста е појасно препознатлива и мерлива, додека заканите и ризиците и можните загрозувања претставуваат елемент кој потешко се препознава и утврдува.

Претходно изнесената потешкотија, Бузан (Buzan B.) ја поврзува со две причини:

1) Субјективната перцепција која се јавува кај поединецот/индивидуата, кога станува збор за индивидуалната или колективната безбедност и можноста одредени закани и ризици кои се доминантни во нивната безбедносна агенда да немаат вистинска реалност, односно можноста за постоење на претеран страв од некои загрозувања,

2) Можноста, односно неможноста да се издиференцираат сериозните или егзистенцијалните закани од нормалните или прифатливите, кои произлегуваат од секојдневното живеење и функционирање на сите сфери на општеството.

Заради целосно разбирање на местото и улогата на заканите, ризиците и загрозувањето во теоријата за безбедност, како и нивно соодветно применување во сеопфатниот процес на управување со безбедноста на системите, во продолжение ќе биде даден посебен осврт на секој од овие елементи.

4.1. Заканите по системите

Природата на современите закани тешко се објаснува ако како појдовна основа се земе единствено сознанието кон кој субјект (држава, систем поединец, група, и сл.) тие се насочени, без да се има предвид поширокиот контекст во кој заканите се случуваат, односно без анализа на околностите.

Во тој контекст, причините за појавата на новото безбедносно опкружување не се поврзуваат само со исчезнувањето на биполарниот безбедносен свет, туку и со модернизацијата на светот, која покрај големите позитивни придобивки донесе и многу негативни, кои во концептот на безбедност се вградуваат како елементи на *ризично општество* (risk society) и ја отворија потребата од појава на нови безбедносни провајдери кои ќе се справуваат со новите закани.¹²

¹² Појавата на новите безбедносни провајдери, всушност значи појава на нови институции и агенции, кои во согласност со воспоставена правна, организа-

Во рамките на теоријата која се занимава со проучување на проблемот на современите безбедносни појави, многу тешко се наоѓа целосно раздвојување на значењето на термините закана (threat) и ризик (risk). Двата термини денес се употребливи во делот на политичките и експертските дебати поврзани со безбедноста. Терминот закана, се употребува кога се сака да се објасни некој несакан, намерен или ненамерен настан кој има потенцијал да предизвика повреда или штета врз одреден субјект. Интензитетот на заканата е пропорционален на ранливоста на субјектот, односно заканата е голема колку што е голема ранливоста и обратно.

Секоја перцепција на несигурност може да се дефинира како закана.

Според теоријата на Сјоберг, заканата се однесува на опасност за која постои висока веројатност дека ќе се случи и ќе предизвика последици (Sjoberg L., 2001). Ваквото определување на заканата во себе опфаќа два елемента, прво се врзува за веројатност и степен на веројатност, односно се поставува условна релација (conditional) дека намерата ќе предизвика повреда или штета (последица). За разлика од ризикот кој се врзува за веројатност, „заканата претставува јасно изразена намера за нанесување повреда“.¹³

Овој автор, понатаму толкувањето на терминот закана го изедначува со терминот ризик, сметајќи дека било која дефиниција преведена и објаснета во различни говорни подрачја создава само дополнителни проблеми и нејаснотии и сугерира двата термина да се употребуваат како синоними. Покрај ова, Сјоберг јасно истакнува дека термините закана и ризик различно се употребуваат и се појаснуваат во природните и општествените науки. Истражувачите кои доаѓаат од општествените науки се приврзаници на конструктивистичкиот пристап, додека претставниците на природните науки повеќе се насочени кон реалистичкиот пристап во дискусиите на безбедносните теории.

4.2. Ризиците по системите

Околностите кои придонесуваат луѓето постојано да се изложени на разновидни опасни ситуации или да имаат чувство на несигурност,

циска и институционална рамка на пазарот нудат услуги поврзани со безбедноста на животот и здравјето на луѓето, нивните материјални добра, како и економските и технолошките процеси. Едни од серијата нови безбедносни провајдери се и агенциите за приватна безбедност.

¹³ Дефиницијата дека „заканата претставува јасно изразена намера за нанесување повреда“, под влијание на терористичките напади од 11 септември 2001 година, се ревидира и упатува на тоа дека „заканата која директно не застрашува е латентна, прикриена и потисната намера за нанесување повреда“.

придонесоа повеќе теоретичари од областа на безбедноста и пошироко, да се зафатат со истражување на терминот „ризик“, негово дефинирање и вградување во концептот на безбедност.

Најопшто објаснување за поимот ризик е дека тој претставува можност/веројатност од повреда, предизвикување на штета или загуба, (дадено според Webster Dictionary)¹⁴, каде најчесто веројатноста и последиците се поврзуваат со физички, технолошки или природни процеси, според тоа дали и како можат објективно да се определат (измерат) преку *процесот на процена на ризикот*.

При определувањето на терминот ризик забележливи се тенденциите тој да се сфати исклучиво како технички термин, или како очекувана и калкулирана (пресметана) вредност (последица) од некој несакан настан.

Ваквото гледиште, од перспектива на општествените науки, се смета за неприфатливо, тргнувајќи од ставот дека ризикот во суштина претставува субјективна категорија, односно субјективно се доживува како дел од социјалната сфера, и како таков не може да биде само објективна мера која ќе се изрази преку квантитативни показатели (број на жртви, урнати или оштетени објекти и друга физичка штета). Според Сјоберг, ризикот претставува очекување на (несакан) настан и претставува пред сè социјална конструкција.

Перцепцијата на ризикот се смета како значаен фактор во процесот на определување на значењето на ризикот. Во оваа смисла, во теоријата се развиваат два правца кои се обидуваат да дадат одговор на прашањата за ризикот, тоа се психометричниот модел и теоријата на културата (Sjoberg L., 1984).

Според првиот модел, ризикот претставува субјективно доживување на поединецот, кој е под влијание на мноштво психолошки, социјални и институционални фактори (Slovic). Но, основниот проблем што доминира во овој модел е како да се измери влијанието на овие фактори врз перцепцијата на поединецот. Додека преку „теоријата на културата“, се настојува да се разбере влијанието на културата, навиките, обичаите, односно одредени норми и вредности кои се препознатливи за некоја група или заедница, и влијанието на сето тоа врз поединечните/групните перцепции за ризикот (Slovic P., 2000).

Кога станува збор за тоа дека перцепцијата на ризикот влијае на начинот на неговото определување и конципирање, треба да се спомене и т.н. „јавна перцепција“ и „реална перцепција“. Јавната перцепција е поврзана со разбирањето и доживувањето на ризикот од страна на јавноста (поединци, групи и сл.) и поблиску е до лаичкото разбирање на

¹⁴ Достапно на: <http://www.merriam-webster.com/dictionary/risk>

ризикот. Реалната перцепција за ризиците доаѓа од страна на експертската заедница, која своите ставови ги поставува врз научни и методолошко поставени истражувања. *Ризиците за кои зборуваат експертите се т.н. реални ризици и нивното објаснување се поткрепува преку принципите на објективност, аналитичност и сеопфатност.* Вториот пристап е релевантен за системите за управување со ризици, кои во различна организациска и институционална форма се воспоставени и функционираат во јавниот и во приватниот сектор во Република Македонија.

Со вклучувањето на сите овие елементи, рискот се поставува на широка основа, со што се проширува неговото основно значење кое произлегува од чисто техничката основа, а концептот на ризик се настојува да се разбере покомплексно. Основната претпоставка која произлегува од комплексниот концепт на ризикот упатува на тоа дека ниту една активност во општеството не е имуна на ризик, ниту пак дека ризикот може во целост да се елиминира. Ризикот може само да се намали (редуцира) на некое прифатливо ниво, кое е дефинирано во безбедносната скала на поединецот, групата, општеството, државата итн.

Последното упатува на неопходноста ризикот да се управува или менаџира¹⁵, како основен предуслов за намалување на несигурноста и избегнување на несакни загуби на човечки животи и други добра. Целисходното управување со ризикот, претставува основа за ефикасен систем за управување со ризик и систем за управување со ризик од катастрофа (James A. Gordon, 2001).

Широките анализи и дискусии кои интензивно се одвиваат во рамките на безбедносните студии, од крајот на минатиот и почетокот на овој век, укажуваат дека концептот на *закана/загрозување* полека исчезнува и губи од своето значење и сè повеќе се заменуваат со терминот *ризик* и со него присутниот синоним несигурност. Оваа тенденција се поврзува со проширувањето и продлабочувањето на концептот на безбедноста и доминацијата на т.н. мека безбедност која е поврзана со неklasичните закани, што произлегуваат од политичката, економската, социјалната, еколошката и слични сфери, како и од големите природни непогоди кои се случуваат ширум светот.

Кога станува збор за термилошко разграничување на значењето на поимите *закана* и *ризик*, и двата поими претставуваат синоним за несигурност. Имајќи предвид некои од дефинициите кои укажуваат дека „заканата претставува јасно изразена намера за повреда, штета итн.“, а ризикот „се поврзува со веројатност, односно можност за после-

¹⁵ „Менаџирањето на ризикот е процес на континуирано донесување на одлуки во однос на идентификуваната опасност и вклучување на сите практични и разумни мерки да се минимизира влијанието на таа опасност“.

дици ...“ може да се констатира дека нивното разграничување треба да се бара во дозата, односно количината на несигурност, која се јавува како последица.

Со оваа констатација се отвора прашањето како да се измери таа доза или количина на несигурност! Концептот на ризик, гледан од двата аспекта, и како техничка категорија и како социјална категорија, дава многу поголеми можности за мерење, односно проценување на количината на несигурност, преку детаљна анализа и оцена на поединечните компоненти (состојки) на ризикот (опасност – изложеност – ранливост – капацитет/ отпорност), а потоа и синтеза, за да се добие збирна оцена за нивото на ризикот, а со тоа и дозата на несигурност која е поврзана со конкретниот ризик.

4.3. Загрозувањето по системите

Загрозувањата претставуваат сегмент од комплексноста на концептот за безбедност. Тие, заедно со заканите и ризиците претставуваат составен дел од термилошката и суштинската дебата во рамките на безбедносната теорија. Агендата на заканите и ризиците со кои се соочува една држава и нејзината национална безбедност, бараат постојан мониторинг и нивно проценување, со цел да се предвиди размерот на очекуваното загрозување и да се планира конкретна безбедносна акција од страна на соодветната институција.

Кога станува збор за операционализација на загрозувањата, тие вообичаено се разгледуваат во некој контекст и корелација со причините за нивното настанување, односно со заканите и ризиците. Во зависност од тоа кои и какви закани се наоѓаат на безбедносната агенда, за такви форми и видови на загрозувања може да се отвори дебата и дискусија. Според тоа се разликуваат:

– *Воени загрозувања*: поврзани се со најтешките форми на безбедносни закани, кои се насочени кон темелните вредности на државата, како: независноста, територијалниот интегритет и суверенитет. Со оглед на тоа што овој тип на закани може да предизвика најтешки форми на загрозување, истите имаат висок приоритет во однос на националната безбедност. Исто така, воените загрозувања се наоѓаат високо и на агендата на личната и јавната перцепција на безбедноста.

– *Политички загрозувања*: произлегуваат и поврзани се со закани и ризици кои се насочени кон организациската стабилност на државата, кои започнуваат како притисоци кон легитимните влади, поттикнување сецесија и сл. Имајќи ја предвид егзистенцијалната важност на политичката стабилност, политичките закани можат да предизвикаат сериозни загрозувања како и воените.

– *Социетални загрозувања*: социеталната безбедност се поврзува со закани кои задираат по идентитетот, културата, јазикот, религијата, ентитетот и други такви вредности, кои една држава, нација ја издвојуваат од друга. Вообичаено загрозувањата кои се поврзани со овие елементи се поврзани со ризици кои произлегуваат од некои внатрешни состојби и процеси во државата, во заедницата или во групата.

– *Економски загрозувања*: произлегуваат од делокругот на економската безбедност. Во овој случај постои проблем со разграничувањето на економските ризици, од т.н. дозволено агресивно натпреварување кое е својствено за пазарната економија (Bienen H. Power, 1992). Заради тоа многу е тешко да се разграничи кога и во кој случај економските закани претставуваат сегмент од националната безбедносна агенда. Националната економија е основа на стабилноста на една држава и извор на финансиска стабилност на националниот безбедносен систем. Заради тоа закани од економска природа често се испреплетени со загрозувања и последици кои задираат и во другите сфери на државните функции.

– *Еколошки загрозувања*: се поврзани со ризиците по природните богатства, животната средина и просторот кои во последните години предизвикуваат големи еколошки загрозувања и деградација на животната средина. Во минатото овие појави беа третирани како некои состојби од природната состојба на живеењето, каде „нема потреба“ од големо ангажирање на државата и дека природната рамнотежа ќе се врати сама по себе. Но сведоци сме дека, во безбедносните агенди на скоро сите држави, па и кај нас, закани и ризици по животната средина се наоѓаат доста високо. Во овој контекст ќе ги споменеме само големите глобални напори за намалување на климатските ризици, а со тоа и директните или индиректните еколошки загрозувања.

Операционализацијата на загрозувањата упатува на потребата од нивно постојано редифинирање и поместување на скалата на безбедносната агенда. Тоа во пракса значи дека видот на приоритетните загрозувања за поединецот, групата и заедницата се менува во зависност од актуелните ризици и закани, а тоа редифинирање се утврдува преку процесот на проценување на ризиците во организиран и институционално воспоставен систем, од страна на државата и нејзините органи, како и специјализирани субјекти (центри, агенции, институти и други установи за професионално менаџирање со ризици).

5. СИСТЕМСКО ПОИМАЊЕ НА РИЗИКОТ

Секоја посложена организација може да се согледа како систем. Внатрешното и надворешното опкружување на тој систем генерира одредени ризици кои имаат свое негативно влијание на истиот. Основен

предизвик за секоја системска организација претставува управувањето, односно менаџирањето со тие ризици. Процесот на предвидување и проценка на ризиците придонесува за ефективност во одлучувањето со тоа што ги зема предвид неизвесноста и можноста за појава на идни, намерни или ненамерни настани и околности, како и нивното влијание на поставената визија, мисија и цели на системот.

Системите за заштита на лица и имот припаѓаат на групата организациони системи во чие функционирање е изразен висок степен на неизвесност. Во основа, тоа се сложени, отворени, динамични и стохастички системи (Кековиќ, 2009). За беспрекорно функционирање на еден безбедносен систем, потребно е да се обезбеди состојба без присуство на опасности, кои можат да резултираат со смртност, повреди, загуби на системот и оштетување на животната и работната средина.

Апсолутна безбедност и заштита не е возможна, затоа што не може да се обезбедат секогаш услови на „неризична средина“, особено кога станува збор за комплексни системи кои се подложни на широк спектар на ризици. Како пример за комплексни системи може да се сметаат современите автоматски системи за контрола на големи технолошки процеси во нуклеарните електрани, системите на критичната инфраструктура (снабдување со енергија, гас, вода, одвод и сл.), комуникациско-информациони системи за контрола на авионски, поморски, железнички и патен сообраќај итн.

Заради сложеноста на денешните системи генерално е невозможно да се елиминираат сите опасности, така што како оптимална цел од безбедносен аспект, станува збор за развој на системи со прифатлив ризик. Оваа цел може да се постигне само ако безбедносните мерки се планираат и се применат порано, уште во фазата на конципирање и изградба на системот, а со нивната примена да се продолжи понатаму, преку организиран процес на спроведување сеопфатни мерки за безбедност и заштита на функционирањето на системот.

Ефикасен безбедносен систем се постигнува преку перманентен процес на идентификување на потенцијалните опасности, процената на ризици и примената на корективни активности за да се елиминираат утврдените слабости или да се намалат ризиците. Намалувањето на ризиците од несреќи се постигнува со редуцирање на веројатноста за нивна појава преку идентификување и отстранување на причините за истите. Ова вклучува и систематски пристап во управувањето со ризиците од несреќи.

Примарна цел на системите е да осигурат навремена детекција на опасностите и да обезбедат воведување соодветен механизам за нивна контрола и елиминација. Низ призмата на системската анализа, посакуваниот квалитет на системот претставува преферираниот исход

на неговото функционирање, додека сите отстапки од посакуваниот квалитет како непожелни се третираат како штета, односно загуба на системот. Загубата може да биде нарушување на перформансот на системот, загрозување на материјално-техничките добра, безбедноста и здравјето на луѓето, нарушување на еколошката рамнотежа, некавалитетен, скап или производ што не може навремено да се испорача, односно секое отстапување од атрибутот на квалитет на однапред дефинирани вредности. *Поради тоа неопходно е ризикот да се набљудува и во однос на квалитет на системот, односно на квалитетот на исполнувањето на целите и функциите заради кои системот е воспоставен.*

За време на својата егзистенција системите се изложени на влијанија од многу надворешни и внатрешни фактори. На овие влијанија системот може да реагира на три начина, и тоа: преку намалување на квалитетот на својата функција, задржување на исто ниво на квалитет и преку зголемување на функционалниот квалитет.

Промената на квалитетот во смисла на зголемување на квалитетот претставува посакувана промена на системот, додека промената во смисла на намалување на квалитетот, претставува непосакувана промена. Ризикот е состојба во која постои можност за појава на непосакувани промени во потребниот квалитет на системот. Мерката за можност од појава на непосакувани промени во квалитетот на функцијата на системот е веројатноста од ризичен настан, додека величината на непосакуваното отстапување претставува мерка за загуба на квалитетот. За поврзување на веројатноста и мерката на загуба се користи поимот „очекувана вредност на ризик“. Очекуваната вредност на ризик претставува производ од веројатноста за ризичен настан и мерката на предизвиканата загуба.

Ризикот врз системот може да биде причинет од различни настани. Настанот се однесува на премин на системот од една состојба во друга. Реализацијата на настаните често не е последица на поединечни причини, туку резултат на појави и развој на редоследна причинска низа на настани. Појавата на т.н. „причински ланец“ иницира серија на внатрешни и надворешни промени (Stanković, Savić, 1999) кои се однесуваат на следните работи:

- откажување на еден елемент од системот (внатрешни нарушувања) и/или недозволен надворешни нарушувања;
- појава на фактори на опасност на неочекувано место и/или во неочекувано време;
- неисправност или непостоење на заштитни средства и/или неадекватно однесување (нови откажувања) на елементите на системот во новите услови на функционирање;
- дејство на факторите на опасност на незаштитените елементи на системот или опкружувањето.

Промените или пречките во функцијата на системот имаат внатрешно или надворешно дејство со карактер кој може да го промени однесувањето на системот. Пример за внатрешни влијанија на системот може да биде краток спој во електричната инсталација, пожар или друг техничко-технолошки проблем, замор, болест или штрајк на вработени и сл. Додека како пример за надворешни влијанија може да е недостаток на енергенси, промена на пазарот на стоки, социјални немири, елементарни непогоди, временски неприлики и друго.

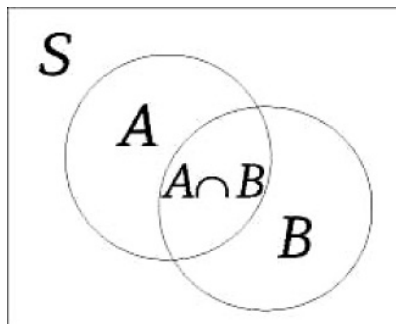
Повратната реакција на системот на надворешните и на внатрешните влијанија може да биде двојна. Одредени промени (прифатливи) може да бидат апсорбирани од системот, при што системот останува во состојба на рамнотежа, додека на други промени (неприфатливи), системот реагира со премин во состојба на алармантност и опасност. Ова претставува состојба на системот со потенцијал да предизвика загрозување на неговата безбедност со последици од повреди и/или штети.

Состојба на ризик врз одреден систем настанува кога во полето на дејство на факторите на опасност се наоѓаат незаштитени елементи на системот. Тоа значи дека ризикот за системот станува извесен при реализација на одредена опасност, или за постоење ризик потребно е да се исполнат следните предуслови:

- постоење конкретна опасност;
- изложеност на луѓе/објекти/природа/деловни процеси, врз кои ќе дејствува конкретната опасност;
- ранливост, односно повредливост на луѓето/објектите/природата/ деловните процеси од влијанието на опасноста (поради непостоење или неадекватен капацитет на системот за заштита).

На следниот дијаграм е дадена илустрација на ризикот од која се гледа дека опасноста и ранливоста претставуваат нужен и поврзан услов за настанување ризик.

Дијаграм 1. Илустрација на ризикот (МеНбтмКОВ, 2003)

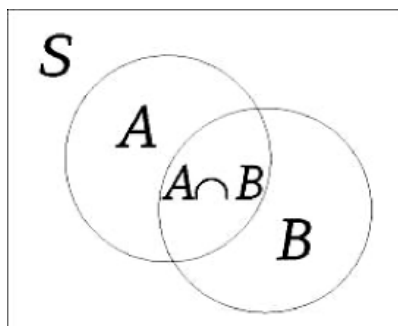


Каде: (A) = опасност за системот, (B) = ранливост на системот, а $(A \cap B)$ = ризик за системот.

Во зависност од интензитетот и времето на изложеност на влијанието на опасност, промената на квалитетот во системот може да биде различна. Ако не се предизвикува непосакувана промена на квалитетот, факторите на опасност се сметаат за апсорбирани, односно компензирани од страна на системот. Во спротивно, постои момент на „ризичен настан“, кој предизвикува непосакувана промена на квалитетот на системот, т.е. го пренесува системот во состојба на откажување или дисфункција.

Илустрацијата на реализација на ризикот е прикажана на следниот дијаграм.

Дијаграм 2. Илустрација на реализација на ризикот



Каде: (A) = ризик за системот, (B) = квалитет на системот, а $(A \cap B)$ = откажување или дисфункција на системот.

Без соодветно разбирање на причинско-последичниот ланец не може да се разбере или да се идентификува вистинскиот фактор за настанување и реализација на ризикот. Поради тоа често се вели дека многу ризици се системски условени, дека во нивната заднина лежат системски грешки или грешки на менаџментот, што секако мора да се има предвид за време на анализата на несреќните случаи и на соодветен начин да се предвидат и да се вградат во процесите и процедурите со кои се уредува функционирањето на системот.

III глава

УПРАВУВАЊЕ СО РИЗИЦИТЕ

1. ПОИМ ЗА РИЗИК И СИСТЕМСКИ РИЗИК

Кога станува збор за „ризик“, сфатен како поим или како состојба во која може да се најдеме, може да се каже дека е многу значаен и речиси неизбежен момент во нашиот секојдневен живот. Носењето на секоја одлука, без разлика дали е врзана за нашиот приватен живот или за некоја деловна ситуација, со себе носи одреден ризик. Самиот збор „ризик“ потекнува од италијанскиот збор *“risicare”*, што значи „се осмелува“. Историјата за ризикот започнува уште од грчките филозофи и арапските математичари и се провлекува низ сета човекова историја меѓу трговците, научниците, интелектуалците и меѓу сите оние што во својата работа се занимаваат со предвидување на иднината и со развивање на различни прогностички методи. Историските записи за првото вистинско проучување на ризикот се сретнуваат од времето на ренесансата. Методите кои денес се употребуваат во управувањето со ризиците и анализата на изборот меѓу различни одлуки во врска со некој настан датираат и се развиени кон крајот на XVII и почетокот на XVIII век.

Проучувајќи ги различните аспекти на општествениот развој во XXI век, истражувачите користат различни термини: информатичко општество, постиндустриски свет, технотронска цивилизација. Меѓутоа, имајќи ја предвид глобалната динамика од крајот на XX век, сè пораширена е концепцијата за ризично општество. Германскиот експерт Улрих Бек го карактеризира нашето време како премин од индустриско општество во ризично општество.

Обидите да се даде единствена дефиниција за ризикот која би била употреблива за сите области на истражување не ги дадоа посакуваните резултати. Всушност, и многу тешко е да се постави универзално поимно дефинирање на ризикот, бидејќи неговото термилошко значење отстапува во зависност од научната и апликативна област во којашто се употребува. Заради избегнување на овие и слични проблеми, за потребите на различни научни дисциплини се формулирани различни дефиниции, кои се прифатени од истражувачите, водејќи се од целите и од предметот на истражувањето.

Според одредени дефиниции кои може да се сретнат во литературата Ризикот, претставува:

- комплексна појава со која истовремено се опишува веројатноста за настанување штетни настани и очекуваната големина на последиците од тој настан во целокупниот систем и текот на утврде-

ната должина на временскиот интервал или текот на некоја одредена мисија. (Вукиќевиќ, Видовиќ, 1995);

- мерата на веројатност дека последиците штетни по животот, здравјето, имотот и/или животната средина ќе се појават како резултат на некои одредени опасности (Sage 1995);
- можност за загуба или повреда, или изложеност на таква можност (Vujošević, 1996);
- состојба во која постои можност за штетна отстапка во однос на посакуваниот исход (Vaughan, 1997);
- можност потенцијалната опасност да се оствари за време и во услови на користење и/или изложување и можното значење на штетата (Luković, 2001);
- степен на веројатност за настанување на техногени или природни појави кои се карактеризираат со настанувањето, формирањето и дејството на опасноста, како и социјалните, економските, еколошките и другите видови на загуби и штети (Подосенова, 2008).

Вообичаено, под ризик се подразбира секоја можност во конкретниот систем која со одредена веројатност може да предизвика неочекувана промена на квалитетот, односно промена или загуба на одредени вредности за системот. Исто така, ризикот подразбира прогноза за можната штета, односно очекувана загуба. Степенот на ризик е функција на веројатноста и последица од ризичниот настан. Последицата од ризикот може да биде позитивна или негативна. Позитивните последици често се нарекуваат можност или шанса. Заканата или опасноста кои стојат во заднината на ризикот се генераторите на потенцијални негативни последици, односно т.н. „непријатен аспект“ од ризикот. Ризикот е сложена, постојана, неизбежна и неизвесна карактеристика на сите настани и појави во денешните услови на современиот живот.

За извесноста говориме дека е ситуација во која сме сигурни во исходот на некој настан, односно во резултатите кои со себе ќе ги повлече донесувањето на некоја одлука. Како што таа сигурност и исходот на настаните се малуваат, така зборуваме за зголемување на ризикот. Од другата страна на извесноста, како целосна спротивност се наоѓа неизвесноста. Разликата меѓу неизвесноста и ризикот е дефинирана уште во 1921 година од страна на F. Knight во книгата „*Ризик, неизвесност и профит*“. За него разликата меѓу неизвесноста и ризикот се однесува на следното: „ако не знаеш со сигурност што ќе се случи, но си запознаен со веројатноста, тоа е неизвесност“. Се смета дека неизвесноста е ситуација во која потполно или делумно недостасуваат информации за можните состојби во рамките на системот, како и на објектите во опкружувањето. За разлика од неизвесноста, ризикот претставува степен на увереност или неувереност на субјектот во сигурноста на реализацијата на својата цел.

На извесноста, односно на неизвесноста за исходот на некој настан влијае на состојбата на опкружувањето во кој се реализира набљудуваниот настан. Со оглед на состојбата на опкружувањето во која некој настан се реализира, постојат:

- *состојба на извесност* (одреденост, детерминираност), кога изборот на конкретните алтернативи води до конкретен, познат исход;
- *состојба на ризик* во која изборот на конкретна алтернатива може да доведе до каков било исход од збирот можни исходи (извесни исходи), при што познатите веројатности се појавуваат во секој од исходите (секоја алтернатива се карактеризира со конечен збир веројатности на исходот); оваа состојба често се нарекува состојба на стохастичка неизвесност;
- *состојба на неизвесност* во која изборот на конкретна алтернатива може да доведе до кој било исход од збирот можни исходи (извесни исходи) при што не е позната веројатноста на појавите од овие исходи (поради непостоењето на соодветни и достапни податоци, како и неможноста за субјективна процена на веројатноста).

Освен неизвесноста, ризикот подразбира и можност за избор, односно постоење поголем број можни алтернативи, најмалку две, а по можност и повеќе варијанти на решенија или акции, со што секогаш може брзо да се одговори на состојба. Ако не постои можност за избор, не може да се зборува за ризик. Една од можните алтернативи секогаш доведува до несакани последици за луѓето (на пр. болест, стрес, смрт), материјални добра (на пр. оштетување, рушење) или природна средина (на пр. загадување, загрозување на некој вид, деградација на природните ресурси).

Според *ISO Guide 73:2009*, ризикот е ефект на неизвесност на целите. Во контекст на оваа дефиниција, а заради нејзино дообјаснување, дадени се и пет напомени.

Напомена 1: Ефектот е отстапување од очекуваното – позитивно и/или негативно.

Напомена 2: Целите може да имаат различни аспекти (финансиски, здравствени и безбедносни, заштита на животната средина) и може да се применат на различни нивоа (на стратегиско, на организационо, на производно и на процесно).

Напомена 3: Ризикот често се карактеризира во однос на потенцијалните настани и последици или на нивна комбинација.

Напомена 4: Ризикот често се изразува како комбинација од последици на некој настан (вклучително и промена на околностите) и придружни веројатности на настанот.

Напомена 5: Неизвесноста е состојба и во случаи на делумен недостиг на информации, разбирање и познавање во врска со настанот, неговите последици или веројатност.

Терминот „ризик“ ги содржи следните елементи кои, поврзани на соодветен начин, ја сочинуваат неговата суштина:

- избор на алтернативи;
- можност за отстапувања од посакуваната цел заради која се вршел изборот на алтернативи;
- веројатноста за постигнување на посакувана цел (резултати);
- непостоење на уверување во постигнување на поставената цел;
- можност за материјални, човечки, еколошки и други загуби, поврзани со реализацијата на избраната алтернатива во услови на неизвесност.

Освен тоа, ризикот е сложена појава, која има многу различни, а често противречни реални основи. Така што може да се зборува за објективна, субјективна и објективно- субјективна природа на ризикот.

Објективната природа на ризикот се врзува со реалното постоење на многуте природни, општествени и технолошки процеси, за разновидност на материјалните и општествени односи, за постоење многубројни и различни врски меѓу елементите и стохастичката природа на многуте процеси во сложените системи (функционирањето и развојот на сложени системи се опишува со помош на статистички закони). Поради тоа не е можно истовремено да се предвиди појавата на посакуваниот резултат. Субјективната природа на ризикот се врзува за човекот и неговите одлуки во потенцијално ризични ситуации. Додека одредени настани (на пример природни катастрофи) се случуваат независно од волјата на човекот, во многу од нив тој е основниот фактор. Човекот може да гради или да не гради нуклеарни центри, да одржува или да не одржува технолошки системи, да води или да не води грижа за своето здравје. Човековиот однос спрема ризикот, т.н. психолошки аспект на ризикот претставува одраз на културата и односот спрема себе и светот во кој живее.

Истражувањата на овој однос покажуваат дека субјективниот простор на ризикот најчесто е дводимензионален. Едната димензија се карактеризира со објективна загрозеност, а другата со степенот на активност на човекот во создавањето и/или спречувањето на опасните ситуации. Заради тоа, новите ризици за кои не постојат адекватни, ефикасни мерки на контрола, за човекот имаат најголем приоритет.

Најпосле, може да стане збор за субјективно-објективна природа на ризикот, со оглед на фактот дека ризикот е условен од процеси како од субјективен карактер, така и од процеси чие постоење не зависи од човековата волја и сознанија.

Поимот кој често се врзува со ризикот е и *веројатноста*. Накратко речено, веројатноста претставува можност за настапување, односно

случување на некој настан. Колку поимот и терминологијата поврзана со веројатноста се комплексни, укажува и фактот на создавањето на *теоријата на веројатноста*, која настојува да воспостави научна основа за квантификација на одреден веројатен настан и да развие пробабилистички модели за нивно предвидување.

Како илустративен пример за квантификација на ризикот може да се земе следниот: ако е извесно дека некој настан ќе се случи, веројатноста за тоа е 1, а ако е сигурно дека нема да се случи, тогаш веројатноста е 0. Веројатноста за ризичен настан кој може негативно да влијае за случување на очекуваниот настан, се наоѓа помеѓу овие две вредности, односно помеѓу 0 и 1.

Исто така, веројатноста за ризичен настан може да се изрази на два начина, како објективна или субјективна. Објективната веројатност ја објаснува долгорочната фреквенција или однесување на некој настан, заснована на претпоставката на голем број набљудувани настани и непроменливи услови или се пресметува врз основа на извршен експеримент и собрани податоци.

Субјективната веројатност би значела сопствено уверување или лична процена за исходот на одреден настан. Таа се разликува од поединец до поединец на неа влијаат различни фактори, како што се: искуството, возраста, интелигенцијата, образованието и многу други карактеристики и специфичности кои го одбележуваат поединецот.

Луѓето имаат суштинска егзистенцијална потреба да живеат во организирана заедница, да ги планираат своите активности заради остварување на своите идеи и замисли, како и да ги произведуваат и распределуваат резултатите од својата работа заради осигурување на својата егзистенција, во услови на општа неизвесност која е својствена за т.н. „ризично општество“.

За во такви услови претприемаштвото да биде успешно, ризикот мора да биде постојано анализиран, проценуван и контролиран од сите аспекти: производниот, комерцијалниот, финансискиот, трговскиот, социјалниот, политичкиот, институционалниот, меѓународниот и други.

Со континуираното проучување и анализа на ризикот може да се дојде до сознанија за потребните мерки и акции кои може да бидат преземени со цел да се намали или да се ублажи ризикот од некој настан, односно зголемување на сигурноста во случај на негова реализација. Заради избегнување на ризикот или намалување на неговите негативни влијанија, поединецот или организацијата преземаат одредени активности во смисла на превенција и намалување на последиците. Непреземањето на никакви активности, многу често придонесува кон ризикот или само по себе претставува ризик. На следните два примера се илустрира претходно кажаното.

Пример 1: некој човек се движи кон аеродром за да стигне на својот лет. Временските услови се многу лоши и можно е летот да биде откажан. Тој човек не е сигурен каков е статусот на неговиот лет и е ставен во состојба на неизвесност, со тоа што нема информации за својот лет, односно не ги ни побарал. Неговите патни планови ќе бидат нарушени доколку летот биде целосно откажан. Заради тоа, тој е „изложен на ризик“.

Пример 2: истовремено, друг човек од друг крај на градот оди на аеродром да стигне на истиот лет. Овој човек презел одредени активности, се јавил на аеродромот да провери дали летот ќе доцни или е откажан. Поради тоа тој се наоѓа во помала неизвесност, односно изложен е на помал ризик да му бидат нарушени неговите патни планови.

Во овој пример две индивидуи се потенцијално изложени на истиот ризик – да го изгубат својот лет. Но поради различно преземените активности тие имаат различно ниво на неизвесност и се изложени на различно ниво на ризик. Ризиците може да се намалат со воведување подобра организација, координација, комуникација, контрола на квалитетот, унапредување и рационализација на работењето, правилен избор на човечки ресурси и нивна постојана обука, заштита на работно место и други мерки.

2. КЛАСИФИКАЦИЈА НА РИЗИЦИТЕ

Независно од видот и целната ориентираност, речиси сите организациски системи се подложни на ризици кои може да влијаат на остварувањето како на нивните визии и мисии, така и на нивните функционални и оперативните цели. Овие цели може да се однесуваат на различни организациски активности, започнувајќи од стратегиски иницијативи па сè до оперативни активности, процеси и проекти, а може да резултираат во заштитни, безбедносни и други исходи кои ќе имаат одредено влијание на репутацијата на организацијата.

Во теоријата, а и во праксата може да се сретне различна категоризација или класификација на ризиците. По општото значење и влијание на организацијата, Киш во својот труд *„Менаџмент на ризикот“*, ризиците ги дели на три категории. Во првата категорија ги става т.н. ризици од „виша сила“, каде што се вбројуваат сите ризици поврзани со природни феномени и од нив предизвикани катастрофи, како на пример: земјотреси, поплави, временски непогоди и сл., кои може да бидат во распон од потполно безначајни до катастрофални. Во другата категорија се класифицирани ризиците од политичка и економска природа, кои се дефинираат како промени (намерни или наметнати) во политичкото и во економското опкружување на организацијата. И третата категорија на ризици е составена од сите ризици кои настануваат во самиот си-

стем или организација, на кои организацијата има директно влијание. Најчесто овие ризици се определуваат како деловни ризици, а се делат на организациски, деловни и финансиски ризици.

Ако се анализираат ризиците поврзани со деловното работење, се заклучува дека деловните организации се соочуваат со неколку вида ризици: трговски ризик, кредитен ризик, ризик на ликвидност, оперативен ризик, правен и регулаторен ризик, деловен ризик, стратегиски ризик и ризик на угледот. Во зависност од тоа дали ризиците се однесуваат на организацијата во целина или на некој нејзин сектор, понатаму ги делиме на *општи* и *посебни* ризици. Ако како критериум се земе брзината на промените во состојбата на системот, постојат: *кумулятивни ризици*, кои се карактеризираат со бавен развој, бавна деградација на процесите и постепена промена на однесување на системот и ризици од несреќа, кои се карактеризираат со голема брзина на развој, брзи процеси на деградација, голема брзина на промени на параметрите и раст на промените на излезните карактеристики на системот.

Од гледна точка на осигурувањето¹⁶, ризиците се делат на *осигурени* и *неосигурени*. Осигурените ризици се ризици за кои постои техничка и административна основа за утврдување на нивната големина (вредност), а со тоа и можност за нивно финансиско покритие. Во праксата можат да се сретнат неколку подвидови на осигурените ризици:

1) *посебни ризици*: претставуваат веројатност на загубите на приходите или средствата како последица на загубата на способноста на заработка на приход,

2) *имотни ризици*: претставуваат ризици на кои се изложува имотот, бидејќи може да дојде до негово оштетување, уништување или отуѓување на сопственоста.

3) *ризици по одговорноста*: вклучуваат можност за губење на постојните средства или иден приход како последица на оштетување на средствата или непочитување на законските обврски кои произлегуваат од намерни или ненамерни акти на загрозување на правата на други личности.

4) *ризици настанати од пропусти на други лица*: вклучуваат можност за финансиска загуба заради неисполнување на обврски кои биле преземени од други личности во текот на извршување на одредени услуги за физички или правни лица.

¹⁶ Од гледна точка на „управувањето со ризик“, осигурувањето од штети и последици станува сè поактуелна политика и конкретно применлива мерка за намалување на ризикот. Всушност осигурувањето претставува практична примена на „Стратегијата за трансфер на ризик“, како една од повеќето стратегии за управување со ризик.

5) *неосигурени ризици*: се оние ризици за кои осигурувањето нема реална основа за одредување осигурителна политика (премија). Вообичаено во категоријата на неосигурени ризици се вбројуваат:

- Шпекулативни ризици, кои означуваат ситуација во која постои веројатност за загуба, но и добивка. Коцкањето е соодветен пример за шпекулативен ризик. Овие ризици доброволно се прифаќаат и не се предмет на осигурување.
- Политички ризици, во коишто влегуваат промени во самата политичка структура, промени во владејачката партија, промени во политиките на постојната влада.
- Технолошки ризик, кој настанува и се должи на промени во технологиите и може да се набљудува како внатрешен или ако надворешен фактор кој може да влијае на организацијата.

Сите ризици кои влијаат на сигурноста на луѓето, имотот и работата, во поширока смисла, претставуваат безбедносен ризик, без разлика на тоа дали се условени од природни, од општествени или од социјални фактори. Кога изворот на ризикот е човечки фактор, тогаш станува збор за антропогени ризици, кои можат да имаат предзнак на ненамерност или намерност. Првите се врзуваат за можноста за настанување на човечка грешка, како последица на замор, немарност, невнимание и слични околности. Ризиците со атрибут на намерност се ризиците од криминални побуди и други користољубиви причини.

Следна можна поделба е поделбата на ризиците според изворот на настанување, предвидливоста и влијанието на технички фактори. Според изворите на настанување, ризиците може да се поделат на интерни (кражби од страна на вработените, разни облици на општ, имотен, бизнис или еколошки криминал) и екстерни (напади на имот, лица и надворешен бизнис). Според предвидливоста ризиците се делат на непредвидливи или тешко предвидливи (природни несреќи и опасности, политичко-безбедносни ризици) и предвидливи (активности на конкуренцијата, даночна политика). Од аспект на влијанието на техничкиот фактор ризиците ги делиме на: технички (пожар, експлозија и други опасности поврзани со технолошки процеси) и нетехнички (човечка грешка, социјални аспекти, прекини на процеси итн).

Од гледна точка на безбедноста, важна е поделбата на *чисти* и *шпекулативни* ризици. За да настане чист ризик, потребно е да постои јасна веројатност дека ќе се случи некаква штета или загуба. Во областа на безбедноста и заштитата, многу чисти ризици се однесуваат на несреќи кои настанале преку дејствувањето на техничкиот фактор, и тие се најповолни од аспект на предвидувањето, односно собирањето податоци од значење за процената, како и примена на соодветни стра-

тегии за намалување на ризикот (на пр. осигурување). Шпекулативните ризици претставуваат и можност за добивка и загуба, но и таа точка на пресек каде организациите, во поголема мера се свесни за предностите отколку за недостатоците, и се осудуваат на ризик. За пример, нудењето безбедносни услуги, кои вклучуваат и некои ризични сценарија, поврзано е со чести телесни повреди на безбедносниот персонал и загуби настанати по зголемување на компензациите за повреди на работното место.

Најголемиот дел од работата на менаџментот на системот или организацијата подразбира процена на идните загуби кои би настанале како последица на ризични настани и отстапките од тие процени. Отстапувањата по правило се поголеми кога станува збор за катастрофални ризици. На пример, терористичкиот напад кој се случи на 11 септември 2001 година во САД е дел од малку веројатно терористичко сценарио, но сепак претставува најголемото можно отстапување од проценетата веројатност и последици (загуби).

Во областа на заштита од ризици, се разликуваат познати и непознати ризици. Вообичаено е за стратегијата за осигурување да покрива исклучиво „познати“ ризици, односно оние неизвесности на кои е можно да се применат одредени методи за процена (пробабилистички методи). Одредени ризици може да бидат познати, но начинот, времето и местото на нивното реализирање се непредвидливи, што е карактеристика за терористичките ризици и природните непогоди. Некои други ризици се „непознати“, како на пример: непознати болести, климатски промени и ефектите кои ги предизвикуваат, социо-технолошките зависности и слични појави.

Современиот начин на живеење се одликува со голема динамика на активности, што остава сè помалку простор за согледување на сите ризици кои нè опкружуваат. На пример, технолошките предности и новите форми на сообраќај ни овозможуваат повеќе, подалеку и побезбедно да патуваме. Меѓутоа, паралелно со тоа расте и нивото на т.н. „Резидуални ризици“, кои се во корелација со зголемената динамика на активности. Резидуалните ризици, се дефинираат како постмодерни или постиндустриски технички поврзани опасности, како што се нуклеарната енергија, биотехнологијата и еколошката нерамнотежа и сл. Тие се неприфатливи за индустријата за осигурување, но се битни за разбирање на општеството кое својот страв го оправдува и го припишува на политички причини и зголемени сомнежи или неподготвеност за воспоставување експертски дијалог.

Поделбата на познати и непознати ризици, како и резидуални ризици, води до полемиката за *прифатливи* и *неприфатливи* ризици. За некоја организација разумно да се соочува со ризиците и да применува

адекватни стратегии за нивно контролирање, важно е да знае кои ризици за неа се прифатливи, а кои неприфатливи. Со економска терминологија, границата на прифатливите ризици е одредена со математичка теорија на веројатност. Во својата книга „*Ризично општество*“, Бек наведува дека сме во состојба на голем премин од класно во општество на ризик, што во иднина ќе влијае на тоа основен посредник на прифатливите ризици да биде индустријата на осигурување (Beck, 1992).

3. КОМПОНЕНЕТИ (ЧИНТЕЛИ) НА РИЗИКОТ

Основните компоненти, односно чинители на ризикот преку кои тој се разгледува и се анализира се однесуваат на: опасноста што се јавува во основата на ризикот, изложеноста која може да претрпи негативни импликации од опасноста, ранливоста и отпорноста, односно капацитетот на системот, организацијата која е изложена на ризик. Врз основа на изнесеното, ризикот може да се претстави на следниот начин:

Ризик = f (опасност, ранливост, изложеност, отпорност)

На следната Слика илустративно е прикажана оваа структура на ризикот:



Слика 1: Ризик прикажан како функција од опасноста, ранливоста, изложеноста и отпорноста

3.1. Опасност

Првата состојка на ризикот – опасноста е дефинирана како веројатност за случување на несреќа/катастрофа во определен период на време, со одреден интензитет и на одредено место/локација (УНЕСКО, 1973 година). Примери за опасности претставуваат земјотресите, поплавите, сушите, силните ветрови, шумските пожари, епидемиите и други. Опасностите се јавуваат како примарни или секундарни појави. На пример, во случај на земјотрес, интензитетот на вибрациите на почвата е примарна опасност. Меѓутоа, вибрациите може да предизвикаат лизгање на терен, или цунами ако епицентарот на земјотресот е под вода, кои можат да предизвикаат значително поголеми човечки и материјални загуби од примарната опасност.

Секоја несреќа, вонредна ситуација или катастрофа е иницирана од некоја опасност – позната или непозната. Постојат многу начини за категоризирање на опасностите, на пример, природни, технички, антропогени (предизвикани од човечки фактор), нуклеарни, еколошки, итн. Категориите се најверојатно исто толку разновидни како и инволвираните дисциплини и сектори. Но, она што е заедничко за сите нив е потенцијалот да предизвикаат сериозни негативни влијанија кои можат да резултираат со вонредна ситуација, криза и катастрофа.

