

УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

Кристина З. Радојевић

**МОДЕЛ ЗА ПРОЦЕНУ ЕФЕКТИВНОСТИ
И ЕФИКАСНОСТИ СИСТЕМА
БЕЗБЕДНОСНОГ МЕНАџМЕНТА**

докторска дисертација

Београд, 2012

UNIVERSITY OF BELGRADE
FACULTY OF SECURITY STUDIES

Kristina Z. Radojević

**AN EFFECTIVENESS AND EFFICIENCY
ASSESSMENT MODEL FOR THE
SECURITY MANAGEMENT SYSTEM**

doctoral dissertation

СТАЊУМ ОДБРАНЕ:

УНИВЕРЗИТЕТ У БЕОГРАДУ
ФАКУЛТЕТ БЕЗБЕДНОСТИ

ПРИМЉЕНО: 26-10-2012.		
Достављено:	Број	Пролог
	598	7-09

Belgrade, 2012

КОМИСИЈА ЗА ОЦЕНУ И ОДБРАНУ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

МЕНТОР:

др Зоран Драгишић, ванредни професор, Универзитет у Београду Факултет
безбедности

ЧЛАНОВИ КОМИСИЈЕ:

др Радомир Милашиновић, редовни професор, Универзитет у Београду Факултет
безбедности

др Милић Радовић, редовни професор, Универзитет у Београду Факултет
организационих наука

ДАТУМ ОДБРАНЕ: _____.

МОДЕЛ ЗА ПРОЦЕНУ ЕФЕКТИВНОСТИ И ЕФИКАСНОСТИ СИСТЕМА БЕЗБЕДНОСНОГ МЕНАЏМЕНТА

РЕЗИМЕ

Један од многобројних проблема са којима су се суочавају организације у земљама у транзицији јесте и проблем реформе система безбедности и заштите на раду, као и заштите животне средине, и увођење нових стандарда у овој области. Кључну улогу у оквиру управљања и контроле овог система треба да има топ менаџмент, и то нарочито преко система безбедносног менаџмента.

У контроли остваривања безбедносне функције организације имају на располагању многобројне инструменте, као што су: буџетска контрола као облик финансијске контроле, као и посебне механизме контроле, при чему се пре свега мисли на рад независних ревизора. Међутим, када је реч о утврђивању успешности рада безбедносног менаџмента, врло је мало постојећих правила и процедура.

Досадашња малобројна истраживања о проблематици безбедносног менаџмента указала су на тешкоће у остваривању ове процене. Као основни проблеми у остваривању контроле безбедносног менаџмента идентификовани су недостатак воље, недовољна стручност и ресурси, као и немогућност утврђивања перформанси безбедносног менаџмента, с обзиром да се његова успешност пре свега огледа у томе да се „ништа лоше не деси“.

Отежавајућу околност за процес безбедносног менаџмента представља и чињеница да у нашој земљи није законски уређен приватни безбедносни сектор, а самим тим ни могућност његове контроле.

Да бисмо утврдили какви су ставови и перцепције запослених на пословима безбедности о управљању безбедношћу, које су препреке у остваривању овог процеса, као и могућност њиховог превазилажења, спровели смо истраживање у привредним организацијама у Републици Србији. Истраживање је спроведено у периоду од маја до октобра 2011. године.

Као истраживачки инструменти у раду су примењени *анкетни упитник* и *експертски интереси*. Упитник који је примењен у истраживању састављен је из три дела. Први део је идентификациони и чине га социо-демографска питања: пол, старост и стручна спрема. Други део односи се на постављена питања у виду скале ставова са утврђеном категоријом, док је трећи део отвореног типа, односно, испитаницима је понуђена могућност да наведу препоруке за унапређење безбедносног менаџмента у организацијама у Републици Србији.

Интервјуи су обављени са појединим стручњацима за безбедност у испитаним организацијама, као и одговорним лицима у њима.

Поред наведених истраживачких инструмената (упитник и интервју), у истраживачком делу је примењен и метод анализе садржаја, пре свега за анализу безбедносних извештаја, нормативних аката и правилника везаних за безбедност, као и на анализу безбедносних стандарда и процедура.

Истраживањем је утврђено да у Републици Србији постоје законске и нормативне регулативе у погледу безбедности и да многи менаџери увиђају њихов значај, али да се сам њихов утицај на рад безбедносног менаџмента врло тешко може одредити.

Наиме, неретко су добијени одговори који указују на то да обавезна правила по питању безбедности само додатно компликују ионако сложене послове који се свакодневно одвијају. Највећи проблем је што се ти послови поверавају обично једном човеку, или малом броју људи, а они при том покривају целокупан и веома сложен систем безбедности, који је сам по себи проблем у великим организацијама.

Већина анкетираних сматра да систем управљања безбедношћу, заправо није уведен на прави начин и развијен у потребној мери. Испитани су, такође, негативно вредновали постојеће стање у својим организацијама по питању процене успешности и мерења перформанси безбедносног менаџмента.

Радам је била обухваћена и анализа неопходних услова за мерење ефективности и ефикасности безбедносног менаџмента. Закључено је да, иако постоји дефинисан законски оквир везан за стандарде безбедности и заштите на раду и заштите животне средине, овај услов није довољан за оцену њиховог значаја. Заправо, већина

испитаних стручњака сматра да стандарди постоје формално, само на папиру, док се њихов конкретан учинак не може директно проценити нити мерити.

На основу анализе интервјуа са стручњацима који су задужени за безбедност у испитаним организацијама, можемо закључити да постоји сагласност да би требало да постоје одређени критеријуми за процену рада система безбедности и заштите на раду, али пре свега знање и воља топ менаџмента за контролом.

Да би топ менаџмент у организацијама у Републици Србији био у стању да спроводи контролу над системом безбедности и заштите на раду, противпожарне заштите и заштите животне средине, и оствари ниво који у том погледу постоји у развијеним земљама, неопходно је да у пракси примењује инструменте који су јој на располагању. Битно је схватити да је систем безбедности и заштите на раду основни део сваке организације, а да безбедносни менаџмент представља део стратешког менаџмента сваке организације. Да би се могла извршити процена и вредновање рада овог система потребно је дефинисати критеријуме за мерење његових перформанси као и одредити поступак њиховог мерења.

Неопходно је пронаћи начин за утврђивање повраћаја на инвестиције у безбедност, обезбедити едукацију запослених по питању безбедности и заштите на раду и заштите животне средине, али и увести и консултације и сарадњу са организацијама цивилног друштва о питањима безбедности и заштите животне средине.

Од изузетне важности је схватање значаја менаџера безбедности за процес контроле и процену рада система безбедности и заштите на раду. Топ менаџмент би требао да озбиљније схвати рад овог дела организације и да у безбедносне извештаје уврсти мишљења, предлоге и савете конкретних људи који се баве безбедношћу и заштитом на раду.

Незаобилазно је да се јасно дефинише и нормативно регулише целокупан сектор безбедности, као и то да организације успоставе систем регуларних и институционализованих односа са организацијама у сектору безбедности, институтима који се баве безбедношћу, здрављем и заштитом на раду, противпожарном заштитом и заштитом животне средине, истраживачким институцијама, невладиним организацијама, медијима, независним државним

органима, међународним организацијама, као и другим стручним групама из области безбедности и заштите.

Али, најважнији услов који треба остварити јесте пре свега воља менаџера и запослених у организацијама да се нешто промени у њима.

На основу свега напред поменутог можемо закључити да је систем безбедносног менаџмента у организацијама у Републици Србији нормативно и институционално устројен, али у функционалном смислу није остварен одговарајући ниво процене и оцене његовог рада, односно није успостављен систем за мерење његове ефективности и ефикасности.

Кључне речи: систем безбедносног менаџмента, безбедност и заштита на раду, перформансе безбедносног менаџмента, ефективност безбедносног менаџмента, ефикасност безбедносног менаџмента

Научна област: интердисциплинарне, мултидисциплинарне и трансдисциплинарне студије

Ужа научна област: Студије безбедности

УДК број: 005:331.45

AN EFFECTIVENESS AND EFFICIENCY ASSESSMENT MODEL FOR THE SECURITY MANAGEMENT SYSTEM

SUMMARY

One among many problems that transition states face with is the problem of security and safety systems, as well as the environmental and fire protection systems reforms and the establishment of the security, health and safety standards. The crucial role within management and control of these systems should be played by top management, i.e. the key element in this process is the responsibility of security and safety management system.

In realization of the security and safety functions organizations have at their disposal various instruments, such as: budget control as a form of financial control, as well as special mechanisms of control, above all the work of independent audit authorities. However, when there is a question on assessing the success of the security and safety management functions, we have very little rules and procedures.

A few studies on problems of security and safety management have indicated obstacles in realization of this assessment. The main problems affecting the implementation of the control of the security and safety management are: the absence of will, insufficient competence and resources, as well as the difficulties in defining indicators for performance measurement, especially if we bear in mind that the success of the security and safety management is shown when “nothing bad has happened“.

Another difficulty for the security and safety management processes is the fact that the Republic of Serbia has not legally regulated the private security sector, which implies the problem of its control.

In order to determine the attitudes and perceptions of the employees in the security and safety sectors on the issues of security and safety management, the obstacles in their functioning, as well as the possibilities for their overcoming, we have conducted a study in the economic corporations in the Republic of Serbia. The investigation has been performed from May to August 2011.

In this work, the *survey questionnaire* and *expert interview* are applied as research tools. The questionnaire implemented in the research is compound of three parts. The first segment contains socio-demographic questions: gender, age and education. The second part relates to questions posed in the shape of attitude scale with established categories, while the third part is open-ended, that is, subjects are offered with possibility to make recommendations for promoting the security and safety management functions in the corporations in the Republic of Serbia.

The interviews have been performed with the security and safety experts in the corporations researched, as well as the responsible persons within the corporations.

Besides the cited research instruments (questionnaire and interview), the technique of content analysis is applied in the research segment of the work, primarily for the analysis of security and safety reports, memos, enactments and rules regarding security and safety, as well as the fire and environmental protection, security and safety standards and procedures.

The study showed that the economic organizations in Republic of Serbia have at their disposal instruments and enactments on security, safety at work and fire protection, as well as environmental protection and that managers alone comprehend their importance, but, the influence of those enactments on the security and safety management functions is difficult to determine, and we cannot recognize a clear, dominant position and the significance of these instruments for the success of the security and safety management systems.

We have encountered some answers that indicate that there are some obligatory rules regarding security, safety and protection which make these processes much more complicated than they already are. The problem here arises from the fact that all those responsibilities are usually delegated to one person or a few persons at most. If we think about the complexness of these jobs alone, we can only imagine how difficult it is for one person to control all those processes in a big organization.

The most of questioned representatives think that security and safety management systems in their organizations have not been implemented and developed in appropriate way. The representatives have also evaluated negatively the conditions of the assessment and performance measurement of their security and safety management systems.

The work has covered an analysis of the necessary conditions for the efficiency and effectiveness measurement of the security and safety management systems, too. We have concluded that, although there is a clearly defined constitutional and legal framework, especially regarding safety and environmental protection standards, this condition is not enough for a detailed assessment of management systems. Really, the most of representative surveyed hold that the standards exist formally, only on paper, while their performances are almost impossible to measure.