Важна карактеристика на опасностите е тоа што тие во својот поим содржат веројатност за појава. Опасноста претставува закана, и не е реален настан. Меѓутоа, секоја опасност може и да се манифестира како реален и штетен настан. Со други зборови, доколку опасноста може да се измери од аспект на реални штети или негативни влијанија, истата повеќе не е опасност, туку настан, несреќа или катастрофа.

Опасноста може да се измери (процени) доколку се идентификуваат елементите кои се во нејзина близина, односно се изложени на негативните ефекти, а колку повеќе детали знаеме за изложените елементи (ранливост/отпорност), толку повеќе можности ќе имаме да го измериме негативниот потенцијал на опасноста.

Ова значи дека опасноста сама за себе не претставува ризик, односно $O \neq R$ (опасност $\neq$ ризик).

3.2. Изложеност

Изложеноста заедно со опасноста е следната компонента на ризикот и битен сегмент преку кој се согледуваат димензиите на потенцијалната несреќа или катастрофа. Изложеноста во практична смисла се изразува како број на луѓе и број на објекти од изградената средина, врз кои може да влијае одредена опасност. За да се проценат

и да се разберат ризиците поврзани со низа опасности, важно е да се карактеризира (разоткрие) изложеноста, имотите на населението, инфраструктурата и економските активности присутни на дадена територија во определено време.

Елементите на изложеност ја отсликуваат квантитативната страна на процената на ризикот бидејќи преку целосната анализа на сите изложени елементи на ризик (население, природна и изградена средина) се обезбедуваат детални податоци преку кои се проценува степенот на загрозеност и се предвидуваат негативните влијанија на оштетувачките ефекти на дадената опасност.

Во најширока смисла на зборот, преку компонентата на изложеност се определува севкупноста на создадените материјални вредности, и социо-економските процеси и системи кои ја карактеризираат и ја одржуваат организацијата и опстојувањето на конкретниот систем или организација. Во случај на нулта изложеност, ефектите на реализација на опасност од кој било интензитет, дури и максимален, се еднакви на нула.

За изложеноста, во литературата од оваа проблематика, често се применува терминот „елементи во ризик“ (elements at risk). Терминот „елемент во ризик“ всушност се однесува само на тие елементи на изложеноста кои се идентификувани како репрезентативни за анализа и процена на ризикот.

3.3. Ранливост

Покрај опасноста и изложеноста, важен предуслов за целосно согледување (проценување) на ризикот, а со тоа и антиципирање на штетните ефекти и потенцијалот од несреќи и катастрофи, претставува и процената на ранливост на присутните (изложени) елементи на ризик на територијата каде што се очекува конкретната опасност.

Ранливоста како елемент кој влијае на крајната форма (ефект) на ризикот укажува на потенцијалот за оштетување и претставува варијабла која упатува на можните загуби под влијание на опасноста (физички и финансиски). Ранливоста претпоставува определување на она што може да се случи на еден дефиниран елемент или група на елементи изложени на ризик во услови на одредена опасност или група опасности. Да се дефинира ранливоста значи хипотетички поставување на прашање, што би се случило доколку одредени настани би погодиле одредени елементи изложени на ризик (поединец, објекти, систем, организација, заедница, и сл.).

При процената на можните штетни последици од појавата на ризични настани и несреќи, преку согледувањето на ранливоста се има за цел да се дефинираат оние фактори кои ги прават одредена заедница,

поединци или други елементи од природната и изградената средина, повеќе или помалку подложни на опасности. Тие фактори вклучуваат показатели за: густина и структура на населението, физичка ранливост (на пример, слаба подлога-почва, употребен градежен материјал, лоша градба, лошо изведени технички системи и линии, итн.), социјални параметри за стандард, односно сиромаштија итн. *Оттука, фокусот на ранливоста преоѓа од „веројатност за последици“ од некоја опасност до „идентификувани причини“ за штети.*

Ранливоста ги претставува внатрешните карактеристики на елементот во ризик, кои секогаш се присутни, па дури и во периодот помеѓу ризични настани (несреќи). Таа не се вклучува и исклучува со доаѓањето и одењето на настаните, туку претставува постојана и динамичка карактеристика која се искажува за време на настан и до степен кој зависи од јачината/интензитетот на опасноста. Ова значи дека ранливоста најчесто може да се измери само индиректно и ретроспективно (по ризичниот настан или несреќа), а мерката која нормално се користи како индиректна мерка се штетите и претрпените загуби, изразени во физички и финансиски показатели.

Ранливоста постојано се менува со текот на времето и обично врз неа влијае дури и самиот штетен настан. На пример, таа може да се зголеми доколку со катастрофата се зголемила сиромаштијата, така што следната катастрофа ќе има уште поголем деструктивен ефект врз осиромашената заедница. Или обратно, еден мал настан би можел да ја подигне свеста кај заедницата и на тој начин да ја намали нејзината ранливост, со вложување во зголемување на отпорноста (на физички градби, просторно уредување итн). Ранливоста е „независна“ од која било одредена јачина на конкретен природен настан, но е зависна од контекстот во кој што се појавува опасноста, односно се случува.

Во одредени формулации, ранливоста концептуално се расчленува во *подложност* (“susceptibility”) и *капацитет за справување, односно отпорност* (“copping capacity” или “resilience”). Со ваквите гледишта се создава определена контроверза помеѓу техничкиот и социјалниот пристап кон определување на ранливоста (Birkmann, 2006). Подложноста го одразува капацитетот на поединците, групите или општествено-економскиот систем да го издржи влијанието на опасноста. Доколку отпорноста е мала, во тој случај, дури и мала опасност може да доведе до пад на системот (Pelling, 2003).

Генералната форма на рedefинираната и социјално димензионирана дефиниција на ранливоста е прикажана преку следната функција:

$$\text{ранливост} = \frac{\text{подложност}}{\text{капацитет за справување (или отпорност)}}$$

3.4. Отпорност

Во реалноста, крајните консеквенци на ризикот не само што зависат од опасноста, ранливоста и изложеноста, туку исто така и од отпорноста на елементот кој се наоѓа во ризик, односно е изложен на опасност, како и неговиот капацитет и способност за справување. Многу дефиниции дадени во литературата укажуваат на големо преклопување меѓу отпорноста и капацитетот за справување кои честопати се користат и како синоними. Овие две димензии на настанот кој предизвикува штети, не можат лесно да се одвојат една од друга.

Капацитетот за справување ги вклучува сите стратегии и мерки кои директно влијаат врз контрола на настанот, со олеснување или амортизирање на ударот на опасноста или обезбедување адаптивни стратегии кои ги модифицираат однесувањата или активностите за да ги намалат или да ги избегнат штетните влијанија.

Отпорноста ги отсликува сите наведени работи како капацитет за справување, дополнително асоцира и на способност за одржување на функционалноста на системот за време на настан и комплетно закрепнување по настанот. Оттука, отпорноста во себе вклучува капацитет за справување, но истовремено претставува и повеќе од тоа. Ова илустративно е прикажано на Слика број 2.



Слика 2: Капацитет за справување и отпорност

4 . УПРАВУВАЊЕ СО РИЗИК

4.1. Управување со ризик – теоретски аспекти

Постојано присутниот тренд за поголем економски развој и пораст на материјалниот и економскиот потенцијал на организациските системи доведува до пропорционален пораст на тежината од последиците од различни ризични настани. Спектарот на дејство на опасните фактори излегува од опсегот на непосредното опкружување на

системот и често зафаќа поширока територија, па и територии на други земји. Со самото тоа расте и бројот од потенцијално загрозувани луѓе и материјални ресурси, како и загрозување на животната средина.

Организираното и планирано преземање на различни мерки насочени кон елиминирање на причините на настанување и/или намалување на ефектот од ризичниот настан, како и мерки за ублажување и отстранување на последиците, доколку дојде до реализација на ризични настани, всушност ја претставуваат основата за *управувањето со ризик*.

Кога станува збор за термиолошко определување на „управувањето со ризик“ или „Risk Management“, во литературата можат да се сретнат различни дефиниции и толкувања. Некои од нив се следните:

- Координирани активности што ја насочуваат и ја контролираат организацијата во врска со ризикот (ISO Guide 73: 2009).
- Управувањето со ризик претставува организиран процес на идентификација и мерење на ризикот со избор, развој и примена на опцијата за негово третирање и мониторинг.¹⁷
- Управувањето со ризик е таков пристап кон управувањето што е заснован врз идентификација и врз контрола на оние области и настани што се потенцијални предизвикувачи на несакани промени во системот (Sage, 1995).
- Управувањето со ризик е аспект на управување со квалитет што има поддржувачка улога во остварување на бараниот квалитет на системот. Основна цел за управување со квалитетот е таква имплементација на стратемскиот план во управувањето што го обезбедува бараниот квалитет на системот, додека целта на управување со ризикот е задржување на квалитетот на системот и во случаи кога се одвиваат ризични настани. Управувањето со ризик треба да обезбеди континуирана егзистенција на системот (Vauglan, 1997).
- Управувањето со ризик подразбира управување со кое се постигнува соодветен баланс помеѓу создавање можности за добивки и минимизирање губитоци (AN/NZS 4360:2004).
- Управувањето со ризик е сеопфатен процес за поддршка во одлучување со управувањето на квалитетот, имплементиран како програма, интегриран преку дефинирани улоги и од-

¹⁷ Systems Engineering Fundamentals (2001), Supplementary Text Prepared by the Defense Acquisition University Press, Fort Belvoir, Virginia (www.dau.mil/pubs/pdf/SEFGuide).

говорности во регулативата, одржувањето, инженерингот и менаџментот на квалитетот.¹⁸

Севкупниот процес на управување со ризици има за цел да создава адекватни претпоставки за донесување правилни, навремени и реални одлуки. Одлучувањето е резултат во процесот на управување со ризиците и детерминирано е со три елементи: извесност, ризик и неизвесност. Како што напредуваме од неизвесноста, преку ризикот – постоењето определен степен за веројатност на настанот – кон извесноста, потенцијалните штети се намалуваат. Суштината на правилното управување со ризици е да се намали можноста (веројатноста) од настапување штетен настан и интензитетот на неговото влијание. Според тоа, процесот на управување со ризици е и влез и излез за процесот на одлучување. Разбирањето како да се премине од ризичен на помалку ризичен план и да се намали вложувањето на ресурси, а со тоа да не се загрозат целите на организацијата е клучно во донесувањето одлуки.

Управувањето со ризик е централен дел од стратегискиот менаџмент на секоја организација. Во сè што се презема постојат поволности и закани по успехот. Предностите и поволностите се согледуваат и во контекст на активноста и во контекст на сите заинтересирани страни. Поради тоа, во поглед на управувањето со ризици, потребно е навремено да се изразат очекувањата и одговорностите во однос на различните нивоа на менаџмент на организацијата и, особено, на сите вработени.

Управувањето со ризик може да биде дефинирано и како процес што има цел да и помогне на организацијата во разбирање и процена на ризикот, да преземе чекори кон зголемување на веројатноста за успех и да ги намали можностите за неуспех и неизвесност од постигање цели и внатре во секоја одделна активност и во вкупното портфолио на активноста. Важноста на овој процес произлегува од самата констатација дека организацијата што анализира ризици и креира одговор за нив, се штити самата себеси од лошите последици на ризикот и се позиционира така што да има предност во одредена ситуација, меѓу конкуренцијата и на пазарот воопшто. Значи, јасно е дека *ризиците во организацијата не смее да се игнорираат, и дека процесот на управување со ризици мора да се одвива во секоја организација, профитна или непрофитна, што го опслужува приватниот или јавниот интерес.*

Бидејќи ризикот се дефинира како неизвесност (до одреден степен), оттаму произлегува наједноставната дефиниција за управување со ризикот како формален процес за *управување со неизвесности* што

¹⁸ Canadian Standard Association. <http://ops.dot.gov/pubs/rsk/std/progstd.pdf>.

може да водат кон несакани исходи, губитоци и слично. Прашањата за вина и одговорност при несаканите настани, кој и кому треба да му ја надомести штетата и на кој начин да се спречат идните несакани настани и нивните последици, го нагласуваат значењето на модерното управување (менаџмент) со ризикот.

Целта на управувањето со ризици е да се идентификуваат релевантните фактори на ризик за одреден (очекуван) настан, а потоа да се изработи план за управување со ризици, за да се намали веројатноста од појава на некој претпоставен ризичен фактор и/или негово лошо влијание врз настанот. Иако ризиците не може целосно да бидат елиминирани, повеќето од нив сепак можат да се предвидат и со нив може да се управува однапред. Со нивна добра анализа и проценка може да се осигури непречено одвивање/развој на текот на ризичниот настан.

Управувањето со ризик треба да биде вклучено во сите фази од развојот на некоја активност, проект и сл. со цел да се овозможи посигурна основа за одлучување и планирање (AN/NZS 4360:2004)¹⁹. Ова во основа опфаќа:

- подобра идентификација на состојбата во системот и присутност на потенцијални опасности;
- проценка на добитоци и загуби од неизвесноста и различноста;
- проактивен менаџмент;
- поефективна распределба и употреба на ресурсите;
- подбиро управување со инциденти, намалување губитоци и трошоци од ризикот, вклучувајќи и комерцијални премии од осигурувањето;
- поголема безбедност и доверба;
- согласност со релевантното законодавство;
- поефективно управување со организацијата.

Од ова произлегуваат основните карактеристики и значење на управувањето со ризик и тоа:²⁰

- се создава основа што на организацијата и овозможува активностите во иднина да се одвиваат доследно и контролирано;
- произведува, структурира и претставува најдобри расположливи информации за ризикот со цел поддршка и олеснување во процесот на одлучување;
- овозможува подобра комуникација помеѓу управувачките одлуки и основа за нивно донесување;

¹⁹ New Zealand Standard on risk management, AS/NZS 4360:2004.

²⁰ Understanding Risk Analysis (1998), A Short Guide for Health, Safety and Environmental Policy Making, Produced by American Chemical Society, Internet Edition. pp.1-39.

- континуирано ги следи сите параметри од процесот подложни на промени и врз основа на информации од повратната врска врши ажурирање на иницијалните излези на елементите на процесот, но во согласност со целокупниот процес на одлучување;
- го испитува целиот спектар на ризици од релативно зачестените случувања со мали последици до мошне малку веројатните инциденти што може да нанесат значителна штета;
- ги идентификува и ги проценува релативните придонеси од активности за намалување на веројатноста од ризични настани и активностите за намалување на последиците доколку ризиците се материјализираат;
- ја олеснува комуникацијата помеѓу системот и јавноста (општеството) во поглед на природата на ризикот и рационалната база за одлучување во поглед на управувањето со дадени ризици;
- ја зголемува, ја интегрира и ја истакнува вредноста на информациите што се однесуваат на безбедноста;
- го следи сиот животен циклус на системот, земајќи ја предвид меѓузависноста на сите фази;
- придонесува кон поефикасно користење/распределба на ресурсите внатре во организацијата;
- го штити и зголемува имотот и имиџот на организацијата;
- ја развива и им дава поддршка на вработените и на базата на знаење во организацијата.

Со оглед на наведените карактеристики, управувањето со ризик не се согледува ниту се применува како посебен (изолиран) процес, туку е вклучено во организациската филозофија, работниот процес и процесот на управување со квалитетот на системот. Затоа може да се забележи и следната карактеристика на управувањето со ризик: информациите за управување со ризик се користат во интеракција со други информации, како што се, на пример, податоците за изводливост кои ќе го подобрат процесот за донесување одлуки.

На ниво на индивидуални компетенции, управувањето со ризици означува знаење, способност, подготвеност на менаџерите во процесот на водење на организацијата непрекинато да ги отстрануваат активните и потенцијалните опасности, деловните и безбедносните ризици и можности за настанување вонредни ситуации. Меѓутоа, за управување со ризици не е доволен само еден „менаџер на ризик“. За управувањето со ризици за да може да ја исполни основната намена, т.е. зголемување на веројатноста за успех и намалување на веројатноста за неуспех и неизвесност од постигнување на целокупните организациски цели, потребно е да се исполнат и други предуслови, како на пример:

- силна ангажираност и учество на повисокиот менаџмент на организацијата, што го чинат раководителите на сите сектори на работа или работни функции, на чело со главниот менаџер,
- организираност на процесот на анализа и одговор на ризиците, што подразбира усогласена хиерархија на работите и задачите во врска со процесите на управување со ризици,
- преведување на стратегијата за управување со ризици во тактички и во оперативни цели;
- распределба на одговорноста за ризик и одговорноста за изведување операции;
- интегрираност на процесот за управување со ризици во организациска култура со ефикасна политика и програма, што подразбира дека сите вработени го разбираат ризикот и својата улога во процесот на управување со него.

Управувањето со ризик мора да ја трансферира стратегијата на системот/организацијата во тактички и во оперативни цели, распоредувајќи ја одговорноста низ целата организациска структура, при што одговорноста за управување со ризик би требало да биде во описот на работата на секој менаџер и вработен. Управувањето со ризик придонесува кон појасно определување на одговорност, помага при мерење на успешноста, поделбата на признанија и на награди. Заради тоа овој процес треба да се интегрира во културата на организацијата заедно со делотворната политика и програма што ја води повисокиот менаџмент за да обезбеди реализација на конкретна цел или одлука.

4.2. Управување со ризик – концептуални аспекти

Управувањето со ризици од концептуален аспект, претставува процес на мониторинг и идентификација на ризикот, негова анализа и процена и избор на соодветна стратегија, мерки и активности за негов третман. Најчесто применувани стратегии за оваа намена се стратегијата за трансфер на ризикот, избегнување на ризикот, избегнување на негативните ефекти, односно ублажување на ризикот, стратегија за прифатлив ризик и други.

Управувањето со ризици и како теорија и како пракса е применлив концепт кога станува збор за природни катастрофи, техничко-технолошки несреќи, ризици од финансиски карактер и сл., но во последно време се настојува, управувањето со ризик да стане применлив концепт во сите области. Концептот на кризен менаџмент и концептот на управување со катастрофи, всушност се темелат на концептот на управување со ризик и ги ползуваат сите негови придобивки.

Еден од поголемите проблеми за имплементација на сеопфатен систем на управување со ризик е стабилна и доволна алокација на

финансиски ресурси, затоа што инвестиција во нешто што во моментот не е профитабилно или видливо е тешко оправдлива инвестиција. Заради балансирана алокација на финансиските ресурси во процесот на управување со ризик се применува пристапот на приоритетизација, користејќи го критериумот на фреквентност или зачестеност на појава и причинети негативни импликации.

Активностите кои се преземаат со концептот на управување со ризик се применуваат преку следните фази:

– *Идентификација на ризикот*: претставува прв чекор во управувањето со ризик. Ризиците се поврзани со потенцијални настани и ситуации, кои кога ќе се случат предизвикуваат одредени несакани, штетни последици и проблеми. Заради тоа постојаниот мониторинг и навремената идентификација на ризикот вообичаено започнува од изворот на проблемот, а тоа е одредена опасност.

– *Анализа на опасноста*: изворот на ризик за конкретен елемент изложен на ризик (систем, поединец, заедница, организација, објект и др.) може да биде надворешен или внатрешен. Првите, се поврзани со опкружувањето (risk environment), односно присутни опасности, а вторите се внатрешните карактеристики на изложениот елемент (ранливост/отпорност).

– *Анализа на проблемот*: вклучува процес преку кој се воопштува потенцијалниот проблем кој може да се јави како последица од идентификуваниот ризик и неговиот извор.

– *Процена на ризикот*: кога опасноста е идентификувана, односно кога е утврден потенцијалниот извор и очекуваниот проблем, се пристапува кон проценка на веројатноста од негово појавување и предвидување на сериозноста на последиците од неговото настанување. Првиот момент, веројатноста, за некои ризици кои почесто се случуваат може да се утврди, но за помалку веројатните ризици тоа е тешко (на пример, ризик од земјотрес), но затоа процената за сериозноста на последиците или штетите (очекувани) е полесно спроведлива, доколку постојат доволно квантифицирани податоци за изложената средина во близина на изворот на опасноста.

Самиот развој на теоријата и на праксата за „управувањето со ризик“ има свои концептуални аспекти кои во изминатите години поминуваа низ одредена генеза на развој, за да го достигнат денешното ниво на разбирање и применување. Заради тоа, во продолжение ќе се даде поопширен осврт на развојот на теоријата на управување со ризик (Risk Management).

Генералната рамка на развојот на концептот за управување со ризик или развојот на „парадигмата за риск менаџмент“, претставува тема на интерес неколку децении наназад. Најстариот, но некаде сè

уште актуелен пристап кон справувањето со присутните ризици, е да се игнорираат нивните закани.

До скоро време, во многу делови од светот, ниту населението ниту властите не сакаа сериозно да ја сфатат опасноста од ризиците кои ги опкружуваат (природни, социјални, еколошки, метеоролошки итн.). Причината за ваквата состојба можеби е поврзана со тоа што последниот „голем деструктивен настан“ се случил во далечното минато и секавањата за нив се губат или пак луѓето под влијание на потребата од постојани миграции, често го менуваат местото на живеење, а со тоа се губи континуитетот на нивната перцепција и меморија за ризикот.

Најчесто луѓето, особено во земјите во развој и неразвиените земји, под притисок на егзистенцијалните ризици (сиромаштија, глад, заразни болести и др.) се помируват со природните опасности, бидејќи се разбираат како феномени на „виша сила“ и дека тука не може многу да се направи. Сепак, ако не можат да се спречат, ризиците може да се намалат, односно да се намали нивното негативно влијание врз луѓето и заедниците.

Во раниот период од развојот на концептуалните аспекти за ризикот, беше евидентна присутноста на поистоветување на ризикот со опасност, или $P=O$ (ризик = опасност), односно целиот индивидуален и општествен капацитет беше насочен кон организација и обезбедување „физичка заштита“ од потенцијалната опасност и отстранување на последиците. Овој пристап кој уште се нарекува „реактивен“ и денес е карактеристичен во многу земји, па и кај нас.

Промените кои ги заговара современиот концепт на управување со ризик, подразбира зголемен проактивен пристап од поединците и од организациите, наспроти постојната инертност во врска со присутните ризици. Оттука, општествата преку своите специјализирани агенции, имаат одговорност да ги определат и да ги дефинираат ризиците и факторите кои водат кон кризи и катастрофи и да одлучуваат за преземањето соодветни акции, како би можеле ризиците да се контролираат или да се управуваат (Birkmann, 2006).

На конференцијата во Јокохама во 1994 (Стратегија од Јокохама), посебен нагласок беше ставен врз социоекономските аспекти како компонента на ефективното управување со ризик и спречување на катастрофи и беше утврдено дека социјалните фактори, економската состојба и довербата во политичката одговорност, културната традиција, религиозните вредности, се исто така важни елементи во дефинирањето на хуманата и социјалната (човековата и општествената) подложност на ризици.

Во периодот од 1990 година до 2000 година, во рамките на Меѓународната декада за намалување на природните катастрофи (International Decade for Natural Disaster Reduction-IDNDR), а сèра и

во рамките на нејзиниот наследник, Меѓународната стратегија за намалување на катастрофи (International Strategy for Disaster Reduction (ISDR), беше потенцирана потребата од посеопфатен пристап во кој ќе се прават обиди за избегнување или ублажување на ризикот пред појавата на несреќата/катастрофата, што истовремено ќе поттикнува на зголемување на свеста на јавноста, поголема посветеност на сите учесници, поголема размена на знаења како и партнерства за имплементација на разните стратегии за намалување на ризикот на сите нивоа (UN-ISDR, 2005).

Овој проактивен концепт е препознатлив и како „циклус на управување со ризикот“, или „спирален“ концепт во кој учењето од катастрофите, може стимулативно да влијае за зајакнување на мерките за адаптирање и измени во просторното планирање наместо пристапот за едноставно создавање социјални и физички услови за живот кои претходно постоеле.

Целта на ISDR е да изгради општества отпорни на ризици од катастрофи со промовирање на зголемена свест за важноста на намалувањето на катастрофите како интегрална компонента на одржливиот развој, со цел да се намалат човечките, социјалните, економските и еколошките загуби од природни опасности, техничко-технолошки катастрофи и катастрофи поврзани со животната средина.

Генералниот императив на концептот на управување со ризик кој се развива и промовира во рамките на глобалната иницијатива преку „Рамката за акција 2005-2015“²¹ е фокусиран на „градење на отпорност“, индивидуална и колективна/општествена. Ова не значи игнорирање на причините (ризиците), туку напротив, обезбедување зголемена свесност за нив и преземање сеопфатни активности за подготвено дочекување и справување со нив. Заради тоа во изминатите години приоритетот на интерес на концептуалниот пристап во управувањето со ризик, беше насочен кон неговите компоненти, како што се ранливост, изложеност, односно дефинирање на елементите на ризик и градење на капацитет за отпорност.

Овој комплексен пристап овозможува подетално осознавање, анализа и процена на секој сегмент засебно и преку нив определување на збирна оцена на ризикот. Врз овој пристап се темелат и насоките, препораките и стандардите врз кои се гради капацитетот во Европската унија и кај многу други земји во светот преку иницијативите на UN-ISDR.^{22, 23, 24}

²¹ Памка за акција од Xjoro 2005-2015: <http://www.unisdr.org/we/coordinate/hfa>.

²² Risk Assessment and Mapping Guidelines for Disaster Management.

²³ Risk mapping a common European methodology.

²⁴ ISO 31000:2009, Risk management.

Република Македонија е во чекор со овие насоки и има евидентен напредок во нивната имплементација, како во нормативната рамка, така и во нивното практикување.

Во продолжение ќе се даде осврт на генезата на развојот на концептот за управување со ризик во контекст на изнесената рамка.

4.3. Генеза на развојот на концептот за управување со ризик

Под влијание на глобалните иницијативи, во периодот на изминатите години, забележливи се промените во однос на пристапот од „одговор на ризици и елиминирање на последиците“ кон пристап на „управување и намалување на ризикот“. Промените во перцепцијата главно беа врзани со промени на пристапот кој беше фокусиран врз опасноста (хазардот) како главен причинител на ризикот и намалување на ризикот единствено со мерки на физичка заштита од опасноста. Подоцна, управувањето со ризик, поголемо внимание посветува на ранливоста на заедниците и поединците, на подготвеноста и капацитетот за рано предупредување, на зголемување на свеста и градење стратегии за справување со несреќи и катастрофи.

Некои од аспектите од развојот на парадигмата за ризикот се однесуваат на следните елементи:

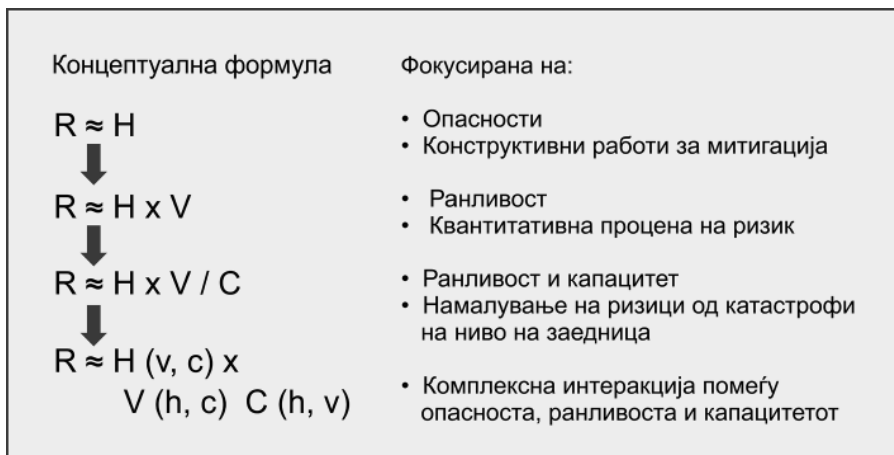
– **Технократска или бихејвиористичка парадигма:** почетните гледишта за ризикот, во рамките на оваа парадигма беа такви што ризикот го сведуваа/поистоветуваа со опасност (hazard) или главно се фокусираа на него. Аналогно на ова, управувањето со ризици или професијата „Риск менаџер“ беше ексклузивно право на професионалци од областа на природните и техничките науки (геолози, инженери, метеоролози, итн.). Сепак, ниту едно од овие гледишта, реално не го опфаќаше прашањето за тоа какви услови создава општеството, во кое луѓето на различен начин се соочуваат со опасностите. Првиот приод беше непомирливо „натуралистички“, при што целата вина беше префрлена на „суровите сили на природата“, а луѓето и општеството единствено се насочуваа кон физичката заштита од опасностите. Ваквата состојба беше присутна сè до појавата на идејата за „ранливоста“ во објаснувањето на катастрофите (Blaikie, 2004).

– **Парадигма на физичка ранливост:** со појавувањето на ранливоста на „сцената на ризикот“, разбирањето на претходно забележливиот фокус на „физичката заштита“ на луѓето и изградените системи, генезата на концептот за управување со ризик се проширува кон аспектот на „однесувањето на луѓето“. Овој концепт доведе до проектирање и користење системи за рано предупредување и едука-

тивни програми за опасностите и подготовка како луѓето да се заштитат од нив. Оваа парадигма траеше две декади и дури беше користена за време на Стратегијата од Јокохама и Планот за акција за безбеден свет (Yokohama Strategy and Plan of Action for a Safer World 1994), при што сите напори беа фокусирани врз зголемување на научните знаења за причините и последиците од природните опасности и олеснување на нивната широка примена во намалувањето на ранливоста на изложениите заедници. Оваа промена во концептот овозможи основа за градење капацитет за сеопфатно управување со ризикот.

– **Парадигма на сложеност:** појавата на новите сфаќања за сложената интеракција меѓу природата и општеството ја предизвика потребата од преземање нов, сложен приод кон сфаќањето на ризикот. Според парадигмата на сложеност, ранливоста не се однесува само на групи или поединци, туку таа е поврзана и со сложени општествени односи и процеси, што упатува на потребата од вклученост на сите општествени сегменти (политика, економија, право, наука, технологија итн.) во процесот на управување со ризиците и обезбедување безбедна работна и животна средина во современите услови на живеење.

Генезата за развој на концептот за управување со ризик, илустративно е претставен на Слика број 3:



Слика 3: Промени во парадигмата на управување со ризик од приод фокусиран врз опасност во приод кој ја препознава сложената интеракција меѓу опасностите, ранливоста и капацитетот на заедницата која е изложена на ризик.

(Извор: Thea Hillhorst, Disaster Studies Wageningen.)

UN-ISDR ризикот го дефинира како „комбинација од веројатност за појава на еден настан и неговите негативни последици“, што претпоставува, „веројатност за појава на штетни последици или очекувани загуби (загуба на човечки животи, повреди, загуба на имот, егзистенција, прекинати економски активности или штети врз животната средина) кои резултираат од интеракциите помеѓу опасностите (природни и предизвикани од човекот) и условите на ранливост“.

Основната функција на ризикот која може да се подели на елементите: опасност, ранливост и елементи изложени на ризик од опасност е прикажана на следната слика:



Слика 4: Функција на ризикот која може да се подели на елементите: опасност, ранливост и изложеност

Овој пристап кој се промовира во рамките на иницијативите на UN-ISDR, во концептуалната рамка која ја дава Davidson во 1997 година, подоцна прифатена од страна на Bollin и соработници во 2003 година,

на ризикот се гледа како на збир од опасност, изложеност, ранливост и мерки поврзани со капацитет. Новиот елемент кој се забележува се однесува на мерки поврзани со капацитет, што подоцна ќе еволуира кон концептот на отпорност.

Опасноста се препознава со веројатност и јачина на феноменот, елементите на изложеност се поврзани со физичката и изградената средина, а капацитетот и мерките се однесуваат на урбано планирање, управување, социјален и економски капацитет (Слика 5).



Слика 5: Дејвидсонова – Болинова концептуална рамка за идентификација на ризик од катастрофа
(Извор: Davidson, 1997; Bollin и сораб., 2003)

„Триаголникот на ризик“ на Juan Carlos Villagrán de León исто така ја дефинира ранливоста во контекст на опасноста и ризикот.²⁵ Овој триаголник на ризик се состои од три компоненти, ранливост, опасност и недоволна подготвеност (отсуство на капацитет). Тој ја дефинира ранливоста како претходно постојните услови кои ги прават инфраструктурата, процесите, услугите и продуктивноста поподложни на влијанието на надворешната опасност. За разлика од позитивната дефиниција на капацитетите за справување, тој го користи терминот „недоволна подготвеност“ за да го опфати недостатокот од капацитети за справување на едно општество или специфичен елемент изложен на ризик.

²⁵ <http://www.ehs.unu.edu/image/view/4868>.

Врз основа на претходно изнесеното, ризикот концепциски се презентира преку следните функционални равенства:

[1] Ризик = Опасност * Ранливост * Број на елементи изложени на ризик, и

[2] Ризик = Опасност * ранливост / Капацитет

Првото равенство [1] повеќе се однесува на проценување на директни (физички, човечки и економски) загуби, додека второто функционално равенство [2] претставува поширока концепциска рамка и овозможува внесување на мулти-димензионални аспекти на ранливоста и капацитетот кои честопати се интегрирани со индикаторите на опасноста.

4.4. Ранливоста во концептот на управување со ризик

Покрај фактот дека процената на опасноста, како и квантификацијата на изложеност се комплексни и мултидисциплинарни аспекти во процесот на управување со ризикот, ранливоста и поврзаните со неа динамички промени во нејзиното толкување и дефинирање, дадоа клучен придонес во промената на парадигмата на управувањето со ризик. Имајќи предвид дека традиционалниот пристап претставува „технократска“ логистика на процената на ризикот која ја фокусира на „сили и дистрибуција на опасноста“ и „квантификација на концентрацијата“ на елементи изложени на ризик, во последните две децении примарното фокусирање на ризик менаџментот се насочува кон „ранливоста“.

Овој пристап придонесе за промена на пристапот од „Намалување ризици од катастрофи“ (DRR) кон „управување со ризик од катастрофа“ (DRM). Глобалните иницијативи за промовирањето на општества кои се отпорни на катастрофи бараше и промена на парадигмата од нејзиниот примарен фокус врз опасностите и нивна квантификација кон идентификација, процена и рангирање на елементите на ранливост (Maskrey, 1993; Lavell, 1996; Bogardi и Birkmann, 2004).

Во литературата се наоѓаат околу триесетина различни дефиниции, концепти и методи за систематизирање на ранливоста (на пример, Chambers, 1989; Bohle 2001, Wisner и сораб., 2004; Downing и сораб., 2006; UN-ISDR, 2004; Pelling, 2003; Luers, 2005; Green, 2004; UN-Habitat, 2003; Schneiderbauer и Ehrlich, 2004; van Dillen, 2004; Turner и сораб., 2003; Cardona, 2004b). Веб страницата на конзорциумот ProVention вклучува околу 20 прирачници и различни водичи за тоа како да се процени ранливоста и ризикот (ProVention Consortium website).²⁶ Овие прирачници,

²⁶ <http://www.proventionconsortium.org/>.

исто така, вклучуваат различни дефиниции и различни концептуални рамки за ранливоста.

Иако на ранливоста треба да се гледа како на нешто што има повеќестрана природа (Bohle, 2002a, 2002b), различните дефиниции и пристапи покажуваат дека не е јасно што токму значи „ранливост“ како клучен елемент од концептот на процена и управување со ризик. Иако не постои универзална дефиниција за ранливост, неколку дисциплини развија свои сопствени дефиниции и аналитички согледувања за тоа што всушност значи ранливоста. Она што е заедничко од нив се однесува на следното:

- *ранливоста е повеќедимензионална*, односно опфаќа/засега различни сегменти (на пример, физичка, социјална, економска, енвиронментална, институционална);
- *ранливоста е динамичка* (ранливоста се менува во текот на времето, во зависност од опаностите и проактивните општествени функции);
- *ранливоста е зависна од насоченоста* (ранливоста може да се изрази во различен размер која се движи од човек, објект, организација, заедница па се до држава);
- *ранливоста е специфична по локација* (за секоја локација ранливоста е различна и специфична во однос на карактеристиките на микропросторот).

Заедничкиот содржател на изнесените гледишта за ранливоста укажува дека таа како компонента на ризикот, се наоѓа во фокусот на интерес и претставува определувачки фактор на вкупниот ефект на ризикот.

Во теоријата од оваа област се зборува за повеќе видови ранливост (прикажано на Слика 6):

– *Физичка ранливост*: што значи потенцијал за физичко влијание врз изградената средина и населението. Степен на загуба во врска со даден елемент изложен на ризик или група елементи изложени на ризик.

– *Економска ранливост*: потенцијално влијание на опасностите врз економските добра и процеси (односно прекин во деловните активности, секундарни влијанија, како што се зголемена сиромаштија и загуба на работни места). Се манифестира преку ранливост на различни економски сектори.

– *Социјална ранливост*: потенцијални влијанија на настаните врз групи како што се сиромашни домаќинства, домаќинства со посебни потреби, хендикепирани, деца, постари, како и врз вкупните социоекономски процеси во општеството.

– *Еколошка ранливост*: потенцијални негативни влијанија на настаните врз животната средина и природните богатства.



Слика 6: Видови ранливост

Денес на способноста да се измери, односно да се процени ранливоста сè повеќе се гледа како на клучен чекор кон ефективно намалување на ризикот и промоција на култура на отпорност на ризици од несреќи. Од аспект на зголемената честина на несреќите и постојаната деградација на животната средина, мерењето на ранливоста е важна задача ако науката сака да го поддржи концептот за градење поотпорен свет (Kasperson и соработници, 2005).

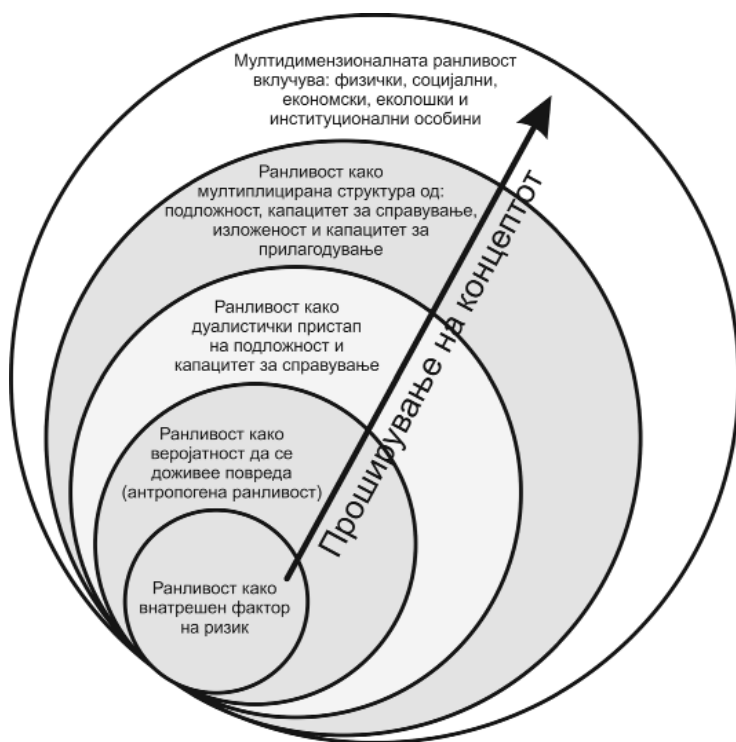
Во овој контекст, Рамката од Хјого ја потенцира потребата од развивање индикатори на ранливост како „клучна активност“, односно:

„Да се развијат системи од индикатори на ризик од катастрофи и ранливост на национално и субнационално ниво кои ќе им овозможат на оние кои донесуваат одлуки да го оценат влијанието на катастрофите врз социјалните, економските и еколошките услови и да ги пренесат резултатите на донесувачите на одлуки, јавноста и народите изложени на ризик“.

Иако меѓународната заедница не формулира водич за тоа како да се развијат индикатори или системи од индикатори за оценка на ранливост (Birkman, 2006), Рамката за акција од Хјого го потенцира фактот дека влијанието на катастрофите врз (1) социјалните, (2) економските, и (3) еколошките услови треба да се истражи преку таквите индикатори. Бидејќи одржливиот развој се карактеризира со три столба – социјален, економски и еколошки (UN, 1993; WCED, 1987).²⁷

²⁷ Светска комисија за животна средина и развој (WCED) (1987). Нашата заедничка иднина: Извештај на Светската комисија за животна средина и развој. Извештај Brundtland, Оксфорд: Oxford University Press.

Проширувањето на концептот на ранливост илустрирано е прикажан на Слика 7. Таа покажува дека концептот започнал со основно поимање на „ранливоста како внатрешен фактор на ризикот“ (првиот внатрешен круг), а потоа процесот се отвора сè до крајната фаза која се препознава како „мултидимензионална ранливост“ (последниот надворешен круг), која во себе ги опфаќа физичките, социјалните, економските, еколошките и институционалните димензии на ризикот.



Слика 7: Концентрични сфери на развој на концептот на ранливост,
(Извор: Birkmann 2005)

Концептите на ранливост според (UN/ISDR, 2004; Cardona, 2004a/b; Wisner, 2002; Thywissen, 2006) ранливоста ја препознаваат како „внатрешна страна на ризикот“ (внатрешниот круг на сликата) и ова може да се дефинира како една општа или појдовна основа. Проширување на оваа дефиниција може да се види кај Wisner (2002), според кого, ранливоста се дефинира како веројатност за повреда, смрт, загуба и нарушување на егзистенцијата во услови на екстреман настан, и/или невообичаени потешкотии во надминувањето негативни влијанија од опасните настани (вториот круг од сликата).

„Веројатноста за повреда“ е проширена со фокусирање врз дуалистичката структура на ранливоста што може да се види во дефинициите дадени од страна на (Визнер –2002), како и делумно во дефинициите дадени од страна на (Чамберс – 1989) и (Бојл – 2001). Визнер јасно ги идентификува „веројатноста за повреда“ и „невообичаени потешкотии во надминување на последиците“ од такви настани како клучни карактеристики на ранливоста. Бојловата двојна структура на ранливоста не се однесува само на „изложеноста“ и „справувањето“ туку по прво се однесува на карактеристиките на ранливоста кои се надворешни во однос на изложениот елемент. Разликувањето на овие две сфери, односно „надворешна изложеност“ и „внатрешни состојби“ има за цел да нагласи дека, ранливоста се однесува и на карактеристики поврзани со капацитети за предвидување и справување. Во овој контекст, третиот круг може да се поврзе со „дуалистичката структура на ранливоста“ што го потенцира фактот дека ранливоста е обликувана и дефинирана од веројатноста за повреда, способноста и капацитетот за справување и елиминирање на последиците од негативните влијанија од опасниот настан (Wisner, 2002).

Дополнително проширување на концептот на ранливост е промената од двојна во повеќекратна структура. Концептуалната рамка на Bohle (2001), веќе го потенцира фактот дека ранливоста е мултиаспектен концепт. Четвртиот круг на сликата го прикажува концептот на повеќекратната структура на ранливост, која опфаќа изложеност, чувствителност, подложност, капацитет за справување, адаптација и одговор.

Концептуалната рамка за холистичкиот пристап во процената на ризикот од катастрофа со теоријата на Кардона (Cardona 1999, 2001) и неговите истражувања заедно со Хуртадо и Барбат во 2000 година. Во нивниот прв концепт, ранливоста се состоеше од изложени елементи при што беа земени предвид неколку димензии или аспекти на ранливоста кои се однесуваа на три категории или фактори на ранливост:

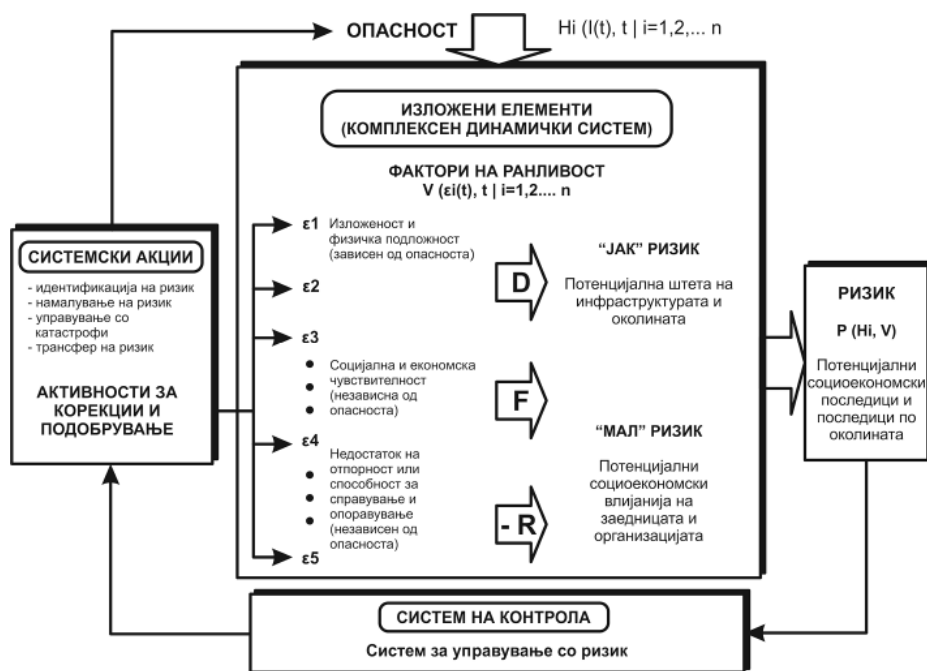
- физичка изложеност и подложност што е назначено како голем ризик кој зависи од опасноста;
- чувствителност на социјалноекономскиот систем што претставува мал ризик и не зависи од опасноста;
- недостаток на способност за справување и опоравување што исто така е дефинирано како мал ризик кој не зависи од опасноста.