On the basis of interview analysis, we can conclude that there is a consensus on necessity to establish certain criteria for assessing the functions of the security, health and safety, fire and environmental protection systems, but above all knowledge and will of the top managers for the control.

For the top management of the corporations in Republic Serbia to be able to conduct control of the security, health and safety at work and fire and environmental protection systems and attain the level of developed countries, it is necessary to apply in practice the instruments at its disposal. It is of essential importance to realize that the security and safety management systems are active and vital parts of the corporation, and that security and safety management represent structural elements of the strategic management in any organization. In order to assess and evaluate the processes of these systems, we need to define criteria for performance measurement, as well to establish the measurement processes.

Nevertheless, the most important condition which needs to be realized is the will of the managers to change something in the way their organizations control these management systems. Top management should take these parts of the organization more seriously, and to try and include in security and safety reports attitudes, suggestions and advices of those who are responsible for security and safety.

It is necessary to design the model for evaluation of the return on security and safety investments, to implement an educational and training systems for these areas, and to establish a system of regular and institutionalized relations with the institutions of security sector, research institutions and the NGO specialized for the issues of safety, security, environmental and fire protection, independent state bodies, media, international

organizations and groups of representatives which are dealing with security, safety and protection issues.

On the basis of all afore-mentioned, we may conclude that the security and safety management systems in the economic organizations in Republic of Serbia are normatively and institutionally organized, but, in functional sense, they have not attained an adequate level of their assessment, i.e. there are not established systems for measurement of their effectiveness and efficacy.

Key words: security management system, safety management system, performance measurement, effectiveness of the security and safety management system, efficacy of the security and safety management system

Scientific domain: inter-disciplinary, multi-disciplinary and trans-disciplinary studies

Narrower scientific domain: Security studies

UDK Number: 005:331.45

С А Д Р Ж А Ј

1. Увод	1
1.1. Проблем истраживања	4
1.2. Предмет истраживања	11
1.2.1. Операционално одређење предмета истраживања	13
1.2.2. Временско и просторно одређење предмета истраживања	14
1.2.3. Дисциплинарно одређење	15
1.3. Циљеви истраживања	15
1.4. Хипотетички оквир истраживања	16
1.5. Начин истраживања	16
1.6. Научна и друштвена оправданост истраживања	18
2. Појмовно одређење безбедносног менаџмента	19
2.1. Појам безбедносног менаџмента	19
2.2. Историјски развој безбедносног менаџмента	23
2.3. Функције безбедносног менаџмента	29
2.3.1. Планирање као функција безбедносног менаџмента	30
2.3.2. Организовање као функција безбедносног менаџмента	41
2.3.3. Координација као функција безбедносног менаџмента	48
2.3.4. Вођење као функција безбедносног менаџмента	55
2.3.5. Контрола као функција безбедносног менаџмента	66
3. Систем безбедносног менаџмента (СБМ)	92
3.1. Директиве „SEVESO“	96
3.1.1. Анализа ризика и израда сценарија према директиви „Seveso II“ ..	103
3.1.2. Предлози за побољшање директиве	106
3.2. Концептуални оквир система безбедносног менаџмента	106
3.3. Модел система безбедносног менаџмента	111
3.3.1. Интегрисано схватање појма безбедности	118
3.3.2. Основне особине интегрисаног система безбедносног менаџмента	120

3.4. Елементи система безбедносног менаџмента	126
3.5. Стандарди који утичу на обликовање СБМ	128
3.5.1. Стандард за заштиту од пожара	128
3.5.2. Стандарди OHSAS 18000	131
3.5.3. Стандарди ISO 14000	133
3.5.4. Стандарди ISO 27000	135
4. Методе за процену активности безбедносног менаџмента	137
4.1. Перформансе система безбедносног менаџмента	141
4.1.1. Приступи мерењу ефективности и ефикасности пословања	145
4.1.2. Фактори који утичу на мерење ефективности и ефикасности	149
4.1.3. Ефективност као перформанса безбедносног менаџмента	151
4.1.4. Ефикасност као перформанса безбедносног менаџмента	152
4.2. Модели за процену перформанси система безбедносног менаџмента	153
4.3. Утврђивање индикатора за процену ефективности и ефикасности система безбедносног менаџмента	159
4.4. Балансирана листа мерила безбедности	163
5. Методе за процену ефективности и ефикасности безбедносног менаџмента у организацијама у републици Србији	171
5.1. Нормативно-правни оквир и стандарди безбедности	173
5.1.1. Систем безбедности и здравља на раду	174
5.1.2. Систем физичко-техничког обезбеђења	186
5.2. Постојећи индикатори ефикасности и ефективности система безбедносног менаџмента	190
5.3. Могућности процене ефективности и ефикасности система безбедносног менаџмента у предузећима у Републици Србији	191
6. Анализа безбедносног менаџмента у предузећима у Републици Србији - Резултати истраживања	197
6.1. Презентација резултата добијених анализом упитника	198

6.1.1. Социо-демографски подаци	199
6.1.2. Оцена значајности појединих елемената система безбедносног менаџмента	202
6.1.3. Оцена задовољства елементима система безбедносног менаџмента	208
6.1.4. Оцена финансијских показатеља рада система безбедносног менаџмента	214
6.2. Дискусија резултата добијених истраживањем	219
7. Модел могућег система за процену ефикасности и ефикасности безбедносног менаџмента	222
7.1. Успостављање система мерења перформанси	223
7.2. Алгоритам за одређивање ефикасности мера заштите у системима безбедносног менаџмента	232
Закључна разматрања	236
Списак литературе	239
Прилог бр. 1 – Упитник за стручњаке безбедности у организацијама у Републици Србији	252
Прилог бр. 2 – Списак интервјуисаних лица	255
Прилог бр. 3 – Питања постављена током интервјуа	256
Скраћенице	258
Биографија аутора	260

1. УВОД

Истраживање у оквиру докторске дисертације под насловом: «Модел за процену ефективности и ефикасности система безбедносног менаџмента», има за циљ да широј научној и стручној јавности која се бави изучавањем безбедносног менаџмента као савременог одговора на безбедносне ризике, укаже на потребу, значај и начин процене система безбедносног менаџмента у условима када се претње и ризици стално развијају и мењају. Тежиште у истраживању односи се на анализу безбедносног менаџмента у предузећима у Републици Србији и утврђивање да ли је он у функционалном и институционалном смислу примерен потребама заштите организација, културних добара и животне средине, у условима када постоје савремене безбедносне претње.

Превенција и ублажавање последица спољашњих и унутрашњих претњи су увек актуелни проблеми у скоро сваком организационом систему. Због тога се, ако не сви, а оно већина организационих система мора дизајнирати тако да укључи безбедност у своје планове. При томе, људи који раде на развоју безбедносног менаџмента морају да узимају у обзир и остале циљеве система, односно да одаберу двојне алтернативе које нуде додатне користи власницима предузећа. Зато је од великог значаја да се безбедност посматра у контексту ширег система.

Многа предузећа у развијеним државама примењују системски приступ у решавању безбедносних проблема. У већини таквих предузећа је уведен систем безбедносног менаџмента који штити организацију од сопствених грешака. Међутим, начини за утврђивање успешности овог система, односно за мерење његове ефикасности и ефективности, нису довољно развијени. Основни проблем, заправо, лежи у чињеници да у многим државама још увек нису униформно и јасно дефинисани стандарди безбедности којих се организације морају придржавати, а који би представљали и оријентир за утврђивање безбедносних циљева. Самим тим, различити су и начини за утврђивање одступања од стандарда. Осим тога, постоји проблем који се односи на „профитабилност“ безбедносног менаџмента. Уколико се безбедност не постави као један од стратешких, општих и основних циљева

организације, њен значај не може бити експлицитно изражен. Наиме, циљ безбедносног менаџмента заправо јесте да се „ништа не догоди“, а отуда произилази и скептицизам запослених у осталим секторима и неминовно се поставља питање оправданости улагања у безбедност.

Ипак се може рећи да у савременим организацијама безбедност представља један од приоритетних циљева. То подразумева да су улагања у системе заштите све већа, па је неопходно одредити у којој мери се та улагања заиста и исплате. Зато је потребно пронаћи начин на који се може утврдити да ли је систем безбедности бољи из године у годину, као и начин за упоређивање система безбедности једне организације са оним у некој сличној организацији. Иако је мерење безбедности тешко, а некад чак изгледа и немогуће, ипак је то једини поуздан начин да се одговори на питање да ли је организација способна да решава безбедносне проблеме и да се успешно носи са безбедносним ризицима. Друга алтернатива је да се организације врате у доба када је једини мотив за доношење безбедносних одлука био страх од катастрофалних последица неких догађаја, несигурност у вези опстанка организације и сумња у постојеће мере заштите.

Докторска дисертација кроз своје предметне садржаје, треба да укаже на међународна решења и искуства у овој области, стање и могућности система безбедносног менаџмента, са посебним нагласком на утицај овог система на повећање безбедности и могућности мерења тог утицаја. При том је нагласак стављен на позитиван утицај који предузећа у Републици Србији могу имати због увођења безбедносног менаџмента у своје системе, будући да је ова област код нас прилично запостављена.

Рад се састоји од теоријског и истраживачког дела, који су рашчлањени у шест поглавља:

У првом поглављу је дато објашњење појма безбедносног менаџмента, са кратким освртом на његов развој и савремено схватање. Безбедносни менаџмент се пре свега посматра као менаџмент процес који се непрекидно одвија у организацији и има за циљ да штити ту организацију од неповољних утицаја. Овде су описане и

функције, односно фазе процеса безбедносног менаџмента и то: планирање, организовање, вођење, координација и контрола.

Друго поглавље се бави теоријским одређењем система безбедносног менаџмента, концептуалним оквиром, као особинама интегрисаног система безбедносног менаџмента. Теоријском анализом су сагледана и представљена питања теоријског приступа дефинисању и схватању интегрисаног система безбедносног менаџмента, одређивања модела и његовог прилагођавања новим околностима. Поред тога, у овом делу рада су објашњени елементи који чине безбедносни менаџмент, као и важећи стандарди који се тичу безбедности и здравља на раду, безбедности информација и заштите од пожара.

Треће поглавље односи се на дефинисање и схватање значаја метода за процену активности система безбедносног менаџмента, у чијем су оквиру образложени сами појмови перформансе, а у оквиру ње и ефикасност и ефективност, принципи и предуслови за њихову процену, као и могућност утврђивања индикатора за ту процену. У овом делу је дат приказ балансиране листе мерила, као могућег средства за приказивање индикатора и процену успешности рада система безбедносног менаџмента.

Четврто поглавље се односи на методе за процену ефикасности и ефективности безбедносног менаџмента које се користе у предузећима у Републици Србији. Посебна пажња посвећена је начину на који је систем безбедносног менаџмента регулисан у Републици Србији, као и постојећим индикаторима за његову процену. Поред тога, овде је дат и преглед могућности, односно начина на који се у постојеће системе безбедносног менаџмента могу интегрисати методе за процену његове ефикасности и ефективности.

У петом поглављу приказани су и објашњени резултати истраживања обављеног у привредним организацијама у Републици Србији. На основу анализе упитника приказана је оцена постојећег стања безбедносног менаџмента и његових елемената од стране запослених на пословима безбедности у испитаним организацијама. Поред тога, на основу анализа извештаја и интервјуа представљени су резултати, односно оцена метода за процену ефикасности и ефективности система

безбедносног менаџмента, али и услова за увођење савременог система безбедносног менаџмента у организације у Републици Србији.

У шестом поглављу је приказан модел могућег система за процену ефективности и ефикасности система безбедносног менаџмента. Посебна је пажња поклоњена успостављању система за мерење перформанси, а дат је и предлог алгорита за одређивање ефикасности мера заштите у системима безбедносног менаџмента.

1.1. Проблем истраживања

Брз развој и све јача конкуренција приморавају савремене организације да „стално проналазе нове начине за успешно пословање“¹. „Нови начини пословања доводе до нових безбедносних ризика.“² Како тврди Далтон, „безбедност се више не своди само на реакцију или одговор на неку претњу, обезбеђивање улаза или пратње појединих важних личности“³. Према Доналдсону: „да би се увидело да ли ће организација да се прилагоди променама или не, као и да ли ће расти или не, потребно је разумети ниво ризика којем је изложена“⁴.

Поред тога, све је већа повезаност између организација, а потреба за техничким знањем свих запослених расте. Ова чињеница доводи до потребе за сталним усавршавањем запослених, промене стратегије и начина планирања, организовања, вођења и контроле у већини пословних организација. Такве промене неминовно утичу и на сектор безбедности. Организације постижу висок ниво безбедности ако имају „добро развијену свест о тренутној ситуацији и позитивно реагују на промене у лидерству и утичу на безбедно понашање запослених“⁵.

¹ Paladino, B., *Innovative Corporate Performance Management*, John Wiley & Sons, Inc., Hoboken, 2011., стр. 6.

² Fay, J. J., *Contemporary Security Management (Second Edition)*, Elsevier Butterworth-Heinemann, Burlington, 2006., стр. 15.

³ Dalton, D. R., *Rethinking Corporate Security in the post 9/11 era*, Elsevier Butterworth-Heinemann, Burlington, 2003., стр. 2.

⁴ Donaldson, T., Dunfee, T. W., *Ties that bind: A social contracts approach to business ethics*, Harvard Business School Press, Boston, 1999., стр. 18.

⁵ Bain, A., *Do we truly understand Safety Culture?*, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 22.

Савремени изазови који се постављају пред организације се крећу од тероризма, с једне, и неконкурентности с друге стране. Било које две крајности могу довести до економског губитка, губитка тржишта, смањеног поверења клијената и слично. Претње су стварне за људе, опипљиву и неопипљиву имовину. „Ове претње се морају препознати и на њих се мора одговорити.“⁶ Неуспех да се то уради може имати само један исход, а то је пропаст организације.

Класичне безбедносне организације морају да се прилагођавају новој безбедносној реалности и да траже решења за нове безбедносне изазове или за промењену феноменологију старих безбедносних претњи⁷, а успех пословања у савременим условима у великој мери зависи од безбедности. Треба напоменути да постоје привредне гране којима је безбедност инхерентна. Ту, између осталих, спадају туризам и угоститељство⁸, саобраћај, инвестирање.⁹ У савременом свету већина менаџера не посматра организације само као профитабилне или не, већ вредност организације расте и у односу на то „колико је дуго и у којој мери организација профитабилна“¹⁰. Због тога се у већини организација „безбедност посматра као приоритет „*top менаџмента*“¹¹, а највиши руководиоци значај безбедности рангирају на нивоу 7,5 на скали до 10¹². Све то утиче да „расте потреба да се безбедност и управљање ризиком укључе у корпоративне стратегије“¹³.

⁶ Dalton, D. R., исто, стр. 25.

⁷ Безбедносне претње или безбедносни проблеми се у раду схватају као угрожавање безбедности, а то су: „друштвене појаве или понашање настало деловањем човека (појединачно или групно), природе или техничких система у дужем периоду које су значајнијег обима, при чему настају или могу настати штетне последице по интегритет човека, његову слободу, имовину и здравље, као и по интегритет и субјективитет државе и њених институција, вредности које она штити, као и вредности међународне заједнице.“ - Стајић, др Љ., *Основи система безбедности*, Правни Факултет, Нови Сад, 2010., стр. 52. При чему, предмет угрожавања у овом раду представља организациони систем.

⁸ О безбедносним проблемима у туризму видети: Santana, G., “Tourism: Toward a Model for Crisis Management,” *Turizam*, Vol. 47, No. 1, 1999.

⁹ Видети: Драгишић, З., *Безбедносни менаџмент*, Службени Гласник РС, Београд, 2007., стр. 9.

¹⁰ Vishwanath, S. R., Krishnamurti, C., *Investment Management*, Springer - Verlag, Heidelberg, 2009., стр. 6.

¹¹ Gerencser, M., Aguirre, D., “Security Concerns Prominent on CEO Agenda,” *strategy + business*, 12 Feb., 2002, <http://www.strategy-business.com/press/enews/article/?ptag-ps=&art=254087&pg=0>.

¹² Скала од 1-10 представља релативне приоритете, где 10 представља највиши приоритет.

¹³ Blyth, M., *Risk and Security Management: Protecting People and Sites Worldwide*, John Wiley & Sons Inc., Hoboken, 2008., стр. 2.

Сам појам „безбедносни менаџмент“¹⁴, у ширем смислу, подразумева „одлучивање о безбедносним циљевима организационог система, о начинима и средствима да се избегну неповољни утицаји који долазе из окружења или самог организационог система, или да се њихов штетан утицај умањи“¹⁵. Детаљније, „безбедносни менаџмент обухвата управљање безбедношћу и здрављем на радном месту, ревизије, управљање кризама и планирање за ванредне ситуације, видео надзор, узнемиравање на радном месту и мобинг, праћење запослених, набавка опреме и људи за физичко обезбеђење, заправо све оно што може утицати на функционисање организације, њену профитабилност или виталност.“¹⁶ Различити изазови, ризици и претње^{17,18} којима је изложена нека организација, као и одговорности које организација има према окружењу у погледу безбедности, пресудно утичу на безбедносни менаџмент, односно начин на који ће бити донете одлуке везане за безбедност. При томе, „безбедност сама по себи није атрибут, већ је својство система које зависи од других атрибута и контекста у којем се систем користи“¹⁹.

¹⁴ „Најједноставније речено, управљање неким послом или менаџмент се састоји од три компоненте: - постављања циљева, - праћења реализације посла и упоређивање резултата са жељеним циљевима и - одлучивања о томе да ли да се промени начин на који се ти циљеви остварују.“ - Esque, T. J., *Making an impact: Building a top-performing organization from the bottom up*, CEP Press, Atlanta, 2001., стр. 18.

¹⁵ Драгишић, З., исто, стр. 14.

¹⁶ Borodzicz, E. P., *Risk, Crisis and Security Management*, John Wiley & Sons Ltd., Chichester, 2005. стр. 50.

¹⁷ Врло су честе забуне око значења ова три појма. Како каже Young: „Ризик се састоји од три компоненте: 1) потенцијала или вероватноће да се претња испољи, 2) рањивости у случају да се претња испољи и 3) утицаја испољене претње ... Безбедносни ризик повезан са претњом је једнак производу вероватноће испољавања претње, рањивости у односу на претњу и утицаја испољене претње.“ - Young, C. S., *Metrics and Methods for Security Risk Management*, Elsevier Inc., Burlington, 2010., стр. 10. Значи, није сваки ризик претња, већ је ризик претња која укључује и величину штете која може настати уколико се претња испољи. Изазов, с друге стране, представља одређено стање, ситуацију или догађај, који може довести до испољавања претње. Broder, J. F., *Risk Analysis and the Security Survey*, 3rd ed., Butterworth-Heinemann, Burlington, 2006., стр. 3.

¹⁸ Треба напоменути да проф. Стајић прави разлику између извора и облика угрожавања, при чему су извори угрожавања „исходиште неке будуће појаве“, а облици „конкретни начини испољавања угрожавања“ - Стајић, др Љ., исто, стр. 53. У том смислу извори се могу поистоветити са изазовима безбедности, а облици са претњама.

¹⁹ Fowler, D., Pierce, R., *Safety Engineering - a Perspective on Systems Engineering, Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 115.

У зависности од циљева организације можемо разликовати безбедносни менаџмент у организацијама којима је пружање безбедносних услуга другим корисницима основна мисија, од безбедносног менаџмента у организацијама које се баве привредним или друштвеним делатностима, а безбедносни менаџмент се налази у функцији очувања и раста организације. „Постоје и привредна предузећа која имају велики значај за безбедност заједнице у којој делују, било због значаја њихових производа и услуга за нормалан живот, уже или шире, заједнице било због опасних сила које садрже њихова постројења и чијим би се оштећењем изазвале велике катастрофе.“²⁰

Безбедносни изазови, ризици и претње у савременом свету су све сложенији, па је за успешну борбу против њих потребно да организације предузму што је могуће више прагматичан и систематичан приступ²¹. „Да би се заштитиле од неповољних утицаја, организације морају да размишљају о увођењу процеса који помаже да се управља ризицима и претњама, а који би обухватао техничке системе, финансијске и људске ресурсе.“²² То значи да безбедност мора да се посматра на интегрисан начин, што се постиже увођењем система безбедносног менаџмента.

Ставови организација према безбедносном менаџменту временом су се мењали упоредо са мењањем схватања појма безбедности, али „основни принципи који се односе на безбедност и процену ризика остају исти“²³. Од 60-тих година прошлог века долази до драстичне промене става према безбедности. Неки аутори сматрају да безбедност делимично добија на значају због неких геополитичких фактора, као што је нпр. завршетак „хладног рата“.²⁴ У новије време аутори су уочили да организације имају корист од увођења ефикасног система за управљање безбедношћу.²⁵ То је утицало и на обликовање структуре безбедносног менаџмента у

²⁰ Драгишић, З., исто.

²¹ Видети: Booz, A. H., *Convergence of Enterprise Security Organizations*, AESMR, 2005.

²² Canadian Aviation Regulations (CARs), Part I, Amendment 2007-2.

²³ Contos, B. T., et al., *Physical and Logical Security Convergence: Powered by Enterprise Security Management*, Elsevier Inc., Burlington, 2007., стр. 19.

²⁴ Видети: Kovacich, G. L., Halibozek, E. P., *The Managers Handbook for Corporate Security*, Butterworth Heinemann, Boston, 2003.

²⁵ Видети: Briggs, R., Edwards, C., *The Business of Resilience*, DEMOS, London, 2006.

организацијама, односно на обликовање различитих модела безбедносног менаџмента.