Според оваа рамка, ранливоста зависи од изложеноста и подложноста на физичките елементи во подрачја изложени на опасности, од една страна, како и од социјалноекономската чувствителност и недостатокот од социјална отпорност и способност за справување, од друга страна. Пристапот го нагласува фактот дека индикаторите или

индексите треба да обезбедат мерење на ранливоста од сеопфатна и мултидисциплинарна перспектива и ги посочува *изложеноста и подложноста* како неопходни услови за постоење на физичкиот (голем) ризик. Од друга страна, веројатноста да се почувствуваат негативни влијанија како социјално-економски ефекти, се исто така услови на ранливост кои се сфаќаат како „мал“ ризик.

Во 2006 година, овој модел беше употребен за проценка на ризикот од катастрофи на национално ниво во рамките на Програмата за индикатори на ризик од катастрофи и управување со ризик за Северна и Јужна Америка (Cardona, 2006) како и на субнационално ниво и за градовите Барселона и Богота (Carreño и соработници, 2005a, 2005b).

На следната слика број 8 прикажана е рамката на овој модел:



Слика 8: Теоретска рамка и модел за холистички пристап за проценка на ризик и управување со катастрофи
(Извор: Cardona и Barbat, 2000²⁸)

²⁸ Преземено од: Holistic Urban Seismic Risk Evaluation of Megacities, Omar D. Cardona and all: <http://barbat.rmee.upc.edu/papers/%5B56a%5D%20Carre%C3%B1o,%20Cardona,%20Marulanda,%20Barbat.%202009.pdf>.

4.5. Управување со ризик – мерки за намалување на ризикот

4.5.1. Собирање, анализа и мапирање на податоци за ризикот

Собирањето, анализата и синтезата на релевантни податоци опфаќа активности за идентификација и мапирање на податоците кои се поврзани за очекуваниот настан, очекуваните последици како и резултатите од проценетото сценарио: локација (каде), почеток и развој (како) и јачина (интензитет, степен).

Преку оваа постапка се обезбедува соодветна печатена збирка (база) на податоци, со обезбедена информатичка поддршка и во зависност од условите вклученост на Географски информациски системи (ГИС), заради просторен приказ на состојбите. На овој начин се систематизираат, се поврзуваат и се визуелизираат податоците за:

- територијата со сите топографски, хидрографски, демографски и други елементи неопходни за потребите на процесот за управување со ризик,
- сите бази на податоци поврзани со компонентите на ризикот, односно информациско-документаристички бази за опасностите, бази со податоци за изложените елементи на ризик (население, изградена средина, природа и друго) и податоци за нивната ранливост,
- сите бази на податоци кои содржат информации за капацитетите на системот (ресурси и сл.)
- резултатите од различни анализи, симулации и сценарија на опасности,

Мапирањето на елементите на ризикот претставува многу корисна техника и алатка во современиот процес на управување со ризици и во значителна мерка го поддржува процесот на донесување одлуки. За да се воспостави конзистентно и ефикасно мапирање, потребно е да се исполнат повеќе предуслови, како на пример: воспоставување стандарди за унифицирана дискретизација (опис – расчленување) на анализираната територија во помали територијални единици со големина (размер) адекватен за успешно следење на сите варијабли кои ја карактеризираат дистрибуцијата и концентracијата на опасностите и изложеноста. Размерот на основните карти треба да биде што помал и адекватен за потребите и резолуцијата којашто е потребна за поставената цел. Во принцип, дискретизацијата започнува од најмалата просторно-административна единица, во согласност со позитивната законска регулатива (катастарска општина, населено место, општина итн.).

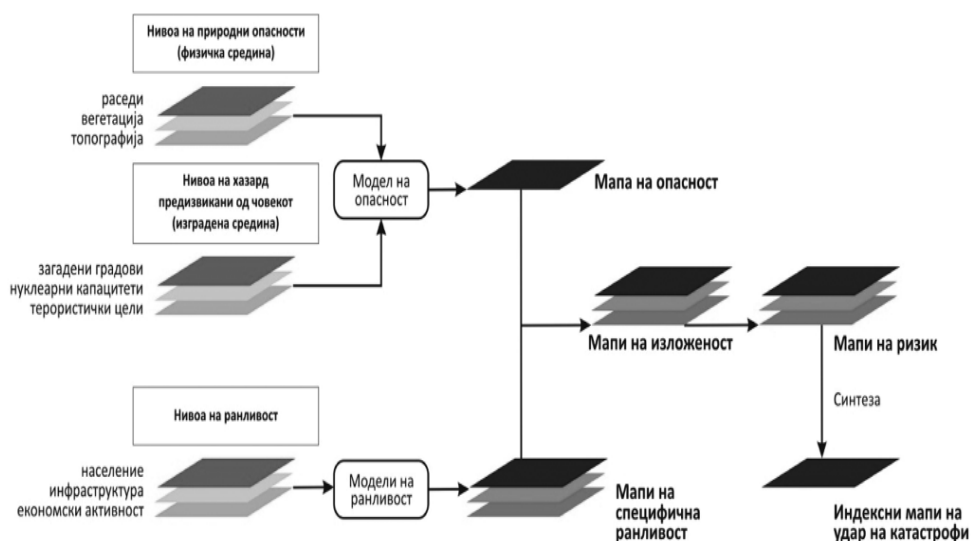
Друг предуслов за успешно мапирање на просторни податоци претставува примената на унифицирана и стандардна координатна мрежа, односно примена на x/y еквилидистантна мрежа. Заради компатибилност и интероперабилност со светските стандарди (WGS84) основата мапа треба да биде усогласена со нив, за да се обезбеди директна комуникација и интеграција на податоците.

Начелен пример за минималната збирка која треба да ја содржат базите со податоци за опасности, изложените елементи на ризик, ресурси и други капацитети на системот, како основни извори на информации за процесот на мапирање на ризикот, се прикажани на следната табела:

Внес на податоци	Проверка на конзистентноста на податоците и грешки при внес
Модификација	Подесување на параметрите, овозможување на модификации
Пребарување	Пребарување на која било локација според кој било податок поврзан за неа (објекти, инфраструктура, користење на земјиште и др. елементи на ризикот)
Статистика	Мултикритериумско пребарување и статистика
Географска или територијална поделба	Можност да се процесираат податоците за специфична географска површина за покривање различни потреби за менаџирање на несреќите и подготовка на планови
Експорт на податоци	Експорт на податоци во стандардни формати (како што се txt, xls, dbf)
Заштита	Ограничен пристап до некој или до сите податоци со дефинирани кориснички протоколи
Излези	Релевантни временски и пробавилистички карти (тематски слоеви), други карти, статистика и аналитички извештаи

Табела 1: Податоци, извори на податоци и функции за процесот на мапирање

На следниот шематски приказ (Слика 9) дадена е визуелизација на поставеноста на потребните бази со податоци и нивната меѓусебна поврзаност за потребите на мапирање и изработка на тематски слоеви за елементите на ризикот, според Насоките за развивање на методологији за процена на ризици и нивни импликации за потребите на Системот за управување со кризи во Република Македонија (Милутиновиќ 3., 2009):



Слика 9: Визуелизација на дел од тематските слоеви (мапи) по фази на нивна изработка

4.5.2. Мониторинг на опасности и рано предупредување

Навремената идентификација, процената, мониторингот на опасностите, како и раното предупредување за нив претставуваат клучни постапки во процесот на управување со ризик и елиминирање и/или намалување на негативните влијанија на ризиците и со нив поврзаните настани и состојби (вонредни, кризни ситуации и катастрофи). Преку овој процес се реализираат активности поврзани со:

- Идентификување на појавата (опасноста) која претставува клучен проблем за генерирање вонредна, кризна ситуација и катастрофа;
- Процена на природните и општествените аспекти на опасноста, како и процесите поврзани со ранливоста и капацитетот на организацијата за справување со несреќи/катастрофи;
- Мониторинг/следење на состојбите на ризикот во горните две области, при што мониторингот на опасноста е „повидлив“ од мониторингот на ранливоста;
- Рано предупредување поткрепено на резултатите од целиот претходен процес и десиминација на податоците до клучните субјекти со цел истото да генерира/поттикне соодветен одговор од надлежните субјекти на претстојните опасности.

Раното предупредување станува круцијална компонента во процесот на управување со ризици. Истото може да овозможи „обезбедување“ на потребно време за избегнување на деструктивните сили

на потенцијалната опасност, а со тоа избегнување загуба на животи и материјални добра. Современиот технолошки развој на алатките за набљудување и предвидување, можностите за моделирање на климатските и геофизичките настани, заедно со подобрените технологии за комуникација, доведоа до прогресивен развој на техничката основа за мониторинг на опасностите и рано предупредување.

Мониторингот на ризици е строго зависен од опасноста. Методологиите и постапките исто така зависат од видот на опасноста. Тие треба да бидат високо специјализирани и насочени кон мониторинг на карактеристичен индикатор или група на карактеристични индикатори кои, како претохдници, ќе ги индицираат (најават) условите кои, со висока веројатност, може да предизвикаат реализирање на одредна опасност и материјализација на негативните ефекти на ризикот поврзан со таа опасност.

Истакнувањето на важноста на мониторингот и раното предупредување бара долгорочна посветеност со изразена политичка, финансиска и институционална поддршка и широко разбирање од надлежните субјекти. Воспоставувањето одржлив систем за управување со ризици и намалување на ризиците од катастрофи, има потреба од постојано ажурирање на податоците за ризиците. Поради тоа постојано треба да се бара развој на технологии за мониторинг на ризикот, што значи и постојано проширување на рамката на процена на ризикот. Мора да се напомене фактот дека постои голема неадекватност или отсуството на општо прифатени пристапи кои ќе наметнат одредени стандарди во оваа област, што доведува до неусогласеност на активности во оваа област.

5. ПОЛИТИКИ И РАМКА ЗА УПРАВУВАЊЕ СО РИЗИК

5.1. Политики за управување со ризик

Политиките за управување со ризици треба да бидат усогласени со целите на организацијата, односно да бидат спроведливи и во основа да ги содржат следните елементи:

- одговорност и овластувања за управување со ризици;
- извршување периодични проверки и верификација на концептот и на политиката за управување со ризици, преку нивно постојано унапредување;
- врски помеѓу политиката и целите на организацијата;
- подготвеност на организацијата за ризици;
- процеси и методи за управување со ризици;
- ресурси што стојат на располагање за остварување на улогата и одговорноста за управување со ризици; и

- начин на кој ќе се мерат резултатите и ќе се известува за резултатите од управувањето со ризици.

Потребно е организацијата да развие практични методи и средства за примена на функциите за управување со ризици, вклучувајќи *распределба на соодветни ресурси* за функцијата управување со ризици, кои ќе го опфатат следното: документирани процеси и процедури, информациски системи, човечки ресурси и вештини како и материјални ресурси неопходни за секој чекор од процесот на управување со ризици.

Заради обезбедување релевантни информации за потребите на процесот на управување со ризици, потребно е системот или организацијата да воспостави интерен информативен систем со механизми на известување. Овие механизми треба да ги опфатат процесите за собирање информации за ризикот, во кои ќе бидат вклучени разни извори во организацијата, земајќи ја предвид нивната чувствителност и значење. За интерната комуникација е особено важно таа да се одвива на законит, правно заснован начин и под мандат на органите за управување, заради осигурување транспарентност и градење доверба во организацијата. Со цел да се обезбедат повратни информации во комуникациите меѓу вработените, интерното известување мора да опфати информации за ефективност и резултати од концептот за управување со ризици.

Исто така, организацијата треба да развие и да примени план за да се обезбеди комуникација со екстерни заинтересирани страни. Покрај ефективната размена на информации, комуникацијата со заинтересираните страни особено би требало да опфати комуникација во случај на вонредна ситуација или несреќа.

Особено е важно управувањето со ризици да стане составен дел од политиките за развој на организацијата, од стратегиското планирање и од процесот на управување со промените. Поради тоа управувањето со ризици треба да биде вклучено во организациската пракса и работни процеси на релевантен, ефективен, ефикасен и одржлив начин.

5.2. Рамка на процесот за управување со ризик (ISO 31000:2009)

Генералната *рамка за управување со ризик* е дефинирана со меѓународниот стандард ISO 31000:2009 (Слика 10). Оваа рамка им помага на организациите ефикасно да управуваат со ризиците преку примена на процесот на управување со ризик на различни нивоа и во специфични контексти на состојби во кои може да дејствува организацијата. Рамката треба да обезбеди информациите за ризикот, изведени од овие процеси, да бидат адекватно соопштени и искористе-

ни како основа за донесување одлуки и одговорности на сите релевантни организациски нивоа.

Оваа рамка за управување со ризик не е препорачана со цел генерално да го опише системот на управување со ризик, туку да им помогне на организациите да го интегрираат управувањето со ризик во својот организациски систем на управување. Значи, организациите треба да ги приспособат елементите на рамката кон своите специфични потреби. Ако постојните практики за управување и процеси на организацијата опфаќаат елементи на управување со ризици, или ако организацијата има веќе усвоен формален процес на управување со ризик за одделни видови ризици или ситуации, тогаш тие треба критички да се разгледаат и да се оцени нивната согласност со овој меѓународен стандард.

Имплементацијата на рамката за управување со ризици опфаќа:

- интегрирање на политиката и процесот на управување со ризик во организациските процеси во согласност со планот;
- комуникација со заинтересираните страни за да се обезбеди концептот за управување со ризик да одговара на потребите на заинтересираните страни;
- донесување одлуки, во согласност со примената на процесот за управување со ризици;
- поставување лице одговорно за имплементација на концептот и
- обука и увежбување.



Слика 10: Приказ на меѓусебната поврзаност на компонентите во рамката за управување со ризици

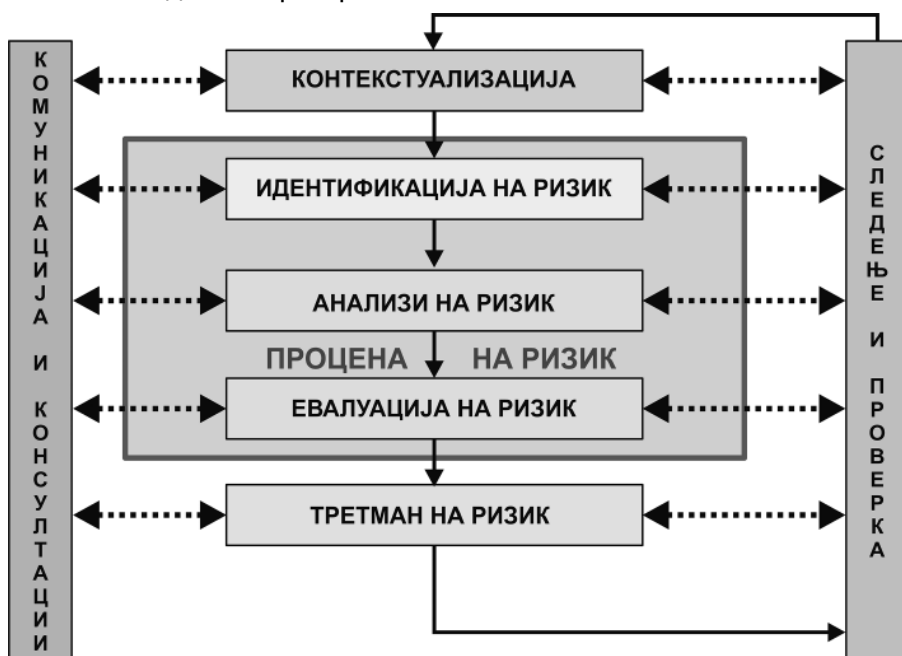
(Извор: ISO TMB on Risk Management ISO CD 31000:2009)

5.2.1. Генерална рамка на процесот на управување со ризик

Управувањето со ризици вклучува разни политики, процедури и практики на процена, следење и контрола на ризикот. Поради фактот дека со ризиците може да се управува на различни начини во зависност од социјалниот контекст, не постојат апсолутно сигурни методи. Во оперативна смисла, управувањето со ризик се дефинира како процес на идентификување, верификување, комуницирање, мерење и мониторинг на клучни ризици што се критични за успехот или неуспехот на системот или организацијата.

Процесот на управување со ризик треба да биде составен дел од управувањето, да биде вграден во организациската култура и пракса, но и приспособен кон деловните процеси во организацијата. Процесот на управување со ризик, според ISO 31000, опфаќа пет активности (Слика 11):

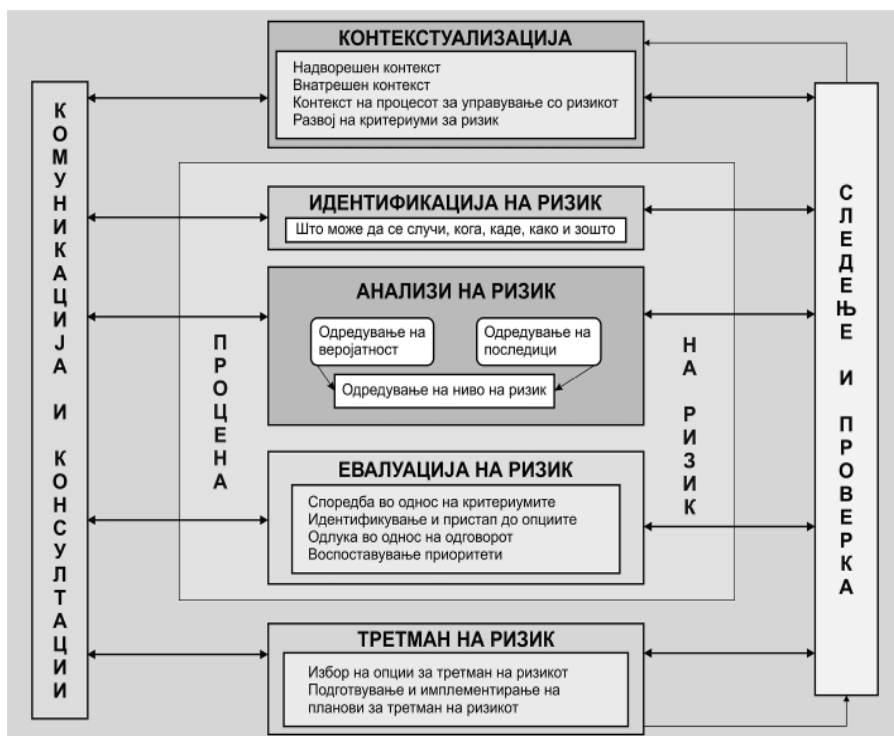
- комуникации и консултации,
- воспоставување контекст (контекстуализација),
- процена на ризикот (идентификација, анализа и евалуација на ризикот)
- третман на ризикот,
- следење и проверка.



Слика 11. Процес на управување со ризик според ISO 31000:2009
(Генерална рамка)
(Извор: ISO 31000:2009)

5.2.2. *Детаљна рамка на процесот на управување со ризик*

Секоја организација треба јасно да ја дефинира својата политика, односно генералната рамка за управување со ризик. За да ја преточи во детални насоки за управување со ризици, што подразбира изработка на соодветен документ (план, насоки, оперативни процедури итн). Без разлика на тоа дали организацијата дејствува во јавен или во приватен сектор, рамката на управувањето со ризици, треба да ги содржи деталите кои треба да се преземаат во процесот на управување со ризик, како што е прикажано на следната шема (Слика 12):



Слика 12. Процес на управување со ризик според ISO 31000:2009 (Детаљна рамка)
(Извор: ISO 31000:2009)

Детаљната рамка во процесот на управување со ризик според ISO 31000:2009, ги појаснува петте фазите или чекорите кои ги поставува генералната рамка за управување со ризици, со цел тие понатаму да се трансферираат во соодветен документ (план, насоки и сл.) на организацијата за управување со ризик, во својот делокруг на одговорности и надлежности:

– *Комуникации и консултации*: заради воспоставување постојана комуникација, консултации и координација помеѓу вклучените субјекти во управувањето со ризици, на сите нивоа, се препорачува организацијата да донесе стандардна процедура со која ќе ги пропише потребните мерки и активности, ќе ги определи носителите за нивно извршување итн.

– *Воспоставување контекст (контекстуализација)*: за потребите на воспоставување целосен контекст во чиешто рамки ќе се спроведуваат активностите за управување со ризик, потребно е датајлно да се разоткрие надворешниот и внатрешниот контекст, потоа контекстот на процесот во кој ќе се спроведуваат активностите за управување со ризикот како и да се развијат критериумите за ризик.

– *Процена на ризикот (идентификација, анализа и евалуација на ризикот)*: оваа фаза претставува многу важен сегмент од процесот на управување со ризици. При идентификацијата на ризикот надлежните субјекти треба да најдат (проценат) одговор на повеќе клучни прашања, како на пример, Што може да се случи, кога, каде, како, зошто? итн. Понатаму преку активностите за анализа на ризикот се настојува што попрецизно да се процени/предвиди веројатноста за случување во контекст на претходно отворените прашања, да се предвидат очекуваните последици и според тоа да се определи нивото на ризикот. Преку евалуацијата на ризикот се врши споредба со поставените критериуми, се разгледуваат опциите и одлуките за одговор и се определуваат приоритети за оперативно дејствување.

– *Третман на ризикот*: Колку наведените активности во претходната фаза ќе бидат целосни и прецизни, толку ефикасни ќе бидат стратегиите, политиките и конкретните мерки и активности за третман на ризикот.

– *Следење и проверка*: заради следење на ефикасноста на преземените мерки и активности во процесот на управување со ризик, како и заради преземање мерки за корекции во плановите, потребно е да се воспостави процедура за следење и проверка.

Со воспоставување формален, организациски и материјално поддржан проце за управување со ризици се настојува во целост да се елиминираат сите ризици. Ова е практично невозможно, па оттука се настојува да се создаде околина во која може да се донесуваат оптимални одлуки, имајќи ги предвид идентификуваните ризици и потенцијалните последици што тие може да ги предизвикаат. Концептот за управување со ризици овозможува системско создавање на реална и одржлива рамка за спречување несреќи, односно за минимизирање на ризиците кои може да се случат како резултат на вообичаените процеси, активности и дејности на системот, односно организацијата.

6. МОНИТОРИНГ И КОНТРОЛА НА ПРОЦЕСОТ ЗА УПРАВУВАЊЕ СО РИЗИЦИ

6.1. Ажурирање на процените на ризик

Секојдневното живеење и работење на човекот како поединец и припадник на различни општествени структури се одвива во услови на постојани закани од различни форми на ризици и опасности. Ризиците се однесуваат на одреден степен на веројатност и очекување дека одредена закана ќе прерасне во конкретна опасност и ќе предизвика загрозување на одредени вредности, кај поединецот, организацијата, локалната заедница или поширокото општество.

Процената како *процес* претставува континуирано и систематизирано согледување за нивото на безбедност на заштитените вредности, наспроти веројатноста од загрозување под влијание на конкретни опасности, во корелација со степенот на изложеност на елементите на ризик и нивната ранливост, односно отпорност. Во процената, се презентираат сознанијата, заклучоците и препораките, поврзани со актуелните и очекуваните ризици за одреден простор и време. Процената не е статичен или еднаш донесен документ, нејзината содржина се ажурира (редовно и вонредно) во согласност со динамиката на промени со која се манифестираат безбедносните појави. Процената претставува основа за планирање, организирање и спроведување превентивни и оперативни мерки и активности, рано предупредување и координација во процесот за управување со ризици.

Проценувањето на безбедносните ризици се остварува во плански, организиран, целисходен и методолошки воспоставен процес, преку кој се доаѓа до одредени сознанија и заклучоци за состојбите и тенденциите на појавите кои претставуваат ризици и опасности за животот и здравјето на луѓето, нивниот имот и работа, природните, материјалните и културните богатства и општата безбедност во општеството. Процената и процесот на проценување во рамките на постапките за управување со ризици, добива на значење затоа што преку него надлежните субјекти спроведуваат: (1) Идентификување на опасностите и нивно рангирање (според интензитет, зачестеност, можни последици и др.); (2) Предвидување на објектот кој може да биде загрозен (изложеност) и како (неговите слабости - ранливост); (3) Истражување на идентификуваните опасности, собирање податоци и информации за нив, нивна анализа и евалуација и мерки на контрола; (4) Документирање на состојбата; (5) Ажурирање – следење на промените (редовно и вонредно - по укажана потреба).

Преку процесот на изработка на процената, се спроведува постојано истражување на податоци и информации кои ќе најдат своја

употреба во постапките за управување со ризикот. Процената на ризиците претставува темелен документ врз основа на кој се планираат, се организираат и се спроведуваат потребните мерки и активности во процесот на управувањето со ризиците. Идеален систем кој ќе ги неутрализира сите ризици, не постои, така да водечки императив на надлежните субјекти, треба да биде, актуелните и потенцијалните ризици да ги сведат на толерантни и прифатливи граници, со цел да се избегнат големи економски, социјални и друг вид нарушувања во функциите на организациите, системите и општеството.

Општата задача на управувањето со ризици, во основа вклучува две работи: *процена* на веројатноста и големината/интензитетот на одредениот ризик и одредување на степенот на вреднување на важноста која организацијата/општеството ја придава на тој ризик. Оттука, процесот на управување со ризикот се состои од две фази: (1) *Процена на ризикот*, што претставува негова квантификација, со користење валидни и проверени податоци и (2) *Вреднување на ризикот*: што опфаќа социјални, економски, финансиски, политички, еколошки и други размислувања за сериозноста на ризикот, балансирање на трошоците за негово третирање (превентивно, оперативно) наспроти потенцијалната корист/штета за поединецот, организациите, системите и општеството како целина.

Процесот на процена на ризикот ќе ја истакне содржината и на другите променливи фактори на ризикот кои со текот на времето може да ја променат или да ја направат процената нерелевантна. За да бидат следени овие елементи, исто така, треба да се воспостават процедури за ажурирање на податоците кои се однесуваат на ранливоста и на другите карактеристики на изложените елементи на ризикот.

Оваа потреба од следење и ажурирање на овие елементи произлегува од карактерот на тие податоци и почестите промени поврзани со нив. Овие промени се однесуваат на следните аспекти.

- Првиот аспект е поврзан со изградената средина, каде промените на елементите изложени на ризик (згради, објекти, инфраструктура и друго) се динамички фактори и се подложни на промени под влијание на урбанистичкото и друго уредување на просторот.
- Следниот аспект се однесува на податоците за населението, кои исто така под влијание на економските и социјалните влијанија се доста променливи и подразбира потреба од постојано ажурирање на променливите фактори, како што се: концентрација, густина, структура, дисперзија итн. и
- Третиот аспект е поврзан со капацитетот за одговор (ресурсите), кој исто така е променлив, односно се зајакнува и слабее, а податоците кои влијаат на тоа треба да се следат и евидентираат.

Заради воспоставување одржлив и организиран процес на мониторинг и ажурирање на процените на ризик, потребно е дефинирање на соодветни методологии и постапки, со кои ќе се определи начинот и постапката, времето и носителите на овие процеси.

6.2. Проверка на системот за управување со ризици

Преку процесот на процената треба да се идентификуваат субјектите (организациите и службите) кои имаат значителна улога во процесот на управување со ризикот, да се нагласи опсегот и целите на нивното вклучување и да се идентификуваат факторите кои можат да влијаат на нивната ефикасност и ефективност. За да бидат следени, факторите на успешно управување со ризикот, кои зависат од организацијата на системот, треба посебно да се развијат соодветни постапки за тоа (процедури или методологии).

Постапките за следење и проверка на системот за управување со ризици треба да се развијат со цел соодветно да се обезбеди тековно следење и ревидирање на овие фактори, како би можело рамката за управување со ризикот, политиките и плановите на организацијата, доколку е потребно, да се подобрат и да се обезбеди ефективна и ажурирана рамка за управување со ризикот.

Со цел да се обезбеди ефикасност во управувањето со ризикот и континуитет во работата на организациите вклучени во управувањето со ризикот, надлежните субјекти треба:

- да ги усогласуваат своите капацитети со утврдените потреби преку процената на ризикот и да се обезбеди редовен процес на ревидирање;
- да се воспостави временска рамка и динамика на достигнување на проектираните и потребните институционални, материјални и други капацитети (техничко опремување, персонално екипирање и др.);
- да се воспостави редовен процес на подготовка на институционалните и системските капацитети (обука, едукација и сл.);
- да се одржува постојано ниво на подготвеност и увежбаност (институционални вежби, системски/меѓусекторски вежби итн.) и
- да се одржува постојано ниво на контакт и соработка со системите за управувањето со ризици од потесното и поширокото опкружување.

Врз основа на резултатите од следењето и проверката, потребно е донесување одлуки за подобрување или корекции на рамката за управување со ризикот, политиките и плановите на организациите. Со овие одлуки треба да се влијае на подобрување на перформансите за управување со ризикот на секој надлежен субјект, како и подобрување

на општата рамка за управување со ризикот. Делотворноста на контролите, исто така, треба да биде следена и документирана, со цел да се обезбедат податоци за подобрување на системот, започнувајќи од формалноправната рамка врз која е поставен, преку организациско-институционалната форма на дејствување, па сè до материјалнотехничката страна на подготвеност.

7. ПРИНЦИПИ ВО УПРАВУВАЊЕТО СО РИЗИК

Ефикасното и ефективно спроведување на процесот за управување со ризик подразбира и придржување до некои од следните принципи:

1. *Управувањето со ризик е составен дел на организациските процеси.* Управувањето со ризик не е самостојна дејност, одвоена од основните активности и од тековните процеси на организацијата. Управувањето со ризик е дел од вкупната одговорност на менаџментот и составен дел од сите проекти и процеси кои се реализираат во согласност со поставените планови и цели на организацијата.

2. *Управувањето со ризик е дел од донесувањето одлуки.* Управувањето со ризик им помага на донесувачите на одлуки да донесат одлуки засновани врз релевантни информации, анализи и процени на состојбите. Управувањето со ризик може да помогне во поставувањето приоритети во акциите и во изборот на алтернативни правци на дејствување. На крај, управувањето со ризик може да му помогне на менаџментот при одлучувањето за тоа дали ризикот е прифатлив или не, како и тоа дали третманот на ризикот ќе биде адекватен и ефикасен.

3. *Управувањето со ризик експлицитно се занимава со неизвесности.* Управувањето со ризик се занимава со оние аспекти за донесување одлуки што ги карактеризира неизвесност, како и со природата и начините за решавање на неизвесноста.

4. *Управувањето со ризик е систематично, структурирано и благовремено.* Систематски, благовремен и структуриран пристап во управувањето со ризици придонесува кон ефикасност и конзистентност, споредливост и сигурност на резултатите.

5. *Управувањето со ризик се занова врз најдобрите достапни информации.* Влезните податоци во процесот на управување со ризик се засновани врз изворите на информации како што се искуството, повратните информации, набљудувањето, прогнозата и експертската оценка. Меѓутоа, донесувачите на одлуки треба да бидат информирани и треба да ги земат предвид ограничувањата што се однесуваат на користените податоци и модели, како и на можноста за несогласување на експертите.

6. *Управувањето со ризик е приспособено кон организацијата.* Управувањето со ризик е во согласност со надворешниот и со внатрешниот контекст на организацијата и со профилот на ризикот.

7. *Управувањето со ризик го зема предвид човечкиот фактор.* Управувањето со ризик мора да ги воочи и да ги препознае можностите, перцепциите и намерите на луѓето надвор и внатре во организацијата, кои би можеле да го олеснат или да го отежнат остварувањето на целите на организацијата. Една од основните карактеристики за безбедносниот систем и системот за заштита на лица, имот и работење е токму тоа што однесувањето на некои делови од системот е тешко да се предвидат, поради пресудната улога на човечкиот фактор.

8. *Управувањето со ризик е транспарентно и отворено за сугестии.* Соодветното и навремено вклучување на битните заинтересирани страни и особено донесувачите на одлуки од сите нивоа на организацијата, осигурува релевантност и ажурност во процесот на управувањето со ризик. Исто така, вклученоста им овозможува на заинтересираните страни да бидат на вистински начин застапени и нивните мислења да бидат земени предвид при одредувањето критериуми за ризикот.

9. *Управувањето со ризик е динамично, итеративно и реагира на промени.* Покрај тоа што претставуваат сложени системи, системите за заштита на лица и имот се отворени и динамични организациски системи. Без оваа карактеристика тие не би можеле да опстанат, т.е. да ја вршат својата функција. Со настапување на интерни и на екстерни настани се менуваат контекстот и сознанијата, се пристапува кон контрола и ревизија, некои ризици се засилуваат и излегуваат на површина, додека други се намалуваат. Организацијата мора да обезбеди процес за управување со ризици што ќе биде во состојба континуирано да детектира и да одговара на промените.

10. *Управувањето со ризици овозможува континуирано подобрување и унапредување на организацијата.* Организациите треба да развијат стратегија за унапредување на зрелоста на своите процеси за управување со ризик, паралелно со сите други аспекти на организацијата.

IV глава

УПРАВУВАЊЕ СО СИСТЕМОТ НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ

1. СОВРЕМЕНИ ПОТРЕБИ ВО ЗАШТИТА НА ЛИЦАТА, ИМОТОТ И РАБОТЕЊЕТО И УПРАВУВАЊЕ СО РИЗИКОТ

Современите промени во областа на безбедноста претставуваат процес што може да се означи како доверување разни задачи од безбедноста (според обемот и квалитетот) на приватниот безбедносен сектор од страна на државата. Овој процес се доведува во врска со низа фактори што лежат во економската, социјалната, политичката и културната сфера во општество. Меѓутоа, се смета дека на овие современи трендови доминантно влијаеле: воведувањето принцип за пазарна економија во сите сфери на општеството наспроти појавата на разни облици на загрозување и современите закани по безбедноста.

Оттука, од една страна, ограниченото буџетирање морало неволно да се одрази врз можноста на надлежните државни органи и на конвенционалните субјекти за безбедност, пред сè на полицијата, во општествата на ризик и во ерата на општа приватизација да ги задоволи пораснатите и сè посложени потреби на граѓаните, општествените групи, стопанските субјекти и другите конзументи на безбедносни услуги со постојните ресурси. Притоа се мисли на широк спектар безбедносни закани и ризици како што се: елементарни непогоди, техничко-технолошки опасности и опасности предизвикани од човечки фактор. Кон тоа придонесува и стравот од криминал, што, покрај објективните показатели за движење на криминалитетот, доведува до загуба на довербата во кривичноправните институции и органите на формална и неформална општествена контрола. Со оглед на корените на криминалот и потребата тој да се спречува во сферата на примарната превенција, постои сериозна аргументација безбедносните потреби да се артикулираат врз најширока општествена основа. Од друга страна, познато е дека човек со квалитетна организација и со помал напор (трошоци) подобро и побрзо постигнува многу поголеми резултати во сите подрачја на своето дејствување. Бројот и облиците на организација денес достигнале такви димензии што е невозможно без научен пристап да се решаваат сè посложените организациски проблеми, а исто така да се воспостави модерна, флексибилна и ефикасна организација која треба да овозможи реализација на најсложените задачи со што го проширува опфатот на човечката индивидуална сила, го забрзува процесот на остварување

на задачите, односно го скратува потребното работно време за негово извршување, па со соодветна организација релативно се намалуваат трошоците за постигнување исти резултати.

Во последните дваесет години се воде големи дискусии за системски или кибернетски пристап кон организацијата (организацијата се разгледува како комплексен, динамичен и отворен систем, кој од една страна е составен од одреден број потсистеми, а од друга страна претставува потсистем на некој друг систем, од повисок ред). Важни карактеристики на организацијата се: целта, односно задачата која се сака да се оствари, усогласеноста во ресурсите на организацијата и нивна рационална употреба, а фокусот е ставен на воспоставување правилни односи помеѓу одделните делови на организацијата, помеѓу деловите и организацијата како целина.

Наведените фактори не само што ја менуваат традиционалната претстава за процесот на проценка на ризикот кој повеќе не се гледа како изолиран процес во рамките на одделните организациони целини туку тие влијаат и врз профилот на современите менаџери за ризик. Иако постојат одредени специфичности поврзани со работата на менаџерот за ризик во јавниот или во приватниот, во непрофитниот или во профитниот сектор, потребите од современ јавен менаџмент, општествено одговорното работење и барањата што се поставуваат пред луѓето кои се најодговорни за прашањата за безбедност и заштита на организациите во земјите на развиено пазарно стопанство сè повеќе ја бришат оваа разлика.

Заштитата на јавниот интерес и целите на општествено одговорното работење бараат обезбедувањето сигурност на трети лица врз комерцијална основа, а одговорноста на менаџерот се врзува (врз начелата за правда и еднаквост во заштитата) за уредно, ефикасно и квалитетно извршување на задачите на безбедноста. Државата помалку или повеќе на поединецот или на корисникот на безбедносните услуги му препушта на кој начин ќе ги артикулира потребите за безбедност (како едно од темелните човечки права).

Во исто време, потребно е да се направи разлика помеѓу интересите на јавниот поредок и на економскиот интерес како јавен. Во западниот свет милиони долари од даночните обврзници дневно се штедат на сметка на партнерството меѓу јавниот и приватниот сектор за безбедност. Многубројните истражувања го покажуваат токму тој парадокс: профитот и економскиот интерес што ја дефинираше линијата на разединување меѓу едниот и другиот сектор сега е точка на вкрстување на нивните интереси. Полицијата веќе не е само сервис на граѓаните со тоа што ги ослободува од стравот од криминал. Оваа до некаде изменета улога на полицијата ги ослободува граѓаните од непотребни

даноци со тоа што разумно ги троши своите ресурси, ги дели со приватниот сектор (и обратно), пренесува дел од одговорностите за (не) безбедноста.

Дел од овие предизвици секако потекнуваат од управувањето со фиксниот и непроменлив буџет, за кој се очекува да биде доволен и да овозможи висококвалитетно извршување на должностите во променливото и сложено опкружување во кое дејствува полицијата. Дополнително за полициските власти финансиските ризици се манифестираат низ разни грешки за време на примената на полициските овластувања во преткривичната постапка, при процесуирањето на кривичните дела или сообраќајните несреќи, при повредите и болестите на припадниците на полицијата и во други случаи.

Со оглед на фактот дека јавните власти имаат ограничени можности во обезбедувањето средства и дека многу од тие можности предизвикуваат негативни последици (земање кредити, политичка штета од зголемувањето данок или барањето средства за вонредни ситуации), генерално се смета дека постојните средства што ги имаат на располагање властите треба да бидат предмет при управувањето со ризик. Ова значи проширена ориентацијата што вклучува управување со сите ризици. Се разбира, фразата „сите ризици“ донекаде е реторичка зашто е апсурдно да се претпостави дека апсолутно сите ризици може да се идентификуваат и да се контролираат. Сепак, оваа фраза е во целосна согласност со развојот на дисциплината „менаџирање на ризикот“, што се движи кон сè поинтегриран и посеопфатен пристап во праксата при управувањето со ризици. Навистина, јавниот сектор донекаде се покажа бавен во усвојувањето на овие поставки, меѓутоа, менувањето на политичките, општествените и економските закани ги присили носителите на власт да обезбедат подобри услуги со сè поограничени ресурси.

Колку е важна организационата рамка во развојот и во примената на мерките за управување со ризик покажува и прашањето за одговорност во профитниот и во непрофитниот сектор. Прашањето за одговорност е во тесна врска со регулативата и со потребата да се почитуваат тесните регулаторни рамки. Вработените можат да искористат отсуство на безбедносно-заштитни процедури во случај да се обвинети за направени пропусти. Меѓутоа, избегнувањето на правилата или одењето по нивниот раб понекогаш е услов да се оствари конкурентска предност или употреба на информацијата во комерцијални цели. Во тоа помага и околноста што пишаните правила и договори никогаш нема да можат до крај да ги предвидат сите ситуации што можат да се случат, а тоа дозволува одредена доза флексибилност па, според тоа, и можност за разни отстапувања што не би се толерирале во нормални околности.

2. ПОЛИТИКА НА ОСИГУРУВАЊЕ ПРИ ЗАШТИТАТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ

Анализите засновани на адекватна пракса потврдуваат дека составен дел на безбедносната политика на организацијата е *внатрешната контрола и политиката на осигурување*. Овие два елемента имаат значително влијание врз остварувањето интегралната функција на безбедноста во рамките на една фирма или претпријатие. Денес има сè повеќе усогласени стратегии помеѓу државата и компаниите за осигурување и за приватна безбедност, но и корисниците на нивните услуги. Притоа пазарот на услуги во осигурувањето е помалку сложен од пазарот за безбедносни услуги, затоа што услугите во безбедноста се под лупата на полицијата и на граѓаните, на нелојалната конкуренција, на високите стандарди и во осигурувањето и во барањата на корисниците. Ова значително влијае безбедносната култура да биде на пониско ниво од осигурителната. Причината за недоволната развиеност на безбедносната култура, меѓу другото, се наоѓа и во тоа што ефектите на безбедноста не се непосредно мерливи, а осигурителните компании со премијата на осигурување му гарантираат на клиентот итна исплата на обештетувањето што влијае врз зајакнување на довербата меѓу едните и другите.

Во отсуство на заеднички настап, постојат две непосакувани ситуации за субјектите на безбедносните и на осигурителните услуги кои, во основа, ги конфронтираат. Квалитетната безбедност не е замена за услугите на осигурувањето, и обратно, тоа што некоја фирма е осигурена, не ја ослободува од обврската да вложува во безбедност. До вистински однос се доаѓа со идентификување на допирните точки на безбедноста и на осигурувањето. Осигурителните компании прецизно ги вреднуваат ризиците и ја утврдуваат цената, а менаџерите на ризик ги проценуваат ризиците и безбедносните мерки, па ги ценат безбедносните услуги. Имено, заедничкиот интерес се гледа во тоа што работите во безбедноста подразбираат примена на превентивни и репресивни мерки, а осигурителните компании преземаат одговорност за сите видови ризик. Тоа практично би значело дека доколку некоја организација користи услуги од безбедноста, осигурителната куќа ја гарантира штетата што корисникот на услугите ќе ја претрпи поради нестручната примена во овластувањата или неодговорноста на персоналот од безбедноста.

Во некои држави професионалните здруженија (комори) за заштита на лица, имот и работење имаат договори со осигурителните компании и посебни клаузули со безбедносните компании со кои од нив се бара задоволување на минимумот безбедносни стандарди како претходен услов за време на склучување на договорот во врска со

осигурувањето. Со тоа истовремено е овозможено цените на осигурителните услуги да не бидат над утврдените критериуми за формирање на тие цени. Финансиските ефекти се очигледни, освен што се намалува цената за превенција.

Важен услов во извршување на услугите за обезбедување е и имотот што се обезбедува да мора да биде осигуран. Во спротивно, може да се случи вредноста на украдените, оштетени или уништени предмети да ја надминува вредноста на вложениот капитал на организацијата што дава безбедносни услуги.

3. ОПКРУЖУВАЊЕТО И ВРЕДНОСТИТЕ НА ОРГАНИЗАЦИЈАТА ШТО СЕ ШТИТАТ

Еден од основните предуслови за управување со ризици е разбирањето за надворешното и за внатрешното опкружување на организацијата.

Разбирањето на надворешниот контекст е важно за да се осигури договорните страни, нивните цели и интереси да бидат разгледани при развивањето на критериумите на ризикот. Тој се заснова врз контекстот на целата организација, но со специфичните детали на законските и на регулаторните услови, се совпаѓа со интересните страни и со другите аспекти на ризикот специфични за подрачјето на примена на процесот за процена на ризик. За време на дефинирање на надворешниот контекст организацијата треба да ги воочи и надворешните фактори кои претставуваат активност на различни субјекти, настани и појави, а физички не се наоѓаат во кругот или во просториите на организацијата.

Специфично, во областа на заштитата на лица, имот и работење аспектите на надворешното опкружување на организацијата ги опфаќаат меѓу другото и следните фактори:

- културното, политичкото, правното, финансиското, економското и конкуретското опкружување;
- клучните фактори и трендови кои влијаат на целите на организацијата;
- перцепцијата и вредностите на интересните и заинтересираните страни.

Покрај наведените фактори особено се важни и:

- безбедносното опкружување (меѓународно, национално или регионално);
- макролокацијата, конкуренцијата и историјата на штетни настани.

Внатрешниот контекст ги подразбира сите фактори внатре во организацијата што може да остварат влијание врз начинот на кој

организацијата врши проценка на ризикот. Внатрешни фактори може да бидат: историјата на штетни настани; големината на организацијата; начинот на организирањето; начинот и степенот на заштитата; дејствувањето на вработените и дејствување на страните што имаат интерес.

Внатрешен контекст претставуваат и заштитуваните вредности на организацијата, чиешто познавање е важна претпоставка за анализа на ранливите места и за прелиминарната анализа на ризикот. Вообичаена е поделбата на заштитуваните вредности на организацијата на:

- номинални (работење, безбедност) и
- неноминални (регулативно-правни норми, углед и страни од интерес).