Према Феју „специфичности појединих организационих система утичу на конципирање и организовање безбедносног менаџмента у њима, али се у општем случају могу уочити поједина питања од којих зависи приступ безбедносним проблемима, као што је утицај на људе, имовину и друштво, затим последице које би настале у случају да се претња игнорише, да ли већ постоје нека решења која би могла успешно да одговоре на претње и сл.“²⁶

У савременим моделима, менаџери безбедности морају да у потпуности разумеју послове којима се организација бави и морају да познају и примењују управљачке функције. То значи да се њихово „знање шири на суштину производа и услуга које пружа организација“²⁷, а безбедносни менаџмент се посматра као процес који је интегрисан у остале функције организације. Самим тим се и безбедносни менаџмент помера ка врху управљања организацијом и представља основни сегмент у стратешком планирању. „Могућност укључивања безбедности у стратешко планирање је од великог значаја за обезбеђивање правилног приступа безбедносном менаџменту, јер се тиме допушта да менаџери доносе добре одлуке и спрече рањивост организације.“²⁸ У овим моделима је неизбежан тимски приступ проблемима, а доминира саветодавна улога менаџера безбедности, што подразумева блиску сарадњу свих пословних јединица са сектором безбедности.

Свака организација, у зависности од потреба и специфичности пословања, усваја неки од постојећих модела, њихову комбинацију, а често долази до развоја и преласка са једног модела на други. У последње време, у свету је систем безбедносног менаџмента, односно *Safety Management System* (SMS – у даљем тексту СБМ) најчешће заступљен модел.

За потребе овог рада, под појмом безбедносног менаџмента у организацији се подразумева систем безбедносног менаџмента (СБМ). Опредељење за овај модел се заснива на чињеници да он, организационо и функционално, одговара савременом

²⁶ Fay, J. J., исто, стр. 492.

²⁷ Dalton, D. R., исто, стр. 24.

²⁸ www.jha.ac/articles/a060.pdf

моделу безбедносног менаџмента, како га је дефинисао Далтон²⁹, односно обухвата фазе од планирања до контроле, које се у суштини своде на фазе процеса менаџмента у ужем смислу.

Да би се безбедносни менаџмент могао развијати, потребно је да делује како на оперативном, тако и на стратешком нивоу. На оперативном нивоу, развој безбедносног менаџмента се може видети у побољшању постојећих и промовисању имплементације нових безбедносних поступака, као и повратној вези са процесом планирања. „На стратешком нивоу, потребно је да се имплементирају одлуке, које обично укључују неколико позиција (политике, програме, финансирање итд.).“³⁰

Имајући у виду наведено, може се закључити колико су бројни захтеви које сви субјекти у организацији морају да испуне у погледу безбедности. На првом месту је захтев познавања и разумевања узрока, извора и врста савремених безбедносних изазова, ризика и претњи. На другом месту је изналажење организационих, функционалних, техничких и других решења која ће бити ефикасан одговор условима угрожавања организационих система, а у оквиру њих и угрожавања људи, материјалних и културних добара и животне средине. Осим тога, да би се утврдило колико је безбедносни менаџмент успешан у испуњавању задатака који се пред њега постављају, као и да би се пронашле и отклониле постојеће слабости у систему, потребно је пронаћи начин за мерење његове перформансе^{31,32}, пре свега за процену његове ефикасности и ефикасности³³. Ипак, треба напоменути да, иако је мерење перформанси важно за пословање, оно има другачији значај када су у питању

²⁹ Видети: Dalton, D. R., исто.

³⁰ www.jha.ac/articles/a060.pdf

³¹ Сам термин „перформанса“ је тешко дефинисати. Сматра се да организација има „добре перформансе“ уколико ефикасно примењује одговарајућу стратегију. - Abdel-Maksoud, A. B., Abdel-Kader, M. G., *Non-Financial Performance Measurement and Management Practices in Manufacturing Firms: A Comparative International Analysis*, Elsevier Ltd., Oxford, 2007., стр. 14.

³² Мерење перформансе представља менаџмент алат који има за циљ да пружи поуздане, релевантне, објективне и правовремене податке о организацији и њеном функционисању. Овако добијени подаци могу утицати на доношење одлука и јачање процеса управљања, што у крајњој линији побољшава перформансе организације. - Callahan, K., *Elements of Effective Governance: Measurement, Accountability and Participation*, Taylor & Francis Group, LLC., Boca Raton, 2007., стр. 23.

³³ „Потребно је тачно дефинисати шта је то што се жели проценити, да би се могло извршити мерење“ - Rossiter, J. R., *Measurement for the Social Sciences: the C-OAR-SE Method and Why It Must Replace Psychometrics*, Springer Science+Business Media, New York, 2011., стр. 44.

безбедност и заштита људског живота³⁴. Зато „неки аутори сматрају да треба више пажње посветити проактивном приступу, који подразумева увођење стандарда безбедности, строго поштовање законске регулативе, као и развијање безбедносне културе и климе“³⁵.

Ефективност и ефикасност су појмови који у себи садрже и повезују циљеве организације и ресурсе које она користи да би остварила своје циљеве.³⁶ Ови су појмови од суштинског значаја за одређивање успешности организације. „Основна мера за одређивање вредности коју нека организација ствара јесте однос уложеног капитала и суме ефективности улаза у оперативне активности и ефикасности њихових излаза.“³⁷ Ефективност у ширем смислу, представља способност организације да прибави неопходне ресурсе и да их што боље искористи ради остварења својих циљева. Уже схваћена, „ефективност се односи на степен остварења циљева организације“³⁸. Односно, ефективност значи „радити праве ствари“³⁹. Ефикасност организације изражава делотворност организације у обављању основних процеса. Она се изражава „односом резултата функционисања организације и улагања која су неопходна да се ти резултати остваре“⁴⁰. Просто речено, „ефикасност подразумева постизање резултата уз што мање трошкова“⁴¹. Јасно је да је ефикасност већа уколико се исти резултати постижу мањим улагањима. Може се рећи да ефикасност значи „радити ствари на прави начин“⁴². „Иако је ефикасност важна, ефективност ипак мора бити на првом месту.“⁴³ Аналогно, ефективност и

³⁴ Видети: Ericsson, K. A., *Development of Professional Expertise: Towards Measurement of Expert Performance and Design of Optimal Learning Environments*, Cambridge University Press, New York, 2009.

³⁵ Rowlinson, S., An Overview of Safety Management Systems, *Construction Safety Management Systems*, Spon Press, London, 2004., pp. 82-88.

³⁶ Видети: www.adizes.co.rs/

³⁷ Garratt, B., *Thin on Top: Why Corporate Governance Matters and How to Measure and Improve Board Performance*, Nicholas Braely Publishing, London, 2003., стр. 147.

³⁸ Живковић, М., *Економика пословања*, 6. издање, Мегатренд универзитет, Београд, 2006., стр. 229.

³⁹ <http://www.smartinsights.com/goal-setting-evaluation/goals-kpis/definition-efficiency-and-effectiveness/>

⁴⁰ Ramanathan, R., *An Introduction to Data Envelopment Analysis: A Tool for Performance Measurement*, Sage Publications India Pvt Ltd., New Delhi, 2003., стр. 26.

⁴¹ Tiller, J. S., *Adaptive Security Management Architecture*, Taylor & Francis Group, Boca Raton, 2011. стр. 23.

⁴² <http://www.smartinsights.com/goal-setting-evaluation/goals-kpis/definition-efficiency-and-effectiveness/>

⁴³ Spitzer, D. R., *Transforming Performance Measurement: Rethinking the Way We Measure and Drive Organizational Success*, AMACOM, New York, 2007., стр. 71.

ефикасност система безбедносног менаџмента се могу користити за одређивање успешности овог система у остваривању безбедносних циљева.

„Да би се могла извршити процена ефикасности и ефикасности система безбедносног менаџмента, потребно је да се о безбедности размишља на исти начин као и о осталим дисциплинама – као о активностима које се могу именовати и чија се успешност може мерити кључним индикаторима.“⁴⁴ Ови индикатори би требало да укључе мерила времена и новца, требало би да буду конзистентно мерени и да буду упоредиви између различитих организација, да би се олакшало сазнавање о најбољим начинима за примену постојећих решења, односно да би се могао спроводити *Benchmarking*⁴⁵.

1.2. Предмет истраживања

Претходна разматрања проблема истраживања захтевају да се изврши дефинисање предмета истраживања. Предмет истраживања се односи на могућности организационих система да измере утицај безбедносног менаџмента на безбедносне изазове, ризике и претње, односно да процене ефикасност и ефикасност система безбедносног менаџмента, као и на могућности предузећа у Републици Србији да организационо и функционално успоставе систем за процену ефикасности и ефикасности безбедносног менаџмента. Предмет истраживања тематски припада наукама менаџмента, заштите, безбедности и одбране. Посматрано у ширем контексту предмет истраживања припада већем броју научних дисциплина (правним, социолошким, организационим, економским и сл.) и као такав има интердисциплинарни карактер.

С обзиром на карактер овог рада, безбедносни менаџмент се посматра као део укупног управљачког процеса предузећа, који обухвата следеће функције:

⁴⁴ Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007., стр. 20.

⁴⁵ *Benchmarking* је континуиран процес идентификације, схватања и прилагођавања производа и услуга у циљу побољшања пословања, а који укључује упоређивање организације и њених делова са најбољима, упоређивање активности организације, производа и услуга, технолошких решења, примену најбоље дефинисаних пословних процеса, планирање будућег развоја и испуњавање захтева клијената и купаца (Harrington, H.J. Harrington, J.S., *High Performance Benchmarking: 20 steps to success*, McGraw-Hill, New York, 1996., стр. 15.).

планирање, организовање, командовање, координацију и контролу. Осим тога, потребно је нагласити да се усваја холистички приступ безбедносном менаџменту, односно систем безбедносног менаџмента представља систем који штити организацију од већине безбедносних изазова, ризика и претњи, било да оне долазе из окружења или из саме организације.

Под ефективношћу безбедносног менаџмента треба подразумевати способност система да задовољи безбедносне потребе организације, и то како краткорочне, тако и дугорочне. Безбедносне потребе се исказују достигнутим стандардима безбедности, безбедним условима у којима организација функционише, односно спречавањем испољавања безбедносних изазова, ризика и претњи и сл. Ефикасност система безбедносног менаџмента се односи на то да се до циља долази што је могуће мањим улагањима. Потреба за ефикасношћу система безбедносног менаџмента условљава његово стално усавршавање и развој у складу са захтевима и могућностима организације, напретком науке, технике и технологије, али и његову флексибилност, односно еластичност, због непрестаних промена безбедносних изазова, ризика и претњи. Као што је рекао Рајхелд: „Мерни систем ствара основу за ефикасан менаџмент“⁴⁶. Да би се могло одредити колико је неки систем ефикасан и ефикасан, потребно је дефинисати мерљиве индикаторе за процену његове ефикасности и ефикасности, а онда и извршити мерење⁴⁷.

Међутим, индикатори за процену система безбедносног менаџмента, сами по себи, не говоре много. Зато се у предмету истраживања посебна пажња посветила начину на који треба приказати добијене мерне резултате. Показало се да је за приказ успешности пословања, једно од најбољих средстава заправо Балансирана листа мерила (*Balanced Scorecard*). Суштина овог менаџмент „алата“ је у томе што даје увид у пословање из више перспектива, а не само финансијске⁴⁸. Односно, „користи

⁴⁶ Reichheld, F., *The Loyalty Effect*, Harvard Business School Press, Boston, 2001., стр. 246.

⁴⁷ „Мерење у подразумева додељивање бројчане вредности особини неког објекта или догађаја према неком установљеном правилу, са циљем да се добију поуздане информације о том објекту или догађају.“ - Boumans, M., *Measurement in Economics: A Handbook*, Elsevier Inc., Burlington, 2007., стр. 3.