Стеknати вредности		Области на влијание кај стекнати вредности
номинални	Работење	Ефикасност во работењето, степен на реализација на поставени цели, континуитет во процесот на работење, континуитет во работење, нарушување на работни процеси, показатели на работни карактеристики.
	Безбедност	Човечки живот, влијание на здравје, степен на штета на ресурси
	Финансиски профит	Состојба на оперативен буџет, стекнати финансии, непредвидени трошоци или загуби
неноминални	Регулативни, правни и други норми	Прекршени регулативи, правна отпорност на пореметување
	Углед	Однос на медиуми, однос на јавноста, доверба на јавноста
	Интересни страни	Негативно влијание на органи, управи или запослени, морал на запослените лица, влијание на интересни и заинтересирани страни

Табела 2. Заштитувани вредности на организацијата

Карактеристиките на организацијата го условуваат карактерот на заштитуваните вредности и профилот на ризик. Некои вредности се универзални, а заедно со нив и ризиците: репутација, човечки ресурси и др. На пример, некои ризици произлегуваат од самите договори. Условите во договорот може да создадат обврска што организацијата може или не може да ја исполни. Природно, одредени договори ќе бидат позначајни за организацијата од некои други. Исто така, повеќето јавни служби даваат услуги и според тоа давањето услуга е релативна грижа на менаџментот.

Во основа, за организацијата чија улога е остварување јавна безбедност, спогодбата со вработените е централен извор за ризик. Одговорноста на вработените, погрешно спроведените процедури за

лишување од слобода, неадекватната истрага итн., претставуваат некои од најголемите предизвици со кои се соочуваат модерните полициски власти. Сепак, ако вработените се добро обучени, мотивирани и ефикасни, тоа може да претставува голем потенцијал за организацијата и за максимизирање на нејзините резултати и обратно, ако споменатите атрибути се негативни, тоа ќе има неповолни последици.

Исто така е важно да се разбере организацијата во однос на:

- сопствените можности и сила, во смисла на ресурси и знаење, (капитал, луѓе, компетенции, процеси, системи и технологии);
- протокот на информации и процесот на донесување одлуки;
- внатрешните заинтересирани страни;
- меѓучовечките односи;
- целите и стратегијата за нивно остварување;
- перцепцијата, вредностите и културата;
- политиката и процесите;
- стандардните референтни модели усвоени од страна на организацијата и
- структурите (управување, улоги и одговорности).

Наведените елементи, исто така, може да претставуваат заштитувани вредности на организацијата и да бараат процена за ризикот, нивната изложеност на ризик и да се согледа каква им е ранливоста.

За да биде управувањето со ризиците ефективно, потребно е организацијата да развие и да примени план така што ќе се обезбеди комуникација со екстерни и интерни заинтересирани страни. Ова треба да опфати:

- комуникација со заинтересираните страни во случај на криза или штетен настан;
- ангажирање соодветни екстерни страни на интерес и овозможување ефективна размена на информации;
- интерно и екстерно известување на законито-правно заснован начин;
- интерно известување за влијанието на концептот за процена на ризик врз односот со страните од интерес, неговата ефективност и резултати;
- достапност на информациите во согласност со законот;
- обезбедување повратна информација за комуникациите и
- користење на комуникациите поради осигурување транспарентност и градење доверба во организацијата.

4. СТАНДАРДИ ОД ОБЛАСТА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ

4.1. Поимот и значењето на стандардот

Во секојдневниот говор поимот стандард се доведува во врска со правилата што произлегуваат од „добрата пракса“. Исто така, стандардите можат да се дефинираат како постапување во согласност со прифатените правила или предвидливо однесување.

Во основа, стандардите се изработуваат и се дефинирани преку процес на споделување на знаење и градење консензус помеѓу технички експерти номинирани од страна на заинтересирани страни – вклучувајќи ја бизнис заедницата, потрошувачите, државните органи и академските институции. Стандардот е документ со доброволна примена, а се состои од технички спецификации базирани на резултатите од искуството и технолошкиот развој.²⁹

Во Законот за стандардизација на Република Македонија, стандард е документ подготвен со консензус и усвоен од страна на признато тело, со кој, заради 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.³⁰

Постојат неколку различни типови на стандарди кои вклучуваат барања и/или препораки во однос на производи, системи, процеси или услуги. Стандардите, исто така, може да претставуваат начин со кој може да се опишат методите на мерење и испитување или да се воспостави заедничка терминологија во рамките на еден специфичен сектор.³¹

Стандардите имаат *дерегулативна* улога: преку законски прописи државата ги поставува суштинските цели за заштита, додека по пат на стандардизацијата се специфицираат технички детали во согласност со правните барања. Сепак, стандардите претставуваат *препораки* и нивната примена во основа е врз доброволен принцип, иако самата примена е обврзувачка според склучените договори.

Во однос на предметот што го регулираат постојат: *стандарди за тестирање на производите и на услугите*, на кои им се специфицирани методите за тестирање поврзани со аспекти за причината и статистички

²⁹ http://www.isrm.gov.mk/mk/button_6.html (посетена на 15.12.2-15 година).

³⁰ http://www.isrm.gov.mk/mk/button_42.html, (посетена на 15.12.2-15 година).

³¹ http://www.isrm.gov.mk/mk/button_6.html (посетена на 15.12.2-15 година).

методи; *технолошки стандарди*, кои имаат важна улога во развојот на нови технологии; *стандарди на услугите* со кои се осигурува услугите да ги исполнуваат бараните побарувања; *технички правила*; итн.

Иако влијанието на стандардите во секојдневните активности често е незабележливо, тие даваат огромен придонес речиси во сите аспекти од нашиот живот. Сите ние однапред подразбираме дека производот што го купуваме со квалитетот одговара на нашите барања, дека ги исполнува претпоставените критериуми за безбедност, сигурност и ефикасност и дека ги обезбедува сите овие погодности за соодветна цена.

Примената на стандарди претставува составен дел од рутинските работи на секоја организација во профитниот и во непрофитниот сектор. Се смета дека на таквиот тренд пресудно влијаат два фактора: брзината на технолошките промени и натпреварувачката природа на пазарот.

Брзината на технолошките промени влијае врз самиот стандард. Не само што развојот на технологијата ја поттикнува потребата од стандарди туку и нивната примена е условена од технолошкиот развој. Поради тоа во процесот на изработка и донесување на меѓународните и на европските стандарди се вклучени меѓународните електротехнички организации, па и самиот почеток на стандардизација историски датира од основањето на Меѓународниот електротехнички комитет (IEC).

Генерално, стандардизацијата помага да се постигне повисок квалитет со пониски трошоци, обезбедувајќи постоење конкуренција помеѓу производителите и оние што ги нудат услугите. Без разлика на специфичностите и разликите, профитните организации мора да сметаат на компетитивната природа на пазарот на кој ги пласираат своите производи и услуги, како втор важен фактор што ја диктира многу раширената свест за значењето на стандардот. За да бидат успешни во рамките на кој и да е пазар, организациите мора да се разликуваат од другите конкуренти. Мора да произведуваат подобри производи, да даваат подобри услуги, да понудат пониски цени на услугите или да ги намалат трошоците за производство или за услуги. Се разбира дека не е зможно сите овие барања лесно да се остварат. Свеста за конкуренција во некои економии како што е јапонската е развиена до тој степен што давањето помош на конкуренцијата да не доживее тотален колапс е составен дел на деловната култура и извор на стратески предности, зашто ѝ помага на организацијата да го усовршува квалитетот на своите услуги и производи.

4.2. Меѓународни и европски стандарди во областа на заштитата лица, имот и работење

Во интерес на извозно ориентираните економии, меѓународните и европските стандарди добиваат приоритет во однос на националните стандарди. Меѓународната стандардизација постои речиси 150 години. Заедно со сознанието дека стандардите можат да го унапредат работењето и да го прошират пазарот, светската индустрија инвестира милијарди долари во стандардизацијата. Меѓународните стандарди што се развиени по пат на отворени процеси и консензус помеѓу заинтересираните страни претставуваат важен чекор во брзиот и ефикасен пристап кон меѓународните пазари.

Во основа под меѓународен стандард се подразбира стандард што го донела меѓународна организација за стандардизација (ISO, IEC, ITU, CEN итн). Меѓународни организации за стандардизација се организации во кои можат да се зачленат соодветни национални тела за стандардизација на секоја држава, и тоа: Меѓународната организација за стандардизација (ISO); Меѓународната електротехничка комисија (IEC); Меѓународната унија за телекомуникации (ITU), Европскиот комитет за стандардизација (CEN); Европскиот комитет за стандардизација во областа на електротехниката (CENELEC); Европскиот институт за стандарди од областа на телекомуникациите (ETSI) и други.

Меѓународната организација за стандардизација (ISO - International Organisation for Standardisation) е најголемата светска институција за развој на стандардите и претставува мрежа на национални институти етаблирани во голем број држави, врз основа еден член-една земја, со седиште во Женева (Швајцарија), од каде што се координира системот. Иако ISO е невладинa организација, многу членови на националните институти или се именувани од страна на извршните власти во своите земји или во исто време се членови на тие извршни власти. Со самото тоа ISO претставува организација во која консензусите се постигнуваат врз основа на решенијата што одговараат на барањата на деловните и на другите групи од интерес, како што се потрошувачите или државната управа.

Во рамките на Меѓународната организација за стандардизација денес се активни преку 200 технички комитети во разни области што се предмет на изработка и донесување на стандардите. Усвојувањето на ISO-стандардот за деловните корисници значи дека доставувачите може да го базираат развојот на своите производи и услуги врз спецификациите што имаат широка прифатеност во нивните сектори, или со други зборови, деловните субјекти кои ги користат меѓународните стандарди

може да се натпреваруваат со конкурентите на пазарите низ сиот свет. За државите, меѓународните стандарди обезбедуваат технолошка и научна база што овозможува креирање соодветна здравствена, безбедноста, еколошка и правна рамка. Постоенето глобална усогласеност што се постигнува со примена на меѓународни стандарди во развојот на производите и давањето услуги, за потрошувачите дава можност за значително поширока понуда и позитивни ефекти од конкурентската борба меѓу доставувачите. Освен тоа, фактот што производот или услугата одговараат на меѓународните стандарди дава гаранција за безбедност, за квалитет и доверливост, а со самото тоа и еден вид сигурност за потрошувачите.

Поради значењето што технологијата го има во развојот и во примената на стандардите, важно е да се истакне улогата на Меѓународната електротехничка комисија (IEC - *International electrotechnical commission*), основана во 1990 година, со цел изработка и донесување стандарди во техничките области.

Во основа покрај наведените од особено значење се и европските стандарди. *Европскиот стандард* е стандард што го донела европската организација за стандардизација. Европските организации за стандардизација се организации во кои можат да се зачленат соодветни национални тела за стандардизација на европските држави и тоа се: Европскиот комитет за стандардизација (CEN); Европскиот комитет за стандардизација во областа на електротехниката (CENELEC); Европскиот институт за стандарди од областа на телекомуникациите (ETSI).

Во согласност со директивата на Европската комисија 98/34/EC, CEN (*The European Committee for Standardization*) е единствената европска организација за планирање, изработка и донесување европски стандарди во сите области на економските активности, освен електротехниката (*SENELC: European Committee for Electrotechnical Standardization*) и телекомуникациите (*ETSI: European Telecommunications Standards Institute*).

Меѓународните стандарди сè повеќе ги зафаќаат системите за менаџмент во јавната и во приватната сфера, вклучувајќи ги и оние прашања за општествената одговорност и безбедност што придонесуваат за нестабилност на поединецот и заедницата (безбедност и здравје на работа, заштита на животната средина, миграциски движења, природни и техничко-технолошки несреќи и катастрофи, криминални и терористички акти и други феномени) и дестимулативно влијаат врз економските активности во заедницата.

Прашањата за безбедност станаа глобални и не познаваат национални граници, па со самото тоа претставуваат област на стандардизација од посебен интерес за државите членки на меѓународните тела за

стандардизација. Високо место на листата (на владините) приоритети за национална политика претставуваат прашањата како што се безбедност на граѓаните, безбедност на критичната инфраструктура и безбедност на производите и услугите. Имајќи го превид значењето на стандардот за целокупниот економски и социјален развој, како цели на стандардизацијата во областа на безбедноста се наведуваат:

- изградба соодветни капацитети во земјите членки со цел вклучување на нивните институции во процесот на меѓународната стандардизација а подоцна и развојот и примена на безбедносните стандарди во сопственото опкружување;
- идентификување на релевантните актери во заедницата и нивните потреби од меѓународно признати стандарди во областа на безбедноста, со цел да се обезбеди меѓународен легитимитет во нивната примена;
- јакнење на националните и на регионалните капацитети за соработка во размената информации, искуства и ресурси во сферата на управување со ризици и кризи во јавниот, во приватниот и во цивилниот сектор;
- развојот на електронските комуникации и експертиза со примена на информатички алатки во усогласување на националните со меѓународните стандарди.

ISO и другите организации, како што е меѓународната организација за стандардизација на полето на телекомуникациите, ја развиле базата, т.е. главните принципи и насоки во полето на безбедноста. ISO-стандардите обезбедуваат систем стандарди во безбедноста и заштитата и принципи за нивна примена.

Систем меѓународни стандарди од областа на безбедноста и заштитата се: Безбедност и здравје на работата OHSAS 18001, Менаџирање на ризици 31000+, Безбедност на храна ISO 22000, Општествена безбедност ISO 22300, Заштита на животната средина ISO 14000+, Менаџмент на ланците за снабдување ISO 28000+, Безбедност на телекомуникациите ITU, Безбедност на информациите ISO 27000+, Менаџирање со квалитетот ISO 9000+.

Наведените стандарди претставуваат добра појдовна основа за развој на севкупниот систем за безбедност и заштита во определена организација. Насоките содржани во наведените стандарди многу лесно може да се диверзифицираат внатре во некоја организација и да се прошират на други системи за да одговараат на дадениот систем, т.е. организација. Примената на вакви стандарди може да се сконцентрира врз оние прашања што се многу значајни од гледна точка на управување, т.е. менаџмент, а тоа се: кој, зошто и како управува со ризикот или со организацијата во даден момент.

Во рамките на системот стандарди од областа на менаџментот на безбедноста и заштитата особено е значајна серијата стандарди за управување со ризици: ISO 31000 и ISO/IEC 31010.³² Бидејќи сите организации и нивните активности вклучуваат ризици со кои мора да се управува, се пропишуваат бројни стандарди на меѓународно и на национално ниво за да се управува со ризиците на најдобар начин. Повеќето стандарди се однесуваат на терминологијата, процесот или методологијата за управување со ризици, на организациската структура и на целите на управувањето со ризици.

Способноста за проценка на ризикот е една од клучните компетенции на секоја организација и на нејзините вработени. Тоа дали организацијата врши и применува проценка на ризикот и резултатите од процената ги вградува во процесот на одлучување, зборува за професионалноста во пристапот кон проблемот за заштита лица, имот и работење.

За да се обезбеди потребната кредибилност во процесот на меѓународната стандардизација, националните организации за стандардизација имаат обврска и одговорност овие факти да ги стават во контекст на националниот дијалог со цел подигнување на свеста за методологијата и праксата во областа што е предмет на дијалог, развивајќи социјална одговорност на сите клучни актери во управувањето со безбедносните ризици и кризни ситуации. Кон ова е потребно да се додадат и барањата за безбедност, зашто сите ќе се согласат дека безбедноста е потребна, но не и како да се оствари.

Опстанокот на нацијата и на граѓаните сè повеќе зависат од безбедноста и одржувањето на критичните функции на заедницата, а тоа ја подразбира способноста да се обезбеди функционирање на власта, економијата и институциите на цивилното општество, да се одржат критичната инфраструктура и демократските принципи на функционирање на државните институции во услови настанати во кризни ситуации. Поради порастот на кризните ситуации во светот и кај нас, напорите на државите, општествените ентитети, деловните заедници и стручната и академската јавност сè повеќе се насочени кон пронаоѓање и воспоставување технички, организациски и управувачки пристапи со цел континуирано управување со кризните ситуации. Како обид тие да се објаснат, да се обединат и да се применат, се усовршуваат теоријата и праксата на општествената безбедност. Тоа всушност има дадено поттик за стандардизација во оваа област. Меѓународната стандардизација во областа на *општествената безбедност* има поставено како цел развивање на капацитетот на заедницата за управување во кризи и

³² ISO/IEC 31010 Risk management – Risk assessment techniques.

овозможување континуитет на стопанските и на деловните активности на зедницата во кризни услови, преку унапредување на техничките, човечките, организациските и функционалните врски (интероперабилност) меѓу сите заинтересирани страни со цел подготвеност на кризни ситуации и адекватно реагирање на нив.

Особено е важно дисеминацијата на меѓународните стандарди да биде препознаена како еден од предусловите за јакнење на стопанските субјекти со примена на стандарди во сферата на управување со кои се овозможува заштита на профитот на компаниите и продолжување на деловните активности во услови предизвикани од кризи, кои, по правило, и најмногу ги погодуваат. На тој начин тие би станале дел од системот за рано предупредување и мрежи за ублажување на последиците од кризните ситуации.

Значаен чекор во правец на донесување европски стандарди на полето на безбедноста и заштитата направен е со основањето на *Техничкиот комитет за општествена безбедност и безбедност на граѓаните* при Европскиот комитет за стандардизација (CEN).³³ Предметни области на стандардизација во сферата на работата на овој комитет се: идентификација и смалување на ризиците од криминал во сферата на производите и услугите; хемиските, биолошките, радиолошките и нуклеарните инциденти; критичната инфраструктура-енергетско снабдување; критичната инфраструктура – изградба и градежно инженерство; безбедноста во синџирот за снабдување; интегрирано управување со границата; услуги во непредвидени ситуации; одбрана од тероризам; безбедност во снабдувањето со вода.³⁴

Европската унија донела низа акти со цел да ја унапреди безбедноста и заштитата на луѓето, имотот и критичната инфраструктура во разни области во праксата за безбедност и заштита. Според смислата и значењето, овие норми го поддржуваат процесот на управување со ризици во широк дијапазон: од природни несреќи и катастрофи, до терористички активности, техничко-технолошки инциденти, ризици по безбедноста и здравјето на работа и во работната околина итн. Со нивна примена се овозможува заштита на луѓето и нивниот имот, физичките ресурси, услугите, информациските технологии, инфраструктурните мрежи и други материјални и културни богатства со чие оштетување или уништување може да настанат сериозни последици по здравјето, безбедноста, економската и социјалната благосостојба или ефикасното функционирање на власта.

³³ CEN/TC 391 Societal and citizen security. <http://www.cen.eu/cen>. 17.04.2011.

³⁴ CEN BT/WG 161 'Protection and Security of the Citizen'. <http://www.cen.eu/cen/Sectors/Sectors/Security%20and%20Defence/Security/Pages/BTWG161.aspx>.

Во голем број директиви донесени од страна на Советот на Европа и Европската комисија се истакнува значењето на управувањето со ризици во овозможувањето слободно движење на стоките и услугите на европскиот пазар, но и со оние сегменти за управување со ризикот со кои, покрај интересите на работодавците, се штитат и интересите на вработените. Според членот 6 од Директивата на Советот на ЕУ 89/391, смислата на процената за ризик кај работодавците лежи токму во подобрувањето на нивото на зашти и во вградувањето оценки и ставови од проценката во сите активности на претпријатието и/или установата, и тоа на сите хиерархиски нивоа.

Во меѓувреме, под капата на Европската комисија и Советот на Европа се донесени и низа други документи што се однесуваат на областа на безбедноста и управувањето во вонредни ситуации.³⁵

4.3. Национална и европска регулатива и пракса во областа на приватната безбедност

4.3.1. Значењето на приватната безбедност во заштитата на лица, имот и работење

Ниту една современа расправа за безбедност не ја заобиколува темата за безбедноста и секако приватната безбедност, затоа што проблемите од областа на безбедноста се појавуваат во секој сегмент од општеството. Решавањето на овие проблеми е голема грижа не само за јавната безбедност, туку и за приватната безбедност затоа што станува повеќе од очигледно дека бизнис заедницата е изложена на безбедносни закани. Во тој контекст, секојдневно се преземаат чекори од страна на одредени фирми/компаниии итн., за воведување на безбедносната компонента, како природен елемент на корпоративната структура.

Во земјите што се наоѓаат во процес на трансформација на сопственичките односи, проширен е делокругот и надлежноста на титуларот на сопственоста, меѓу другото, и во областа на заштитата на лица и имот. Освен тоа што се прошири кругот на стекнати вредности и приватните сопственици станаа заинтересирани за дополнително обезбедување на својот имот и профит. Аналогно на тоа новите облици на криминалитет ги доведуваат во прашање постојните капацитети на државните органи делотворно да им се спротистават на новите предизвици. Ваквиот тренд го охрабри развојот на приватната безбедност. Иако станува збор

³⁵ COM(2009) 82 final.http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/com_2009_82en.pdf. 06.05.2011.

за услужна дејност, нејзините ефекти најдобро можат да се измерат со превенција на загрозувањето на луѓето, имотот и со превенција на губитоците кога е во прашање профитот.

Освен приватизација и развојот на внатрешниот пазар за стоки и услуги, вториот важен фактор во развојот на приватната безбедност што го одредува и нејзиното место во системот за национална безбедност е европеизација и глобализација на економијата. Глобализацијата на производството, финансиите и информациите бара општо прифатени стандарди на она подрачје од безбедноста што претставува додаток на дејноста на државните органи. Во спротивно, аномалиите што произлегуваат од невоедначеноста во националните регулативи ќе се одразат врз квалитетот во извршување на работите од приватната безбедност и врз задоволството од давањето безбедносни услуги.

Имајќи го предвид фактот дека станува збор за дејност што не ја извршуваат државните органи не смее да се извлекува заклучок дека е во прашање дополнување на безбедноста што не ја гарантира државата.³⁶ Улогата на државата во заштита на јавните интереси се протега во поставување и контрола на почитувањето законски прописи во оваа област, со што индиректно се појавува како гарант во приватната сфера на безбедноста.

Раководејќи се според либералистичките концепции за безбедност, приватната безбедност, поради својата неразвиеност, е особено на мета на критиката на теоретичарите за човечка и општествена безбедност, првенствено од причини што граѓаните или општествените групи, во недостиг од резултати, мерливи показатели и перформанси на услугите за безбедност, често не се во можност да разликуваат квалитетни од не-квалитетни услуги, развиени од неразвиени стандарди во јавниот ред.

4.3.2. Приватната безбедност во системот на националната безбедност

Од моментот кога приватната безбедност почнува да влијае врз националната и јавната безбедност, државата е должна да го гарантира квалитетот на услугите со воспоставување делотворен надзор над законитоста на работата на агенциите што ги даваат тие услуги. Значи, заштитата на јавниот интерес бара воведување минимум правила во секторот на приватната безбедност, со чијашто помош ова основно начело ќе ја реши колизијата помеѓу приватниот интерес (обезбедувањето и нудењето сигурност на трети лица врз комерцијани основи) и јавниот

³⁶ Ваква одредба е присутна и во некои законодавства што ја уредуваат областа на т.н. недржавна безбедност.

интерес, кој всушност претставува уредено, квалитетно и делотворно извршување на дејноста од приватната безбедност.

Еден од инструментите за заштита на јавниот интерес е воспоставувањето *адекватен лиценцен режим*, т.е. општи и посебни услови пропишани за извршување дејност од приватната безбедност, остварување надзор, задолжително водење евиденција, утврдени овластувања итн.

Воспоставување соодветен лиценцен режим треба да овозможи транспарентно извршување на приватната безбедност, што се уредува со доделување лиценца под одредени услови и во согласност со законската регулатива.

Инспекцискиот надзор над дејноста на субјектите од приватната безбедност треба да обезбеди овие работи да се извршуваат во границите на зоната на одговорност. Државата со закон му го доверува извршувањето на дејноста приватно обезбедување на приватниот безбедносен сектор, при што извршувањето на надзорната дејност е во надлежност на полицијата, барем додека приватниот сектор не го достигне потребното ниво на професионализација. Во подоцнежниот период, надзорната функција сè повеќе ја преземаат еснафските здруженија, комори и сл., а државата само ја утврдува потребната рамка што го гарантира легитимитетот на оваа дејност. Во спротивно приватната пракса врз себе ќе ги преземе работите што се во надлежност на државните органи – полицијата.

Инспекцискиот надзор на подрачје на приватната безбедност е нужен од правни и од практични причини. Од правен аспект, делотворниот инспекциски надзор треба да обезбеди законското извршување на работите од безбедноста и спречување можни злоупотреби. Примената на овластувањата се одразува врз човековите права и слободи. Исто така, на агенциите и на работниците за обезбедување не им е дозволено да извршуваат работи што се во надлежност на државните органи (пред сè полициски и правосудни).³⁷ Истото се однесува за извршувањето работи во корист на странски или домашни разузнавачки служби.

Многу е важно инспекцискиот надзор да се уреди така што надлежниот орган ќе ги задржи исклучиво контролно-надзорните овластувања, но не и можноста за самостојно арбитрирање кај повреди на законитоста. Со тоа оваа материја се уредува така што сè е подредено на меѓусебната избалансираност кај различните инстанци во општествената контрола.

Задолжителната обука на персоналот за безбедност е еден од показателите на грижа на агенциите, но пред сè на државата за со-

³⁷ Такви се работите за принудна наплата на долг, прогон на извршители на кривични дела и сл.

одветен профил и квалитет на персоналот за безбедност. Таа е важен предуслов за законското, делотворно, стручно и етичко извршување на работите во дејноста приватна безбедност. Задолжителната обука ја намалува потенцијалната опасност од можно настанување санкционирани и правно недозволен однесувања до кои најчесто се доаѓа во ситуации на примена на овластувања од страна на работниците за обезбедување. Со тоа се штити не само персоналот за безбедност туку и клиентот од високите барања за оштета што може да настанат во случај на телесни повреди и прекумерна употреба на сила.³⁸

По повод развојот на приватната безбедност во рамките на системот за национална безбедност, често во праксата и во законодавството се потенцира *односот помеѓу јавниот и приватниот интерес*.

Јавната власт се наоѓа во процес на трансформација од бирократизиран државен апарат во јавен сервис. Клучната точка во разликата помеѓу јавниот и приватниот сектор за безбедност е профитот. Првиот сектор ги сервисира јавните, а вториот приватните интереси.

Ова прашање е во непосредна врска со дилемата: кој е должен, кој знае, кој сака и кој може да има активна улога во тој систем. Државните (конвенционални) субјекти за безбедност имаат надлежност во сферата за заштита на лица и имот пропишана со закон. Меѓутоа, кога ќе преминеме на теренот на факултативното постапување на државните органи, не наоѓаме соодветни мерила за плаќање по дело. Државниот орган- полицијата не смее да дејствува според пазарните принципи, зашто со тоа би го загрозила пазарниот натпревар каде би претставувала привилегиран ривал во однос на оние даватели на услуги кои плаќаат данок. Се смета дека излезот е во доверувањето дела од јавните работи на приватниот сектор, во исто време кога оваа дејност сè повеќе се децентрализира и полициските надлежности се пренесуваат врз локалната самоуправа или врз регионалната управа. Со други зборови, економскиот интерес и профит се главниот мотиватор на превентивното постапување.³⁹

Прашањето за усогласување на јавните и на приватните интереси е присутно во многу расправи поврзани со развојот на законската регулатива, кога се укажува на значењето на начелото за сооднос и на начелото за заштита на јавниот интерес.

³⁸ Некои законодавства ја уредиле оваа област така што обуката се реализира како јавно овластување.

³⁹ Барањата за превентивно постапување се во непосредна врска со мерењето на нејзините дела што е посебно дискутабилно. Имено, тешко се воспоставува инструментариум врз основа на кој јасно би се видело дека вложувањето во превентивата го унапредило профитот.

Начелото за сооднос треба да обезбеди рамнотежа помеѓу поставената цел и средствата употребени за нејзиното остварување. Се состои од три елементи кои воедно претставуваат и критериуми за примена на овластувањата: примена на сила во согласност со поставената цел; употреба на средства за принуда со кои со најмалку штетни последици се постигнува целта од примената на овластувањата и самата примена на овластувањата, односно начело според кое слободата и правата на човекот и на граѓанинот се основа и мерка на овластувањата и одговорноста.

Примената на ова начело особено е изразена за време на инспекцискиот надзор врз извршувањето работи од приватната безбедност, а во согласност со уставното начело за слобода на приватната иницијатива. Инспекторот мора да води сметка да пронајде вистинска мерка во вршењето на инспекцискиот надзор што овозможува делотворен инспекциски надзор. Ова начело мора да биде евидентно при дефинирање на *посебните услови* за извршување дејност од приватната безбедност со кои се дозволува органичување на начелата на слобода на приватната иницијатива за *целта дозволена со устав*. Во конкретниот случај, тоа е *заштита на јавниот интерес*.

Начелото *заштита на јавниот интерес* е видливо од намерата на државата да пропише услови под кои одредени субјекти можат да извршуваат работи од приватната безбедност. Тогаш на сцена настапуваат регулаторните механизми со кои им се ограничуваат правата на оние што продаваат и купуваат безбедносни услуги, со правата и обврските на сите други кои учествуваат во правниот промет на полето на приватната безбедност.

Генерално, наместо расправи за конфликтот на вредност на одговорноста кон јавните или приватните интереси, што прима карактеристики на ривалство помеѓу двата сектора за безбедност (јавниот и приватниот), многу автори ја истакнуваат потребата од конструктивен дијалог кон кој треба да се стремат во изградбата на безбедноста заснована врз партнерство. Можеби т.н. „сива зона“ е нешто што би можело да се трансформира во партнерство помеѓу двата сектора, под услов да постои еднаква или слична претстава за тоа што претставува партнерство кај двете страни.⁴⁰ Искуствата потврдуваат дека за полицијата партнерството често се сведува на постапување и лојалност кон пропишите што ја изедначуваат одговорноста на припадниците на приватниот

⁴⁰ Најчесто станува збор за принудна наплата во побарувањето (израмнување долгови) и други работи од т.н. сива зона во надлежност на едниот или на другиот сектор.

сектор со полицијата во поглед на почитувањето на јавните интереси. За приватниот сектор партнерството подразбира изедначен статус во поглед на осигурувањето на безбедноста, заедничките владини проекти и професионализам во односите помеѓу двата субјекта.⁴¹

Врз основа на партнерство помеѓу двата сектора би се градело меѓусебното разбирање и свест за заедничките потреби во поглед на партнерството, што како последица би имало помалку конфликтни ситуации со кои се оптоварени овие односи. Како резултат на ваков пристап и повисоко ниво на „респект“ помеѓу двата субјекта, евидентен е порастот на решени случаи произлезени од заеднички акции. Ќе се покаже дека ваков пристап е неопходен кога е во прашање современиот кризен менаџмент, кој се базира врз новиот пристап кон јавниот менаџмент и користење алтернативни ресурси што во суштина претставува еден вид *win-win* ситуација.

Достигнатото ниво на развој и соработка меѓу јавниот и приватниот безбедносен сектор во определен општествено-политички систем зависи од голем број фактори, меѓу кои: местото што го заземаат во општеството, начинот на одлучување за позицијата и улогата на овие сектори во државата, нивниот придонес и вистинско значење, начинот на финансирање на овие сектори, природата на односи меѓу корисниците на безбедност и тие што ја даваат, работниот статус на вработените кои даваат услуги на одреден корисник итн. (Ahić J., 2009).

Се смета дека јавно-приватното партнерство ЈПП (PPP-Public Private Partnerships) овозможува јасна спецификација на целите, правата и одговорностите во законско обврзувачка форма. Покрај тоа, долгорочните и скапи заложби на ЈПП можат да доведат до постигнување подобра распределба на ризиците помеѓу владата и извршителите во приватната безбедност. Во минатото, владата беше дизајнер, надзорник и добавувач на услуги. Преку „јавно-приватните партнерствата за безбедност“ полето е израмнето и владата и приватните безбедносни компании работат заедно на секое ниво, и тоа: (Ortiz Carlos, 2010) од регрутација и обука до воено распоредување, со што партнерствата за безбедност овозможуваат воени и безбедносни активности низ сиот развиен свет. Поради помалите буџети за одбрана, западните сојузници на САД можеби ги применуваат принципите на јавно-приватно партнерство особено темелно,

⁴¹ Канадските искуства илустрираат позитивни примери на ваква сооработка со унапредување во делотворноста и на полицијата и на приватниот безбедносен сектор, во исто време служејќи им на интересите на јавната безбедност. Тоа е овозможено со бесплатни семинари за примена на овластувањата, прекршочното и кривичното законодавство, пишувањето извештаи и сведочењето пред суд.

со цел да се намали трошењето преку делење на финансиските ризици со добавувачите во приватниот сектор. Во замена, корпорациите добија прилично постојана основа во менаџментот на монополот на сила преку делумна сопственост на одбранбената и безбедносната инфраструктура или нивното работење или поддршка (Ortiz Carlos, 2010).

Од историски аспект односот меѓу јавниот и приватниот безбедносен сектор не бил секогаш најдобар. Некогаш полицијата го потценувала приватното обезбедување, кое пак почувствувало дека полицијата нема интерес за неговиот домен на дејствување. Меѓутоа во денешно време се тежнее кон остварување на овие партнерства, чија примарна цел е напредокот и развој на јавниот и на приватниот безбедносен сектор (Dempsey S.John, 2011).

Оттука, најчестите активности на партнерства и соработка вклучуваат:

- воспоставување деловни контакти, вклучувајќи и деловен ручек;
- споделување информации, како што се локални криминални стремежи, модус операнди (начини на работа), информации за инциденти, електронски адреси, веб страници и инфо-билтени;
- програми за спречување криминал, здружено учество на безбедносното поле, развивање заеднички методи за спречување криминал и здружување на силите за остварување на општите интереси во справување со видео пиратерија, графити, лажна тревога и програми за надзор на соседство;
- споделување средства односно, позајмување на техничката и на јазичната стручност, позајмување компјутерска опрема, „купување пари“, позајмување и безбедносни направи и подготовката на бележник со контакти и други информации;
- обучување, како на пример хостинг на посебни експерти и говорници;
- обезбедување законска рамка што ја вклучува поддршката и нацртот на закони;
- заедничко дејствување, како на пример, истрага на сложени финансиски измами или компјутерски престапи; носење заеднички безбедносен план за заштита од природни катастрофи, престрелки и насилства во училиштата како и насилство на работно место, и здружени операции за прекршоци, како на пример, улична кражба;
- истражувања и изработка на водич за подготовка и преглед на: проучувања и протоколи во врска со лажна тревога, криминал со дрога на работно место, насилство на работно место, инфо-телевизија од затворен тип и слично (Dempsey S.John, 2011).

4.3.3. Регулирање на приватната безбедност во националните држави

Во основа, некаква форма на регулатива влијае на поединецот речиси секој ден. Додека една личност со автомобилот патува на работа се среќава со бројни правила: да поседува возачка дозвола и осигурување, да му биде исправно возилото и да почитува одредени правила и прописи. Ако тој го пушти своето радио ќе слуша станици што се подложни на правила, односно има одредена фреквенција за употреба и е регулирано колку реклами ќе пуштат и кои теми може да ги обработуваат. Потоа тој ќе пристигне на работа во фирма во која, исто така, треба да почитува правила врзани со нејзиното работење. Исто така и фирмата во која работи се раководи според одредени правила на однесување кои мора да ги почитува за да опстои или да не биде доведена во незавидна состојба. Со други зборови повеќе е од потребно да бидат регулирани сите прашања во сите домени вклучувајќи ја и приватната безбедност (George Bruce and Button Mark, 2004).

Регулативата е од суштинско значење во поглед на законското работење на фирмата/компанијата и соодветното регулирање значи дека ќе се покрие една премногу чувствителна област во оваа сфера. Регулативата, исто така, може да помогне за подобро да се согледаат одредени состојби со што би се обезбедило што е можно подобро и порационално да се стават во функција сите ресурси. Од ова произлегува дека регулативата е клучен и корисен елемент во работењето на самата фирма/компанија што им помага на раководните тимови да воспостават соодветен баланс меѓу остварените и планираните активности. Без соодветна регулатива тие ќе се претворат во слепи набљудувачи на процесот што може да доведе до отстапувања на планираните цели и задачи и ќе бидат ограничени без можност да го коригираат, а со тоа и да го подобрат своето работење, како и работењето на приватниот субјект. Со други зборови, прописот може да се толкува како обичен формален механизам на контрола кој е воспоставен со цел да се насочува однесувањето и да се обезбеди универзална примена на законот. Во принцип, ние тврдиме дека поголема регулатива може да доведе до зголемена одговорност (O'Connor Lippert, Greenfield & Boyle, 2004).

Регулирањето на приватната безбедност во национални рамки е повеќе од потребна, но сепак, нејзиното целосно ефектуирање пред сè зависи од антиципативниот пристап на субјектите што се задолжени за изготвување ваков документ што за секој субјект инволвиран во оваа активност е доста тешка и одговорна работа. Нивниот ангажман за создавање подобра регулатива ќе помогне да се направи разлика меѓу чесни и дискредитирани приватни компании за обезбедување, и на крајот да се отстранат вторите.

Генерално, регулативата може да придонесе за подобрување на професионализмот на приватните компании за обезбедување, но може да придонесе и кон зголемување на довербата на јавноста. Професионализмот е категоријална црта што се однесува на одредени вредности, вештини, ориентација и управување. Принципите на фер однесување, интегритет, грижа за човековите права, одговорност и минимална употреба на сила се основните елементи во секој концепт на демократското управување. Професионализмот не смее да се вмеша во дискриминаторно, корумпирано или насилно искористување на својата моќ. Самостојноста (ограниченоста) што ја има приватниот безбедносен сектор се базира врз довербата на општеството дека овој сектор ќе прифати дел од вредностите што ќе ја условува демократската рамно тежа на етичко и на професионално водење (Fluri P., Hadžić M., 2004). Излегувањето од преграатките на професионализмот ќе резултира со грубо, корумпирано и некомпетитивно однесување, а во некои случаи може да доведе дури и до јавни скандали, што ја наметнува потребата од сериозна регулатива во овој сектор (Born H. Caparini M. and Cole E., 2007).

Значи, приватниот безбедносен сектор треба да биде предмет на законска регулатива за определување на начинот на работа, условите за вршење приватно обезбедување, санкционирање на можните злоупотреби на работата итн. Затоа регулативата е широк концепт што го опфаќа сетот на закони, правила и одредби што се однесуваат на работата на поединци и на фирми. Според Франсис, регулативата може да се дефинира како интервенција на државата во активностите на приватните сфери за да ги реализира јавните цели (Francis J., 2004). Поконкретно, Ајснер ја дефинира регулативата како нешто што вклучува широк спектар начела што ја контролираат економската активност и последиците од неа, а тоа значи нивен влез и излез од одреден пазар, цени, стапки на поврат и начини на натпревар (Eisner M.A., Eisner M.A., 1993). Прописите што ги регулираат приватните фирми за обезбедување вообичаено ги поставуваат стандардите што се потребни да бидат исполнети од страна на овие субјекти, што значи тие можат да вклучуваат барање едно одредено лице да биде одговорно за одреден субјект, минимално ниво на осигурување, соодветна опрема и минимално ниво на ресурси. Исто така, одредени законски акти го задолжуваат раководното лице на фирмата да ги обезбеди дополнителните барања кои се однесуваат на неговите овластувања од аспект на чување листи на вработени, водење евиденција за инциденти, обврска да ги информираат властите за специфични видови инциденти и обврската за носење идентификации.

Како што потенциравме досега, концептот на регулација, особено законската регулатива, ги обединува различните делови на политиката на приватно обезбедување и претставува институционално средство

преку кое можат да бидат остварени целите на приватната фирма за обезбедување. Според определени размислувања регулацијата создава еден механизам преку кој се оформуваат активностите на приватниот безбедносен сектор. Според застапниците на обновената легитимност пак, регулацијата создава еден механизам преку кој се добиваат потребните извори на легитимност од државата и на тој начин се зголемува актуелноста на нивните услуги. Според тоа на регулацијата треба да се смета како на централен елемент околу кој се врти политиката на приватното обезбедување (White Adam, 2010).

Денес особено важно е прашањето што прави една влада за да ја регулира оваа област. Одговорот на ова прашање треба да создава можност владата да ги реализира бројните алтернативи коишто и стојат на располагање и да ги одбере регулаторните опции што ќе му овозможат на приватниот безбедносен сектор да функционира ефикасно, истовремено заштитувајќи ги човековите права. Секако, ако причините на владата за регулација не се совпаѓаат со целите на компаниите коишто се оперативни во нивните граници, или едноставно не успеат да ги увидат тие цели, тогаш компаниите или фирмите ќе се соочат со многу тешка иднина којашто може да присили некоја компанија да дејствува надвор од прописите за да опстои. Во таа насока, целта за регулирање на приватните компании за обезбедување не треба да биде во насока да ги компромитираат бизнисите што се практикуваат во земјите сè додека тие практики не ги компромитираат меѓународните стандарди за човекови права. Осигурувањето на одржување на овој баланс нема да биде едноставна задача за одговорните за регулирање на работата на приватниот безбедносен сектор (Kinsey Christopher, 2006).

Постојат неколку причини зошто приватната безбедност и приватниот безбедносен сектор треба да бидат регулирани, и тоа: за да се осигура дека тие нема негативно да влијаат на мирот, безбедноста и разрешувањето на конфликтите, за да се осигура дека нивната употреба е истовремено легална и легитимна и е во согласност со човековите права, за да се осигура дека тие нема да ја поткопаат владината политика; за да се спречи тие да нанесат економска штета на нивните клиенти; за да се осигура дека ќе се одговорни за своите постапки и за оние на нивните работодавачи; за да се осигура да се што е можно потранспарентни; за да се спречи преоѓање од легална во нелегална определба; за да се гарантира дека тие на ниту еден начин нема да го поткопаат суверенитетот на државите.⁴² Исто така, приватниот безбедно-

⁴² Foreign Affairs Committee, Private Military Companies, London, The Stationery Office, 2002.

сен сектор треба да биде регулиран заради: гарантирање на уставните права на граѓаните (гаранција против злоупотреба и приватни вооружени групи); исклучување на криминалните и на „непожелните“ елементи од индустријата („расчистување на пазарот“); јасно дефинирање на поделбата на надлежности меѓу полицијата/другите актери од јавното обезбедување и приватните компании за обезбедување, и врз основа на тоа, дефинирање на улогата на секој актер во јавно-приватното партнерство; овозможување ефикасна контрола и систем за санкционирање; зголемување на квалитетот на услугите и со тоа да се зголеми заштитата на граѓаните, просториите, стоката, итн.; додавање кредибилитет на приватните услуги за обезбедување. Ова е тешка задача бидејќи целите на законодавецот не се сосема исти со целите на приватните компании за обезбедување (= наоѓање деликатен баланс на национално ниво). На крајот може да се заклучи дека во областа на регулативата, приватното обезбедување се смета за дел од активноста поврзана со спроведување на законот, речиси секаде во Европа.⁴³

Јасно е дека за кое било движење и обид да се воспостави регулација на овој сектор ќе треба многу време тој да се договори и да се спроведе (имплементира). Иако е многу јасно дека повеќето легални опции за злоупотреба на приватните компании за обезбедување е поверојатна на национално ниво, а не на меѓународно ниво. Постојната национална регулатива варира во квалитетот и ефикасноста во многу земји. Повеќето земји имаат донесено закони со многу недостатоци, а во некои земји законска регулатива воопшто и не постои. Во многу случаи легални се т.н. „сиви зони“ што вклучуваат и екстратериторијални прашања и проблеми што се однесуваат на мешање на државните и на приватните актери кои работат заедно. Ова значи дека секоја држава која на кој било начин е замешана во регулирање на приватната безбедност и на нејзините активности има потреба да ги развива законите кои се релевантни за фирмите за обезбедување како и законите кои би ги регулирале нивните активности (Ahić J., 2009).

4.3.4. Хармонизација на националните со европските стандарди во областа на приватната безбедност

Европеизацијата на пазарот на стоки и услуги не ги поштеди ниту интегрирачките процеси во областа на безбедносните услуги. Во меѓувреме, сличностите и разликите во поглед на нормираноста и прак-

⁴³ Општ преглед на услугите за приватно обезбедување во Европа, презентација на Натали де Мулдер на конференцијата „Македонски денови за приватно обезбедување 2013“, Скопје, 30/10/2013.

сата на приватната безбедност во индустриски развиените и во другите земји заземаат сè позначајна улога од аспект на интересот на приватните сопственици, но и на јавните интереси и на интересите на националната безбедност. Во отсуство на законски и други стандарди што се усогласени со европските и со меѓународните регулативи, приватната безбедност може негативно да влијае врз внатрешната безбедност и воопшто врз националната безбедност во контекст на слободно движење на стоката и услугите на европскиот пазар и на транснационалниот карактер на заканите по безбедноста.

Значајно е да се истакне дека во европското право постои релативно развиен систем на преседани, настанати врз основа на активноста на Европската комисија, која повеќе пати го покренувала прашањето за почитување на општите начела на единствениот европски пазар, како што се слобода на давање на услуги, населување или слобода на движење, во националните законодавства на одделните држави членки при регулирањето на приватниот сектор за безбедност. Така, Европскиот суд за правда, преку низа одлуки, ја востанови својата надлежност над материјата врзана и за приватниот сектор за безбедност, бидејќи како сегмент на стопанскиот сектор потпаѓа под единствениот (внатрешен) пазар на ЕУ (Maravić, D., 2008).