⁴⁸ Како тврди Епштајн, један од основних изазова савременог пословања јесте да се симултано управља социјалним и финансијским питањима, као и утицајем на животну средину, зато што су ови циљеви у великој мери супротстављени. Видети: Epstein, M. J., *The Challenges of Simultaneously*

скуп мерила која омогућавају свим запосленим и менаџменту да се усредсреде на основне циљеве организације, да се увиде кључни процеси у организацији, као и да се оствари веза између стратегије, пословног плана и активности запослених.⁴⁹ Балансирана листа мерила је *балансирана* јер дели мерила активности организације или индикаторе у четири примарне *перспективе*: финансије, клијенти, унутрашњи пословни процес и учење и раст. Сматра се да ове четири области, када се посматрају заједно, дају јаснији портрет организације.⁵⁰ Будући да се безбедносни менаџмент посматра као саставни део укупног пословања, јасно је да је аналогно могуће направити и специфичну листу, односно Балансирану листу безбедносних мерила (*Security Balanced Scorecard*). Оваква листа би приказала индикаторе безбедности и њихове међусобне везе, али и утицај на укупно пословање, и то на јасан и концизан начин. Тиме би се омогућио бољи увид у систем безбедносног менаџмента, али и упоређивање овог система између различитих организационих система⁵¹.

1.2.1. Операционално одређење предмета истраживања

Предмет истраживања биће реализован кроз следеће сегменте истраживања:

Први, који представља приказ система безбедносног менаџмента и проблема који су повезани са његовом проценом у системима, као актуелних проблема у савременом свету. Анализом ће се сагледати следећа питања: преглед дефинисања и схватања безбедносног менаџмента, његових задатака, функција, ефикасности и ефикасности, мерљивих индикатора и атрибута, позиционирање у организационим системима, међународно-правни оквир и национална регулатива у развијеним земљама.

Improving Social and Financial Performances: New Research Results, *Performance Measurement and Management Control: Inovative Concepts and Practices*, Emerald Group Publishing Ltd., Bingley, 2010., pp. 9-18.

⁴⁹ Wade, D., Recardo, R., *Corporate Performance Management: how to build a better organization through measurement-driven strategic alignment*, Butterworth-Heinemann, Woburn, 2001., стр. 5, 6.

⁵⁰ Неки теоретичари сматрају да балансирана листа мерила не може бити идеално решење за примену у пракси, будући да су индикатори у њој у великој мери неповезани, чак некад између њих постоји негативна корелација. - Meyer, M. W., *Rethinking Performance Measurement: Beyond Balanced Scorecard*, Cambridge University Press, New York, 2003., стр. 2.

⁵¹ Између осталих, као моћно средство за упоређивање, издваја се *Benchmarking*. Детаљније: Османагић Беденик, Н., Ивезић, В., Бенчмаркинг као инструмент савременог контролинга, *Зборник економског факултета у Загребу*, година 4, Загреб, 2006., стр. 331-346.

Други сегмент предмета истраживања се односи на дефинисање и анализу проблема који се односе на процену ефективности и ефикасности безбедносног менаџмента у организацијама. Таква анализа ће обухватити и актуелне моделе који се користе за процену ефективности и ефикасности безбедносних активности, постојећих и предложених стандарда безбедности у различитим областима, са покушајем уопштавања проблема. Посебна пажња у овом делу биће посвећена развоју Балансиране листе безбедносних мерила, као начина за евалуацију и упоређивање система безбедносног менаџмента између више организационих система.

Трећи сегмент се односи на истраживање стања и проблема у овој области у Републици Србији. Посебно ће се анализирати нормативно-правни проблеми, организациони и функционални проблеми, као и подаци који се односе на начин конципирања и процене ефективности и ефикасности безбедносног менаџмента у организацијама у нашој земљи.

Четврти сегмент се односи на конципирање и представљање могућег новог модела за процену ефективности и ефикасности безбедносног менаџмента, који би, са мањим преправкама, био примењив у већини организационих система, независно од привредне гране у којој се она налазе. Овим се покушава премостити јаз између недовољног поклањања пажње питањима безбедности и могућим начинима да безбедносни менаџмент добије заслужено место у укупном систему управљања, посебно у предузећима у Србији.

1.2.2. Временско и просторно одређење предмета истраживања

Предмет истраживања је наметнуо потребу изучавања безбедносног менаџмента у новијем периоду, односно у времену када се радикално мења безбедносна слика света и када се и ти системи функционално и институционално усмеравају ка мирнодопским опасностима.

Овакво временско одређење предмета истраживања у потпуности се односи и на проучавање стања безбедности у предузећима у нашој држави, њихове садашње и будуће орјентације.

У циљу добијања валидних резултата истраживања који су дефинисани проблемом и предметом истраживања теоријском анализом је обухваћен простор Републике Србије. У разматрању појединих индикатора изашло се из наведеног просторног оквира и у њега су укључени и други организациони системи за које је било могуће пронаћи отворене изворе који реално одсликавају стање безбедносног менаџмента.

1.2.3. Дисциплинарно одређење предмета истраживања

Предмет истраживања тематски припада наукама менаџмента, заштите, безбедности и одбране. Посматрано у ширем контексту предмет истраживања припада већем броју научних дисциплина (правним, социолошким, организационим, економским и сл.) и као такав има интердисциплинарни карактер.

1.3. Циљеви истраживања

Основни циљ овог истраживања односи се на истраживање могућности савремених организационих система да функционално одговоре на све изазове безбедности који се пред њих постављају. Резултати истраживања треба јасно да укажу на могуће правце развоја модела за процену ефикасности и ефикасности безбедносног менаџмента у организационим системима.

Научни циљ истраживања је да изврши научну дескрипцију (описивање) са елементима класификације и научну експланацију (објашњење) процеса евалуације система безбедносног менаџмента, у односу на његову организацију и могућност функционисања у условима спречавања и отклањања претњи одређеним системима. Научни циљ је такође употпунити теоријска сазнања о безбедносном менаџменту, стању, реалним могућностима система безбедносног менаџмента, као и о адекватности функција које он обавља у циљу ефикасне заштите система, запослених, клијената и животне средине.

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

– потпуније, реалније и објективније сагледају постојећи функционални и организациони аспекти безбедносног менаџмента и могућности процене његовог утицаја на спречавање угрожавања у организационим системима;

– предложи одређена практична решења у циљу доградње и развоја система за процену ефективности и ефикасности безбедносног менаџмента у појединим предузећима, при чему се морају уважити реалне потребе и могућности.

1.4. Хипотетички оквир истраживања

Садашњи ниво организованости и функционисања система за процену ефективности и ефикасности безбедносног менаџмента у организацијама у Републици Србији није адекватан потребама, односно не даје реалне резултате о утицају безбедносног менаџмента на превенцију и ублажавање последица угрожавања безбедности и заштиту организација, свих субјеката, животне средине и културних добара.

Посебне хипотезе које се могу извести су:

1. Нормативно-правни оквир о безбедносним стандардима није адекватно имплементиран, у смислу да стандарди безбедности нису добро дефинисани;

2. Индикатори безбедности нису добро дефинисани нити су у корелацији са процесом безбедносног менаџмента, а правила и процедуре за њихово мерење нису усклађени са стварним стањем у тој области;

3. Модели за процену ефективности безбедносних активности у организацијама у Републици Србији нису примењиви, односно нису прилагођени безбедносном менаџменту у њима;

4. Модели за процену ефикасности безбедносних активности у организацијама у Републици Србији нису примењиви, односно нису прилагођени безбедносном менаџменту у њима.

1.5. Начин истраживања

Начин истраживања као и избор метода истраживања условљени су дефинисаним проблемом истраживања, теоријским и операционализованим

предметом истраживања, дефинисаним циљевима и хипотезама истраживања. Због природе и сложености предмета, јасно је да је у првом реду коришћено анкетно истраживање, квалитативне (као што је анализа садржаја), али и неке квантитативне методе и технике, као што су стандардизовани упитник, скале процене, скале ставова и сл.

Ово истраживање има карактер комбинованог теоријско-емпиријског приступа. Имајући у виду комплексност проблема и предмета истраживања примењени су мултиметодски приступ и комплементарна анализа доступних извора података. У раду су комплементарно коришћене следеће методе истраживања: преглед научне и стручне литературе, анализа нормативноправне регулативе, метод анализе садржаја, метод испитивања (анкета и експертски интервју) и статистичке технике за обраду и приказивање добијених резултата. Упитник је електронским путем достављен на адресе привредних организација према списку Привредног Регистра Републике Србије. Где је и кад је било могуће, обављен је интервју са стручњацима за безбедност запосленим у већим привредним субјектима у Републици Србији.

У циљу свеобухватног сагледавања проблема примењене су различите методе истраживања, а подаци добијени коришћењем сваке од њих требало је да омогуће анализу различитих аспеката везаних за овај проблем, а који се односе на нормативне инструменте, техничке предуслове и могућности и друштвене потребе. С обзиром на примену различитих метода у овом истраживању, основни принцип који је примењиван је принцип триангулације. Применом принципа триангулације постиже се објективно и систематско сагледавање истраживаног проблема. Поштовање овог принципа омогућава проверу и употпуњавање података добијених различитим методским приступима, чиме се умањују евентуални недостаци у примени појединачних метода.

1.6. Научна и друштвена оправданост истраживања

Научна оправданост истраживања огледа се у проширивању и продубљивању знања везаних за предмет истраживања и уграђивање тих сазнања у теоријски фонд наука менаџмента, заштите и безбедности.

Намена рада је да изгради реалну слику стања у овој области и пружи смернице за тежак и компликован процес осмишљавања савременог и одрживог безбедносног менаџмента који ће, у организационом и функционалном смислу, обезбедити максималну координираност свих субјеката и остварити високу ефективност и ефикасност у спречавању и сузбијању последица појава угрожавања.

2. ПОЈМОВНО ОДРЕЂЕЊЕ БЕЗБЕДНОСНОГ МЕНАЏМЕНТА

Реч „менаџмент“ потиче од енглеске речи *manage*, што значи управљање предузећем или јавним подухватима.

Појава менаџмента се везује за далеку прошлост, али почетак његове шире примене се везује за период индустријализације. Тек је примена индустријских метода у производњи материјалних добара и појава веће конкуренције на тржишту, условила потребу за проналажењем и применом нових метода и техника које омогућују да се тај процес одвија што рационалније у циљу повећања профита.

Почетак индустријализације означио је и крупне политичке промене. Стварање великих националних држава, на супрот уситњених феудалних државица, условило је огромно повећање и усложњавање државног апарата. Држава постаје огромна организација, са великим бројем надлежности, које практично додирују, у мањој или већој мери, све области јавног и приватног живота. Таква организација је захтевала развој посебних метода и техника које би омогућиле ефикасно функционисање свих државних органа, што је условило развој менаџмента у јавном сектору.

Подела капиталистичког друштва на јавну и приватну сферу, нашла је свој израз и области менаџмента. Међутим, израз менаџмент углавном се користио за делатности везане за управљање предузећима, док се за управљање државним органима, нарочито војском и полицијом, много чешће употребљавао термин руковођење и командовање, као посебне функције менаџмента.