Што се однесува до Советот на Европа, може да се заклучи дека тој не се занимавал особено со специфични прашања од приватниот сектор за безбедност, но Советот на Европа сепак усвои низа конвенции и препораки релевантни и за функционирањето на приватните безбедносни компании. Пред сè станува збор за конвенции и препораки што се однесуваат на заштита на човековите права и владеење на правото во државите членки. Тука пред сè се мисли на Европската конвенција за човекови права, но и на членовите што се однесуваат на забраната на тортура, нечовечно или понижувачко постапување, правото на приватност, право на слобода и безбедност, забрана на дискриминација и слични одредби. Исто така, заслужува да се спомене и Конвенцијата за заштита на поединецот во врска со автоматската обработка на личните податоци, потоа Препораката за потребата од хармонизација на националната регулатива што се однесува на оружје, како и на други документи.

Анализата на законодавства со кои се регулира пазарот на приватната безбедност покажува значајни разлики во нормирањето и во праксата на приватната безбедност во мнозинството земји членки на ЕУ. Во опкружувањето во кое се укинуваат законските бариери во извршување на дејноста од приватната безбедност вон националните граници како и слободното движење на стока и услуги, би требало да се обрне внимание врз недостигот од хармонизација на основните законски стандарди

со кои се регулира овој сектор. И додека земјите членки на ЕУ повеќе не можат да го ограничат пристапот на странските фирми и компании и на поединци кои сакаат да ги понудат своите услуги од приватната безбедност надвор од своите граници, во исто време самите се ограничени да спроведат контрола над квалитетот и над професионализмот во извршувањето дејност од приватната безбедност. Во компаративна студија за законодавство со кое се регулира приватната безбедност, се тврди дека слободата на движење на стоки и услуги во оваа област отвора низа прашања (Brion, Kaminski, 2001), и тоа:

- ниво на безбедност на граѓаните кои повеќе не се во состојба да ја воочат разликата помеѓу понудените стандарди за квалитет од страна на различните вршители на услуги;
- заштита на фирмите и на вработени во тој сектор како последица на нивната немоќ да се соочат со конкуренцијата што не ги исполнува истите стандарди за квалитет и за обученост на персоналот;
- намалување на стандардот во јавниот ред како резултат од појава на компании и поединци на пазарот кои не го почитуваат законот на државата во која ја извршуваат својата дејност.

Развојот на конструктивниот пристап за решавање на овие прашања е особено важен, зашто големината и улогата на приватната безбедност многу се зголеми во последните години, особено во контекст на нејзиниот неоспорен придонес кон внатрешната безбедност на државите. Во ситуација кога безбедносните работи во сè поголем број му се доверуваат на приватниот сектор клучно е прашањето за ревидирање на националната законска рамка. Начинот тоа да се постигне е хармонизација на законските одредби врз основа на имплементација на минималните основни стандарди. Постапувањето минимум стандарди придонесува кон развој на професионализмот во овој сектор. Таков пристап сигурно би барал и подобра распределба на информациите врзани за разликите во законските стандарди помеѓу државите членки за да им се овозможи на потенцијалните клиенти исправно донесување одлуки при изборот услуги од безбедноста.

Одредувањето минимални стандарди воопшто не е лесна задача, особено ако тоа се однесува на трансфер на чувствителни информации за прашања како што се кривични досиеја и имплементацијата.

Разгледувањето на хармонизација на стандардите опфаќа специфични одредби што важат во секторот за приватна безбедност, и тоа во однос на:

- обемот на активности на приватната безбедност;
- степенот на пропишаност;
- исполнување услови за извршување дејности од приватната безбедност;

- рестрикции поврзани со оперативна проверка на сопственикот/раководното лице;
- рестрикции поврзани за оперативна проверка на персоналот;
- исполнување услови за извршување на дејноста;
- минимални услови за обука и образование;
- прописи што регулираат носење униформа и употреба на (огнено) оружје;
- одредби што регулираат употреба на службени кучиња;
- одредби што се однесуваат на надзорот и санкциите што се применуваат во рамките на секторот.

Во моментот, на ниво на Европската Унија не се одвива процес на хармонизација на законодавството кога е во прашање приватниот сектор за безбедност. Постојната Европска конфедерација на услуги за обезбедување (CoESS) ги промовира минималните услови за работа на приватните безбедносни компании на европско ниво. Исто така, постои и Правило на служба за приватниот безбедносен сектор (*Code of Conduct*),³⁹ што треба да придонесе во подигање на стандардот на услугите што ги признаваат овие компании и да гарантира високо ниво професионална етика во постапување со вработените во овој сектор. Меѓутоа, и покрај овие обиди за „мека“ хармонизација на регулативата во оваа област, и понатаму постојат значајни разлики во националните законодавства (Maravić, 2008).

4.4. Национални стандарди во областа на заштитата на лица, имот и работење

Стандардите долго време биле привилегија на богатите земји и со нив му се трасирал патот на крупниот капитал во помалку развиените подрачја. Бројни меѓународни документи денес особено ја апострофираат улогата на *земјите во развој* во креирањето нови стандарди, со чие прифаќање и примена се овозможува нивните производи, услуги и останати ресурси да бидат усогласени со глобалните барања и опкружувањето, со што би станале поконкурентни и попривлечни за странски вложувања. Се смета дека една од главните причини за досегашното ниско ниво на учество на земјите во развој во меѓународната стандардизација е ниското ниво приоритети што овие стандарди ги имаат во стратегии за развој на тие земји. Значи, тоа беше разбирливо во ситуација кога меѓународните стандарди биле привилегиран инструмент за развој на модерните економии и за трансфер на технологијата во меѓународни рамки.

Денес овие приоритети се менуваат, што е особено случај со изградбата високодоверливи системи, производи и услуги во земјите во

транзиција што ги бара развиениот свет и чии бенефити од користењето ги ужива, и кога е во прашање примарен, секундарен или терцијарен сектор од стопанството. Динамиката за прифаќање на меѓународните безбедносни стандарди, донесувањето национална легислатива во согласност со тие стандарди и нивна имплементација се неопходните услови за пристап кон европските и евроатлантските организации.

Во согласност со прокламираното определување на нашата држава за членство во ЕУ, преземени се редица чекори за приспособување на регулативата, односно усогласување на нашиот правен систем со правните стандарди на земјите од Европската унија.

Почитувајќи ги принципите на современиот менаџмент, во праксата на функционирање на јавните и на приватните институции во Македонија се развива процесен модел на менаџмент со квалитетот и тоа:

- Системи за менаџмент со квалитет – Барања (ISO 9001:2000),
- Системи за менаџмент на животна средина – Барања со упатства за користење (ISO 14001:2004),
- Оцена на сообразност,
- Систем за управување со безбедноста на храната – Барања за сите организации вклучени во синџирот на храната (ISO 22000:2005),
- Информациска технологија – Безбедносни техники – Системи за управување со безбедност на информации – Барања итн.

Како национална организација за стандардизација, Институтот за стандардизација на Република Македонија (ISPM) е национално тело за стандардизација што ги претставува националните интереси во меѓународните, европските и регионалните организации за стандардизација, ги промовира стандардизациските активности и преку здружување на јавните и приватните заинтересирани страни. Генерално, ISPM подготвува и усвојува доброволни национални стандарди.⁴⁴

Институтот за стандардизација на Република Македонија е основан во март 2003 година, врз основа на Законот за стандардизација („Службен весник на Република Македонија“ бр. 54/02) и со Одлука на Владата на Република Македонија („Службен весник на Република Македонија“ бр. 14/03). Овие предуслови овозможуваат Институтот за стандардизација на Република Македонија – ISPM да постои како посебна јавна установа, одделувајќи се од Заводот за стандардизација и метрологија.⁴⁵ Во март 2003 година беше извршен пренос на член-

⁴⁴ <http://isrm.gov.mk/> (посетена на 15.12.2015 година).

⁴⁵ Со Законот за стандардизација се уредуваат целите и принципите на македонската национална стандардизација, статусот на ISPM како и неговите задачи, зачленувањето и

ството во ISO (Меѓународната организација за стандардизација) од Бирото за стандардизација и метрологија на ISCPM. Подоцна, во 2003 година, ISCPM стана придружен член во CEN (Европски комитет за стандардизација). Во 2005 година, ISCPM беше прифатен како асоцијативен член во IEC (Меѓународната електротехничка комисија), а во март 2005 година стана придружен член во CENELEC (Европскиот комитет за електротехничка стандардизација). ETSI (Европскиот институт за телекомуникациски стандарди) во декември 2006 година го призна ISCPM како NSO (национално тело за стандардизација).⁴⁶

Значи, Република Македонија презема неопходни мерки со цел да се забрза развојот на стандардизацијата како еден од столбовите на инфраструктурата на квалитет, да се поттикне учеството во работата на европските тела за стандардизација (CEN, CENELEC, ETSI, EA, WELMEC, EUROMED и др.), како и да се поттикне користењето на техничките прописи на Заедницата и европските постапки за стандарди, тестирање и за оцена на сообразноста.⁴⁷

Целите на македонската стандардизација опфаќаат: унапредувањето на квалитетот и зголемување на нивото на безбедност на производите, постапките и услугите, придонесува за подобрување на квалитетот на животот и здравјето на луѓето, безбедноста на имотот и заштитата на животната средина и природата.⁴⁸

Мора да се истекне дека Институтот за стандардизација на Република Македонија досега нема донесено национални стандарди од областа на безбедноста на лица, имот и работење. Оттука, донесувањето национални стандарди од областа на приватната безбедност треба да биде мотивирано од бројни причини. Оваа област денеска станува значајна индустриска (стопанска) дејност што остварува профит, вработува голем број работници за обезбедување, но и одговара за безбедноста во голем процентуален сооднос за објекти во државата. Општо познато е дека токму во приватниот сектор за безбедност е концентрирано истражувањето, развојот и примената на најсовремените

неговото финансирање, подготовката, усвојувањето и објавувањето на македонските национални стандарди и нивната примена. Со Статутот на ISCPM се уредува името, седиштето и организацијата на ISCPM, неговата дејност, застапувањето и претставувањето, органите и нивните надлежности и одговорности, правата и обврските на членовите на ISCPM, финансирањето и други прашања во врска со неговото работење. Види http://www.isrm.gov.mk/mk/button_4.html, (посетена на 15.12.2015 година).

⁴⁶ http://www.isrm.gov.mk/mk/button_4.html, (посетена на 15.12.2015 година).

⁴⁷ http://www.isrm.gov.mk/mk/button_4.html, (посетена на 15.12.2015 година).

⁴⁸ http://www.isrm.gov.mk/mk/button_42.html, (посетена на 15.12.2015 година).

технологии од областа на безбедноста и заштитата (GPS, примена на електрохемиска заштита на готовината, алармни системи, видео-обезбедување итн).

4.5. Корист од примена на стандардите

Примената на стандарди од областа на безбедноста бара користење мерливи показатели за да се докажуваат предностите на нивна примена и пред општеството и пред економијата и работењето. Тоа не е едноставно зашто помеѓу воведувањето стандарди и измерливи резултати може да постои долга временска дистанца.

Во најопшта смисла, фактот дека стандардите се применуваат во некој сегмент, сам по себе има одредени предности. Покрај тоа што државата има интерес да ги применува, стандардите имаат бројни *економски бенефити*. Играат голема улога во економскиот раст и развој на патенти и лиценци.⁴⁹ Понатаму, меѓународните стандарди помагаат во елиминирање на техничките пречки во трговијата. Бидејќи европските стандарди му овозможуваат на бизнисот да дејствува на европскиот пазар, тие се исто така столбови на европскиот внатрешен пазар.

Дури 80% од европските стандарди водат потекло од националните стандарди, што претставува извонредно достигнување за националните стопанства и за земјите „извознички на стандард“. Со тоа се развива пазарната логика во донесувањето стандарди и се создаваат поволни услови за учество на глобалниот пазар. На пример, во интерес на извозно ориентираната германска економија, меѓународните и европските стандарди добиваат приоритет во однос на националните стандарди.

Со учество во стандардизацијата се остваруваат значајни *бенефити за бизнисот*. Прво, соработката со истражувачките ентитети му овозможува на деловниот сектор пристап кон знаењата *know how*, кои им се потребни за стратешки планови и анализа на пазарот. Често пристапот кон изворите на знаења се зема како главен мотив за учество на заинтересираните страни во стандардизацијата, што овозможува одредени компетитивни предности и изградба конкурентски позиции на пазарот.

⁴⁹ Научните студии во Германија покажуваат дека стандардите ги генерираат економските добивки од 1% на германскиот национален доход. Со примена на стандардите германското стопанство на годишно ниво има приход од 16 милијарди евра. Вообичаена пракса е и доделување годишни награди за најдобро достигнување и презентација во примената стандарди. Извор: Gesamtwirtschaftlicher Nutzen der Normung, DIN, Deutsches Institut für Normung e. V., Berlin, Wien, Zurich, Beuth, 2000.

Една од важните предности во примената стандарди се *бенефитите од интеракцијата помеѓу производот и системот*. Со примена на европските стандарди, новиот Airbus A330/A340 бара многу помал број делови во однос на стариот модел A300/A310. Резултатите се девет милијарди долари годишна заштеда, благодарејќи му на помалиот простор потребен за складирање производи.

Постојат непобитни докази дека *деловните губитоци се последица на невложување во безбедноста*, односно од неприменувањето стандарди што ја регулираат оваа област. Овие губитоци се директни или мерливи, произлезени од непосредното загрозување на имот ранлив на разни криминални активности, а индиректни и често тешко мерливи, како последица на определен безбедносен настан, и се манифестираат со пад на профитот а, во потешки случаи, и со банкрот, поради губиток на имиџот кај клиентите и на довербата на јавноста во производите и услугите.

Стандардите се критериум во одлучувањето на инвеститорите и овозможуваат унапредување на врските со опкружувањето. Со примена на стандардите актерите во некој правен промет може да го предвидат однесувањето на другата страна, а извесноста во планирањето, договарањето и инвестициите, се манифестира со намалување на бројот на непредвидени ситуации. Врз ова сознание всушност се заснова смислата на управувањето со ризици што, во основа, претставува управување со неизвесности.

Стандардите претставуваат фактор за превенција на инциденти, што може да се измери со бројот на избегнати инциденти. Бидејќи репутацијата е критичен фактор за успехот на секој ентитет, на тој пат истовремено се минимизираат ризиците за одговорност при случувањето штетни настани.

Освен тоа останува прашањето што се случува со бројот на корективни мерки што можат да ги измерат несаканите отстапувања од планот. Во вакви околности, стандардите се и катализатор на договорените односи. На пример, при инсистирањето кај снабдувачите да ги стандардизираат своите услуги, организациите настојуваат да ја избегнат зависноста од одредени снабдувачи, што може да се покаже како корисно, особено во кризни ситуации.

Во дејностите каде технологијата е стратегиски фокус на една организација, што е сè повеќе случај во областа на безбедноста, примарно е да се искористат можностите што резултирале од техничките и научните промени и развој.⁵⁰ Со воведувањето нови технологии и со

⁵⁰ VW („Фолксвагеновите“) автомобили ги намалиле трошоците за поправка како последица од несреќни случаи: „Дизајнот ориентиран кон одржувањето“,

унапредувањето на менаџментот во иновациите, стандардите се катализатор на новите идеи во создавањето безбедно опкружување и перформанси на организација што води сметка за интеракција на (новиот) производ и системот.

Стандардите во областа на безбедноста претставуваат ривалска предност во разни гранки на стопанството, особено во оние што се на удар на криминалот и на други закани. Така е со туризмот, стопанска гранка што бележи сè поголем раст во вкупната структура на светски услуги, но и кој е обележен како т.н. „мека мета“ на тероризмот. Од таа причина, безбедноста како важен атрибут на туристичките понуди и услуги последните години зазема високо место во перцепцијата на туристите при изборот на туристичка дестинација. На тој начин, примената безбедносни стандарди станува генератор на профитот, па задачата на менаџерот за безбедност е со примена на стандардите да овозможи безбедни услови за работење. Притоа се води сметка за оправданите трошоци наспроти бенефитот од примена на стандардите.⁵¹

Примената на стандарди е сè повеќе област на интересирање во управувањето со човечки ресурси како одделна научна дисциплина, но и како гранка на управување. Освен тоа што стандардите содржат јасни критериуми за прием и селекција на вработените, тие влијаат врз порастот на мотивација кај вработените. Успех од примена на стандардот што е и метрички поддржан е што може да се користи и да се мотивираат вработените. Исто така, метриките претставуваат делотворен начин што ќе помогне да се соопштат информациите за достигнуањата на вработените. Секој вработен подобро реагира и ги спроведува стандардите доколку резултатите од неговата работа се доведуваат во врска со примената на стандарди и доколку е свесен дека стандардите му се важни на раководството.

освен што го скратува времето потребно за поправка на автомобилот, води и кон намалување на премиите за осигурување на возилата во случај на несреќа.

⁵¹ На пр. нема смисла да се потрошат 100.000 денари на заштита од кражба за предмети вредни 10.000 денари, особено ако може да се плати осигурување или да се тргнат предметите на побезбедна локација.

V глава

ПРОЦЕНА И КОНТРОЛА НА РИЗИКОТ

1. ТЕРМИНОЛОШКО ОДРЕДУВАЊЕ НА ПОИМОТ ПРОЦЕНА НА РИЗИК

Процената на ризик опфаќа примена на логични и систематични методи за: комуницирање и консултации во текот на овој процес; воспоставување организациски контекст за идентификација, анализа и проценка на ризикот поврзани со која и да е активност, производ, функција или процес и адекватно известување и архивирање во врска со резултатите од процената. За да може организацијата да изврши ефективна проценка на ризикот, претходно мора да го дефинира контекстот на проблемот. По завршената проценка организацијата треба да изврши третман на ризикот.

Целта за изработка и примена на процената на ризикот е создавање услови за донесување ефикасни и ефективни одлуки во процесот на заштитата на лица, имот и работење втемелени врз сеопфатната проценка на ризикот.

Процената на ризикот бара стриктна и одржлива примена од страна на менаџментот на организацијата и стратегиско и оперативно планирање. Менаџментот треба:

- да ја артикулира и да ја одобри процената на ризикот;
- да ги извести сите заинтересирани страни и страните од интерес за предностите на процената на ризикот;
- да ги дефинира индикаторите на перформансот (успехот) на процената на ризикот што одговараат на организациските перформанси;
- да осигура поклопување на мерките востановени врз основа на процената на ризик со целите и стратегијата на организацијата;
- да обезбеди законитост и усогласеност со правните акти и стандарди и
- да обезбеди поделба на ресурсите неопходни за потребите на проценка на ризикот.

2. ОДГОВОРНОСТА И РЕСУРСИТЕ ЗА ПРОЦЕНА НА РИЗИКОТ

Организацијата мора да ги дефинира одговорноста и овластувањата, примената и одржливоста на процесот за проценка на ризикот. Ова може да се оствари со:

- воспоставување и дефинирање на работното место и работите на менаџерот за ризик;

- примена на соодветни механизми за признанија, награди, пофалби и санкции;
- воспоставување матрица за резултатите од интерното и/или екстерното известување за напредок;
- спецификација на носителите на ризик или категории на ризик со цел примена на мерки за третман на ризикот, одржување контрола на ризикот и интерно известување за релевантните информации за ризикот;
- спецификација на одговорноста за развој, примена и одржување на концептот за проценка на ризикот.

Во пракса, процената на ризик не е гаранција дека носителите на одлуки ќе постапат во согласност со препорачаните мерки за заштита што произлегуваат од извршената проценка. Сепак, самото постоење документи за проценка на ризик го обврзува менаџментот резултатите од процената да ги вградува во конечните одлуки, поради ризик на професионална одговорност во случај на настанување штетна појава.

Организацијата мора да ги применува практичните методи и средства за реализација на процесот за проценка на ризик, вклучувајќи ја поделбата на соодветни ресурси за процесот на проценка на ризик.

Процената на ризик мора да ги опфати следните елементи:

- а). документирани процеси и процедури;
- б). информатичка поддршка;
- в). човечки ресурси; и
- г). други ресурси неопходни за секоја фаза од процесот за проценка на ризик.

Од суштинско значење во процесот на проценка на ризикот е активно учество на сите вработени во организацијата.

3. КОНТЕКСТ НА ПРОЦЕНАТА НА РИЗИКОТ

Контекстот во процената на ризикот може да варира во однос на потребите на организацијата, во зависност од тоа дали се дава или се бара услугата за заштита на лица, имот и работење. Контекстот може да вклучува, но не е ограничен на:

- определување одговорност;
- определување длабочина и широчина на активноста за проценка на ризикот што треба да се спроведе;
- определување обем на проектот, процесот, функцијата или активноста во поглед на времето и локацијата;
- дефинирање на проектот, процесот, функцијата, активноста и нивните цели и предмет;
- определување однос помеѓу одреден проект или активност со други проекти или активности на организацијата;

- одредување барање за методологијата на проценка на ризикот;
- утврдување на начинот на кој се проценува ефектот од процената на ризикот;
- идентификација и спецификација на одлуките што треба да се донесат;
- идентификација на неопходни студии за рамките и обемот, нивниот опфат, цели и ресурси неопходни за таква студија.

Посветувањето внимание врз овие и врз други релевантни фактори треба да помогне усвоениот пристап за проценка на ризикот да биде соодветен на ситуацијата и на ризиците што влијаат во постигнување на целите, а во согласност со дефинираните и прифатени цели.

Да го илустрираме значењето на контекстот за проценка на ризикот со следните примери.

Моралните, етичките и религиозните убедувања може да претставуваат товар за работодавецот. Ова е помалку очигледно во западните култури, а мошне често на Блискиот Исток и во Азија. Се разбира, спогодбата со вработените не е унилатерална, зашто и вработените и нивните претставници ќе бараат остварување на своите интереси. Од ова произлегува дека мултилатералната природа на договорот значи дека целта треба да претставува оптимализација а не максимализација во корист на работодавецот.

За праксата на кризниот менаџмент клучната вредност во контрактуаријанскиот пристап се состои во тоа што ризиците произлегуваат од бројните спогодби што се склучени, зашто заинтересираните страни гледаат корист од нив. Во овој контекст, менаџментот на ризикот исто така мора да биде сфатен како сеопфатен. Интересно е дека во САД постои важна историска илустрација на оваа идеја: компензација на работниците. Во САД пред усвојувањето на актот за компензација на работниците постоел систем кога работниците се одрекувале од правото да го тужат работодавецот за повреди при работа и смрт во замена за гаранции поврзани со одредени погодности при лечењето. Настаните што уследиле довеле до компензација на работниците, од постепено признавање на синдикатот и работодавците кои сфатиле дека спогодбата со вработените е од обострана корист и дека безбедноста во работната средина има влијание и врз вработените и врз работодавецот. Според тоа, менаџментот на работната средина е сфатен како тема на кризниот менаџмент а менаџментот на ризик како тема од општ интерес. Се разбира, компензацијата на работниците во праксата е далеку од идеалниот општествен компромис.⁵²

⁵² Најголемиот научник на своето време кој се занимавал со проблемите на социјалното осигурување, Едвин Вит (Edwin Witte) во 1973 година заклучил дека, иако компензацијата на работниците е далеку од совршена,

3.1. Идентификација на потенцијални опасности

Идентификација на потенцијални опасности подразбира идентификација на хазард, фактори на ризик и опасности и изложеност на ризици релевантни за целите на политиката за работење на организацијата. Наведените поими се цврсто поврзани: така, на пример, *хазардот* може да биде контејнер со гориво складиран во непосредна близина на печка. *Пожарот* што може да настане од тој хазард претставува *опасност*, а *складот* што притоа може да изгори е *изложен на ризик*.

Организацијата треба да ги идентификува изворите на ризик, настаните или низата околности и нивните потенцијални последици. Целта на овој чекор е составување сеопфатна листа потенцијални опасности засновани на оние настани и околности што може да помогнат, да спречат, да намалат или да забават остварување на целите. Сеопфатната идентификација и регистрирање на потенцијалните опасности што може да резултираат со негативни последици е од суштинска важност, зашто потенцијалната опасност што во овој стадиум не е идентификувана останува неопфатена со понатамошната анализа. Идентификацијата треба да ги вклучи сите потенцијални опасности без разлика дали се тие под контрола на организацијата или не, без разлика на тоа дали во дадениот момент се актуелни или не се актуелни.

Организацијата треба да примени орудија и техники за идентификација на ризици што одговараат на нејзините цели и можности, како и на ризиците со кои организацијата фактички се соочува. Во оваа фаза на проценка на ризици, според стандардот ISO/ IEC 31010, се препорачува користење на следните техники: „бура од идеи“ (*Brainstorming*), структурирани или полуструктурирани интервјуа, делфи-техника, анализа со користење „листа за проверка“ (*Checklist Analysis*), прелиминарна анализа на хазард, анализа на хазард и оперативност (HAZOP), анализа на хазард и на критични контролни точки (HACCP), анализа „што ако“ (*What-If Analysis*) (SWIFT), анализа на сценарија и други постапки.

Во идентификацијата на потенцијалните опасности мошне важни се релевантните и ажурираните информации. Тоа се однесува и на соодветните претходни информации за ризикот, ако е можно да се дојде до информации од таков вид. Во идентификацијата на потенцијални опасности исто така би требало да бидат вклучени експерти кои имаат соодветно знаење. По идентификацијата на она што би можело да се случи, неопходно е да се разгледаат причините и сценаријата што пока-

таа претставува вид демократско решение што им обезбедува корист на сите страни, со минимални трошоци. Неговата теорија е позната како „теорија на најмалиот општествен трошок за компензација на работници“.

жуваат до какви последици може да дојде. Сите причини треба да бидат земени предвид. При идентификација на потенцијалните опасности исто така е важно да се разгледаат потенцијалните опасности што се во врска со неискористените прилики.

ПРЕЛИМИНАРНАТА МАТРИЦА НА РИЗИЦИ ТАБЕЛАРНО ЈА РЕПРЕЗЕНТИРА ИЗЛОЖЕНОСТА НА ОРГАНИЗАЦИЈАТА И НА НЕЈЗИНИТЕ СТЕКНАТИ ВРЕДНОСТИ, ПОРТФОЛИЈА ИЛИ ПОЕДИНЕЧНИ СЕГМЕНТИ И ПОТЕНЦИЈАЛНИТЕ ЕФЕКТИ ВРЗ ОРГАНИЗАЦИЈАТА ВО ЦЕЛИНА ИЛИ ВРЗ ОДДЕЛНИ СТЕКНАТИ ВРЕДНОСТИ. МАТРИЦАТА НА РИЗИК ОБЕЗБЕДУВА СТРУКТУРА ЗА СИСТЕМАТСКА АНАЛИЗА НА РИЗИКОТ, ГО СТИМУЛИРА РАЗМИСЛУВАЊЕТО ЗА РЕТКИ НАСТАНИ И ПОМАГА ВО ПОДЕЛБАТА НА ОДГОВОРНОСТ МЕЃУ ЧЛЕНОВИТЕ НА ТИМОТ (табела 3).

Извори на ризици	стекнати вредности					
	работење	безбедност	финансиски учинок работење	регулативно правни и други норми	углед	интересни страни
општо работење	Неизмирување обврски спрема добавувачите					
опасност по безбедноста и здравјето при работа		Нарушување на здравјето и животот на вработените				
правни опасности			потпишу- вање штетен договор			
Опасности од против- правно дејствување				Истекување класифицирани информации како деловна тајна		
Опасности од пожар					уништу- вање имот	
Опасности од елементарни и други несреки						уништу- вање имот
Опасности поради неусогласе- ност на стандарди						Работење без гаранција за квалитет

Табела 3. Пример за прелиминарна матрица на хазард
(Извор: Keković, Kesetović, Prevencija krize - hrestomatija, Fakultet bezbednosti,
Beograd, 2006.)

Целта на прелиминарната анализа е фокусирање врз најзначајните ризици, со тоа што не треба да се занемарат и малите ризици што може да имаат значаен кумулативен ефект. Прелиминарната анализа одредува еден или повеќе од следните правци на дејствување:

- третирање на ризикот без понатамошно оценување;
- издвојување занемарливи ризици што не би го оправдале третманот;
- да се продолжи со сеопфатна и детаљна проценка на ризикот.

Иницијалните претпоставки и резултати од прелиминарната анализа на ризикот пожелно е да се документираат.

3.2. Анализа на ризикот

Анализата на ризикот го опфаќа разгледувањето на причините и изворите на потенцијалните опасности, нивните позитивни и негативни последици и веројатноста од појавување потенцијални опасности, земајќи го предвид присуството (или отсуството) и ефикасноста на постојните мерки на контрола. Потенцијалните опасности се анализираат така што се одредуваат последиците и веројатноста од нивното настанување, а секако се земаат предвид и други важни особини. Настанот или низата околности може да имаат повеќекратни последици и може да влијаат врз поголем број цели. Исто така, во разгледувањето треба да се земе постојната контрола на ризикот и неговата делотворност. Анализата на ризици нуди информација за оценка на ризикот и за одлуките дали кон ризиците треба да се преземат мерки и кои се соодветни (најприфатливи) стратегии во третирање ризици.

Начинот на кој е изразена веројатноста од настанување потенцијални опасности и нивните последици и начинот на кој тие се комбинираат со целта за оценување на степенот на ризик, ќе варира во зависност од видот на опасноста и од намерата каква излезна информација за проценка на ризикот ќе се користи. Сите елементи мора да бидат анализирани во согласност со критериумот за анализа на ризик дефиниран во методологијата за проценка на ризикот. Исто така е важно да се разгледа меѓузависноста од различни опасности, ризици и нивни извори.

Сигурноста на оценката од ризици и нивната чувствителност на предуслови и претпоставки мора да биде разгледана во анализата и ефективно да им бидат пренесени на носителите на одлуки и на останатите страни од интерес, доколку тоа се бара. Факторите како што се разединување во мислењата на експертите или ограничувања на моделите треба јасно да бидат предочени, дури и нагласени.

На анализата од ризици треба да ѝ се пријде со различен степен на детаљност што зависи од видот на опасноста, намерата на анализата и информацијата, податоците и изворите што се достапни. Анализата може да биде квалитативна, полуквантитативна и квантитативна, во зависност од околностите. Во пракса, квалитативната анализа често се

применува прва, со цел доаѓање до општа индикација за големината на опасноста и откривање на најголемите опасности. Таму каде што е тоа можно треба да се изврши и квантитативна анализа од ризици како следен чекор. Без разлика на тоа кој вид анализа ќе се примени, мора да се изврши квантификација на степенот од ризици.

Последиците може да се одредат со изработка на модел од исходот на некој настан или низа настани, или со екстраполација од експерименталните проучувања, или од достапните податоци. Последиците може да се изразат во вид на определени и неопределени влијанија. Во некои случаи неопходно е да се располага со повеќе од една нумеричка или описна вредност, за да се прецизираат последиците за различни времиња, места, групи или ситуации.

3.3. Оцена на ризикот

Цел на оцената од ризици претставува помош во донесувањето одлуки врз основа на резултатите од анализа на ризици за тоа со кои ризици треба да се работи и за приоритетите во третманот на ризиците. Оцената на ризик го опфаќа споредувањето на степенот од ризици што се пронајдени во текот на процесот на анализа со критериумите за ризици кои се добиени во тек на разгледување на целиот контекст.

Во ситуациите каде што треба да се изврши избор помеѓу опции, тој ќе зависи од контекстот на организацијата. Одлуките треба да го земат предвид поширокиот контекст од ризици и да вклучат разгледување на толеранција на ризиците што ги утврдиле други организации, а од кои што организацијата ќе има корист. Етичките, легислативните, финансиските и другите околности, вклучувајќи ја и перцепцијата на ризици, исто така влијаат врз донесувањето конечна одлука.

Врз основа на оценка на ризиците се донесуваат одлуки за: потребата и начинот на третирање на ризиците; одредување приоритетни ризици и преземање конкретни активности. Доколку степенот на ризик не ги задоволи критериумите за ризици (не е прифатлив ризик), тогаш на тој ризик треба да се работи (ризикот би требало да биде третиран/разгледуван). Во некои услови оцената на ризикот може да доведе до одлука за продолжување на понатамошната анализа. Оцената на ризикот може исто така да води и кон одлука ризикот понатаму да не се ублажува на ниту еден начин освен реализација на постојната контрола на ризикот. Оваа одлука ќе зависи од склоноста на организацијата кон ризик и од поставените критериуми за ризици.

Природата на одлуките што треба да се донесат и критериумите за нивно донесување се востановени при анализа на контекстот на про-

блемот, но во оваа фаза тие мора повторно да бидат ажурирани, поради запознавање со повеќе детали за ризиците што се идентификувани. Наједноставната рамка за дефинирање критериуми за ризиците е таа што ги дели ризиците на оние што треба да се третираат и на оние на кои не им е потребен третман, меѓутоа, тоа не ја дефинира границата помеѓу овие ризици. Одлуката за тоа дали и како да се третира ризикот зависи и од трошоците и користа за преземање ризик и од трошоците и користа што настануваат со примена на засилена контрола на ризикот.

Нивото на ризик е директно зависно од примената на адекватни мерки за контрола и нивна ефикасност. Прашања што треба да се разгледаат во тој контекст во основа се следните:

1. Која од постојните мерки за контрола треба да се примени за постојниот ризик?
2. Дали со примената на тие мерки е можно адекватно да се третира ризикот на прифатливо ниво?
3. Дали во пракса мерките за контрола се спроведуваат според пропишаниот начин?
4. Дали мерките се доволно ефикасни во дадениот момент?

Нивото на ефикасност за одреден вид контрола или пакет контролни постапки може да биде изразен квалитативно, полуквантитативно или квантитативно. Во поголемиот број случаи не е можно да се гарантира прецизност со високо ниво, но тоа може да биде корисно за да се изрази и да се документира ефикасноста во контрола на ризици, така што да може да се донесе одлука за тоа дали е најцелисходно напорите да се насочат во правец на подобрување на контролата или на обезбедување соодветни третмани за различни ризици.

4. ТРЕТМАН НА РИЗИЦИ

Третирање на ризикот подразбира избор на една или на повеќе опции за постапување со ризикот и примена на тие опции. Третман на ризик може да вклучи и цикличен процес на оценување на третманот на ризик. Заклучокот дека преостанатите (резидуални) ризици не е можно да се третираат, води до создавање нови опции на третирање ризик и проценка на нивните ефекти до постигање соодветен степен од преостанатиот ризик што организацијата може да го намали според критериумот за ризици.

Изборот на соодветна опција за третман на ризици опфаќа балансирање на трошоците и на напорите во примена на опциите и користа што може да се извлече од тоа. Голем број опции за третман на ризици може да бидат разгледани и применети одделно или во комбинација. Организацијата може да има корист од усвојување комбинација од опции за третман на ризици.

Одлуките треба да ги земат предвид ретките ризици што резултираат со сериозни последици, со што може да се оправдаат акциите за третман на ризици што не се оправдани со финансиски трошоци. Правните и регулаторните барања и општествената одговорност го надминуваат значењето на финансиските трошоци на анализата за корисност.

Опциите за третирање ризици треба да ги разгледаат вредностите и перцепцијата на страните од интерес и да понудат кои се тие соодветни начини на комуникација со нив. Ако опциите за третирање ризик може да имаат влијание за ризик во организацијата, овие области мора да бидат вклучени во одлуката. Иако можеби подеднакво ефективни, некои опции за третирање ризици може да бидат поприфатливи за страните од интерес од други.

Доколку ресурсите за третман на ризици се ограничени, планот за третирање ризици треба јасно да го идентификува редоследот на приоритети по кој одредени опции за третирање ризик ќе бидат применети. Целосните трошоци за преземање акција треба да се споредат со буџетската заштеда.

Самиот третман на ризици може да доведе до ризик. Големiot ризик може да биде и неуспех или неефикасност на мерките за третман на ризици. Би требало надгледувањето врз примената на мерките да биде составен дел од планот за третман на ризици, за да се провери дали мерките се ефективни.

Процесот на третирање ризици исто така може да доведе и до секундарни ризици што треба да се проценат, намалат, надгледуваат и да се изврши нивна ревизија. Овие секундарни ризици треба да бидат вградени во истиот план за третирање ризици како и оние претходните и со нив не треба да се има работа како со нови ризици. Исто така, потребно е да биде идентификувана поврзаноста помеѓу два ризика.

По третирање на ризикот, носителите на одлуки и заинтересираните страни мора да бидат претпазливи што се однесува до природата и до степенот на преостанатиот ризик. Преостанатиот ризик треба да биде документиран и подложен на контрола и ревизија, а онаму каде што е погодно, и на понатамошен третман во согласност со новите околности.

Третманот на ризици опфаќа: избор на опциите за контролирање или ублажување на ризиците и опција за изводливост како и анализа на цената-користа.

4.1. Опции за контролирање или ублажување на ризиците

Ризиците може да се контролираат и со нив да се управува на различни начини а, во врска со тоа, постојат неколку пристапи (Sage, 1995):

- *пристап за прифаќање ризик*, во кој се занемарува постоењето што и да е поврзано со ризик, т.е. не се зема предвид можноста нештата да се случат поинаку од она како што е планирано;

- *пристап на ретроактивно управување со ризикот*, кој подразбира обиди за намалување на последиците по реализација на ризичен настан; ретроактивниот пристап подразбира управување со губитоци (штети);
- *пристап на интерактивно управување со ризик*, во кој за секоја фаза во животниот циклус на системот однапред се преземаат мерки ризикот да не настане;
- *пристап на планско управување со ризик*, што бара планирање и предвидување можности за појава на ризик, а потоа усвојување на оние активности со кои на најдобар начин се контролира можниот ризик; со ризикот се управува на тој начин што малку е веројатно да се појави каков и да е непланиран настан.

Јасно е дека на управувањето со ризик треба да му се пристапи од гледна точка на планско управување со ризик. Интерактивниот пристап има своја предност, но тој не може да ги предвиди и да ги спречи сите ризици. Во исклучителни прилики ќе се појават ризични ситуации, иако се применети и планскиот и интерактивниот пристап. Тоа покажува дека постои потреба и од ретроактивно управување, но тоа мора да биде поддржано со планско и интерактивно управување.

Во тек на повеќедециниската пракса на управување со ризик во разни области се искристализираа одредени правила, како насочувачи при одлучувањето за тоа на кој начин најефикасно ќе се контролираат ризиците. Наведуваме некои од нив:⁵³

1. Не треба да се ризикува повеќе од она што може да го дозволи сопствениот капитал.
2. Треба да се размислува за последиците од ризици.
3. Не треба да се ризикува многу поради малку.
4. Позитивно решение се прифаќа само при отсуство на сомнеж.
5. При постоење сомнеж се избира негативното решение.
6. Не треба да се мисли дека секогаш постои само едно решение; можно е да постојат и други.

Првото правило укажува на тоа дека пред вложување средства во ризичен потфат треба да се одреди максималниот можен губиток од потфатот, да се спореди губитокот со потребните вложувања и сопствените финансиски средства (капиталот). Односот помеѓу максималниот можен губиток и сопствениот капитал го претставува коефициентот на ризик. Истражувањата покажале дека оптималната вредност на коефи-

⁵³ Основные правила риск-менеджмента. Види: <http://www.risk24.ru/pravilarisk.htm>. 22.04.2011.

циентот на ризик е 0,3 а вредностите на коефициентот на ризик еднаков или поголем од 0,7 може да доведат до банкрот.

Второто правило се однесува на фактот дека треба да се води сметка и за веројатноста од појава на ризичен настан и за неговите последици, а врз основа на квантификација на ризикот да се донесе одлука за начинот на постапување со ризикот (третирање ризици).

Третото правило јасно се покажува кај осигурување на ризикот, а се однесува на одредување прифатлив однос помеѓу премијата на осигурувањето и износот на осигурувањето. Премија на осигурувањето е износот што осигуреникот го плаќа кај осигурувачот за осигурениот ризик. Износ на осигурувањето е паричната вредност на која се осигурани материјалните вредности, одговорноста, животот или здравјето на осигуреникот. Ризикот не треба да се задржи, односно потребно е да се трансферира на осигурувањето, доколку обемот на губитокот е релативно голем во споредба со економијата на износот на осигурувањето.

Другите три правила се меѓусебно поврзани и говорат за тоа дека во ситуации во кои, според наше мислење, е можно само едно решение, треба уште еднаш да се размисли и, по можност, да се најде уште некое решение. Можно е такви решенија да постојат. Доколку повторната анализа покаже дека други решенија нема, тогаш треба да се одлучува според принципот „по претпоставка полошото (решение)“, т.е. ако постои сомнеж, се избира негативно решение.

Поголемиот број теоретичари на ризици се согласуваат дека стратегиска цел е да се контролира, т.е. превенира ризикот, а не да се финансира кога ќе се случат негативни последици.

Понекогаш се смета дека управувањето со ризик е серија чекори: прво, организацијата ги проценува ризиците, потоа се обидува да ги контролира, потоа бара начин да ги „финансира“ ризиците што не може да ги контролира. Во праксата ова ретко се случува, зашто процената, контролата и финансирањето често мора да се извршат симултано. Сепак, општ принцип е контролата на ризици да е подобра од нивното финансирање.⁵⁴

Денес во тек е општата дебата околу стратегиските програми за финансирање ризици, која се обидува да ги развие комплексните повеќегодишни инструменти за финансирање осигурани ризици или самофинансирање ризици. Од друга страна, контролата на ризици бара долготрајни напори и активности за повисок менаџмент во организацијата.

⁵⁴ Според принципите на осигурување, речиси секогаш е помалку скапо да се превенира губитокот отколку да се плаќа за него кога ќе се појави.

Супститутот осигурување често го преценуваат стратегиите и програмите за управување со ризик. За помалите организации, со ограничена способност да ги предвидат идните губитоци, улогата на осигурувањето е да ја намали неизвесноста. За организациите што можат да ги предвидат идните губитоци со поголема извесност, стабилноста на буџетот е клучно место што ја оправдува улогата на осигурувањето. Предностите на осигурување во финансирањето ризици особено се изразени кај организациите што немаат капацитет прецизно да ги предвидат губитоците. Ако организацијата, или дури локалната власт, имаат можност за предвидување на губитоците, може да се случи користа од осигурувањето да биде далеку помала, зашто организацијата ќе направи сè за да го контролира ризикот. Ако понудата на осигурувањето е несоодветна, локалните власти ќе мора да водат сметка за стабилност на буџетот и за алтернатива на осигурувањето преку самоосигурување, лимитирано осигурување итн. Особено поради ограничениот буџет за финансирање вонредни настани, локалните власти мора да изнаоѓаат правилен баланс во политиката за финансирање ризици.

Може да заклучиме дека опциите за третирање ризици не е задолжително да се исклучуваат една со друга, а исто така не би требало да не се применуваат и во сите околности. Опциите го вклучуваат следното:

1. избегнување ризици така што нема да се почне или да се продолжи со активност што ќе доведе до појава на ризик;
2. барање можност така што ќе се почне или продолжи со активност што може да доведе до ризик или да го одржи;
3. остварување влијание врз веројатноста;
4. остварување влијание врз последиците;
5. поделба на ризикот со уште една или со повеќе страни; и
6. задржување на ризикот, со свесен избор или несвесно.

Во пракса многу од овие опции се применуваат истовремено, при што намалувањето ризици во основа е цел на секоја опција за третирање ризици.

Интегрираниот пристап на контролата ризици на вработените, со кои се соочуваат сите организации, мора да содржи координиран план што вклучува некои од следните елементи:

- склучување договор,
- процедура на проценка (*screening*), вработувања, напредувања, отпуштања,
- безбедносни мерки,
- осигурување на лојалните вработени.
- обука и професионален развој,
- безбедност на работното место и здравствени мерки,
- компензација/стимулација на вработените,

- односи со синдикатот,
- менаџмент на односите со јавност,
- интеграција на процените за ризици на човечки ресурси со плановите за контингенција (за вонредни ситуации),
- стратешко планирање на работната сила,
- постапување во случај на дискриминација и/или малтретирање на работното место,
- стратегија за инвестирање во работна сила.

4.2. Опции за изводливост

Секоја опција за третман на ризици треба да биде земена предвид според етапите за проценка на ризици. Анализата на секоја опција мора да ја земе предвид и цената за измена на процедурите или производите (на услугите) во согласност со мерките за третман на ризици. Анализата за изводливост треба да ја изведат стручни финансиски органи, а резултатите од анализата треба да ги достават до носителот на одлуките.

4.3. Анализа на цената-користа

Анализа на цената-користа е последниот чекор пред имплементација на предложените мерки за третман на ризици. Потребно е да се утврди колкава е вистинската цена за имплементација на предложените опции за третман на ризици и да се определи големината на финансиските и на другите трошоци што настануваат со примена на предложените мерки. Анализата треба да ја изведат стручни финансиски органи, а резултатите од анализата треба да ги достават до носителот на одлуките.

5. КОНТРОЛА, РЕВИЗИЈА И ДОКУМЕНТИРАЊЕ НА ПРОЦЕСОТ ЗА ПРОЦЕНА НА РИЗИЦИ

Сите елементи од процесот за проценка на ризици мора да бидат изложени на постојана контрола и ревизија. Процената на ризици резултира со одредување мерки за третман на ризици, што треба да му помогнат на носителот на одлуки да ги анализира идните активности на организацијата. Реализацијата на одлуките претпоставува постоење план за третирање ризици и имплементација на мерки на сите нивоа на управување.