2.1. Појам безбедносног менаџмента

Менаџмент је дисциплина која може бити примењена на различите организације. Менаџмент примењен на предузеће представља менаџмент предузећа или пословни менаџмент, менаџмент примењен на образовне институције је менаџмент у образовању, менаџмент у полицији називамо полицијски менаџмент, менаџмент у јавним службама називамо јавни менаџмент и слично. Практично колико постоји врста организација толико може бити различитих дисциплина

менаџмента. То наравно не значи да је свако поље људске делатности на које се примењује менаџмент уједно и посебна научна дисциплина. Основни принципи науке менаџмента примењују се на све области људског рада, док се посебне методе и технике менаџмента примењују у свакој посебној организацији, у зависност од њене специфичности. Основни задатак менаџмента сваке организације је да повећа виталност организације, односно њену способност преживљавања у различитим околностима, уз просперитет и раст организације.

Појам „безбедносни менаџмент“ је релативно новијег датума, па можемо рећи да још увек не постоји коначна дефиниција. Дакле, сам појам овај појам је још увек у фази развоја. Међутим, можемо издвојити неке од дефиниција. Како тврди проф. Драгишић, „под појмом безбедносни менаџмент, у ширем смислу, подразумева се одлучивање о безбедносним циљевима организационог система, о начинима и средствима да се избегну неповољни утицаји који долазе из окружења или самог организационог система, или да се њихов штетан утицај умањи“.⁵² Како тврди Мекри, безбедносни менаџмент обухвата велики опсег послова и разликује се од предузећа до предузећа. Он обухвата „обезбеђење лица и имовине, надзорне и алармне системе, заштиту током преноса имовине и вредности“, али и „консултантске услуге, управљање ризиком, заштиту података, истраге и задатке везане за кадровске ресурсе“.⁵³ Према Тривану систем безбедносног менаџмента у предузећу, „поред физичке и техничке заштите лица, имовине и операција, мора да укључи у себе прикупљање података и процену ризика, заштиту од пожара, експлозија и акцидената, заштиту и безбедност на радном месту“⁵⁴, али и да ствара основу за доношење менаџерских одлука, обезбеђује приступ поверљивим информацијама за топ менаџмент и установљава процесе и процедуре за заштиту и безбедност података. Дакле, овај систем мора да „интегрише све аспекте безбедности и заштите“⁵⁵. Бороцић дефинише безбедносни менаџмент преко активности које он

⁵² Драгишић, З., исто, стр. 14.

⁵³ McCrie, R. D., *Security Operations Management*, Butterworth-Heinemann, Boston, 2001., стр. 24.

⁵⁴ Trivan, D., Corporate safety in the Republic of Serbia: overview and prospects, *Corporate security in dynamic global environment – challenges and risks*, Institute for Corporative Security Studies, Ljubljana, 2012., p. 227-236.

⁵⁵ Исто.

обухвата: „безбедносни менаџмент обухвата управљање безбедношћу и здрављем на радном месту, ревизије, управљање кризама и планирање за ванредне ситуације, видео надзор, узнемиравање на радном месту и мобинг, праћење запослених, набавка опреме и људи за физичко обезбеђење, заправо све оно што може утицати на функционисање организације, њену профитабилност или виталност.“⁵⁶

У организацијама које се баве пружањем безбедносних услуга другим корисницима, а то су, пре свега, државне безбедносне службе, безбедносни менаџмент представља основни, али не и једини, облик менаџмента пошто такве организације обављају и читав низ других функција (финансијске, планске, кадровске, развојне и др.). Слична је ситуација и приватним предузећима која пружају услуге безбедности другим организацијама. Менаџмент таквих предузећа мора да води рачуна и опстанку таквог предузећа на тржишту, његовом развоју и расту, ризицима, изазовима и претњама са којима се таква предузећа срећу на тржишту, што заправо чини класичан безбедносни менаџмент сваког привредног предузећа. Поред тога, у зависности који ниво услуга предузеће пружа, менаџери тих предузећа учествују у креирању одлука везаних за безбедност у другим организацијама, што их, на посредан начин, чини безбедносним менаџерима других организација. Место безбедносног менаџмента у свакој организацији одређено је његовом функцијом и задатком. Основна функције безбедносног менаџмента су процењивање актуелних и потенцијалних безбедносних претњи, изазова и ризика, предузимање мера ради отклањања опасности, успостављање организације која ће бити способна да заштити предузеће, или другу организацију, од свих облика угрожавања, да контролише спровођење безбедносних мера и функционисање система безбедности, да пружа одговарајуће информације топ менаџменту, или политичком руководству, да израђује безбедносне анализе у циљу опстанка и раста организације и пружања пуне сигурности свим запосленима.⁵⁷ Основни циљеви безбедносног менаџмента сваке организације су повећање контролабилности и флексибилности организације, као важних елемената њене виталности.

⁵⁶ Borodzicz, E. P., исто, стр. 50.

⁵⁷ Видети: Драгишић, З., исто, стр. 15.

Флексибилност организације је директно зависна од брзине добијања информација и она представља способност организације да благовремено и са минимумом губитака избегне опасности, док контролабилност представља способност организације да предвиђа могуће изворе угрожавања и властите могућности да на угрожавања адекватно одговори.

Полазиште за безбедносни менаџмент сваке организације представљају циљеви које је та организација поставила пре себе. Безбедносни менаџмент увек мора да се налази у функцији достизања и очувања вредност које су интересне групе које воде неку организацију дефинисале као циљеве организације. Природно је да се циљеви организације повремено преиспитују и мењају. Промена циљева се веома често дешава управо под утицајем безбедносног менаџмента, због промена у окружењу које чине да се неки циљеви не могу постићи, или се не могу постићи без значајних губитака, што доводи до одлуке топ менаџмента да се од неког циља одустане или да се он замени другим циљем. Стратешки циљеви организације се веома ретко мењају и они, у правилу, доводе до крупних промена у стратегији организације, док се промене на тактичком и оперативном нивоу дешавају знатно чешће и без значајнијих промена стратегије организације.

Задатак безбедносног менаџмента је заштита виталних вредност организације, унапређивање и развој организације и достизање њених циљева. Безбедносни менаџмент не доноси стратешке одлуке, али значајном утиче на њихово доношење тако што топ менаџменту обезбеђује информације и процене на основу којих се дефинишу стратешки циљеви и доносе оперативне одлуке од којих, у крајњој линији, зависи опстанак и развој организације. Један од главних циљева безбедносног менаџмента је успостављање и очување организације која треба да пружи максималну безбедност пословања, остваривање циљева организације, безбедност запосленима и очува безбедност средине у којој се обавља пословање. Организација је и главна последица менаџмента, по начину на који је нека организација устројена и по њеном функционисању можемо много закључити о квалитету менаџмента.

Безбедносни менаџмент може се поделити на безбедносни менаџмент јавног сектора и безбедносни менаџмент приватног сектора. У безбедносни менаџмент

јавног сектора спадају активности парламента, владе, шефа државе, судства, војске, полиције, обавештајно-безбедносних служби, локалне самоуправе и других државних органа на унапређењу безбедности заједнице и одговора безбедносним ризицима, изазовима и претњама кроз успостављање организације, планирања, руковођења и контроле над пословима и организацијама чији је циљ пружање безбедности заједници. Безбедносни менаџмент приватног сектора у првом реду обухвата менаџмент активности привредних и других предузећа на заштити властитог пословања и запослених. У оквиру приватног безбедносног менаџмента спадају и активности приватних предузећа која пружају услуге безбедности и различити облици самозаштите коју организују грађани ради властите безбедности.

Америчко Удружење за Индустријску Безбедност (*The American Society for Industrial Security - ASIS*) је дошло до закључка да у савременом свету организације морају да се прилагођавају ризицима путем тзв. „конвергенције“ безбедности. Они овај процес сматрају глобалним трендом, а дефинишу га као: „идентификовање безбедносних ризика и међузависности између пословних функција и процеса унутар предузећа и развијање пословних решења којима се може управљати, а који служе као одговор на уочене ризике и међузависности“⁵⁸. Ова дефиниција јасно указује на то да безбедност више није само функционална активност, већ представља „додату вредност“ укупној пословној мисији.

Међутим, сложеност овог појма се може схватити путем увида у саме историјске околности које су довеле до потребе његовог дефинисања.

2.2. Историјски развој безбедносног менаџмента

Историјски посматрано, менаџмент је настао у веома далекој прошлости и везао се за способност да се са што мањим улагањима остваре што бољи резултати. Неке облике управљања организацијама које данас називамо „менаџмент“, налазимо још код старих цивилизација. Изградња великих објеката, организација пољопривредне производње, уређење државних послова, али и припреме за вођење ратова и одбрану од освајача, подразумевали су организовање, планирање,

⁵⁸ Booz, A. H., исто, стр. 2.

руковођење и контролу. Успешност руководиоца на свим нивоима организовања старих друштава била је пресудан фактор који је омогућавао опстанак и раст цивилизација.

Безбедносни менаџмент још увек није конституисан као посебна научна дисциплина, мада се све више изучава као наставни предмет и постоји вишевековна пракса примене различитих метода у организацији, руковођењу и командовању, планирању и контроли организација које су се бавиле питањима безбедности. Од настанка првих држава питања вођења војски, које су кроз дуги историјски период биле и једине организације које су се бавиле питањима безбедности, њихове организације, руковођења војском у рату и миру, решавање питања снабдевања и обуке војске и друга питања везана за војску била су у центру пажње свих владара тога времена. Искуства која су стицана у управљању, руковођењу и командовању војском временом су се преносила и на друге организације, а од 20. века почело је и њихово теоријско уобличавање. Један од првих теоретичара који је то уочио и експлицитно указао је Фајол. Он је у својој књизи „Опште и индустријско управљање” из 1916. године, поделио пословање предузећа на шест пословних функција: техничку, комерцијалну, финансијску, безбедносну, рачуноводствену и административну. „Издвајање безбедности као посебне пословне функције предузећа, поставило је темеље проучавању безбедносног менаџмента, и увођењу посебних организационих целина у предузећа која се баве заштитом пословања“.⁵⁹ Теорије организације, представљају главни теоријски извор који безбедносни менаџмент преузима из наука менаџмента, док науке безбедности дају основни теоријски концепт на коме се заснивају сва истраживања и пракса безбедносног менаџмента. Многи теоретичари организације и менаџмента су дали допринос развоју безбедносног менаџмента. Тако се нпр. Веберова теорија бирократије може применити у бирократизованим безбедносним организацијама, као што су војска и полиција, док се кибернетски модел управљања примењује у безбедносном

⁵⁹ Драгишић, З., исто, стр. 30.

менаџменту многих предузећа⁶⁰. Данас, менаџмент сваке организације посебну пажњу поклања безбедности као основном услову опстанка и просперитета.

Различите организације имају различите безбедносне изазове, ризике и претње, па се тако ризици којима је изложена држава као организација у великој мери разликују од изазова којима је изложено привредно предузеће или културна установа. Различити изазови, ризици и претње којима је изложена нека организација, као и одговорности које организација има према окружењу у погледу безбедности, пресудно утичу на безбедносни менаџмент, односно начин на који ће бити донете одлуке везане за безбедност. Место безбедносног менаџмента у организацији је у првом реду одређено схватањем појма безбедности у ширем и ужем окружењу, као и од односа организације према изазовима, ризицима и претњама са којима се суочава.

Ставови организација према безбедносном менаџменту временом су се мењали упоредо са мењањем схватања појма безбедности. Од 60-тих година прошлог века долази до драстичне промене става према безбедности. То је утицало и на обликовање структуре безбедносног менаџмента у организацијама, односно на обликовање различитих модела безбедносног менаџмента. У складу са тим, Далтон⁶¹ разликује следеће моделе:

- Пре 60-тих година прошлог века, безбедносни менаџмент се сводио на улогу коју има ноћни чувар. У оваквом систему првенствена дужност чувара је да служи као очи и уши организације. Основни задатак се сводио на заштиту од пожара. Чак и данас пожар остаје главна претња за имовину;

- До краја друге половине XX века, улога безбедности у организацијама се проширила. Иако је дошло до промена у области безбедности, велики број организација безбедносни менаџмент укључује у сектор одржавања. Међутим, већина организација прихвата ширу улогу безбедносног менаџмента, укључујући послове физичког обезбеђења. У овом контексту, послови безбедносног менаџмента обухватају и реаговање на медицинске хитне случајеве, контролу саобраћаја, пратњу запослених и послове рецепције. Овакав модел организовања безбедносног

⁶⁰ Више о утицају теорија организације и менаџмента на безбедносни менаџмент видети: Драгишић, З., исто.

⁶¹ Видети: Dalton, D. R., исто, стр. 21.

менаџмента је увођен у организације према потребама, па се у складу са њима и ширила сама његова улога. „Главни задатак безбедносног менаџмента је да осигура да опрема и процеси остану продуктивни“.⁶² Овај операционални модел и данас представља једну од највећих пословних јединица коју допуњује униформисано особље у матичној организацији или се за те услуге ангажује трећа страна. Спроводе се истраживања, али се у суштини своде на прекршаје које чине запослени или ситне крађе;

- У једном кратком периоду постало је популарно да се „безбедност“ означава термином „спречавање губитака“.⁶³ Овај термин се и даље користи у сектору малопродаје. Намера оваквог термина је да се покуша да се безбедности да значај нечега што доприноси повећању вредности⁶⁴. То је допринело да остале категорије запослених и менаџера јасније сагледају улогу безбедносног менаџмента. Тек тада је безбедносном менаџменту пружена прилика да учествује у проактивним иницијативама. Од тада је почело развијање програма за повећање свести запослених у погледу безбедности;

- Временом су почели да се развијају многи иновативни приступи безбедносном менаџменту. Један од модела се односи на организовање безбедносног менаџмента као „центра за профит и губитак“⁶⁵. Углавном је овакав начин организовања промашај, јер се ретко дешава да менаџер безбедности има искуство у вођењу послова, с обзиром да је његов примарни задатак да управља одељењем које се односи на безбедност;

- Други модел се односи на додавање задатака попут достављање поште, слање и примање пошиљака, услуге достављања хране, сигурности итд.;

- Један од начина конципирања безбедносног менаџмента се односи на проширење одговорности на истраживање осетљивијих инцидената повезаних са безбедношћу. „Улога безбедности је од кључне важности за опстанак предузећа, тако

⁶² Caralli, R. A., Wilson, W. R., *The Challenges of Security Management*, Networked Systems Survivability Program, Software Engineering Institute, www.cert.org/archive/pdf/ESMchallenges.

⁶³ Dalton, D. R., исто, стр. 21.

⁶⁴ Безбеднија организација је стабилнија, а самим тим и њена вредност на тржишту расте. О томе детаљније: Graham, B., Dodd, D. L., *Security Analysis*, 6th ed., McGraw Hill Inc., New York, 2009.

⁶⁵ Dalton, D. R., исто, стр. 22.

да је најбољи начин организовања онај у коме организација штити саму себе, али многе организације не могу да приуште велике издатке за безбедносни менаџмент“.⁶⁶ У овим моделима се задржала улога заштите руководиоца и систем инжењеринг у домену безбедности, тако да је безбедносни менаџмент заиста постао прави ентитет у оквиру организације. Међутим, хијерархија односа у погледу извештавања у овом моделу остаје непромењена;

- Временом долази до промене у пословању и заоштрава се трка са конкуренцијом, па и организације морају да рedefинишу своје пословање. Тиме је безбедносни менаџмент дошао на дневни ред. Долази до промена не само у структури већ и у фундаменталном систему пружања услуга. Нови модел безбедносног менаџмента подразумева да у организацији постоји мала група стручњака за безбедност који пружају „консултантске и специјализоване услуге“⁶⁷. Ови унутрашњи консултантски тимови немају директну одговорност за униформисано обезбеђење. Функција се помера на управљање постројењима или некретнинама, као продужетак потпуне заштите имовине;

- Будући да се многе организације све више окрећу глобалном пословању, долази до развоја још једног модела безбедносног менаџмента, односно до тзв. „глобалне безбедности“⁶⁸. Менаџери безбедности у овом моделу имају консултантску улогу, односно дају савете крајњим потрошачима, унутрашњим партнерима, по питању користи које се могу имати или ризика који се могу избећи уколико се прате одобрене стратегије безбедности. Они се приклањају експертизи спољних партнера и схватају да се њихов допринос вредности дефинише у смислу онога што се назива „најбоља пословна пракса“. Највећа разлика између овог и других модела је у могућности да се менаџери безбедности првенствено посматрају као пословни менаџери. Заштита имовине не мора да се намеће пословним операцијама, већ се посматра као процес који доприноси повећању вредности

⁶⁶ Caralli, R. A., Wilson, W. R., исто.

⁶⁷ Dalton, D. R., исто.

⁶⁸ Исто.

пословања у складу са принципима управљања на основу вредности⁶⁹. Штавише, „постоји равнотежа између ресурса, одређивања стручних тимова и технологије и начина деловања“⁷⁰. Овај модел је изграђен на сарадњи са унутрашњим партнерима, а не на такмичењу са њима. Са аспекта пружања услуга, овај модел задржава неке одговорности по питању безбедности. На пример, истраживање остаје као функција, али се нагласак ставља на префињенија и осетљивија питања. Често се задржавају послови безбедности, с тим што се више пажње поклања развијању стандарда и обезбеђењу провера квалитета овог система. Обезбеђење руководиоца остаје као одговорност, али се фокусира на развијање стандарда и политика и планирање догађаја;

Током последње деценије се почео развијати још један модел. У овом периоду долази до потпуног редефинисања безбедносног менаџмента. О њему се почиње размишљати на стратегијском нивоу, тако да се и циљеви безбедносног менаџмента усаглашавају са највишим циљевима организације.⁷¹ До сада је често долазило до промене термина којима се означавају функције менаџмента безбедности у различитим моделима, а да при том послови којима се менаџери баве нису суштински другачији. То доводи до конфузије. Међутим, овом проблему се додаје и недостатак јасно дефинисаног безбедносног програма који одражава искључиву оријентацију на заштиту имовине. Наиме, модел безбедносног менаџмента обухвата и заштиту неопипљиве имовине. Овај модел се може назвати „тотална заштита имовине“⁷². У осталим моделима се фокус првенствено ставља на физички опипљиву имовину. Укључивање одговорности за неопипљиву имовину подразумева сарадњу са осталим пословним јединицама по питањима интелектуалне својине, конкурентске обавештајне службе и осталих аспеката власништва и поверљивих информација. Нови модели почињу да обухватају и активно укључивање менаџера безбедности у

⁶⁹ Више: Yücesan, E., *Competitive Supply Chains: A Value-Based Management Perspective*, Palgrave Macmillan, Chippenham, 2007.

⁷⁰ Dalton, D. R., исто, стр. 23.

⁷¹ Видети: Davies, S. J., Hertig, C. A., *Security Supervision and Management*, 3rd edition, IFPO, Elsevier, Burlington, 2008.

⁷² Dalton, D. R., исто, стр. 23.

обликовање стратешког планирања⁷³ и развоја пословања. Истраживачка улога се шири на геополитичко предвиђање. То укључује и подршку у одлучивању приликом проширивања пословања и на нестабилна тржишта. Менаџери безбедности се укључују и у процесе који се тичу потенцијалних интеграција предузећа или набавки. Будући да организације шире асортиман својих услуга да би остале конкурентне, оне траже спољне партнере и савезе. Ово често подразумева развијање односа са приватним компанијама или неким страним организацијама. Овде је задатак безбедносног менаџмента да прибави све потребне информације да би се одредио интегритет руководства потенцијалних партнерских организација.

Савремене теорије о пројектовању организације респектују значај безбедности за успешност пословања, као посебне, али не изоловане функције менаџмента јер се потреба за безбедношћу налази у свим функцијама деловања једне организације. Управљање сваком од функција организације подразумева анализирање безбедносне угрожености дате функције и пројектовање мера ради отклањања безбедносне претње датој функцији организације. Безбедносни менаџмент посебних функција организације, уколико није реч о безбедносно посебно угроженим или значајним функцијама, инкорпориран је у општи оперативни менаџмент организационе јединице и представља део опште организационе и безбедносне културе. „На нивоу оперативног менаџмента, безбедносна функција инкорпорирана је у опште принципе деловања организације, и најчешће, се не издваја као посебна организациона целина, већ је спровођење безбедносних мера и процедура део операционализације стратешких планова топ менаџмента“.⁷⁴

2.3. Функције безбедносног менаџмента

Основне функције безбедносног менаџмента су: *планирање, организовање, руковођење и командовање (вођење), координација и контрола*. Функције безбедносног менаџмента одговарају функцијама менаџмента у другим гранама људске делатности. Наведених пет функција безбедносног менаџмента уједно

⁷³ Видети: Tyson, D., *Security Convergence – Managing Enterprise Security Risk*, Elsevier Inc., Burlington, 2007., стр. 202.

⁷⁴ Драгишић, З., исто, стр. 15.

представљају пет макро фаза у менаџмент процесу безбедности, било да је реч безбедносном менаџменту у јавном или приватном сектору. Наравно, свака функција безбедносног менаџмента има своје специфичности у зависности да ли се ради о јавном или приватном сектору, тако би било оправдано безбедносни менаџмент јавног и приватног сектора посматрати као две одвојене дисциплине. Међутим и оваква подела има значајна ограничења имајући у виду да се јавни и приватни интереси често преплићу и стичу у деловању једне организације.

2.3.1. Планирање као функција безбедносног менаџмента

Сваки менаџер и свака организација покушава да усмери своје понашање тако да у будућности произведе што више пожељних, што мање непожељних последица. Планирање представља један од начина да се то постигне. Оно потиче из потребе за сигурношћу и извесношћу, као једне од основних људских потреба. Планирање се базира на систематичном и континуираном размишљању о будућности пре него што се донесе одлука о деловању, уз покушај предвиђања последица које ће наше садашње деловање имати у будућности.

Планирање је суштинска фаза менаџмент процеса, а одговорност за планирање се дели између свих менаџерских нивоа. Планирање, најкраће речено, представља „формулисање циљева и начина њиховог остварења, које је у функцији креирања и прилагођавањем организационе структуре, стила руковођења и модела контроле“⁷⁵. Планирање се односи на избор циљева и начина њиховог остварења. Процес планирања резултира планским одлукама. Главна планска одлука су циљеви, док су остале одлуке у служби достизања дефинисаних циљева. Планске одлуке представљају основни оквир за менаџерски тим, а у односу на њих сваки менаџерски ниво, доноси властите планске одлуке.