Плановите за третирање ризици содржат:

1. список на лица кои се одговорни за одобрување на планот и на лица кои се одговорни за примена на планот;

2. предложени акции;
3. мерки на дејствување и ограничување;
4. барање за надгледување и известување;
5. очекувана корист;
6. временско усогласување на предложените акции и остварување цели.

Плановите за третман на ризик треба да бидат интегрирани во управувачките процеси на организацијата и за нив би требало да се разговара со соодветните страни од интерес.

Контролата и ревизијата треба да овозможат:

- адекватна употреба на резултатите од анализите и поуки извлечени од настаните, промените и трендовите;
- детектирање промени во надворешен и во внатрешен контекст, вклучувајќи ги и промените на самиот ризик што може да бараат преиспитување на опциите од третманот на ризици и приоритети во третман на ризици;
- проверка дали мерките за контрола на ризик и третман се ефективни и во плановите и во реализацијата.

Контролата и ревизијата може да се спроведуваат по пат на редовни проверки, периодично или одненадеж и ненајавено, во согласност со процената на менаџментот. Пожелно е да се планираат сите наведени аспекти на контрола и никако не е доволно потпирање само на повремена ревизија и контроли.

Резултатите од контролите и ревизиите треба бидат евидентирани и врз нивна основа треба да бидат направени извештаи за интерна и за надворешна јавност. Кога е тоа потребно, исто така, може да се користат како влезни информации за ревизија на концептот за управување со ризици во процесот на управување со организацијата.

Организацијата мора да воспостави процедура за евидентирање на активностите во процена на ризиците. Во процесот за процена на ризици архивата претставува основа во усовршувањето методи, алатки и целокупниот процес. Архивирањето документи поврзани за процена на ризиците треба да се практикува во класичен и во електронски облик. Неопходноста од евидентирање и од постоење архива е поврзана со потребата за известување – редовно или вонредно – и вршење анализа.

Одлуките за формирање архива треба да земат предвид:

- користа од дополнително користење на информациите за целите на управувањето;
- правни, регулаторни и оперативни потреби на архивата;
- методот на пристап, пронаоѓање и складирање податоци;
- периодот на чување; и
- чувствителноста и степенот на тајност на податоците.

На крај, организацијата што применува проценка на ризици мора да обезбеди *информатичка поддршка во процесот за проценка на ризици*. Тоа подразбира поседување информатичка опрема со соодветен софтвер со чија помош може да се применува методологијата за проценка на ризици, со можност за регистрирање, анализирање и известување.

6. ТЕХНИКИ ЗА ПРОЦЕНА НА РИЗИЦИ СПОРЕД СТАНДАРДОТ ISO/IEC 31010

Техниките за проценка на ризици се постапки со кои се врши мерење, односно се предвидуваат консеквенци од ризиците и влијание што појавувањето на ризиците го имаат врз определен проект, активност или настан. Постојат повеќе техники за проценка на ризици, а изборот на техниката што ќе се примени зависи од барањето на заинтересираните страни, од природата на ризикот што се анализира, од достапноста на релевантните податоци, од ресурсите што се на располагање, од начинот на прикажување на резултатите итн. Во зависност од мерливоста на резултатот, техниките за проценка на ризици може да бидат:

- квалитативни, кога резултатот е невозможно да се искаже со бројки туку се користат определени описни оценки;
- квантитативни, кога резултатот е нумерички јасен;
- полуквантитативни, кога со комбинирање на двата претходни модела на посреден начин ќе се дојде до определени насоки.

При избор на техниката треба да се има предвид применливоста, точноста, ограничувањата, прифатливоста на методологијата и алтернативната методологија. Нивото на бараните детали зависи од определеноста на побарувањето, од достапноста на доверливите податоци и од креирањето на одлуките според потребите на организацијата. Некои методи и степен на анализа на деталите може да бидат законски дефинирани или по пат за барања искажани во стандарди.

Квалитативната проценка ја дефинира веројатноста и последиците според однапред поставени нивои (високи, средни, ниски итн.). *Полуквантитативните методи* користат нумерички скали за одредување веројатност и последици и го определуваат нивото на ризик со нивно комбинирање и користење математички формули. *Квантитативната анализа* ги проценува практичните вредности на последиците и веројатноста од нивно настанување и, во тој контекст, ги проценува нивоата на ризици во одделни единици. Целосна квантитативна анализа нема секогаш да биде можна, поради недостиг од податоци, влијанија на човечкиот фактор и друго или поради тоа што примената на квантитативната анализа не е оправдана или неопходна. Во такви околности,

паралелното полуквантитативно или квантитативно рангирање на ризиците од страна на менаџерите за ризици, кои се добро едуцирани, може да биде мошне ефикасно.

Во случаите на примена на квалитативната анализа мора да бидат објаснети сите термини што се користат, а основата врз која се засноваат сите критериуми мора да биде забележана (снимена). Дури и кога е во прашање квантитативната анализа, мора да се има предвид дека нивоата на пресметаниот ризик се само процени. Нивоата на ризици треба да бидат прикажани со примена на најсоодветни техники за тој вид ризици и во облик што е прифатлив од аспект на процена на ризици. Во некои случаи големината на ризиците може да се изрази како распределба на веројатноста над редица последици (материјални губитоци, човечки жртви, финансиски загуби итн.).

За процена на ризици, односно за одредени фази во процената (идентификација, анализа и евалуација на ризици), со стандардот ISO/IEC 31010 се препорачани техники и алатки. Техниките на процена на ризици содржани во овој стандард служат како поткрепа на меѓународниот стандард ISO 31000 и обезбедуваат упатство за избор и примена на систематични техники за процена на ризици.

7. ПРАВНА ОСНОВА ЗА ПРОЦЕНА НА РИЗИЦИ И НОРМАТИВНИ АКТИ НА ОРГАНИЗАЦИЈАТА

Законите, прописите и другите општи правни акти го сочинуваат нормативното опкружување во кое секоја организација ја извршува својата дејност. Адекватноста на нормативните решенија е важен фактор за работење на организацијата врз кои тие не може да влијаат но на кој, сепак, мора да се приспособат. Значењето на квалитетните законски (и воопшто нормативни) решенија се основен предуслов за остварување на дејноста и работењето во организацијата. Доколку, на пример, не постои законска рамка што создава основа за системско спречување или ублажување последици од природни катастрофи, односно од елементарни непогоди (поплави, земјотреси, свлечишта, пожари итн.) и останати вонредни ситуации ниту се овозможува единствен, навремен и организиран одговор на нив, далеку се помали шансите самоиницијативното, ситуациското и несинхронизираното дејствување да даде соодветни резултати. Ако нема цврста нормативна рамка со која надлежните субјекти наоѓаат систематско, организирано и воедначено дејствување и ако нема утврдени санкции за непочитување на пропишаните процедури и мерки, можноста одреден хазард или опасност, ризик или група поврзани ризици да прераснат во катастрофа, секако повеќекратно се зголемува.

Законски и подзаконски прописи што се директно или индиректно поврзани за доменот на проценка на ризици има навистина многу, па обидот за создавање нивен исцрпен попис, барем на ова место, не би бил од голема корист.

7.1. Внатрешни нормативни акти на организацијата како средство за проценка и контрола на ризиците

Државната регулатива не е единствениот нормативен феномен кој треба да се земе предвид во однос на оваа дејност. Организациите имаат права и должности да создаваат внатрешно обврзувачки правни прописи со кои се регулираат бројни прашања, меѓу другото, и во домените на управувањето со ризиците во областа на приватното обезбедување. Под правни акти на компаниите и други организации, се подразбираат општи правни акти донесени од страна на органите на правното лице врз основа на законски овластувања, а со цел регулирање на одредени правни односи внатре во претпријатието/фирмата. Во категоријата на внатрешни правни акти спаѓаат: статут, основачки акт, правилници (на пример правилник за работа или правилник за дисциплинска одговорност), деловник за работа на надзорниот и управниот одбор итн.

Сите интерни правни акти спаѓаат во доменот на т.н. недржавно или автономно право. Внатрешната правна регулатива претставува моќно оружје во областа на менаџирањето со ризици. Преку внатрешните акти претпријатието/фирмата самостојно ги уредува прашањата за проценка, превенција и контрола на ризиците кои не се регулирани со државни правни акти или применува законски норми, приспособувајќи ги кон специфичностите на сопствената организација, структура, дејност и систем на работење. На овој начин внатрешните акти може да надоместат барем некои недостатоци на екстерната регулатива и да создадат оптимален систем за спроведување на законските обврски во доменот на управување со кризи. На пример, и кога екстерните правни норми не создаваат соодветна основа за превенција на кризата, претпријатието или друга организација може да пропише внатрешни процедури кои ќе ја намалат веројатноста за настанување кризни ситуации. Тука станува збор за процес на инструментализација на правните овластувања на организацијата за целите на кризниот менаџмент. Исто така, дури и во ситуација во која примената на кривични санкции на државно ниво е незадоволителна, односно поголема е веројатноста од извршување кривични дела против имотот на организацијата, таа може по пат на внатрешна регулатива да создаде одговарачки систем на процедури и мерки за сопствена заштита, со чие остварување би се одвратиле потенцијалните извршители. На пример, ако фирмата воспостави адекватен систем

на физичко-техничка заштита и со интерни правни норми пропише обврски на сите вработени во врска со почитување на безбедносните правила, како и санкции за нивно непочитување, а со тоа и редовно и неселективно да ги спроведува, и го казнува секое кршење на работната дисциплина во овој домен, односно да развие ефикасен систем на брзо правно реагирање поради зачувување на своите права и интереси, таа, иако „заробена“ во неповолното надворешно опкружување, станува успешно организиран ентитет, кој може, барем релативно ефикасно да се спротивстави на безбедносните закани од појави како имотен криминалитет. Мислиме дека непостоењето адекватни внатрешни нормативни регулативи според тоа би можело да се карактеризираат како важен правен ризик. Називот „правен ризик“ го користиме бидејќи карактерот на ризикот е правен, затоа што самиот факт за непостоење на одредени норми е фактор на ризик. Според тоа, оправдано е таквите ризици да се наречат со терминот *правни ризици*.

Во претходните примери, пак, како ризични не ги наведовме само ситуациите врзани за непостоење на регулатива, туку и оние што произлегуваат од нејзиното неприменување. Суштински, тоа е сличен проблем како и кај државната регулатива. Речиси подеднакво ризично е да се нема регулатива и да се има, но сепак како и да се применува погрешно или воопшто да не се спроведува. Така, ризик е и неспроведувањето на адекватните нормативни регулативи. Повторно, ризик е и да се има регулатива во областа на заштитата на имот, лица и работење, но и да се нема во поврзаните домени. Да речеме, организацијата ги утврдила процедурите и мерките за приватната безбедност, но нема правилник за систематизација на работни места со кој се воведуваат соодветни позиции задолжени за нивно спроведување, потоа на пример нема правилник за деловна тајна, а се занимава со дејности во кои тајноста на податоците е важен елемент во работењето, или нема правилник за дисциплинска одговорност кој го санкционира кршењето на внатрешните прописи. Слична ситуација би настанала во случај организацијата да нема ефикасно организирани служби за брзо правно реагирање во кризите кои вклучуваат нормативни аспекти.

Мислиме дека водејќи сметка за различните безбедносни закани, би можела да се направи следната класификација на правните ризици кои потенцијално загрозуваат лица, имот или работењето на организацијата. Имено, секоја организација при процената на ризиците мора да утврди дали во нејзината рамка постои:⁵⁵

⁵⁵ Класификацијата која следува е дел од Стандардите за проценка на ризици во заштитата на лица, имот и работење, кои се усвоени во Институтот за стандардизација на

- внатрешна нормативна регулатива со која се предвидува процедурата за прогласување на одредени документи за деловна тајна и се воведуваат адекватни методи за заштита на тајноста на работните податоци;
- правилник за систематизација на работните места, кој ги пропишува соодветните работни места во чиј делокруг се наоѓаат работи поврзани со чување деловни тајни и заштита на корисниците од индустриска шпионажа и други ризици на работењето;
- внатрешна регулатива со која се предвидува дисциплинска одговорност на лица заради несовесно работење и/или непочитување на внатрешните процедури во областа на безбедноста на лица, имот и работење кои ги предизвикале или би можеле да предизвикаат негативни имотни и неимотни последици за корисниците;⁵⁶
- внатрешна регулатива со која се предвидува надлежноста во областа на надзор и контрола на законитоста на работењето, почитување на внатрешните процедури од страна на вработените и одговорните лица и спроведување мерки за превенција и третирање на ризикот;⁵⁷
- внатрешни процедури за мониторинг на реализацијата на работните договори и превенција од настанување имотни штети по завршување на неповолни работни аранжмани;
- адекватно следење судски, управни и други спорови и постапки кои ги води корисникот;
- адекватен систем на внатрешна заштита од ризик од криминално дејствување и ризик од нелојална работна конкуренција, кој се согледува во ангажирање на стручни сектори со задача следење и брзо правно реагирање во случај на појава на овие ризици;⁵⁸
- регулатива со која се конституира адекватен систем на внатрешна контрола над работата на вработените задолжени за

Република Србија и е практичен методолошки инструмент за примена на српскиот стандард SRPS A.L2.002, од 2008 година.

⁵⁶ Оваа материја може да биде регулирана со Правилникот за работа или со посебен правилник.

⁵⁷ Регулирањето на тие прашања може да биде предмет на Статутот, Правилникот за работа и внатрешни процедури.

⁵⁸ Системот за внатрешна заштита може да биде конституиран и регулиран во рамките на Правилникот за внатрешна контрола и внатрешни процедури за совладување на ризикот.

безбедност на лица, имот и работењето, и воведува обврска за поднесување редовни извештаи за сите инциденти и акциденти кои го загрозиле работењето, лицата или имотот на организацијата;⁵⁹

Анализата и оцената на претходно наведените категории на ризици и инструментализацијата на внатрешните правни регулативи за потребите на превенција и сузбивање на ризиците се комплексни задачи. Сепак, дадената класификација претставува солиден ориентир за проценка на потенцијалните последици и веројатноста за нивното остварување. Мислиме дека организацијата која во голема мера ги исполнува стандардите поставени со оваа класификација би можела реално да ја намали веројатноста од настапувањето на одредени ризици.

Исто така, се смета дека правните ризици се категорија на ризици која ги опфаќа сите останати, затоа што другите видови ризици секогаш можат, барем и делумно, да се изразат во правна смисла. На пример, ризиците од пожар или ризиците од загрозување на здравјето при работа имаат нормативна димензија, затоа што процедурите за нивната превенција се предвидени со државната регулатива, а можат да се пропишат и конкретизираат и со внатрешни правни норми. Ризиците од противправно дејствување, пак, се врзани за правни прописи кои се кршат со такви акти. Според тоа, јасно е дека недостатоците во правната димензија на организациското дејствување сами по себе претставуваат категорија на ризик чие значење се согледува во сите преостанати групи на ризици.

Сепак, нормативните акти на претпријатието мора да ги задоволат строгите критериуми и стандарди во доменот на проценка и превенција на ризици како би станале адекватен инструмент на организацискиот менаџмент. Веруваме дека на секоја организација нивната правилна изработка и примена „ќе и се исплатат“ од повеќе причини како имплементацијата на стандардите, т.е. правила и процедури за проценка на ризици по пат на нивна внатрешна норматизација е оптимален начин за предупредување за безбедносните ризици. Потоа, примената на стандардите го оплеснува процесот на спроведување на законските обврски на фирмата/компанијата. Конечно, стандардизацијата на мерките и постапките за контрола на ризикот во рамките на нормативните акти произведува правни обврски за сите членови на организацијата, го зголемува степенот на одговорност и го подига нивото на безбедносна култура во фирмата.

⁵⁹ Работните места се систематизираат со Правилникот за работа, а со внатрешните процедури се одредува надлежноста на одредени лица во рамките на работниот процес.

Резултат на процесот на нормативизација на стандардите во областа на превенцијата и контрола на ризици треба да биде конституирање интегриран систем на правна заштита, кој би се пресликал во постоењето адекватна регулатива и организација на сектори и служби, засновани врз нејзина основа, со задача вршење надзор над процесот на имплементација на нормите. На овој начин може да се спречат и да се сузбијат бројни безбедносни ризици и да се остварат следните цели: јасна распределба на надлежноста, процесите и работните задачи, ефикасна организација на правните служби, координација на правните служби и безбедносниот сектор и внатрешна правна контрола над работењето, ефикасен надзор над примената на законите, внатрешни нормативни акти и процедури во областа на кризниот менаџмент. Исто така, со нормирањето на обврската за поднесување на редовни извештаи за безбедносната состојба на фирмата и случувањата кои ја загрозиле, би се создала рамка за континуирано приспособување на регулативата во согласност со потребите на претпријатието.

8. КОРПОРАТИВНА БЕЗБЕДНОСТ И ПРОЦЕНА НА РИЗИЦИ

Работите на корпоративната безбедност опфаќаат заштита на имот, лица и работење на организацијата, превенција на криминално дејствување на екстерни и интерни субјекти и внатрешен надзор над законитоста на работата на вработените и менаџментот. Ризиците за безбедноста на корпорацијата можеме да ги поделиме на оние што настануваат како резултат на противправно дејствување на екстерни субјекти (лица кои се наоѓаат надвор од организацијата – вонорганизационски актери) и оние што се резултат на дејствувањето на внатрешни субјекти (вработени, раководители – организациски актери).

Познавањето на законските прописи со кои се предвидуваат облиците на криминалното однесување и се пропишуваат казни и други санкции за извршителите на кривични дела може да биде важен елемент на превенцијата и контрола на ризиците. Лицата задолжени за создавање и примена на безбедносните мерки во рамките на претпријатието/фирмата (раководители и вработени) мора да бидат запознаени со извесен број кривично-правни норми, од неколку причини. Прво, зачестеноста на одредени видови криминалитет укажува на веројатноста дека претпријатието/фирмата ќе стане жртва на кривично дело што ниту малку занемарливо. Штетните последици на тие дела можат да бидат огромни (особено во случаите на разбојништво, кражба, компјутерски криминал, тешки дела против општата безбедност, саботажа, диверзија итн.), како за имотот и човечките ресурси, така и за имиџот на правните лица.

Видовите криминални активности кои најчестичесто и најопасно ги погодуваат претпријатијата/фирмите се: имотен криминалитет (особено следните кривични дела: кражба, тешка кражба, разбојништво, ситна кражба, измами и затајувања); компјутерски криминал (особено кривичните дела: правење и внесување компјутерски вируси, компјутерски измами, компјутерска шпионажа, оштетени компјутерски податоци и програми), кривични дела против интелектуална сопственост (особено кривичното дело: повреда на правото на патент) и кривични дела против општата сигурност на луѓето и имотот (особено: предизвикување општа опасност, тешки дела против општата сигурност на луѓето и имотот). Меѓу набројаните, пак, особено се истакнуваат имотниот и компјутерскиот криминал.

Вработените кои присуствуваат при извршување кривично дело или раководителите кои се запознаени со околностите околу тоа дело стануваат значајни сведоци во понатамошната судска постапка доколку, благодарение на познавањето на некоја кривична норма, умеат да проценат на која конкретна околност поврзана со извршувањето на делото треба да обрнат внимание. Деталите кои на прв поглед се помалку значајни или му се провлекле на просечен набљудувач, можат да бидат од клучно значење за правна квалификација на кривичното дело. Со самото тоа, споменатите околности се од пресудно значење во процесот на докажување на злосторството и донесување одлука за вината и казната. Познавањето на тие детали на лицата одговорни за безбедноста директно им помагаат за заштита на легитимните интереси на претпријатието/фирмата и за отстранување на настанатите штетни последици.

Исто така, правните поими за одредено кривично дело до некаде се разликуваат од значењето кое им го придаваме во секојдневниот говор. На пример, однесувањето кое просто го нарекуваме крадење, во правна смисла може да претставува дејство на некое сосема друго кривично дело (пр. одземање туѓи работи, неовластено користење туѓо моторно возило, затајување, разбојничка кражба итн). Секојдневниот говор не ги познава ниту нијансираните разлики кои во правото се основ за различно казнување (на пр. кражба, тешка кражба, ситна кражба или затајување и проневера). Трето, пропуштањето на законските обврски врзан за пријавувањето на кривични дела, како и нивното подготвување, повлекува кривична одговорност на надлежното лице.

Доколку сакаме да ги категоризираме ризиците од различните видови деликти, мораме да земеме предвид колкава е тежината на нивната потенцијална последица и веројатноста од нивното остварување. Со спојувањето на овие два фактора ја добиваме големината на конкретниот ризик. Да речеме, јасно е дека заканата од остварување на кривичното

дело разбојништво против имотот на организацијата носи потенцијално многу тешки последици и дека веројатноста неговото настапување во просечно заштитена организација - која е, во замислениот пример, банка - е релативно висока, како резултат добиваме висок ризик од криминално дејствување во овој облик. Исто, ако замислиме каква било фирма/претпријатие кое се занимава со стопански дејности, во согласност со работната логика на современата ера, користи информациски технологии, заканата од остварување дела на компјутерски криминал е многу сериозна, затоа што последиците можат да бидат оневозможување или значително отежнување на постапката за електронска обработка и пренос на податоци во рамките на организацијата, што следствено води кон загрозување на целокупното работење. Веројатноста за настапување на последиците, пак, е на високо ниво поради софистицираноста на компјутерскиот криминал, лесната достапност до средствата за извршување и постоењето лица кои се високо специјализирани за оваа противправна дејност, особено во однос на компјутерските мрежи на успешните компании.

Слична логика може да се примени и на другите облици на криминално дејствување. Факт е дека фирмата/претпријатијата и останатите организации во сферата на стопанството се поподложни на одредени кривични дела во однос на други. Тука пред сè мислиме на кривични дела од областа на имотниот, економскиот и компјутерскиот криминал, но и на оние врзани за општата безбедност на луѓето, имотот и интелектуалната сопственост. Неоспорно е дека претпријатието може да биде објект и на други кривични дела, но би било речиси невозможно да се проценат сите потенцијални ризици од криминално дејствување, особено оние чија веројатност за настапување, во однос на претпријатието е мала. Мислиме дека процесот за проценка на ризици, според тоа, треба да опфати анализа и оценка на ризиците од извршување *кривични дела кои најфреквентно се случуваат во организацијата, а можат да остават тешки последици на нејзиниот имот и работење.*

Исто така, предвид би требало да се земат оние кривични дела кои имаат непосредна врска со активноста на организацијата, а не оние чиј објект станува организацијата под влијание на околностите, затоа што и предвидливоста на вторите е објективно многу мала. На пример, шансата лице вработено во одредено претпријатие/фирма да стане жртва на кривично дело убиство или силување не е во значајна мера ниту поголема ниту помала во однос на лицата кои немаат никаква врска со претпријатието/фирмата. Затоа и не постои индикатор кој би можел да ни укаже на зголемена опасност од настапување на овие кривични дела. Но, од друга страна, јасно е дека малопродажен објект или банка (и вработените во нив) попрво можат да станат објект на кривично дело

кражба или разбојништво, отколку просечен граѓанин. Според тоа, имотниот криминалитет е ризик кој кај споменатите организации објективно е поголем од просечно, односно логично е да се вклучи во процесот на анализа на ризикот, за разлика од убиство и силување, затоа што ризикот од нивното остварување е просечен. Понатаму, потребно е да се води сметка за фактот дека јавните претпријатија, установи, па и државните органи, имаат потреба за управување со ризикот, особено во ситуации кога вршат работни дејности. Колку за пример, и државните органи можат да ангажираат (тоа го прават редовно) приватно обезбедување и да побараат консалтинг услуги од областа на процена на ризици од загрозување на имотот кој им е даден на располагање и лицата кои работат за нив. Според тоа, анализата и оценката на ризикот во нивниот случај мора да ги опфатат и криминалните феномени карактеристични за доменот во кој се наоѓаат, па така во категоризацијата треба да се додадат и кривичните дела против уставното уредување и безбедноста на државата.

Како и кај кривичните дела, кои се најважен облик на загрозување на безбедноста на организацијата, кај дисциплинските деликти и прекршоци мора да се земат предвид тежината и веројатноста на последиците, како и нивната фреквенција. Ниту еден од овие облици на противправно дејствување, сепак, нема значење ниту тежина како криминално дејствување. Не може, да говориме дека ризикот од извршување на прекршок против претпријатието треба да се стави во ист ранг со ризиците од криминални акти или од елементарни непогоди и пожари. Затоа во рамки на категоријата на ризици од противправно дејствување тие заземаат дури споредно место во однос на криминалните ризици и се врзуваат исклучиво со деликти на интерни субјекти.

Врз основа на изнесеното, сметаме дека при процена на ризиците од противправно дејствување екстерните субјекти на организацијата мора да утврдат дали постои опасност таа да стане објект на кривични дела, и тоа:⁶⁰

- *против уставното уредување и безбедноста – тероризам, диверзија, шпионажа;*
- *против општата безбедност на луѓето и имотот – предизвикување општа опасност, уништување и оштетување на јавни уреди;*
- *против имот – кражби, разбојнички кражби, разбојништво;*
- *против безбедноста на компјутерски податоци – оштетување на компјутерски податоци и програми;*

⁶⁰ Стандарди за процена на ризици во заштита на лица, имот и работење во Р.Србија.

- *против интелектуална сопственост – неовластено искористување на авторско дело или предмети од сродно право, повреда на правото на патент итн.*

Ако на ризиците од криминално дејствување на екстерни субјекти им ги додадеме и оние што потекнуваат од внатрешни извори, без разлика на тоа дали по својата природа се кривични дела или други облици на казнено однесување, добиваме комплетна слика за опасноста од оваа категорија на ризици која и се заканува на организацијата. При процена на ризикот од противправно дејствување на внатрешни субјекти организацијата мора да утврди дали постои опасност корисникот, поради незаконското дејствување на вработените или раководителите, да стане објект на следните деликти:

- *кривични дела против уставното уредување и безбедноста – саботажи;*
- *кривични дела против општата безбедност на луѓе и имот – предизвикување опасност поради необезбедување мерки за заштита при работа;*
- *кривични дела против стопанството – перење пари и издавање деловни тајни;*
- *кривични дела против имот – кражба, измами;*
- *кривични дела против службена должност – проневери, издавање службени тајни;*
- *кривични дела против безбедноста на компјутерските податоци – компјутерски саботажи, компјутерски измами;*
- *кривични дела против правата по основ на работа – повреди на правата по основ на работа и социјално осигурување, не преземање мерки за заштита при работа;*
- *прекршоци против безбедноста и здравјето на работа – непреземање превентивни мерки за заштита на животот и здравјето на вработените;*
- *дисциплински деликти во областа на кршење на работните обврски врзани за задачите на обезбедување лица, имот и работење итн.*

Последниот наведен ризик тесно е поврзан со претходната категорија, затоа што се однесува на внатрешното дејствување кое е во спротивност со организациските акти, и тоа во сегментот на заштита и нејзината безбедност. Ризикот од прекршоци во областа на безбедноста и здравјето на работа, пак, е важен поради фактот дека постои државна регулатива која недвосмислено ги пропишува обврските во дадениот домен, односно прекршокот на законските одредби е директен ризик како за вработените, така и за претпријатието/фирми.

Што се однесува на наведените кривични дела, како во категоријата на екстерни, така и интерни ризици, наведена е група кривични дела со заеднички заштитен објект кој, според Кривичниот законик, припаѓаат на одредено кривично дело кое го карактеризираме како посебно ризично за организацијата од гледна точка на приватната безбедност.

Секако, и покрај наведените образложенија, треба да се потенцира дека оваа класификација не треба да ги опфати сите кривични дела од Кривичниот законик и споредното кривично законодавство кои ги задоволуваат критериумите на фреквентноста, релативно високиот степен на предвидливост, тежина и веројатност за остварување последици по претпријатието/фирмата.

Примери на процена на ризикот од противправно дејствување против корпорацијата

ПРИМЕР 1

Закана: Извршување кривични дела чија последица се согледува како повреда или загрозување на лица, имот или работење на организацијата.

Степени на закана

1. максимална – непостоење систем за физичко-техничко обезбедување лица, имот и работење и преземање на редовните и пропишаните мерки за заштита на вработените, инфраструктурата и имотот од извршување на кривични дела, вработени кои не се обучени за навремено препознавање на заканата од настапување на кривични дела и правилно реагирање, кое би можело да ги ублажи или спречи последиците;
2. голема – непостоење на систем за физичко-техничко обезбедување лица, имот и работење со преземање на мерки за заштита кои не се покажале како адекватни или се применуваат селективно и нередовно, вработени кои не се обучени за навремено препознавање на заканата од настапување на кривични дела и правилно реагирање кое би можело да ги ублажи последиците, но во претходните случаи е забележана правилна реакција на вработените како резултат на нивна лична иницијатива;
3. средна – постоење систем на физичко-техничко обезбедување лица, имот и работење и преземање мерки за заштита само во однос на закани од извршување имотни кривични дела и кривични дела против општата сигурност на лица и имот, но не

и од другите видови загрозувања, вработени кои се обучени за навремено препознавање на закана од настанување на кривични дела и правилно реагирање кое би можело да ги ублажи или спречи последиците, но само во однос на одредени кривични дела, додека реакцијата во случај на другите кривични дела во претходните случаи се сведува на лична иницијатива, ниско ниво на информатичка писменост на вработените;

4. мала – постоење систем на физичко-техничко обезбедување лица, имот и работење и преземање на редовните и пропишаните мерки на заштита во однос на заканата од извршување имотни кривични дела, кривични дела против општата безбедност на луѓето и имотот и кривични дела против интелектуалната сопственост (развиени механизми на фактичка и на правна заштита на деловни тајни кои се однесуваат на авторско или сродно право, патент и правото на изум), со постоење на извесен степен на заштита од компјутерски криминалитет, вработени кои се обучени за навремено препознавање на закана од настанување на кривични дела и правилно реагирање, кое би можело да ги ублажи или спречи последиците, високо ниво на информатичка писменост на вработените;
5. минимална – постоење систем на физичко-техничко обезбедување на лица, имот и работење, како и преземање редовни и пропишани мерки за заштита во однос на заканите од извршување имотни кривични дела, кривични дела против општата безбедност на луѓето и имотот и кривични дела против интелектуална сопственост (развиени механизми на фактичка и правна заштита на деловни тајни кои се однесуваат на авторското или сродно право, патент и правото на изум), користење најсовремени компјутерски програми и системи за заштита од компјутерски криминалитет, вработени кои се обучени за навремено препознавање на закана од настапување на кривични дела и правилно реагирање кое би можело да ги ублажи или спречи последиците, високо ниво на информатичка писменост на вработените, ангажирање вработени кои се специјализирани за заштита од високотехнолошки криминалитет.

Последици: Нарушување на телесниот интегритет на лицето, настапување на имотна штета од големи размери, уништување или оштетување на важни инфраструктурни објекти, нарушување на работниот углед и кредитните способности на организацијата, уништување или оштетување на компјутерски податоци и програми од значење за работењето на организацијата, оневозможување или значително

отежнување на постапката за електронска обработка и пренос на податоци во рамките на организацијата, изгубена добивка како последица на губење на патент или неможноста од користење на предметот на авторско или друго сродно право.

Мерки за третирање на ризикот

1. воведување адекватен систем на физичко-техничко обезбедување на лица, имот и работење;
2. пропишување и редовно спроведување соодветни мерки за заштита од извршување кривични дела на штета на организацијата;
3. едукација на вработените за навремено препознавање на закани од настанување на кривични дела и правилно реагирање, што би можело да ги спречи или ублажи последиците;
4. набавка и користење на софтвер за заштита на компјутерските системи, податоци и програми;
5. подигање на нивото на информатичката писменост на вработените.

ПРИМЕР 2

Закана: Извршување кривични дела, прекршоци или стопански престапи кои може да предизвикаат повреда или загрозување на лица, имотот или работењето на организацијата и/или може да доведат до кривична одговорност на самата организација како правно лице.

Степени на закана

1. максимална – непостоење редовни и систематични внатрешни контроли над законитоста на работата на вработените и менаџментот, преземање посебни мерки за заштита на важните инфраструктурни објекти, ниско ниво на доверба помеѓу раководните органи и вработените, недоволна соработка со државните органи во процесот на расветлување на кривични дела за кои се обвинети лица од организацијата;
2. голема – постоење внатрешна контрола која не се покажала како доволно ефикасна, редовна и систематична, преземање на посебни мерки на заштита само во однос на најважните инфраструктурни објекти, ниско ниво на доверба помеѓу раководните органи и вработените;
3. средна – постоење редовни и систематични внатрешни контроли над законитоста на работата на вработените и менаџментот, со повремени пропусти кои оставиле значајни штетни последици, преземање посебни мерки на заштита на важни инфра-

структурни објекти, недоволно високо ниво на доверба помеѓу раководните органи и вработените, соработка со државните органи во процесот на расветлување на кривични дела за кои се обвинети лица од организацијата во поголемиот број, но не и во сите случаи;

4. мала – постоење редовни и систематични внатрешни контроли над законитоста на работењето на вработените и менаџментот, со повремени ситни пропусти, кои не оставиле значајни штетни последици, преземање потребни мерки за заштита на важни инфраструктурни објекти, високо ниво на доверба меѓу раководните органи и вработените, задоволителна соработка со државните органи во процесот на расветлување кривични дела за кои се обвинети лица од организацијата;
5. минимална – постоење редовни и систематични внатрешни контроли над законитоста на работењето на вработените и менаџментот, преземање посебни мерки за заштита на важни инфраструктурни објекти, високо ниво на доверба помеѓу раководните органи и вработените, задоволителна соработка со државните органи во процесот на расветлување кривични дела за кои се обвинети лица од организацијата, постоење свест (меѓу сите лица кои ја сочинуваат организацијата) за значењето на спроведувањето на редовен надзор над законитоста на работата на одговорните лица и другите вработени и последиците од нивното противзаконско дејствување.

Последици. Нарушување на телесниот интегритет на лица, настапување на имотна штета од големи размери, уништување или оштетување на важни инфраструктурни објекти, нарушување на деловниот углед и кредитната способност на организацијата, уништување или оштетување на компјутерски податоци и програми од значење за работењето на организацијата, оневозможување или значително отежнување на постапката за електронска обработка и пренос на податоци во рамките на организацијата, казнување на организацијата и одговорните лица поради кривични дела, прекршоци и стопански престапи.

VI глава

МЕТОДОЛОГИИ ЗА ПРОЦЕНА НА РИЗИЦИ

1. ПРАВНА, ОРГАНИЗАЦИСКА И ИНСТИТУЦИОНАЛНА РАМКА ЗА ПРОЦЕНАТА НА РИЗИЦИ ВО РЕПУБЛИКА МАКЕДОНИЈА

Формално правните основи на системот за проценка на безбедносните ризици во Република Македонија, како и неговата организациска и институционална поставеност, генерално се дадени со Законот за заштита и спасување,⁶¹ Законот за управување со кризи,⁶² Законот за безбедност и здравје при работа⁶³ (кога станува забор за безбедност на лица при работа) и други релевантни закони, а деталите за уредувањето на начинот и постапката за изработка на процените се пропишани со посебни методологии.⁶⁴

Заради избегнување на дилемите кои произлегуваат од сличната законска надлежност која произлегува од Законот за заштита и спасување и Законот за управување со кризи, на почетокот од понатамошната елаборација го напоменуваме фактот дека станува забор за законска обврска и надлежност за изработка и ажурирање на различни процени, *според опсег и според содржина*. Имено, Законот за заштита и спасување дава обврска за изработка на проценка за загрозеност „од природни непогоди и други несреќи“, додека Законот за управување со кризи пропишува обврска за изработка на проценка на загрозеноста на Р. Македонија „од сите ризици и опасности“, со што оваа проценка ја поставува како поширока и според опсег и според содржина од процената која се однесува само на природни непогоди и други несреќи.

⁶¹ Закон за заштита и спасување (пречистен текст), (Сл. весник на Р. Македонија, бр. 93/2012 и 41/2014, член 34).

⁶² Закон за управување со кризи, („Службен весник на Р. Македонија“ бр. 29/2005, 36/2011 и 41/2014).

⁶³ Закон за безбедност и здравје при работа („Сл. весник на РМ“ бр. 92/2007; 136/2011).

⁶⁴ Методологија за содржината и начинот на проценување на опасностите и планирање на заштитата и спасувањето. („Сл. весник на Република Македонија“ бр. 76/06), и со Уредба за методологијата на изработка на процената, нејзината содржина, структура, начин на чување и ажурирање, како и определувањето субјекти во системот за управување со кризи на кои им се доставува целосна или извод од процената („Службен весник на Р. Македонија“ бр. 13/2011).

Всушност, процената која се изработува во рамките на системот за управување со кризи, според законската поставеност, во себе треба да ги опфаќа, односно интегрира сите други процени, кои се однесуваат на посебни ризици, а ги изработуваат за тоа предметно надлежните органи.

1.1. Процена на загрозеност од ризици за природни непогоди и други несреќи

Законот за заштита и спасување заштитата и спасувањето во Република Македонија ја поставува како работа од јавен интерес за граѓаните. Мерките и активностите на заштитата и спасувањето ги организираат и ги спроведуваат органите на државната управа, органите на единиците на локалната самоуправа, јавните претпријатија, јавните установи и служби, трговските друштва, здруженијата на граѓани, граѓаните и силите за заштита и спасување, на начин кој е уреден со овој закон.

Законот за заштита и спасување, во основните одредби, подетално ги елаборира ризиците и опасностите за кои е потребно градење цивилни механизми и капацитети за нивно третирање. Така во член 2, точка 1, и 2, законодавецот дава појаснување за тоа што се подразбира под „природни непогоди и други несреќи“:

– „*Природни непогоди*“ се земјотреси, поплави, лизгање на земјиште, снежни лавини и наноси, голомразица, град, суша кои со природни неконтролирани сили ја загрозуваат животната средина, животот и здравјето на луѓето, материјалните добра, животинскиот и растителниот свет и културното наследство.

– „*Други несреќи*“ се настани кои се резултат на одредени превиди и грешки во извршувањето на секојдневните стопански и други активности, како и невнимание при ракување со опасни материи и средства при производство, складирање и транспорт на истите (пожари, големи несреќи во патниот, железничкиот и воздушниот сообраќај, несреќи во рудници, индустриски несреќи предизвикани од експлозии и други техничко-технолошки причини, паѓање на радиоактивни врнежи, прашини и талози, излевање нафта и нафтени деривати и други отровни хемикалии, експлозии на гасови, запаливи течности и гасови, како и други горливи материи кои со воздухот создаваат експлозивни смеси и други експлозивни материјали од поголем размер).

Во истиот член од Законот, законодавецот го определува терминолошкото значење на поимот „*ризик*“ на следниот начин: како „веројатност за настанување на загуби, повреди или штети од природни непогоди и од други несреќи, на кои би биле изложени граѓаните, природните богатства, растителниот и животинскиот свет, добрата во општа употреба како и предметите и објектите од особено културно и историско значење“.

Заради организирано спроведување на заштитата и спасувањето, врз основа на Законот, се донесува План за заштита и спасување од природни непогоди и други несреќи кој се изработува врз основа на Проценка на загрозеност од природни непогоди и други несреќи.⁶⁵ Процената на загрозеност од природни непогоди и други несреќи за територијата на Републиката ја донесува Владата на Република Македонија, додека процената на загрозеност од природни непогоди и други несреќи за подрачјето на општината ја донесува Советот на општината, односно Советот на Градот Скопје.

Содржинската анализа на „Методологијата за содржината и начинот на проценување на опасностите и планирање на заштитата и спасувањето“ укажува на тоа дека станува збор за документ кој малку посветува внимание на пропишување на методологијата (начин и постапки) за проценување ризици и опасности, односно само се определува листа на природни и други опасности кои се карактеристични за подрачјето на Р. Македонија и повеќе се фокусира на оперативниот сегмент, односно на изработка на Планот за заштита и спасување и разработка на потребните мерки (технички и хуманитарни), како и активностите кои треба да ги преземат надлежните органи.

Според истиот закон, *„процената на загрозеност од природни непогоди и други несреќи за потребите на трговските друштва, јавните претпријатија, установи и служби ја донесува органот на управување во истите“*. Оваа законска одредба упатува на потребата и неопходноста организациите од овој карактер (трговски друштва, јавни претпријатија, јавни установи и др.) *да изработат и да донесат или да прифатат адекватен документ* (методологија, стандардна процедура итн.) кој ќе биде основа за изработка на Проценка на ризици и загрозеност на нивните системски вредности (живот и здравје на луѓето, севкупните ресурси, работните процеси и сл.).

1.2. Проценка на загрозеност од ризици и опасности

Со Законот за управување со кризи се дадени основните одредби за изработка на процената за загрозеност од сите ризици и опасности, во рамките на системот за управување со кризи на Република Македонија. Законот е структуриран во десет тематски целини (глави) и предвидува повеќе подзаконски акти. Во првата глава од Законот даден е основниот термиолошки пристап. Во втората глава, Законот предвидува одредби со кои се овозможува изработка на локални процени, односно процени за

⁶⁵ Проценка на загрозеност на Република Македонија од природни и други несреќи. („Сл. весник на Република Македонија“ бр. 117/10).

загрозеноста на подрачјата на општините и градот Скопје. Третата глава од законот го регулира воспоставувањето и функционирањето на владините тела во системот за управување со кризи (Управувачки комитет и Група за проценка) кои имаат посебно место и улога во поставувањето на формално-правната рамка за изработка, за верификување и за донесување на процената за загрозеност на Република Македонија од сите ризици и опасности. Главата 6 од Законот е целосно посветена на „Процената на загрозеност на безбедноста на Република Македонија“. Во оваа глава (во два члена) дадени се основните наележности, додека целосното уредување на оваа област, законодавецот предвидел да биде извршено од страна на Владата со посебна уредба – Уредба за методологијата за изработка на процената, на загрозеноста на безбедноста на Република Македонија од сите ризици и опасности, нејзината содржина и структура, начинот на чување и ажурирање, како и определувањето на субјектите во системот за управување со кризи на кои им се доставува целосна или извод од процената.

Содржинската анализа на оваа уредба укажува на тоа дека таа претставува сеопфатен правен документ кој предвидува воспоставување холистички пристап во процесот на изработка на процената за загрозеност, каде целосно се применети меѓународните стандарди и критериуми од оваа област. Пристапот во изработката на процената кој е уреден со оваа уредба е во целосна согласност со сите аспекти на меѓународните стандарди и искуства, кои беа предмет на разработка во *Главата 3 – Управување со ризик*.

Првата глава од уредбата е посветена на дефинирање на поимите кои се употребени во Уредбата, а се од фундаментално значење за самиот процес на изработка на процената и разбирањето на управувањето со ризик. Ова значење добива поголема тежина ако се земе предвид фактот дека во Законот за управување со кризи и во Законот за заштита и спасување, како и во методологијата за проценување на опасностите и планирање на заштитата и спасувањето, не се дадени квалитетни и сеопфатни дефиниции во врска со процената и клучните термини кои се поврзани со неа и од тој аспект оваа уредба има голем придонес во заокружувањето на националната правна рамка која го уредува управувањето со ризици во Република Македонија.

Клучните термини кои се од значење за процесот на управување со ризици, како и од значење за уредување на постапката за изработка на процената од сите ризици и опасности, кои се дадени во уредбата се однесуваат на следните поими:

„Ризик“ е комбинација од повеќе меѓусебно зависни фактори кои влијаат на веројатноста, одредена опасност да прерасне во несреќа или катастрофа и да се реализираат нејзините негативни последици.

– „*Опасност*“ е природен феномен, човечка активност, техничко-технолошка хаварија или друг вид појава која може да предизвика: загуба на живот, повреди или други влијанија врз здравјето, имотна штета, загуба на средствата за егзистенција и услуги, општествено и економско нарушување, како и штета врз животната средина.

– „*Ранливост*“ е присуството на посебни карактеристики, специфики и околности на поединецот, заедницата, системите или објектите кои ги прават подложни на негативните влијанија и оштетувачките ефекти на дадената опасност.

– „*Изложеност*“ е присуството на луѓе, материјални добра, природни богатства, системи, објекти или други елементи во зоните на опасност и кои со тоа присуство и сопствената ранливост се подложни на потенцијални загуби, оштетувања и други негативни влијанија.

– „*Процена на ризик*“ е утврдена методологија/постапка со која се одредува природата и обемот на ризикот со анализа на потенцијалните опасности и со оценување на постоечките услови на ранливост кои заедно би можеле потенцијално да им наштетат на изложените луѓе, имот, услуги, средства за егзистенција и животната средина од која што зависат.

– „*Анализа на ризик*“ е дел од процесот на процената на ризикот (и со тоа поврзаното мапирање на ризик) која вклучува преглед на техничките карактеристики на опасностите, како што се нивната локација, интензитет, зачестеност и веројатност; анализа на изложеноста и на ранливоста вклучително и физичките, социјалните, здравствените, економските и еколошките димензии (последици) и оцена за способноста на преовладувачките и алтернативните капацитети за справување во однос на веројатните сценарија на ризикот.

– „*Управување со ризик*“ е систематски процес на употреба на правни механизми, организациски и оперативни способности и капацитети за спроведување стратегии, политики, како и конкретни мерки и активности за превенција и справување со цел да се намалат негативните влијанија на опасноста и можноста таа да прерасне во поголема несреќа или катастрофа.

Ако се направи споредбена анализа на овие дефиниции со толковникот на поими кој го дава Меѓународната стратегија за намалување на ризици на Обединетите нации (УНИСДР)⁶⁶ и со Меѓународниот стандард ИСО 73:2002 – „Речник за управување со ризик“⁶⁷, ќе се воочи дека постои висок степен на усогласеност со дефинициите и

⁶⁶ Повеќе на: http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf.

⁶⁷ Повеќе на: <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en>.

коментарите кои се дадени таму, што упатува на усогласеност и компатибилност на националната со меѓународната формално правна и оперативна рамка на процесот на управување со ризик и процената на ризици, како негова комплементарна мерка.

Втората глава од Уредбата се однесува на содржината и на структурата на процената и го претставува носечкиот дел од уредбата. Всушност во оваа глава се дефинирани сите елементи кои процената треба да ги содржи во себе. Генерално процената е поделена на два дела, *Општ дел и Посебен дел.*

■ *Општиот дел* на процената ги опфаќа елементите кои се однесуваат на: генералниот опис на целите на процената; територијалниот опфат на процената (подрачјата на општините, градот Скопје и Република Македонија); геостратегиските карактеристики; административно-управните единици на територијата и институциите на системот за управување со кризи; нивна меѓусебна интеракција, комуникација, координација и соработка; извори на податоци и информации, нивно вреднување и употреба, како и механизми за нивна размена; географски, демографски и социјално-економски податоци како елементи на ризикот, поврзани со номенклатурата на средства и други добра изложени на ризик. Општиот дел претставува статичен или помалку променлив дел во Процената, кој во себе ги содржи карактеристиките и спецификите на територијата за која се однесува процената.

■ *Посебниот дел* од процената, се однесува на променливите категории, ја содржи динамичната фаза, која е насочена кон следење, идентификација, откривање, детаљна анализа и проценка на присутните опасности на дадената територија, утврдување на засегнатите елементи изложени на опасностите и нивната ранливост (објекти, инфраструктура, наследство, животна средина итн.), со квантитативна и квалитативна анализа и проценка на способноста на системот за управување со кризи, да превенира, рано да предупреди, да информира и да алармира, како и да координира со оперативен одговор и надминување на последици од различни појави на кризи и кризни состојби.

Управувањето ризици кое се спроведува во рамките на системот за управување со кризи во Република Македонија има широка поставеност, *го сочинуваат сите органи на државната власт, приватниот и граѓанскиот сектор, високообразовните институции и други субјекти.* Ваквата системска организација подразбира уредување на односи и врски на функционирање помеѓу сите вклучени страни, без разлика дали нивната улога е како обезбедувачи на информации или како корисници на информациите.

Функционирањето на еден таков систем за управување со ризици, се темели на принципите кои се карактеристични за „управувањето со системи или системскиот менаџмент“ каде се подразбира извршување

на сите функции (планирање, организирање, раководење, координација и контрола) и работење на менаџерите во услови кога организацијата ги исполнува критериумите на систем составен од повеќе слоеви (потсистеми), во услови на комплексно опкружување, во услови на неизвеснот, како и во услови на донесување одлуки во кратки рокови и под притисок од ризици и закани.

Во илустративна смисла, претходно изнесеното значи, дека за потребите на процесот за управување со ризик на еден систем или организација се користат врските со останатите системи од поширокото и потесното опкружување, како и со неговите потсистеми или организациски единици. Во практичната примена, функционирањето на овој системски модел предвидува обезбедување услови за: влез, процес (обработка), излез и повратни информации за функциите на системот. Кога станува збор за процена на безбедносните ризици, овие процеси се однесуваат на следното:

- *влезот*, го претставуваат информациите кои се однесуваат на закните, ризиците и опасностите и очекуваните (предвидените) ситуации и состојби;
- *процесот (обработката)*, се извршува преку внатрешно воспоставениот организациски систем, заради добивање адекватни анализи, евалуација, оцени, заклучоци, препораки и сл.;
- *излезот*, претставува конкретна активност, преземена мерка, реализирана задача (превентивна, реактивна) во насока на намалување на ризикот и подобрување на состојбата и
- *повратните информации*, претставуваат повратна спрега која повторно преку функциите на менаџментот овозможува корекции за следниот циклус на влезни информации и ажурирање на процените.

Вака поставениот принцип на системски менаџмент се остварува како процес во кој најпрво се поставува дијагноза и идентификација на ситуацијата (процена), потоа се дефинираат основните проблеми, се поставуваат приоритетните цели на системот/организацијата, се утврдуваат техники за решавање на проблемот и се презема конкретна активност. Потоа следи анализа на факторите кои влијаеле на појавата на ситуацијата и повратни информации за потребните корекции и промени (Стефаноски С., 2015).

1.3. Процена на штети од елементарни и од други непогоди

Единствената методологија за процена на штети од елементарни и од други непогоди, за прв пат беше развиена во раните 70-ти години на минатиот век и беше модифицирана и подобрена во 1987 година („Службен весник на СФРЈ“ бр. 27/87), а во 2001 година беше донесена

од страна на Владата на Република Македонија.⁶⁸ Во текот на изминатите повеќе од три децении оваа методологија има успешна примена во спроведени процени на штети од случени несреќи и катастрофи, како во Македонија⁶⁹ (Гевгелија 1990 година; Битола, 1994 година), така и во поранешна СФРЈ (Црна Гора, 1979 година; Копаноник, 1980 година; Книн, 1986 година), но и пошироко во светот (Алжир, 1980 година; Мексико, 1985 година; Иран, 1990 година).

Методологијата претставува алатка која го пропишува начинот и постапката за утврдување на висината и обемот на штети, односно ги поврзува причините (ризикот) со последиците (штети). Целта на процената која се спроведува врз основа на оваа методологија е да се утврди видот и големината на предизвиканата штета во вредносни и физички показатели, по територија на случување и по оштетени објекти, инфраструктура, средства и други блага, кои се утврдени со детаљна номенклатура.⁷⁰ Резултатите од процената, надлежните субјекти ги користат за отстранување на штетите, ублажување и отстранување на последиците, како и преземање мерки за рехабилитирање од настаната елементарна непогода.

Оваа Методологија има посебен придонес во овој сегмент бидејќи покрај уредувањето на процесот на проценка на штети, придонесува и во дефинирањето на причините за штетите, односно *ги дефинира ризиците и опасностите*.

Впечатливо кај оваа Методологија е тоа што во дефинирањето на ризиците, односно причините за штети, излегува од опсегот на „елементарни непогоди“ и под категоријата „*други непогоди*“ се третираат оние што не се спомнати како елементарни, а предизвикуваат штети на имотот или го загрозуваат животот и здравјето на луѓето (јавни демонстрации или манифестации, терористички акти, сторени насилни казниви дела ако сторителот е непознат, штета направена од меѓународна воена или друга организација, воен конфликт, вонредна и/или кризна состојба и сл.

При процената на штети, врз основа на оваа методологија, се анализираат три главни аспекти:

1. *Штетите* (директно влијание), што се однесуваат на влијанието врз добрата, градежниот фонд и друга сопственост, проценети

⁶⁸ („Службен весник на Р.Македонија“ бр. 75/01).

⁶⁹ Потенцирани се само поизразени земјотреси кои беа проследени со оценка на големи оштетувања и загуби на материјални добра.

⁷⁰ Номенклатурата на објекти, инфраструктура, средства и други блага е составен дел на Единствената методологија за проценка на штети, и претставува функционална алатка преку која може да се дефинира „изложеноста“ на конкретна опасност.

според договорени единични цени на нивна замена. Процената го вклучува нивото на оштетување (односно, дали доброто може да се рехабилитира/санира или е целосно уништено).

2. *Загубите* (индиректно влијание), што се однесуваат на загуби врз кои несреќата ќе има влијание како што се намалени приходи, зголемени расходи итн., па сè до времето во кое добрата ќе станат повторно функционални. Истите се квантифицираат според вредноста на влијанието во времето на катастрофата.
3. *Економските влијанија* (понекогаш наречени секундарни влијанија) што вклучуваат фискални влијанија, импликации врз зголемувањето на бруто националниот производ итн.

Од аспект на темата на оваа содржина, Методологијата би можела да се употреби за проценка на загуби на поединечни добра, несреќи од помали размери кои се појавуваат на ограничена територија или зафатен субјект/организација, како и масовни катастрофи кои инволвираат голем дел или дури целата територија на земјата. Методологијата ефикасно ги поврзува физичките оштетувања со економските загуби како и директните и индиректните загуби.

Практичната примена на оваа методологија бара конзистентни активности поврзани со спроведување на следните активности:

- организирање и изведување теренска контрола (директен увид) на оштетените добра од страна на тим од специјалисти кои ќе соберат податоци за физичките оштетувања во стандарден облик (пропишан образец), што претставува составен дел од методологијата;
- кабинетска анализа и синтеза на податоци за физичките штети утврдени за време на теренската контрола;
- официјално усвојување на листа на просечни цени за сите работи кои се неопходни за санација/замена и/или санација и зајакнување (враќање на конструкцијата во првобитна состојба) на оштетените добра;
- пресметка на загубите во согласност со официјално усвоената листа на цени.
- собирање и презентирање на резултатите во пропишаниот сумарен облик.

1.4. Безбедност и здравје при работа

Безбедноста и здравјето при работа претставува уставна категорија со статус на основно право на секој вработен кое влегува во групата на „уставно гарантирани основни економски, социјални, културни и хуманитарни права на човекот“ (член 32 став 1 од Уставот на Република Македонија). Речиси во сите земји оваа област е регулирана со закон-

ски и со подзаконски акти. Законската регулатива од оваа област во Р. Македонија се однесува на Законот за безбедност и здравје при работа (Сл. весник на РМ бр.92/2007, 136/2011) и група подзаконски акти кои севкупно ги организираат и ги уредуваат работите поврзани со безбедноста и здравјето при работа.

Поимот „ризик“ во овој закон се дефинира на следниот начин: „Ризик е веројатност за настанување на повреди, заболувања или оштетување на здравјето на вработениот, како резултат на опасност при работа“. Врз основа на овој закон (член 9) работодавачот е должен да ги спроведува активности за безбедност и здравје при работа, придржувајќи се до следните основни принципи:

- избегнување на ризици;
- *проценување на ризиците* кои не можат да се избегнат;
- справување со ризиците на самиот почеток;
- приспособување на работата кон поединецот, особено во однос на карактеристиките на работното место и работната средина;
- изборот на личната заштитна опрема;
- развивање целосна безбедносна стратегија која опфаќа, технологија, организација на работа, работни услови, меѓучовечки односи и фактори кои влијаат врз работната средина;
- давање приоритет на колективните безбедносни мерки наспроти поединечните мерки и
- обезбедување соодветни упатства и инструкции и известувања на вработените.

Врз основа на овие активности се утврдуваат мерките за безбедност и здравје при работа, обврските на работодавачот и правата и обврските на вработените од оваа област, како и превентивните мерки против професионалните ризици, отстранувањето на ризичните фактори за несреќа информирање, консултирање, обука на работниците и нивно учество во планирањето и преземањето мерки за безбедност и здравје при работа. Одредбите од овој закон се применуваат во сите дејности на јавниот и приватниот сектор, за сите лица осигурени од повреда на работното место или професионалните болести според позитивните законски прописи.

Кога станува збор за безбедноста и здравјето при работа не се означува само заштита на вработениот од физички повреди и професионални ризици, туку и заштита на неговата личност што претставува доста комплексно прашање кое во денешно време станува сè поактуелно кога станува забор за сеопфатен пристап кон процената на ризици и организирање на заштита на лица, имот и работење. Притоа работодавачот има обврска да обезбеди безбедност и здравје при работа за неговите вработени од секој аспект поврзан со работата, вклучувајќи за-

штита од професионални ризици, обезбедување информации и обука и обезбедување соодветна организација за заштита и потребни средства.

Во согласност со член 11 од Законот, секој работодавач мора да изготви и да спроведе Изјава за безбедност за секое работно место, прецизирајќи го начинот, како и мерките кои треба да се преземат. *„Изјавата за безбедност се заснова врз идентификација на опасноста и проценка на ризиците по безбедноста и здравјето на работното место и во работната средина на која се однесува изјавата за безбедност“*. Оваа законска обврска претставува императив и услов секој правен субјект да организира и спроведе процес на проценка на ризиците во областа на своите надлежности и дејствување.

Без разлика на дејноста на работење, работодавачот согласно член 17 од Законот, мора да обезбеди мерки за безбедност и здравје при работа особено со:

- назначување едно или повеќе стручни лица за безбедност (интерно или надворешно),
- донесување безбедносни мерки против пожар во согласност со посебни прописи,
- донесување мерки за прва помош и евакуација во случај на опасност,
- обука на вработените за безбедно извршување на работата врз основа на сопствена програма,
- обезбедување опрема за лична заштита за вработените и нејзината употреба, доколку преземените безбедносни мерки во работната средина не се доволни,
- вршење повремени прегледи и испитување на работната средина и опрема.

Законот предвидува и обврска на работодавачот, во зависност од природата на процесот на работа да организира и да презема заштитни мерки, евакуација, спасување и прва помош во случај на извесна ситуација која може да ја загрози нивната безбедност и здравје (*елементарна непогода, пожари, експлозии, испуштање на опасни материји над дозволената граница и слично*) и да ги оспособи лицата кои ќе ги спроведуваат тие мерки. Работодавачот мора да ги информира вработените и нивните претставници за секој вид ризик на работното место, како и за безбедносните мерки потребни за контрола на ризиците и елиминирање на штетните последици.

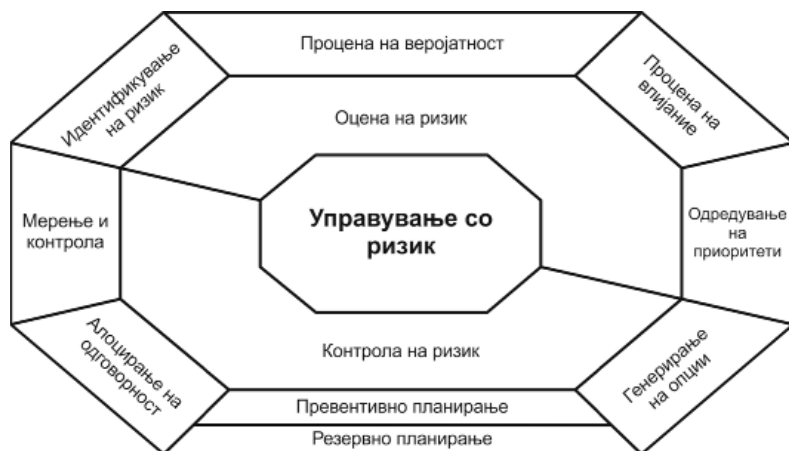
Заради квалитетно и ефикасно планирање и организирање на овие мерки, неопходно е да се спроведе сеопфатна проценка на ризиците поврзани со безбедноста на лицата и материјалните добра во процесот на работењето. Според одредбите од Законот, оваа проценка може да биде спроведена од овластено (сертифицирано) правно или физичко лице.

Меѓутоа од посебна важност е потребата од правно регулирање на основата за изработка на процената, што подразбира прифаќање и донесување соодветен документ (методологија, насоки, процедури и сл.) кои ќе бидат усогласени со меѓународните стандарди од областа на Управување со ризик, општествена безбедност и особено со стандардите за проценка на ризик.

2. МЕТОДОЛОГИЈА (ПОСТАПКИ) ЗА ПРОЦЕНА НА РИЗИЦИ ВО СПРОВЕДУВАЊЕТО НА ЗАШТИТАТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ

Методите, техниките и постапките на практичната примена на процесот на проценка на ризикот вообичаено се пропишуваат со конкретна методологија за проценка на ризици. Преку процесот на процената на ризикот треба да се предвиди и да се оцени очекуваното ниво на загрозување на безбедноста и да се препорачаат соодветни превентивни и оперативни мерки за заштита на системот или организацијата во целина, на нивните составни елементи, како и заштита на вкупните ресурси со кои се располага.

Фазата на проценка на ризик воедно е и најсложениот сегмент од целиот циклус на управувањето со ризикот, која бара да биде интегрирана во сите организациони процеси и активности, со соодветна посветеност на сите нивоа на менаџментот и на сите нивоа на одвивање на функционалните (деловните) процеси (Слика 13).



Слика 13. Местото и улогата на процената на ризикот во процесот на управување со ризици во организацијата
(Извор: Благоје Пауновиќ, Економија на претпријатијата-претпријатие, опкружување и вложувања, Белград, 2006)

Во Република Македонија нема формално воспоставена „Методологија за проценка на ризици во спроведувањето на заштитата на лица, имот и работење“ или друг документ со кој се внесува стандардизација во оваа област.⁷¹ Од достапните материјали кои можат да се добијат (увидат) на веб-страницата на Институтот за стандардизација на Р. Македонија, како усвоени стандарди од областа на „Општествена безбедност“ постојат следните три документи:

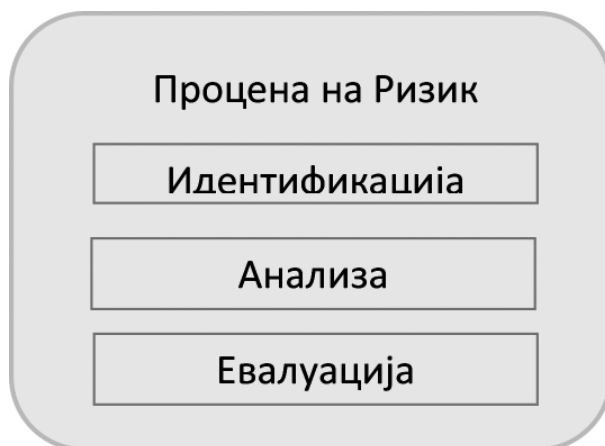
- МКС ISO 22301:2013 (Општествена безбедност) – деловна непрекинливост на системите за менаџмент со квалитет – Барања;
- МКТИ ISO/TR 22312:2012 (Општествена безбедност) – технолошки способности;
- МКТС ISO/PAS 22399:2012 (Општествена безбедност) – упатства за подготвеност за инциденти и оперативен континуиран менаџмент.

Заради обезбедување поблиски информации во врска со општите постапки при спроведувањето на проценка на ризик, во продолжение ќе се претстави кратка анализа на овој процес според меѓународниот стандард *ISO 31000:2009*.

Според општата и детаљната рамка на овој стандард, (прелиминарно објаснето во Глава 3 од овој труд), процесот на проценка на ризик претставува сеопфатен процес кој опфаќа *идентификација на ризикот, анализа на ризикот и евалуација или оцена на ризикот*. Во процесот на проценка на ризикот се врши споредба на проценетиот степен на ризик (ниво на загрозеност) со однапред утврдени критериуми и се одредува рамнотежата меѓу потенцијалните придобивки и негативните резултати. Тоа овозможува донесување одлуки за обемот и природата на потребната обработка и третман, т.е. одговор на ризикот според неговиот приоритет, така што, на оние активности од организацијата кои се со поголема изложеност на ризик им се дава и поголем приоритет.

Процесот на проценка на ризикот треба да претставува итеративен процес, т.е. треба да се повторува повеќе пати, бидејќи состојбата со ризиците претставува „жива материја“, што значи дека се случуваат чести промени или во текот на работата може да се откријат нови ризици, а постојните може да се променат. Со тоа се менуваат и приоритетите и класификацијата на ризиците. Овој процес на проценка на ризикот е претставен на Слика број 14.

⁷¹ Според Законот за стандардизација: „Стандардизацијата претставува активност чија цел е воспоставување правила за општа или повторлива употреба заради постигнување оптимален степен на уреденост во одредено подрачје“.



Слика 14. Процес на проценка на ризикот

2.1. Идентификување на потенцијалните опасности

Идентификувањето на потенцијалните опасности подразбира редослед на активности, случувања и вклучување субјекти кои се релевантни за целите на организацијата. Преку организиран и координиран процес, системот треба да воспостави стандардизирани процеси за идентификација на изворите на опасности, случувањата и околностите во коишто се појавуваат, како и потенцијалните штети и последици, кои се очекуваат како крајни консеквенци на ризикот.

Идентификацијата на потенцијалните ризици или прелиминарната анализа е препорачливо да се спроведува според „групи на опасности“ кои треба да бидат категоризирани според исти или слични индикатори, како на пример:⁷²

- потенцијални опасности кои се предвидуваат во рамките на редовните работни/деловни процеси на организацијата;
- потенцијални опасности по безбедноста на животот и здавјето на луѓето на работното место и во работната околина;
- потенцијални опасности поврзани со правна регулатива, организациски и/или институционални слабости;⁷³

⁷² Категоризацијата е препорачливо да биде пропишана со формално правен и стандардизиран документ (пример: SRPS A.L2. 003:2010 - Društvena bezbednost - "Procena rizika u zaštiti lica, imovine i poslovanja", на Р. Србија.

⁷³ Опасностите од овие категории, влегуваат во групата на т.н. „Системски ризици“.

- потенцијални опасности од незаконско противправно дејствување на внатрешни и на надворешни фактори;
- потенцијални опасности од пожар, поплава и други опасности поврзани со техничко-технолошките процеси во организацијата или потесното опкружување;
- потенцијални опасности од елементарни непогоди и други несреќи, на кои е подложен микропросторот каде организацијата е лоцирана и работи;
- потенцијални опасности од отсуство на стандарди или нивна неусогласеност и
- други потенцијални опасности кои се поврзани со актуелни случувања поврзани со политички, економски, социјални и други состојби во државата (немири, протести, штрајкови и сл.).

Процесот на идентификација на ризикот започнува уште во фазата на планирањето на активностите и трае сè до нивното завршување. Опфаќа препознавање, предвидување и документирање на ризиците кои би можеле да се појават и да влијаат врз остварувањето на дефинираните цели. Во пракса се користат повеќе методи и техники за идентификација на ризикот, од кои најпознати се:

- Анализа на предностите, слабостите, можностите и заканите, (SWOT анализа: англ. Streengths, Weaknesses, Opportunities, Threats);
- Анализа на неуспехот на режимот и ефектите, (FMEA анализа, англ: Failure Mode and Effects Analysis);
- Анализа на стеблото на грешки, (FTA анализа,англ: Fault Tree Analysis).

Најкористена техника за идентификација на ризикот е SWOT анализата. Таа претставува алатка за стратешко планирање на управувањето со ризик, со која на едноставен начин и релативно брзо можат да се утврдат сите фактори (позитивни, негативни, надворешни и внатрешни), кои влијаат врз остварувањето на целите.

„Предностите и слабостите“ претставуваат внатрешни фактори кои може да се контролираат и може да бидат: технички, финансиски, капацитет во човечки и материјално-технички ресурси, способности и др. Предностите претставуваат позитивни фактори, односно најдобри делови кои треба да се нагласат и да се искористат, додека слабостите се негативни фактори и претставуваат недостатоци, односно осетливи делови подложни на потенцијалните ризици, кои треба да се елиминираат.

„Можностите и заканите“ се надворешни фактори кои обично се надвор од контрола на системот/организацијата и не можат или делумно можат да се контролираат. Поврзани се со социолошки, со политички, со демографски, со економски, со трговски и со други прилики. Можно-

стите се позитивни и посакувани фактори кои треба да се искористат, а заканите се негативни, односно непожелни фактори и претставуваат опасности кои треба да се проценат/предвидат, избегнат, третираат, елиминираат или надминат.

2.2. Процес на анализа на ризикот

За некои категории на ризици, доколку постои добра збирка (база) на податоци, преку спроведување квалитетен процес на анализа, тој може целосно да се дискредитира, а со тоа и попрецизно „да се измери“. Како пример за такви ризици во еден деловен субјект, може да се издвојат: прекини и застои во производството, број на провални кражби на готови производи и сировини, настанати пожари на објекти и постројки, прекини во снабдување со енергенси, ограничувања на пристап до пазари итн.

Од друга страна постојат и други ризици, за кои е потешко да се анализираат и целосно да се осознаат, како на пример: степен на квалитет на работа, самоиницијативност и елан кај вработените, влијанието на конкуретниот пазар, влијанието на јавното мислење и задоволството од квалитет, и слично, бидејќи за ова е потребно спроведување на по-комплицирани техники и инструменти за прибирање и анализа на податоците поврзани со наведените и слични ризици. Меѓутоа, со квалитетно спроведена анализа на ризикот, со помош на квалитативни методи и статистички податоци, се решаваат потешкотиите во одредувањето на ризиците кои во праксата не можат да се квантифицираат со бројни вредности.

Тоа значи дека квалитативната анализа на ризикот не се базира врз апсолутни вредности, туку квалитативно ги пресметува параметрите на ризикот. Меѓутоа, иако процената на ризикот се врши квалитативно, вредностите се квантифицираат, т.е. вредноста на ризикот често се претставува како нумеричка вредност. Бидејќи квалитативната метода претставува квантификација на субјективно проценети параметри, таа се базира на субјективна проценка и така добиените вредности не се апсолутни, туку се релативни. Со оглед на тоа дека квалитативните параметри се оценуваат субјективно, пожелно е да се врши анализа и проценка од страна на повеќе експерти, а потоа да се разгледаат резултатите од сите анализи. Во оваа анализа многу важна улога има искуството, стручноста и способноста на лицата кои ја вршат анализата и процената на ризикот, како и квалитетот на статистичките податоци.

Според ISO 31000:2009, со анализата на ризикот се утврдуваат комбинациите од веројатностите за појава на идентификуваниот ризик. Земајќи ја во предвид веројатноста, се одредува приоритетот и нивото

на влијанието на анализираниот ризик, како и очекуваното ниво на потенцијалните последици и ефекти, доколку тој се оствари, односно се реализира. Во зависност од утврдените показатели (индикатори), ризикот се обележува во категорија со високо, средно или ниско влијание врз остварувањето на целите на организацијата. Резултатите од квалитативно спроведена анализа се прикажуваат во форма на матрица на ризик и други форми за илустрација и визуелизација. Со процесот на анализа на ризикот, може да се одредат и некои дополнителни фактори, како што се дозволеното ниво на толеранција на ризикот и дозволените ограничувања во вид на трошок, време и квалитет.

2.3. Процес на евалуација на ризикот

Процесот на евалуација или оцена на ризикот има за цел да ги процени веројатностите за постигање на одредените цели, да ги препознае ризиците на кои е потребно да им се посвети најголемо внимание со квантифицирање на нивниот удел во вкупниот ризик, да ја одреди најдобрата одлука кога некои услови се неизвесни и да ги одреди веројатностите на можните исходи.

Евалуацијата на ризикот се базира на нумерички вредности, при што се добива нумерички зададена оцена, т.е. квантитативната оцена на ризикот. Вредностите на ресурсите се прикажуваат во парични единици, додека ранливоста од заканата и последицата од ризикот, т.е. факторот на изложеност на ризикот, се изразуваат во процентуални загуби/штети од вредноста на ресурсите.

Ризикот може да се пресмета како функција од веројатноста за појава на одреден настан и последиците предизвикани од појавата на тој настан:

$$\text{Ризикот} = \text{веројатност за појава на некој настан} = \text{последицата од појава тој настан}$$

Во процесот на евалуација на ризикот, се користи квантитативна анализа со примена на нумеричка процена на веројатноста дека целите ќе се реализираат во рамките на планираните трошоци и временски рок, со што се добива и подобар и пообјективен увид на ризиците.

За ваква анализа, потребно е да се познаваат некои статистички методи, како, на пример техниката „Monte Carlo”, бидејќи за неа постојат специјализирани софтверски решенија. Но, и покрај напредните софтверски решенија кои се користат, и тука е неопходна и драгоцената потребата од човечкото знаење, експертиза и искуство.

Методот „Monte Carlo” претставува повторлив процес и се темели на случајни предизвикувања на настани со помош на симулации, а ре-

зултатот претставува распределба на веројатности. Тоа значи дека овој метод повеќе пати ги повторува проценетото време и трошок, избирајќи случајни вредности при секое повторување, а со симулација се добиваат веројатностите на можните временски рокови и можниот трошок (како пример на процена ефект од деловен процес).

2.4. Процес на третман на ризикот

Откако ќе се идентификуваат и ќе се утврдат ризиците и откако ќе се направи нивна анализа и евалуација, прашањето што се наметнува, во превентивна или во оперативна смисла е, што понатаму со нив. Следната активност во процесот е третман на ризикот, кога се спроведуваат планираните мерки за одговор на истиот. Според ISO 31000:2009, третманот на ризикот е процес на проектирање и имплементација на специфични ефективни стратегии, и разработка на планови за максимизирање на позитивните ефекти, односно потенцијалните придобивки и минимизирање на негативните ефекти (заканите и опасностите).

Одговорот на ризикот треба да биде навремен, ефикасен, ефективен, соодветен со важноста на ризикот и да претставува резултат на усогласени активности на сите заинтересирани страни. Стратегијата на планирањето на одговорот на ризикот зависи од тоа дали се планира одговор на негативен ризик, или одговор на позитивен ризик.

1) Одговорите на негативните ризици (заканите и опасностите) може да бидат реализирани преку преземање на следните активности:

- ризикот да се избегне;
- ризикот да се префрли (трансферира);
- ризикот да се ублажи.

Доколку ризикот треба да се избегне, потребно е да се промени и самиот план на активната, проектот, програмата и сл., за да може се отстранат ризиците и да се заштитат целите од негативните ефекти. Тоа може да се постигне, на пример, со додавање време или ресурси. Иако ризикот не може секогаш целосно да се избегне, тој може делумно да се префрли во друга област.

Префрлањето или трансфер на ризикот претставува стратегија на ослободување од ризикот и неговиот негативен ефект (штети), при што ризикот се префрла во друг систем или друга претходно договорена страна (најчесто осигурување од ризик). Со тоа се добива ефект на намалување на крајните консеквенци од вкупниот ризик.

Ублажувањето на ризикот се врши со цел да се намали веројатноста за појава на ризикот и да се намали неговото влијание на прифатливо ниво. За ублажување на ризикот потребна е контрола на ризикот, односно контрола и мониторинг на веројатноста за појава на одреден настан и одредување на последиците ако тој се оствари.

2) Одговорите на позитивните ризици (можностите и околностите) може да бидат:

- ризикот да се искористи;
- ризикот да се подели;
- ризикот да се зголеми.

Искористувањето на ризикот претставува искористување на позитивниот ризик, односно искористување на можностите и приликите.

Да се подели ризикот значи во искористувањето на можностите и приликите да се вклучи уште некој партнер, кој со своето знаење, стручност и експертиза ќе го поддржи остварувањето на приликите и достигнувањето на можностите.

Стратегијата на зголемување на позитивниот ризик се заснова на зголемување на веројатноста на позитивниот ефект од ризикот.

3. ПРОЦЕНА НА ПОСТОЈНИОТ И ПОТРЕБНИОТ КАПАЦИТЕТ НА ОДГОВОРНИОТ СУБЈЕКТ ЗА УПРАВУВАЊЕ СО РИЗИК

3.1. Процена на постојниот и потребниот капацитет – општа рамка

Тргувајќи од фактот дека ризикот како комплексна појава, се идентификува, се анализира и се проценува преку разгледување на показателите за неговите посебни елементи, како што се: опасност, изложеност, ранливост и капацитет за одговор, неминовно се наметнува потребата за развивање и примена на посебни методологии, постапки и процедури кои ќе бидат целно ориентирани кон нив. Потребниот капацитет кој треба да го има или да го достигне одговорниот субјект, претставува важна алка од целосниот ланец на управување со ризикот. Заради тоа во продолжение ќе се даде посебен осврт на важноста од постоење посебна постапка или методологија за проценка на постојниот и потребниот капацитет на одговорниот, односно надлежниот субјект за управување со ризици.

За да се процени постојниот и/или потребниот капацитет на одговорниот или надлежниот субјект, потребно е да постојат прецизни одредници каде што се поставени критериумите во исполнувањето на нивните должности, поврзани со целиот циклус на управување со ризик. За исполнување на овие критериуми неопходно е да се дефинираат субјектите кои ќе ги контролираат политиките за намалување на ризиците како и субјектите кои ќе воспостават потребни стандарди и индикатори, како генерална рамка преку која ќе се мери ефективноста и ефикасноста на превземените мерки и активности.

Под терминот „одговорни или надлежни субјекти“ во контекст на оваа содржина се подразбираат владините и приватните субјекти, како и други деловни организации кои спроведуваат безбедносни и заштитни активности од областа на обезбедување и заштита на имот и лица, планирање на безбедносни мерки во работењето, спроведување на активности за превенција и намалување на материјалните штети и повреди, како и подготвеност за спроведување на планираните мерки за основна физичка заштита и комплексно управување со ризици и опасности.

Заради исполнување на своите задачи и надлежности, одговорните или надлежни субјекти е неопходно да располагаат со задоволително ниво на капацитет и способност да ги спроведат сите мерки за ефикасно управување со ризици од несреќи и вонредни ситуации. Во врска со тоа, потребно е да се воспостават стандардни процедури со кои ќе се пропише начинот и постапката за спроведување на процената на постојниот и потребниот капацитет на одговорните или надлежните субјекти за управување со ризик, во чиишто рамки:

- ќе се определат надлежностите, нивните улоги и области на одговорност/надлежност;
- ќе се идентификуваат потенцијалните опасности (и закани) во рамките на определените области на одговорност;
- ќе се проценат опасностите и заканите;
- ќе се анализира изложеноста и ранливоста во контекст на потенцијалната опасност;
- ќе се оцени постојниот (расположлив) капацитет;
- ќе се дефинираат мерки и активност кои треба да се преземат во случај на недоволен капацитет.

Преку процесот на проценка на капацитетот на надлежните субјекти, нивните улоги и области на одговорност, треба да се обезбедат податоци поврзани со следните прашања:

- што е покриено/обезбедено во областа на одговорност на субјектот;
- дали надлежниот субјект има една или повеќе улоги поврзани со ризикот и ранливоста во рамките на својата областа на одговорност;
- дали тие улоги се совпаѓаат или се различни и организациски одвоени една од друга во случај на одговорност во повеќе улоги;
- дали, во рамките на областа на одговорност на субјектот, постојат надлежности кои претставуваат критични општествени и јавни функции од аспект на подготвеност во случај на итна ситуација.

Со спроведувањето на процената, определените субјекти треба да оценат дали и во која мерка се подложни на опасности, закани или ранливост, коишто сериозно можат да ги намалат нивните функционални капацитети. Во рамките на тој процес определениот субјект, треба да

ги земе предвид и ризиците кои се помалку веројатни, но кои може да предизвикаат големи последици врз неговите функции за време на итна ситуација. Тоа може да бидат ризици од внатрешен карактер, како што се големи отсуства на персонал (заради големи загуби на човечки животи, ограничена пристапност или недостапност во периодот по ризичниот настан), функционални штети и/или рушење на критична инфраструктура, но, исто така, може да бидат и надворешни ризици, како што се прекин во техничките системи за испорака на витални услуги, транспортните патишта, комуникациите, нефункционалност на друга критична инфраструктура итн.

Многу важна работа е одговорниот субјект однапред да определи или да одреди кои од нејзините функции мора постојано да бидат одржувани, односно непречено да функционираат заради успешно извршување на поставените цели и задачи и кои ресурси имаат примарен карактер од аспект на функционалноста на субјектот. На пример, одредена институција која управува или контролира ресурс од јавниот сектор кој се смета за критичен за општеството од аспект на подготвеност за итна состојба треба да го вклучи овој ресурс во нејзините анализи на ризик и оцена на ранливост. Тоа би можело да биде институција која управува со специјален персонал или материјални ресурси како што се оние што одговараат на несреќите или вршат санација на последици и штети. Тоа, исто така, би можело да биде институција која има административна улога поврзана со некој облик на витална техничка инфраструктура, како што е снабдување со електрична енергија, гас, вода, комуникациско-контролни системи и слично.

3.2. Процена на постојниот и потребниот капацитет – посебни чекори

Преку процесот на идентификување на потенцијалните опасности во рамките на областа на одговорност на одреден надлежен субјект/институција, треба да се настојува да се постигнат следните работи:

- да се зголемат знаењата и свеста на субјектот/организацијата со цел да се зајакне неговата и општествената подготвеност за функционирање во услови на ризик од итна ситуација,
- да се пронајдат причините и условите кои дозволуваат ескалација на настан од низок интензитет во ситуација која сериозно ќе го загрози функционалниот капацитет во областите на надлежност и одговорност на конкретниот субјект и
- да се откријат критичните зависимости во рамките на посебните единици на субјектот, помеѓу секторската поврзаност и влијание, како и функционалната зависност од аспект на просторна разместеност на различни географските подрачја.

3.2.1. Процена на потенцијалните опасности

Откако ќе бидат целосно идентификувани присутните и потенцијалните опасности, во рамките на одговорностите на надлежниот субјект, односно институција, следниот чекор претставува нивна процена, односно процена на веројатноста за нивна појава и последиците кои тие ќе ги предизвикаат. Процената на опасностите вклучува и определување на став за тоа како тие се поврзани едни со други.

Како посебно карактеристични ситуации кои треба да бидат анализирани се состојбите кои вклучуваат сериозни прекини во критичните општествени функции кои бараат координација на одговор од повеќе различни субјекти или органи. Појавата на исклучителни настани е ретка. Поради тоа, доволно е да се направи генерална процена за тоа колку е веројатен настан од такви размери и фокусот да се насочи на анализа на последиците и процена дали капацитетите на одговорниот субјект/организација се доволни за справување со последиците.

На следната слика е прикажан дијаграм на резултат од процена за веројатност/последича од рутински и исклучително ризичен настан:



Слика 15: Дијаграм на веројатност/последича

Веројатноста за појава на исклучителен настан може да се процени врз краткорочна, среднорочна и долгорочна основа. Искуството од праксата укажува дека краткорочниот период во овој контекст се однесува на период до две години, среднорочниот на период од две до четири години, а долгорочниот се однесува на период од пет до петнаесет години. Кај некои опасности, степенот на точност на процената има тенденција за намалување со зголемување на должината на временскиот период.

Сепак периодот од една до две години, во зависност од природата на опасноста, понекогаш е премногу краток за да се извршат потребните следења и мерења и заради тоа веројатноста претежно се оценува врз среднорочна основа.

На следната табела даден е пример на многу едноставна скала за приказ на резултатите, заснована врз квалитативен опис и процена на веројатност:

Ниво	Опис на веројатност врз среднорочна основа
1	Многу мала веројатност
2	Мала веројатност
3	Средна веројатност
4	Голема веројатност
5	Многу голема веројатност

Табела број 4: Скала за приказ на резултатите заснована врз квалитативен опис и процена на веројатност

3.2.2. Процена на можни последици

Преку процесот на процена на можни последици треба да се настојува да се предвидат сите директни и индиректни (негативни) влијанија кои можат да произлезат под дејство на идентификуваните опасности во одредени околности и услови. Во некои случаи, постои можност процената на последиците да се поврзе со веќе воспоставени класификациони системи. Ова овозможува пообјективни анализи на ранливоста во контекст на дадената опасност. На пример, Меѓународната скала за нуклеарни инциденти, која се користи при известување за инциденти и предвидување последици во нуклеарни електрани претставува пример за таков класификационен систем. Друг пример се инструкциите за енергетски постројки и безбедност на брани. Овие инструкции ги земаат предвид ризиците поврзани со загуба или сериозни повреди на човечки животи, како и загуба на општествени, просторни и економски вредности во случај на рушење на брана.

Во зависност од областа на надлежности на одговорниот субјект, последиците ќе бидат проценети во контекст на различни типови на вредности, како, на пример, вредности поврзани со човековиот живот и здравје, економски вредности, техничко-технолошки вредности, еколошки вредности, вредностите на животинскиот и растителниот свет итн. Оттука, врз основа на својата област на одговорност, секоја институција треба да ги дефинира типовите на вредности за кои еден

исклучителен настан може да претставува опасност. Она што е важно е дека постои јасна поврзаност меѓу последиците и она што „вреди“ да биде заштитено во рамките на областа на одговорности на субјектот, односно институцијата.

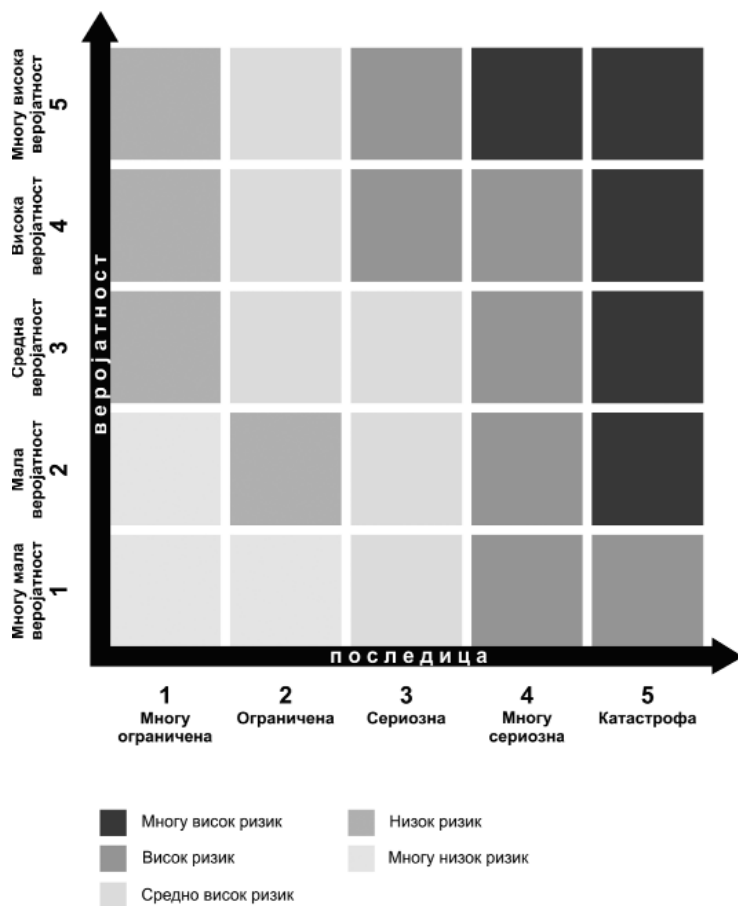
При процената на ризиците во праксата постои тенденција за нивно рангирање, врз основа на процената за можните, односно со очекуваните последици. Оваа проценка и категоризација може да биде извршена на различни начини и со различни методи. На следната табела е даден начелен пример за проценка на последици заснована врз „скала на веројатност“ која се движи од еден или многу ограничени последици до пет или катастрофални последици:

Ниво	Последици	Опис
1	Многу ограничени	Помали директни влијанија врз здравјето, многу ограничени прекини на општествените функции, минлива недоверба во функцијата на одговорниот субјект/ институција.
2	Ограничени	Умерени директни влијанија врз здравјето, ограничени прекини на општествени функции, минлива недоверба во функцијата на одговорниот субјект/ институција.
3	Сериозни	Значителни директни или умерени индиректни влијанија врз здравјето, сериозни прекини во општествените функции, перманентна недоверба во функцијата на одговорниот субјект/ институција.
4	Многу сериозни	Големи директни или значителни индиректни влијанија врз здравјето, многу сериозни прекини во општествените функции, постојана недоверба во функцијата на одговорниот субјект/ институција.
5	Катастрофални	Катастрофални директни или големи индиректни влијанија врз здравјето, екстремни прекини во општествените функции, длабоко вкоренета недоверба во општествените институции во функцијата на одговорниот субјект/ институција.

Табела број 5. Скала на класификација на последици.

Извор: СЕМА (Шведска агенција за управување со вонредни ситуации)
 Препораки 2008:93 „Водич во анализата на ризик и ранливост на надлежни агенции“

Резултатите од спроведената проценка на ризиците можат да бидат презентирани во различни форми на приказ, како на пример во облик на „матрица на ризик“, каде што во веројатноста и последиците се рангираат од 1 до 5, при што на лесно сфатлив и разбирлив начин, ризикот од конкретна опасност се рангира од многу низок до многу висок.



Сл. 16. Приказ на резултати од оцена на ризик во матричен облик

За да се добие јасен увид за подготвеноста на одговорниот субјект за управување со итна ситуација, неговите капацитети треба да се анализираат во однос на сите идентификувани опасности. Капацитетот кој е потребен за справување со сериозни итни ситуации или капацитетот на подготвеност за управување со ризик во случај на вонредна ситуација, генерално се состои од следните три компоненти:

- капацитет за справување со вонредни околности,
- оперативен капацитет и
- капацитет за справување со сериозни прекини на критични општествени и други јавни функции.

Процената на капацитет за подготвеност во случај на итна ситуација се засновува врз систематско користење на индикатори кои обезбедуваат подобро знаење за тоа кои фактори треба да бидат земени

предвид. Ова, исто така, го олеснува меѓусебното и со текот на времето споредување на процените на капацитетите на различни субјекти или институции. Кои индикатори ќе бидат релевантни зависи од надлежностите на субјектот, но и од очекуваното сценарио за развој на ризикот.

3.2.3. Капацитет за справување вонредни околности

За време на сериозни ризични настани, еден надлежен субјект треба да има добар капацитет во рамките на својата област на одговорност, за да може да ги извршува своите функции, да донесува одлуки во сферата на операциите или одговорностите, брзо да дистрибуира точни и веродостојни информации, и кога е тоа неопходно, да врши координација со другите субјекти и нивните мерки. Способноста за справување со вонредни околности е поврзана со капацитетот да се предводат, да се координираат и да се соопштуваат мерките кои се преземаат за справување со сериозни вонредни ситуации.

Генералните индикатори преку кои може да се оцени капацитетот на еден субјект или систем за справување со вонредни околности, може да бидат групирани во следните неколку категории на мерки и активности: раководење, координирање и информирање, алармирање, отворени извори на информации, правила и регулативи, практично искуство и сл. Иако овие индикатори се општи, тие се оценети како применливи за повеќето институции. За некои од нив, би можело да биде неопходно понатамошно расчленување или дополнување на индикаторите според критериуми кои ќе бидат повеќе адаптирани кон потребите на субјектот/институцијата. Овие генерални индикатори (во форма на “checklist” се претставени на следниот табеларен преглед:

ГЕНЕРАЛНИ ИНДИКАТОРИ ЗА ПРОЦЕНА НА КАПАЦИТЕТ
Раководење, координирање и информирање
Постои план за справување со вонредни околности им е познат на членовите на организацијата.
Постои организација за справување со вонредни околности која е обучена и редовно спроведува обуки и вежби.
Субјектот ги има неопходните ресурси, има на располагање технички системи, комуникации и ситуационен мониторинг и може да функционира дваесет и четири часа најмалку во текот на една недела.
Постои мрежа за координација и редовно се извршуваат проверки и вежби за координација.
Постојат рутина и техничка поддршка за информирање на јавноста и медиумите, како и за внатрешно информирање.

Алармирање
Постојат практикувани рутини за алармирање
Целосно обучен персонал за справување со вонредни околности, кој е секогаш на повик и подготвен да ја врши својата должност.
Отворени извори на информации
Постојат отворени извори на информации кои може да обезбедат рано предупредување за сериозни вонредни ситуации,
Постојат рутини и техничка поддршка за брзо ширење на информациите во рамките на субјектот, но и на други субјекти.
Правила и регулативи
Постојат правни основи за тоа како и со што треба да се справи со вонредната ситуација.
Постојат инструкции и политики за тоа како субјектот/институцијата ќе се справи со ситуацијата.
Постојат процедури кои се применуваат во текот на ситуацијата.
Распределбата на овластувањата на институциите е дефинирана.
Практично искуство
Доживеан реален инцидент има акумулирано искуство.
Спроведени подготовки има сличности со увежбувана ситуација.

Табела број 6. Генарелни индикатори

Оперативен капацитет

Надлежниот субјект треба да има добар капацитет во сферата на своите одговорности со што се овозможува побрзо иницирање на мерки за придонес кон справувањето со последиците од појавените ризици, како и спроведување на неопходни мерки за помош, за заштита и за намалување на ефектите од вонредната ситуација. Агенциите и секторите кои треба да ја спречат или да се справат со некоја итна ситуација како и оние што треба да ги спречат или да се справат со последиците од ситуацијата треба да имаат соодветен капацитет на оперативна способност.

Индикатори за следење и оцена на оперативниот капацитет се групирани во рамките на следните области: раководење, координирање и информирање, материјални ресурси, човечки ресурси; правила и регулативи, и практично искуство.

ИНДИКАТОРИ ЗА ПРОЦЕНА НА ОПЕРАТИВЕН КАПАЦИТЕТ
Раководење, координирање и информирање
Постои целосно обучена организација за управување која може да ги води операциите како одговор на вонредната ситуација.
Субјектот ги има неопходните ресурси, има на располагање технички системи, комуникации и ситуационен мониторинг и може да функционира дваесет и четири часа најмалку во текот на една недела.
Постојат рутини и техничка поддршка за информирање на јавноста и медиумите како и внатрешно информирање.
Материјални ресурси
Постојат достапни материјални ресурси веднаш по појавата на вонредната ситуација.
Има расположливи материјални ресурси најмалку за една недела.
Постои можност за реалоцирање внатрешни материјални ресурси како и можност за примање дополнителни надворешни материјални ресурси.
Човечки ресурси
Достапни се целосно обучени човечки ресурси веднаш по појавата на ситуацијата.
Човечките ресурси можат да оперираат најмалку една недела.
Постои можност за реалоцирање на човечки ресурси во рамките на субјектот, како и можност за прием на надворешни дополнителни човечки ресурси.
Правила и регулативи
Постојат правила и регулативи за надлежностите на субјектот за справување со вонредната ситуација.
Постојат политики за тоа како субјектот ќе се справи со ситуацијата.
Постојат процедури кои се применуваат во текот на ситуацијата.
Постои систем на дефинирана распределба на овластувањата во рамките на субјектите.
Практично искуство
Доживеан реален инцидент има сличности со анализираната ситуација.
Направена вежба, има сличности со анализираната ситуација.

Табела број 7. Индикатори за следење и оцена на оперативниот капацитет

Капацитет за справување со сериозни прекини на критични функции

Потребата од соодветен капацитет за справување со сериозни прекини на критични општествени и други јавни функции е неопходна,

бидејќи со тоа се овозможува извршување на потребните оперативни активности на такво ниво што системот/организацијата сè уште ќе може да функционира и да ги обезбедува основните услуги, безбедност и грижа во случај на сериозни прекини. Ова значи дека надлежниот субјект или систем има обврска да се справи со кои било последици од вонредната ситуација поврзани со сопственото функционирање, особено во делот што може да се опише како критичен од гледна точка на поседување оперативен капацитет за справување со итна ситуација.

Индикаторите за проценка на капацитет за справување со сериозни прекини на критични јавни функции се поврзани со следните категории: основно ниво на безбедност; резервни комуникациски системи; резервни сили; капацитет да се премести критичната функција на друга локација; материјални ресурси; човечки ресурси; правила и регулативи и практично искуство.

ИНДИКАТОРИ ЗА КАПАЦИТЕТ ЗА СПРАВУВАЊЕ СО СЕРИОЗНИ ПРЕКИНИ НА КРИТИЧНИ ОПШТЕСТВЕНИ И ДРУГИ ЈАВНИ ФУНКЦИИ
Основни нивоа на безбедност
Постојат минимални нивоа за тоа што треба да се обезбеди
Резервни комуникациски системи
Информатичка технологија
Телефонија
Радио врски
Резервни сили
Достапни се обучени и увежбани резервни сили кои можат да бидат оперативни најмалку една недела
Капацитет да се префрли критичната општествена функција на друга локација
Материјални ресурси
Постои капацитет да се префрли функцијата на друга (безбедна) локација
Постојат достапни материјални ресурси веднаш по појавата на ситуацијата
Има материјални ресурси најмалку за една недела
Постои можност за реалокација на внатрешни материјални ресурси како и можност за примање надворешни дополнителни материјални ресурси
Човечки ресурси
Целосно обучени човечки ресурси кои се достапни веднаш по појавата на ситуацијата
Човечките ресурси може да оперираат најмалку една недела
Постои можност за реалоцирање на човечки ресурси во рамките на субјектот, како и примање надворешни дополнителни човечки ресурси

Правила и регулативи
Постојат правни основи за тоа како субјектот треба да се справи со ситуацијата.
Постојат инструкции и политики за тоа како субјектот ќе се справи со ситуацијата.
Постојат процедури кои се применуваат во текот на ситуацијата.
Распределбата на овластувањата на телата е дефинирана.
Практично искуство
Доживеан реален инцидент има сличности со анализирана ситуација
Направена вежба има сличности со анализирана ситуација

Табела број 8. Индикаторите за проценка на капацитет за справување со сериозни прекини на критични јавни функции

Скала за проценка на капацитет

По спроведениот процес за селекција на релевантните индикатори во контекст на одредена ситуација, се пристапува кон претставување на резултатите од оцената на капацитетот, односно кон „рангирање“ на капацитетот. Процената треба да се изврши за еден, два или сите три вида на капацитет во зависност од улогата и сферата на одговорност на надлежниот субјект/организација. Податоците кои ќе се добијат како резултат, треба да се употребат за добивање сеопфатна слика за тоа како капацитетите во разни области би можеле да бидат развивани од година во година, за компарација меѓу различните агенции и сектори како и за сумирање на разните процени добиени од институциите во една колективна проценка на способноста на целиот систем.

Скалата за проценка се состои од четири нивоа и е претставена на следната табела:

Ниво	Опис на капацитет
1	Капацитетот е добар
2	Капацитетот е главно добар, но има некои недостатоци
3	Постои одреден капацитет, но тој е недоволен
4	Не постои капацитет или постои многу мал капацитет

Табела број 9. Скала на проценка

Во основа, ако изнесената проценка укажува дека *капацитетот е добар* не значи дека една вонредна ситуација ќе помине незабележа-

на, туку се смета дека одговорниот субјект има ресурси и капацитет да ги решава прашањата кои се критични за неговиот систем и неговата функција за време на некоја вонредна ситуација. Главно *добар капацитет*, но со одредени недостатоци значи дека, системот располага со капацитет до одреден степен, но тој во ови на зголемено ангажирање ќе ги манифестира своите недостатоци. Ова може да се однесува, на пример, на некои закажани операции во болници кои се откажуваат или значително доцнење на транспорт на лица и стоки, што значи дека надлежниот субјект нема доволно ресурси да ги изврши своите функции во целост и без задоцнување или откажување. Од друга страна, недоволен капацитет може, на пример, да значи дека се откажува транспорт на лица и стоки, дека луѓето се изложени на значителни финансиски загуби или дека се применува некој облик на рационализација. Ресурсите на надлежниот субјект се значително помали од тие што се неопходни за решавање на проблемите кои се критични за системот за време на вонредната ситуација. Дека нема капацитет или дека има *многу мал капацитет*, значи дека одговорниот субјект, има многу мал капацитет и не е подготвен за извршување на своите надлежности и функции.

VIII глава

МЕНАЏЕР НА РИЗИЦИ

1. МЕСТОТО НА МЕНАѢЕРОТ НА РИЗИЦИ ВО УПРАВУВАЊЕТО СО ОРГАНИЗАЦИЈАТА

Современото општество и современата организација претпоставуваат постоење на голем број услови за нивно успешно и безбедно функционирање. Носителите на активностите и задачите, т.е луѓето, на различни начини се обидуваат да избегнат негативни случувања, односно, ги сведуваат на најмала можна мера. Тоа го прават со проактивно и реактивно дејствување.

Од успешноста на процесот на проактивно дејствување, односно превенцијата, зависи степенот на ангажирање на ресурси во реактивната фаза на дејствување, односно фаза која настапува од моментот кога настапуваат негативните последици. За превентивното дејствување да биде ефикасно неопходно е да се согледаат сите потенцијални опасности кои и се закануваат на организацијата според местото, времето и начинот на дејствување. Постоењето на опасноста е сигнал за загрозување на штитените вредности, но вистинската мерка за можноста потенцијалната опасност да стане штетен настан организацијата ја добива со извршување процена на ризикот за идентификување на опасноста.

Процената на ризици е доста сложен процес во кој е неопходно да се примени мултидисциплинарен пристап на набљудување на потенцијалната опасност и влијанието на неа. За да можат потенцијалните опасности да се согледаат на адекватен начин неопходно е процената да ја вршат стручни лица, кои се обучени и оспособени за таков вид работа.

Значи, промените кои се случија во сферата на безбедноста не само што ја менуваат традиционалната претстава за процесот на проценка на ризици, на кој повеќе не се гледа како на линеарен процес, изолиран во рамките на одделните организациони целини, туку веќе влијаат и на профилот на современите менаѢери на ризици. Иако постои одредена специфичност врзана за работата на менаѢерот на ризици во јавниот или приватниот, непрофитабилниот или профитабилниот сектор, потребата од современ јавен менаѢмент, општествено одговорно работење и барања кои се поставуваат пред најодговорните луѓе за прашања од безбедноста и заштита на организацијата во земјите со развиена трговска економија, се повеќе се бришат овие разлики.

Карактеристиките на потврдениот безбедносен менаџер и менаџерот на ризици даваат предност на кандидатите кои, покрај тоа што претставуваат стручњаци за безбедност, имаат атрибути на деловно ориентирани луѓе кои ги познаваат вештините на бизнисот. Самото управување со ризици е процес кој овозможува овие две вештини да се интегрираат во деловната парадигма во која безбедноста е нераскинлив дел на деловната политика и целите на организацијата – со збор, една во низа деловни функции или организациони целини. Процесот на управување со ризици кој ги собира раководителите на разни деловни функции ја прави онаа точка на пресек во која доаѓа до израз одговорноста на безбедносниот менаџер и за јавни (прашањето за општествена одговорност) и за економски интереси (заштеда на ресурси и стекнување профит). Ова е од особено значење за пазарот на земјите во транзиција, затоа што од безбедносниот менаџер⁷⁴ се очекува безбедноста да ја трансформира во компонента која е можно да се опише со економски термини. Попрецизно, потребно е да се одговори што носи вложувањето во безбедноста од аспект на ризиците придобивките, и кој е прифатлив ризик за организацијата, кој нема да ги загрози безбедносните потреби, со минимални губитоци за организацијата.

Позицијата менаџер на ризици во системот за управување со организацијата во пракса е определена со значењето што и се придава на функцијата безбедност. Кога се говори дека работите на безбедноста се остваруваат како „деловна“ функција, тогаш безбедносната функција се набљудува како функција на општиот менаџмент на организацијата. Во тој случај, проблемот за безбедноста на штитените вредности не може да се сведе на физичко-техничката компонента, односно заштита од насилнички акти. Тоа воедно би значело и дека безбедноста како деловна функција се остварува на сите организациски нивоа, преку примена на безбедносно-заштитни процедури од страна на сите вработени, со кои се пропишува нечие однесување, без разлика на местото, времето и карактерот на загрозените вредности.

Оттука, без разлика на неизедначената пракса кај нас и во светот работите на безбедноста треба да ги водат безбедносни менаџери, менаџери на ризици, кризни менаџери и сл., и од сите нив се очекува да бидат личности со изразена деловна ориентација. Современиот менаџер на овие работи ја разбива илузијата за „истрошен“ полициски службеник. Покрај знаењата и искуствата врзани за полициските вештини, истражни техники и дејства, современите барања на пазарот

⁷⁴ Голем е бројот примери, особено помеѓу развиените компании, работите на безбедносниот менаџмент и ризик менаџментот да ги вршат исти лица.

водат кон релевантни компетенции во областа на безбедност на информациите, познавање на вештините на работењето, организацијата, комуникација, мотивација итн.

2. БАРАЊА ЗА КВАЛИФИКУВАНОСТ НА МЕНАѢЕРОТ НА РИЗИЦИ

Со оглед на тоа дека менаѢерот на ризици треба да врши сложени и одговорни работи, тој е должен да одговори и на одредени барања во согласност со законите и стандардите, со чие исполнување би се создале претпоставки за сигурно вршење на работите на процена на ризици во заштитата на лица, имот и работење.

Условите кои во таа смисла кандидатот треба да ги исполни се:

1. образование: да поседува висока (ВСС) школска спрема од научни области сродни на работите во областа на безбедноста;
2. работен стаж: а) најмалку 3 години;
3. стручно искуство: а) најмалку една година на работите за заштита на лица, имот и работење;
4. други услови: а) уверение за неказнување (соодветна безбедносна проверка), б) државјанство, в) општа здравствена способност (психофизичка способност-лекарско уверение издадено од надлежна здравствена установа)
5. специјалистичка обука: а) совладана програма за стручна обука за процена на ризици во заштита на лица, имот и работење – во согласност со прописите и шемата за сертификација на лица за вршење на работи за процена на ризици при заштита на лица, имот и работење;
6. положен стручен испит

За добивање лиценца за процена на ризици во заштитата на лица, имот и работење, треба да се отвори можноста истото да се дополни во соодветниот закон за приватно Законот за приватно обезбедување.

Посебна квалификуваност: се препорачува поседување, со наведени докази:

- а) познавање најмалку еден странски јазик;
- б) постдипломско специјалистичко усовршување од областа на безбедноста, односно области сродни на работите кои се вршат при давање услуги за обезбедување на лица, имот и работење;
- в) положен стручен испит од областа на заштита од пожар;
- г) положен стручен испит за стручно лице во областа на безбедност и здравје на работното место и работната околина.

3. ОПИС НА РАБОТИТЕ

Менаџерот на ризици е личност од составот на организацијата или екстерно лице кое поседува сертификат за вршење на работи за процена на ризици. Во согласност со прифатената шема за сертификација на стручни лица за процена на ризици во заштита на лица, имот и работење, менаџерот за ризици е способен да ги врши следните работи:

- да ја познава и да ја следи состојбата на процесот на работење во организацијата, од аспект на согледување на факторите кои се важни за процена на ризици;
- да одржува постојан контакт со сите заинтересирани страни за прашања кои се актуелни за процената на ризици;
- да ја следи законската регулатива, стандардите и прописите кои ја регулираат, првенствено областа на процена на ризици, а потоа и другите кои имаат значајно влијание на безбедносната состојба на организацијата;
- да учествува на семинари, едукации и усовршување од областа на процена на ризици;
- да учествува во предлагање мерки и да изработи план за имплементација на мерките предложени врз основа на процена на ризици;
- да врши надзор на примена на мерките од планот за имплементација на мерки;
- да го известува надредениот за состојбата во организацијата по прашања на заштита на лица, имот и работење во области кои му се дефинирани во описот на работата;
- да соработува со одговорното лице за заштита во организацијата по прашања од областа на процена на ризици во заштита на лица, имот и работење;
- да учествува во изработка на план за обука на вработените во организацијата, кој се однесува на превенција на вонредни случувања и постапување во ситуации кои можат да ги загрозат штитените вредности;
- да обезбедува реализација на теми поврзани за процена на ризици во заштита на лица, имот и работење, дефинирани во програмата за обука на вработените;
- да учествува во анализа на програмите за обука, да дава предлози за иновации и дополнувања во согласност со научните и стручни достигнувања во областа на процена на ризици, промени на законските регулативи и промени во важечките стандарди;
- да ја следи работата на процена на загрозеноста и да поднесува предлози засновани врз процена на ризици.

МенаѢерот на ризици, како стручно лице за работи за процена на ризици при заштита на лица, имот и работење мора да обезбеди синхронизација на сите работи и активности неопходни за успешна реализација на процената на ризици. Општата стратегија за работа на менаѢерот на ризици подразбира физичка и правна идентификација на штитените вредности, идентификација на одговорноста за одредени сегменти на процената на ризици, утврдување на целите на процената, утврдување на ефективен датум на процената, собирање и анализа на податоци кои се потребни за примена на методите на процената, примена на методите на процена, донесување заклучок, предлог-мерки и изработка на извештај.

Во постапката за процена на ризици, основна претпоставка е објективноста. Покрај објективноста, во постапката за процена, неопходно е да се имаат предвид и специфичните професионални стандарди и етичките правила. Најважна активност во процената на ризици, секако е примена на соодветните пристапи и методи на процена, со почитување на законските и другите општо прифатени регулативи.

МенаѢерот на ризици своето работно време го поминува на различни места и локации, во зависност од планот за процена на ризици. Работата на менаѢерот на ризици бара и висок степен на концентрација, а за тоа му е неопходен простор во кој нема бучава. Најчесто тоа се одовоени канцеларии во кои сасмостојно ги анализира проблемите, врши пресметки и изработува извештаи. МенаѢерот на ризици често е под голем притисок и стрес поради самата природа на работата, односно, потребно е да поседува обемно знаење од областа во која работи, како би можел да ги согледа заканите и ризиците заради создавање на претпоставки за ефикасно предвидување.

Од личните карактеристики неопходно е да поседува: прецизност, аналитичност, способност за одделување на важното од помалку важно-то, објективност, способност за утврдување на вредност, одлична способност за усна и писмена комуникација, способност да изврши упатства и да ги издаде на други, да толкува документи, да разбира процедури, да води писмена кореспонденција и разговори со вработните, а за тоа се неопходни извонредни комуникациски и организациски вештини. Исто така, потребна е способност за работа во услови на преоптоварување на работа, недостаток на време и на информации.

МенаѢерот на ризици би требало да зазема такво место во системот за управување во организацијата да има можност за директна комуникација со највисокиот менаѢер и со клучните луѓе во организацијата.

4. УПАТСТВО ЗА ПРИБИРАЊЕ НА ПОДАТОЦИ

Основен проблем на менаџерот на ризици е да обезбеди квалитетни информации неопходни за процена на ризикот.

Ефективно и ефикасно прибирање на податоци подразбира примена на одредени правила во работата, засновани на научно и практично проверени сознанија.

Организацијата на прибирање на податоци се состои од неколку фази:

- дефинирање на контекстот (проектирање);
- организирање;
- реализација;
- составување записи.

Дефинирање на контекстот (проектирање) на собирањето на податоци е почетна фаза во која менаџерот на ризици мора да осмисли што сака да дознае, за што сака да собере податоци, да ја анализира состојбата на постојните податоци, каде може да пронајде податоци, со кого треба да оствари контакт, да направи идејна скица на патот што го води до податоците кои ги бара.

Организирањето е логичен продолжеток на првата фаза и се состои од два дела: планирање и практично организирање за прибирање податоци.

Планирањето треба да резултира со план, чија содржина треба да биде таква, така што пред сè, менаџерот на ризици, а потоа и сите други кои се важни за прибирање на бараните податоци треба да добијат претстава и прецизни насоки што, кога и како треба да се работи, за да може менаџерот на ризици да добие валиден податок.

Практичното организирање овозможува менаџерот на ризици да ги изврши сите подготовки кои се предвидени со планот за прибирање податоци. Цел на практичното организирање е сите планирани лица, материјали, ресурси и опкружување во моментот на собирање податоци да бидат на место и во состојба што ја предвидел менаџерот на ризици.

Реализацијата претставува активирање на планот за прибирање податоци, а самата работа на прибирање податоци се базира со примена на различни методи. Ако е неопходно, менаџерот на ризици ќе врши мерење и проверка на добиените податоци. Евентуално, ако има повеќе извори на податоците, врши нивно поврзување и унапредување заради добивање покомплексни податоци. Методите што ги има на располагање се: испитување, набљудување, експеримент, студија на случај, анализа на документи, текстови, разговор со вработените, барање и собирање извештаи итн.

Составувањето записи е завршна фаза во која менаџерот на ризици врши обликување на податоците на најприфатлив начин за ефикасна процена на ризиците. Записите може да се водат во пишана и во електронска форма. Кај изработката на записи менаџерот на ризици треба да настојува приоритетно да ги прибира податоците кои ги бара пропишаниот стандард. Во случај на нејаснотија, двосмисленост или непрецизни податоци, треба да се врши негова проверка, а дури потоа врши внесување во записот.

Добиениот податок мора да исполнува одредени квалитети како што се:

- валидност на податокот – дали податокот е добиен на правилен начин;
- сигурност на податокот – проверен податок;
- доследност на податокот – ист податок од повеќе видови извори;
- објективност на податокот – податокот е потврден од повеќе лица;
- потполност на податокот – нема показатели дека податокот е неточен.

Менаџерот на ризици, прибира податоци потребни за процена на ризици од менаџерите по сектори, односно од вработените на разни работни места, од архива, од јавни служби или од други релевантни извори.

БИБЛИОГРАФИЈА:

1. Adelsberger Z., (2008), Upravljanje rizicima i poboljšanje kvalitete, Kvalitet, br.1–2, Poslovna politika, Beograd.
2. Adelsberger Z., Buntak, K. (2009), Zajednički kriteriji kao zahtjevi za integraciju sistema upravljanja, Kvalitet, br. 1–2.
3. Ahić J., (2009), Sistemi privatne sigurnosti, Sarajevo.
4. Alibabić Š., (2002), Teorija organizacije obrazovanja odraslih, Institut za pedagogiju i andragogiju Filozofskog fakulteta u Beogradu, Beograd.
5. American Heritage Dictionary (1990): New York.
6. Anderson V. & Johnson, L., (2000), System Thinking Basics, From Concepts to Causal Loops, MA Pegasus Communications, Waltham.
7. Argenti J., (1989): Practical Corporate Planning, UNWIN – Paperbacks, London.
8. Arsovski S., Stepanović, B., (2009), Integrisani sistemi menadžmenta u proizvodnji i distribuciji toplotne energije, Kvalitet, br. 11–12.
9. Avanesov E., Risk Management in ISO 9000 Series Standards.
10. Бакрески О., Триван Д. и Митевски С. (2012), Корпорациски безбедносен систем, Комора на Република Македонија за обезбедување на лица и имот, Скопје.
11. Бакрески О., Даничиќ М., Кешетовиќ Ж. и Митевски С. (2015), Приватна безбедност, Комора на РМ за приватно обезбедување, Скопје.
12. Balaban N., Ristić, Ž., Đurković, J., (1996), Principi informatike, Savremena administracija, Beograd.
13. Banks E., (2005), Catastrophic Risk – Analysis and Management, John Wiley and Sons.
14. Baranoff E., (2004), Risk Management and Insurance, Wiley, Danvers, USA.
15. Barraba V., Zaltman G., (1990) Hearing the Voice of the Market, Harvard Business School Press.

16. Белов П. Г., (1996), Теоретические основы системной инженерии безопасности, ГНТП „Безопасность“, МИБ СТС, Москва.
17. Beck U., (1992), Risk Society: Towards a New Modernity, Sage, London.
18. Bertalanffy L., (1968), General System Theory (Foundations, Development, Applications) Penguin Books, London.
19. Betts F., (1992), How Systems Thinking Applies to Education, Improving School Quality, vol. 50. No 1.
20. Bienien H. Power., (1992), Economics and Security, The United States and Japan in Fokus, Westview Press.
21. Birkmann J., (2006) Measuring Vulnerability to Promote Disaster-resilient Societies: Conceptual Frameworks and Definitions.
22. Birkmann J., (editor), (2006), Measuring Vulnerability to Natural Hazards – Towards Disaster Resilient Societies”, New York, United Nations University.
23. Blaikie P., (2004) At all: At Risk: Natural Hazards, People’s Vulnerability, and Disasters, New York, NY: Routledge. 2nd Edition.
24. Bohm D., (1989), The Search for Meaning - “The New Spirit in Science and Philosophy”, Crucible.
25. Born H., Caparini M. and Cole E., (2007), Regulating Private Security in Europe: Status and Prospects, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Policy Paper – №20, p.5.
26. Borodzicz E., (2005), Risk, Crisis and Security Management, John Wiley and Sons, New York.
27. Brion, Kaminski, (2001), Студија о законодавству којом се регулише сектор приватне безбедности, CoeES, Brisel.
28. Buzan B., (1998), Security: A New Framework for Analysis, Boulder CO, Lynne Rienner.
29. Viner N., (1964), Kibernetika i drustvo, Neolit, Belgrad.
30. Volkov V, (2001), Dezinformacija, Nas dom, Beograd.
31. Vrsec M., (1991), Pojam sigurnosti, opasnosti i ugrozenosti, priricnik br. 6, Zagreb.
32. White A., (2010), The Politics of Private Security-Regulation, Reform and Re-Legitimation, Palgrave Macmillan, New York.
33. William A., (1978), Forecasting. An Appraisal for Policy – Makers and Planners, The Johns Hopkins Press, London.

34. Георгиева Л., (2006), Менаџирање на ризици; Филозофски факултет, Скопје.
35. Георгиева Л., (2008), Препознавање на хуманата димензија на безбедноста: предизвици и перспективи за концептот во Македонија, во одбрани текстови од Конференции за Превенција и човекова безбедност 2005-2007, Фондација Фридрих Еберт, Скопје.
36. George B., Button M., (2004), Private Security, Palgrave Macmillan, New York.
37. Gesamtwirtschaftlicher Nutzen der Normung, (2000), DIN, Deutsches Institut für Normung e. V., Berlin, Wien, Zurich, Beuth.
38. Gigliotti R. and Ronald J., (1991), Emergency Planning for Maximum Protection, Butterworth-Heinemann, New York.
39. Glaesser D., (2006), Crisis management in the tourism industry. Oxford, UK:Butterworth–Heinemann.
40. Godišnjak reforme sektora bezbednosti u Srbiji, (2009), Centar za civilnovojne odnose, M. Hadžić i dr. (ur.), Beograd.
41. Goldberg B. E., (1994), System Engineering „Toolbox“ for Design-Oriented Engineers.
42. Darmer J., (1977) Management Planning and Control Systems, Advanced Concepts and Cases, (Richard D.) Inc., Homewood, Illinois.
43. David W. Ewing, (1973) The Practice of Planning, Harper and Row Publishers, New York.
44. Davis P., (1994), New Challenges for Defense Planning, RAND, Santa Monica.
45. Dempsey S.John, (2011) Introduction to Private Security, Wadsworth, Cengage Learning.
46. Directorate of Defense Policy, (1998), The Strategic Defense Review, London.
47. Drucker P., (1997) Management, Pan books Ltd., London.
48. Ѓорески, В., (2005), Планирање на одбраната на РМ, модел и методологија согласно системот за ППБ, докторска дисертација.
49. Eisner M. A., (1993), Regulatory Politics in Transition, Baltimore-Maryland: John Hopkins University Press.
50. Ericsson J., (2001), Threat politics: New perspective on security, risk and crisis management, Ashgate Publishing Limited.

51. EU Crisis Response Stapability, (2001), Institutions and Processes for Conflict Prevention and Management, ICG Issues Report No 2, Brussels.
52. Ilić G. P. (2009), Odgovornost pravnih lica za krivična dela, Bilten Okružnog suda u Beogradu, Intermex, Beograd.
53. Ilić, S., Marković, M., Dimitrijević, P. (2001), Nauka o upravljanju, Savremena administracija, Beograd.
54. Ivanović, M. ISO 9004:2009 – od QMS-a do poslovne izvrsnosti (2009), Kvalitet, br. 9–10.
55. Иванова, Ј. И., Приходко, В. И. (2008), Теорија организације, превод З. Симић-Лекић, Факултет заштите на раду у Нишу, Ниш.
56. Jugović, P. T., (2007), Prilog definiranju kvalitete transportno-logističke usluge na prometnom pravcu, Pomorstvo, god. 21, br. 2, Rijeka.
57. Kljajić, M., (1994), Teorija sistemov, Moderna organizacija, Kranj.
58. Кралеv Т., (1984), Теорија на системите, информациите и информативните системи, Студентски центар, Скопје.
59. Keković, Z., (2009), Sistemi bezbednosti, Fakultet bezbednosti, Beograd.
60. Keković, Z., Komazec, N., Glišić, G. (2008), Pristup metodologiji procene rizika, NBP - Journal of Criminalistics and Law, Vol 14. No 3, Kriminalističko policijska akademija, Beograd.
61. Keković, Z., Nikolić, V. (2006), „Upravljanje rizicima kao preduslov efikasnog kriznog menadžmenta“, u: Z. Keković, Ž. Kešetović, Krizni menadžment I –prevencija krize, Univerzitet u Beogradu – Fakultet bezbednosti, Beograd.
62. Kešetović, Ž., Keković, Z. (2008), Sistemi kriznog menadžmenta, Univerzitet Sinergija – Fakultet za bezbjednost i zaštitu, Banja Luka.
63. Kinsey Christopher, (2006), Corporate Soldiers and Interational Security-The Rise of Private Military Companies, London and New York, Routledge.
64. Knight, F. H., (1921), Risk, Uncertainty, and Profit, First edition, Hart, Schaffner & Marx; Boston: Houghton. Mifflin Company, The Riverside Press, Cambridge.
65. Košutić, B., Lukić, R. (2008), Uvod u pravo, dvadeset peto izdanje, Službeni glasnik, Beograd.
66. Corporate Soldiers and Interational Security, (2006), London and New York, Routledge.
67. Krstić, B., Sekulić, V. (2007), Upravljanje performansama preduzeća, Ekonomski fakultet, Niš. Kuljba, B. B., Stanković, M., Savić, S. (1999),

- Primena Petri-mreže za modeliranje rizičnih događaja, Preventivni inženjering, godina VII, broj 2, Beograd.
68. Landaner C., (1947), Theory of National Economic Planning, Berkeley and Los Angeles, University of California Press.
69. Living with legacy, (2005), SALW Survey of the Republic of Serbia, UNDP.
70. Luecke, R., (2004), Crisis Management: Master the Skills to Prevent Disasters. Boston, USA: Harvard Business School Publishing Corporation. Boston, USA: Harvard Business School Publishing Corporation.
71. Luković S., (2000), Priručnik za procenu profesionalnih rizika, Zaštita, Beograd.
72. Maravić D., (2008), O potrebi zakonskog regulisanja sektora privatnog obezbeđenja u Srbiji, Srpska pravna revija, br. 7, Beograd.
73. Massie L. J., (1987), Essentials of Management, New Jersey, USA, Prentice Hall/Inc.
74. Milisavljević M., Todorović J., (1987), Poslovna i razvojna politika samoupravnog preduzeća, Savremena administracija, Beograd.
75. Milne E.T., (1975), Business Forecasting: A Managerial Approach, Longman, London.
76. Mokhiber, R. (2007)., Twenty Things you Should Know About Corporate Crime. Corporate Crime Reporter.
77. Moskow M., (1987), Strategic Planning in Business and Government, Committee for Economic Development, New York.
78. Murray, T. and McKim, E., (2000), Introduction: the policy issues in policing and private security, in: Police and Private Security: What the Future Holds, A Canadian Association of Chiefs of Police Publication, Ottawa.
79. Меньшиков, Б. Б., Швыряев, А. А. (2003), Опасные химические объекты и техногенный риск, Государственный Университет имени М. В.Ломоносова, Москва.
80. Меньшиков, В. В. (2003), Безопасность жизнедеятельности: безопасность и экологичность технических систем, Хемический факультет МГУ им. М.В. Ломоносова, Москва.
81. Милутиновић З. и други, (2009), Насоки за развивање на методологији за процена на ризици и опасности и нивните импликације, Европски центар за повредливост на индустриски и витални системи (ECILS), Скопје.

82. Митревска М., (2008), Кризен менаџмент, Филозофски факултет, Скопје.
83. Михајлов К., (1971), Деловна политика на работната организација, Економски факултет-Скопје, Скопје.
84. Новачевски Д., (1987), Основи на теорија за системите на информации, Скопје, Наша книга.
85. O'Connor L., Greenfield & Boyle, (2004), 'After the "Quiet Revolution": The Self-Regulation of Ontario Contract Security Agencies', Policing & Society, Vol. 14, No. 2.
86. Omar D. Cardona and all: Holistic Urban Seismic Risk Evaluation of Megacities,
87. Omerbegović-Bijelović, J. (1998), Metaupravljanje i kvalitet upravljanja, Zadužbina Andrejević, Beograd.
88. Ortiz Carlos, (2010), Private Armed Forces and Global Security, Praeger, An Imprint of ABC-CLIO, Santa Barbara, California – Denver, Colorado – Ohford, England.
89. Периќ Ж., (1980), Планирање и пословна политика ОУР, Саремена администрација, Београд.
90. Поповска З., (2006), Управување со системите, Економски факултет, Скопје.
91. Pelling M., (2003), "The Vulnerability of Cities – Natural Disasters and Social Resilience", Earthscan Publications Ltd., ISBN-185383- 830-6, London.
92. Petronijević, M. (2009), Korporativna strategija upravljanja rizikom, Kvalitet, br. 7–8, Poslovna politika, Beograd.
93. Potkonjak, N. (1982), Metodološki problemi sistemnih proučavanja u pedagogiji, Prosveta, Beograd.
94. Quarantelli E., L., (ed.), (1998), What is a Disaster?, Routledge, NY/ London.
95. Robertson D., (1987), A Dictionary of Modern Defense and Strategy, London.
96. Rosenthal U., Michel T. Charles and Paul Hart. (1989): The World of Crises and Crises Management. In Coping with Crises: The Management of Disasters, Riots and Terrorism.
97. Rus V., (1982), Radna organizacija kao otvoreni sistem – polazišne pretpostavke, u: Psihologija i sociologija organizacije, Školska knjiga, Zagreb.

98. Sage A., (1995), *Systems Engineering for Risk Management*, Computer supported Risk management, Kluwer Academic Publishers, Netherlands.
99. Sarin, R. K., Weber, M., (1993), Risk-value models, *European Journal of Operations Research*.
100. Стаменковски А., (1996), Планирање на одбраната, Ѓурѓа, Скопје.
101. Станковиќ Т., (2004), Планирање, Факултет за цивилна одбрана, Белград.
102. Стефаноски С., (2015), Процената и управувањето со безбедносните ризици, како основа за ефикасен кризен менаџмент во Република Македонија, Докторска дисертација, Филозофски факултет, Скопје.
103. Savić S., Stanković M., (2009), *Teorija sistema i rizika*, materijal za pripremanje ispita, Fakultet zaštite na radu u Nišu, Niš.
104. Sjöberg L., (2001), Risk perception: Taking on Societal Salience, in *Threats politics, New perspectives on security, risk and crisis management*, Ashgate.
105. Sjöberg L.: Understanding the process and Consequences of risk perception, in Mosleh & R.A. Rari, (1984), 4th Conference on Probabilistic safety assessment and management, New York.
106. Slović P., (2000), *The Perception of Risk*, Earthscan, London.
107. Fluri P., Hadžić M. (eds.) (2004), *Sourcebook on Security Sector Reform*, Geneva Centre for the Democratic Control of Armed Forces/Centre for Civil-Military Relations, Belgrade, Geneva/Belgrade.
108. Srđević, B., Radović, B. (1997), *Sistemska analiza i informatika u upravljanju ekološkim sistemima*, Zbornik radova sa EKO-konferencije, Novi Sad.
109. Srića, V. (1981), *Sistem, informacija, kompjuter – primena sistemskog mišljenja u ekonomiji*, Informator, Zagreb.
110. Stejner G., (1997), *Strategic Planning*, New York, London, Toronto, Sidney, Singapore, Free Press Paperbacks, Published by Simon Schuster.
111. Hebib, E., (2009), *Škola kao sistem*, Institut za pedagogiju i andragogiju Filozofskog fakulteta u Beogradu, Beograd.
112. Heleta, M. (2009), *Novi pristup u razvoju menadžmenta kvaliteta*, Kvalitet.
113. Hicks H., (1972), *The Management of Organizations*, McGraw-Hill Books Company, Inc., New York.
114. Henry L.Sisk, (1968) *Management and Organization*, South-Western Publishing Company, Cincinnati, Ohio.

115. Čubra N., (1977), Kibernetika u rukovođenju razvojem oružanih snaga, Vojnoizdavački zavod, Beograd.
116. Чепујноски Ѓ., Ќосев С., (2005), Економско планирање, Економски факултет, Скопје.
117. Đurđević Z., (2003), Kaznena odgovornost i kazneni postupak prema pravnim osobama u Republici Hrvatskoj, Hrvatski ljetopis za kazneno pravo i praksu, vol. 10, Zagreb.
118. Jakson J., (1986), Corporate Information Menagment, Prentice Hall, Englewood Cliffs, New Jersey.
119. James A. Gordon, (2001), Risk assessment and Management in Local Government Emergency Planning.
120. Joseph L. M., (1987), Essentials of Menagment, 4th edition, Prentice Hall, Englewood Cliffs, New Jersey.
121. Шуклев Б., (2002), Деловно планирање, Економски факултет, Скопје.

Нормативни акти, стандарди и електронски извори:

1. Закон за управување со кризи, (“Службен весник на Р. Македонија“ бр. 29/2005, 36/2011 и 41/2014),
2. Закон за заштита и спасување (пречистен текст), (Сл. весник на Р. Македонија, бр. 93/2012 и 41/2014, член 34),
3. Уредба за методологијата на изработка на процената, нејзината содржина, структура, начин на чување и ажурирање, како и определувањето на субјекти во системот за управување со кризи на кои им се доставува целосна или извод од процената (“Службен весник на Р. Македонија“ бр. 13/2011)
4. Единствената методологија за процена на штети, (“Сл. Весник на РМ”, бр. 75/01),
5. Krivični zakonik (Službeni glasnik RS, br. 85/05, 88/05, 107/05, 72/09, 111/09).
6. Национална стратегија за заштита и спасување. (“Сл. весник на Република Македонија” бр. 23 од 19/09),
7. Процена на загрозеност на Република Македонија од природни и други несреќи. (Сл. весник на Република Македонија бр. 117/10),
8. BSI BS 4778-2 (1991), Quality Vocabulary.

9. Canadian Standard Association. <http://ops.dot.gov/pubs/rsk/std/progstd.pdf>.
10. CEN BT/WG 161 'Protection and Security of the Citizen'. <http://www.cen.eu/cen/Sectors/Sectors/Security%20and%20Defence/Security/Pages/BTWG161.aspx>.
11. CEN/TC 391 Societal and citizen security. <http://www.cen.eu/cen>. 17.04.2011.
12. COESS Confederation of European Security Services. <http://www.coess.org>. 17.04.2011.
13. Цхадая, Н. Д., Подосенова, Н. С. (2008), Управление безопасностью труда, ЦентрЛитНефтеГаз, Москва.
14. Code of conduct and ethics for the private security sector, CoESS and UNI –Europe. http://www.coess.org/documents/code_of_conduct.pdf. 07.05.2011.
15. DAIEC61508_Guide. www.tuevued.de/uploads/images/.../Basic_guide_IEC.pdf.
16. EN. Commission of the European Communities. A Community approach on the prevention of natural and man-made disasters, Brussels, (2009), COM(2009) 82 final. http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/com_2009_82en.pdf. 06.05.2011.
17. Functional safety and IEC 61508. http://www.ida.liu.se/~snt/teaching/SCRTS/IEC61508_Guide.pdf. 06.05.2011.
18. ISO 9001 Sistem za upravljanje kvalitetom.
19. ISO/DIS 9004:2009 Managing for the sustained success of an organization.
20. ISO 14001 Sistem za upravljanje zaštitom životne sredine.
21. ISO 17000 Upravljanje kvalitetom tela za ocenu usaglašenosti.
22. ISO 22000 Sistem za upravljanje bezbednošću hrane.
23. ISO 27001 Sistem za upravljanje bezbednošću informacija.
24. ISO 31000 Risk management – Principles and guidelines on implementation.
25. ISO GUIDE 73: 2009 Risk management – Vocabulary.
26. ISO/IEC 31010 Risk management – Risk assessment techniques.
27. IEC 61508, IEC 61511 (1998), Functional safety in the Process Industry – risk reduction with Safety Instrumented Systems.

28. OECD report, (23.04.2011): Emerging risks in the 21st century. <http://www.oecd.org/dataoecd/23/56/19134071.pdf>.
29. OHSAS-18001 Sistem za upravljanje bezbednošću i zdravljem na radu.
30. Основные правила риск-менеджмента. <http://www.risk24.ru/pravilarisk.htm>. 22.04.2011.
31. PAS 99 (Publicly Available Specification), (25.04.2011), Integrated Management. <http://www.bsigroup.com/en/Assessment>.
32. Понятие риска и его сущность. <http://www.risk24.ru/risk.htm>. 06.04.2011.
33. Pravilnik o metodologiji za procenu opasnosti od hemijskog udesa i od zagađivanja životne sredine, merama pripreme i merama za otklanjanje posledica, Službeni glasnik RS, br. 60/94.
34. Pravilnik o načinu i postupku procene rizika na radnom mestu i u radnoj okolini Službeni glasnik RS, br. 72/06, 84/06 – ispravka, 30/10.
35. Risk Management Program Standard, Produced by Joint Risk Management Program Standard Team, DRAFT, Internet edition. <http://ops.dot.gov/pubs/rsk/std/progstd.pdf>.
36. SRPS A.L2.001:2008, Društvena bezbednost – Usluge privatnog obezbeđenja – Rečnik, Službeni glasnik RS, br. 104/2008.
37. SRPS A.L2.002:2008, Društvena bezbednost – Usluge privatnog obezbeđenja – Zahtevi i uputstvo za ocenjivanje usaglašenosti, Službeni glasnik RS, br.07/2009.
38. SRPS A.L2.003:2010, Društvena bezbednost – Procena rizika u zaštiti lica, imovine i poslovanja. Službeni glasnik RS, br. 92/2010.
39. SEC 1626 Risk assessment and mapping guidelines for disaster management, Commission staff working paper, Brussels, 21.12.2010.
40. www.unece.org/trade/wp6/documents/.../Report_Avanesov.pdf. 12.03.2011.
41. AS/NZS 4360:2004 (2004), Australia/New Zealand Standard for Risk Management.
42. MiSRaR (Mitigating Spatial Relevant Risks in European Regions and Towns) (2009), Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands. http://www.misrar.nl/UserFiles/File/BP_1_ZHZ_annex%202%20National_Riskassesme
43. http://ec.europa.eu/echo/civil_protection/civil/pdffdocs/prevention. 03 04.2011

44. http://www.fema.gov/plan/prevent/fhm/rm_main.shtm.10.04.2011
45. <http://www.risk24.ru@funriskman.htm>.28.04.2011
46. <http://www.merriam-webster.com/dictionary/risk>
47. <http://www.un.org>,
48. <http://www.unisdr.org>,
49. <https://www.iso.org>
50. <http://www.osce.org>,
51. <http://www.eeas.europa.eu>,
52. <http://www.nato.int>,
53. <http://cuk.gov.mk>

BN 978-6-086550-59



9 786086 550592

ПЛАНИРАЊЕ И ПРОЦЕНА НА РИЗИК ВО ФУНКЦИЈА НА ЗАШТИТА НА ЛИЦА, ИМОТ И РАБОТЕЊЕ

ЗОРАН КЕКОВИЌ ОЛИВЕР БАКРЕСКИ
СТЕВКО СТЕФАНОВСКИ СЛАВИЦА ПАВЛОВИЌ