Постоје две основне врсте планирања у безбедносном менаџменту: стратегијско планирање и оперативно планирање⁷⁶. Стратегијско планирање је у функцији остваривања мисије као разлога постојања организације и визије као

⁷⁵ Драгишић, З., исто, стр. 46.

⁷⁶ Видети: Тодоровић, Ј., Ђуричин, Д., Јаношевић, С.: *Стратегијски менаџмент*, Економски факултет, Београд, 2003., стр.53-83.

начина да се оствари мисија. Оперативно планирање конкретизује мисију и визију кроз оперативно вођење посла на дневном нивоу. Оперативно планирање се бави детаљима у границама дефинисаног оквира и прописивањем правила понашања. Оперативно планирање као резултат има две врсте планских одлука: једнократне планске одлуке и перманентне планске одлуке. Једнократне планске одлуке служе за прецизирање правца акције која је дефинисана стратешким одлукама и користи се за решавање тренутних безбедносних, или других, акутних проблема чије се понављање не очекује у будућности. Основни типови једнократних планских одлука које се користе у безбедносном менаџменту су програм и пројекат.⁷⁷ Перманентне планске одлуке се користе за артикулисање планских активности које се понављају у дужем временском периоду. Одређене појаве се јављају перманентно и са веома високим степеном предвидивости, па је рационално, ради скраћивања времена за доношење одлука и планирање донети планске одлуке које ће у дужем временском периоду покрити овакве појаве. Овакве одлуке могу довести до проблема ако дође до битнијих промена у безбедносним појавама на које се односе, због тога је веома важно да се ове одлуке у континуитету анализирају и прилагођавају променама које настају у окружењу на које се ове одлуке односе. Главне перманентне планске одлуке су: политике, процедуре и правила.⁷⁸

У процесу безбедносног планирања, као дела стратешког планирања, дефинишу се и стратегије организације и безбедносна политика, која представља резултанту планирања. Концепт стратешког планирања настао је 1970-тих година упоредо са појавом императива промена. Промене су неопходан услов опстанка и раста организација у савременим условима. Да би се плански ишло у сусрет променама неопходно је постојање стратегије у оквиру које ће се одредити могући одговори на изазове који организацију чекају у будућности. „Стратешко планирање потиче од државних организација које су вековима доносиле стратегије које су се

⁷⁷ У другим областима планирања у ову врсту одлука спада још и бизнис план, али се он у безбедносном менаџменту користи изузетно ретко, у оквиру бизнис плана већих организација, које безбедносне организације штите. Драгишић, З., исто, стр. 77.

⁷⁸ Више о томе: Драгишић, З., исто, стр. 78-80.

углавном односиле на вођење ратова“.⁷⁹ Стратешко планирање је процес у коме се дефинишу стратешки циљеви и бирају главни начини за њихово остварење. Главна планска одлука стратешког планирања је стратегија, која зависи од области друштвеног живота у коме се доноси. Постоје два различита гледишта о природи стратегије. Према првом, „стратегија је општи програм формулисања и остварења циљева како би се остварила мисија“⁸⁰. Према другом схватању, стратегија је модел одговора организације на окружење, другим речима свака организација успоставља односе са окружењем посредством стратегије. Такав поглед подразумева да свака организација има стратегију, без обзира да ли је она експлицитно формулисана и примењена. Оваква стратегија плод је реакције организације на окружење и она подразумева реактивну улогу менаџера, за разлику од првог приступа који менаџеру одређује проактивну улогу. Добро дефинисана стратегија мора обухватити оба аспекта, и мада је безбедносни менаџмент по својој суштини реактиван, проактиван приступ је неопходан ради антиципирања опасности и могућности да се опасности отклоне и преброде.⁸¹ Гари Деслер под стратешким менаџментом подразумева “процес идентификовања мисија организације у складу са унутрашњим капацитетима организације и захтевима који организацији долазе из окружења”⁸². Деслер стратешко планирање посматра кроз пет корака који су кључни за дефинисање стратегије. Први корак је дефинисање послова којима се организација бави и мисија које у том послу треба да оствари. Други важан корак у дефинисању стратегије је превођење мисије у стратешке циљеве. Веома је важно да се визије топ менаџмента операционализују кроз оперативне стратешке циљеве. Трећи корак је формулисање стратегије да се постигну стратешки циљеви. Четврти корак је примена стратегије. Примена подразумева да се стратегија преведе у акцију, а акција у резултат. И на крају пети корак је контрола, односно евалуација постигнутих циљева, односно процена напретка кроз остварење стратешких циљева и корективна акција, уколико је потребна. „Основни задатак менаџера безбедности је да у току процеса

⁷⁹ Драгишић, З., исто, стр. 80.

⁸⁰ Годоровић, Ј., Ђуричин, Д., Јаношевић, С.: исто, стр. 62.

⁸¹ Више о томе: Драгишић, З., исто, стр. 81.

⁸² Dessler, G., *Management, Leading Organizations in the 21st Century*, FIU, New Jersey, 2004., стр. 158.

израде стратегије намеће вредности и циљеве који се односе на безбедност пословања и да обезбеди што боље место у организацији за службе које се баве питањима безбедности, односно што боље позиције у буџету“.⁸³

У јавном безбедносном менаџменту стратешким планирањем се баве највиши органи државне власти. Резултат државног стратешког планирања су стратегије које се доносе у готово свим областима друштвеног и јавног живота у унутрашњој политици, међународним односима, привреди, образовању, друштвеном развоју и у области националне безбедности.

Планирање у свакој области менаџмента представља процес који се састоји од више међусобно повезаних фаза. Прва фаза у планирању је дефинисање циљева. Свако планирање мора поћи од одлуке шта се жели остварити у оквиру организације, или њеног дела. Прецизно дефинисање циљева спречава расипање ресурса, а идентификовање приоритета доводи до ефективне употребе ресурса. Менаџери безбедности у приватним организацијама најчешће добијају готове циљеве организације, које дефинише топ менаџмент, а од њих се очекује да омогуће безбедно спровођење циљева. У јавном сектору, као што је војска, полиција или обавештајно-безбедносне службе циљеви који се постављају руководиоцима свих нивоа представљају део државне политике, на коју руководиоци ових органа немају утицај.

Менаџери безбедности у приватним организацијама треба да оцене кризни потенцијал циљева које пред организацију поставља топ менаџмент, и да уколико су покушаји остваривања тих циљева угрожени неком врстом ризика, о томе известе топ менаџмент. Покушај остварења неких циљева може изазвати безбедносне проблеме који се према вероватноћи догађања могу кретати од мало вероватних до извесних, а према интензитету угрожавања од незнатних до катастрофалних. Задатак безбедносног менаџмента је да процени кризни потенцијал циља и предложи прихватање циља, његову супституцију или одустајање од циља, у зависности од вероватноће неповољних догађаја и процењеног интензитета ризика.

⁸³ Драгишић, З., исто, стр. 82.

У приватним организацијама циљеве безбедности често дефинишу сами менаџери безбедности, у оквиру основних циљева организације. Безбедносни циљеви се увек односе на неко стање безбедности, које се може изразити квантитативним величинама. Као циљ се може поставити потпуно спречавање неповољних безбедносних догађаја нулте толеранције, и одржавање у прихватљивим границама толеранције свих осталих неповољних догађаја. Без правилно одабраних циљева, не могу се дефинисати ни друге планске одлуке које доприносе реализацији циљева.

Када се дефинишу циљеви, следи израда безбедносне процене. То је основни корак у планирању безбедносних мера и постављању организационе структуре која треба да спроведе прописане безбедносне мере и поступке. Безбедносна процена треба да да одговоре на следећа питања: Који су главни безбедносни изазови, ризици и претње заједници или организацији која је предмет заштите?; Каква је природа конкретних безбедносних изазова, ризика и претњи и како би се они могли испољити у процењиваном временском периоду?; Ко су носиоци безбедносног угрожавања, ко су њихови савезници а ко противници?; Какве су политичке, кадровске, организационе, техничко-технолошке и финансијске могућности организације да се супротстави угрожавању?. Одговори на ова питања дају слику безбедносне ситуације и указују на главне безбедносне проблеме, због чијег решења се прописују безбедносне мере и процедуре и доносе безбедносни планови. Од квалитета безбедносне процене зависи квалитет целокупног система безбедности, јер је она основни путоказ за обликовање организације и за све остале мере које се касније предузимају.

Према врсти организације на коју се односе безбедносне процене могу бити јавне или приватне. Према домаћају безбедносне процене могу бити опште, посебне и *ad hoc* процене. Опште јавне безбедносне процене се односе на укупну процену стања безбедност на једном подручју у одређеном времену. Опште јавне безбедносне процене се према територији на коју се односе могу поделити на међународне - глобалне и регионалне и националне безбедносне процене. Општа приватна безбедносна процена односи се на укупно безбедносно стање организације која се штити. Опште јавне безбедносне процене доносе се од стране политичких органа,

међународних или националних. Опште националне безбедносне процене најчешће су интегрални део стратегијско-доктринарних докумената које доноси највиша државна власт, најчешће парламент. Стратегије националне безбедности имају обавезујући карактер за све нивое јавног безбедносног менаџмента, а безбедносне процене које се налазе у тим документима, представљају полазну основу за израду посебних безбедносних процена и свих планских одлука из области безбедности.

Посебне безбедносне процене доносе се за одређене области рада или одређене уже територије. Посебне јавне безбедносне процене доносе поједина министарства, за ресоре који су им поверени, или за само једну област из ресора. Рецимо, министарство унутрашњих послова доноси безбедносне процене за све области које се налазе у надлежности тог министарства. Посебне безбедносне процене могу се односити само на стање безбедности јавног саобраћаја, криминал, или само поједина кривична дела, на стање безбедности у заштити од пожара и сл. Посебна јавна безбедносна процена може се односити и на поједине територијалне области државе. Посебне приватне безбедносне процене односе се на одређене области рада организације која се штити. На пример у некој фабрици може се посебно доносити процена угрожености производње, маркетинга или сектора развоја. Поред тога посебна безбедносна процена може се односити и на поједине врсте угрожавања, као што су рецимо крађе, саботаже или продори конкуренције. *Ad hoc* безбедносне процене односе се на поједине конкретне догађаје, најчешће их доносе нижи руководиоци, и то су на пример процене које доноси полицијски старешина у вези са обезбеђењем неког скупа, хапшењем неког лица за које се претпоставља да може бити опасно или менаџер безбедности у вези са изненадним безбедносним догађајем, као што је непланиран пренос новца или друге драгоцености, па је потребно на лицу места брзо проценити ситуацију пре него што се донесе одлука. Овакве безбедносне процене често се саопштавају у „усменој форми“⁸⁴. Приликом израде безбедносне процене треба обезбедити јединствен методолошки приступ у оцени стања безбедности и изради безбедносне процене. Међутим, јасно је да јединствене методолошке поставке није могуће обезбедити на националном нивоу, пошто постоји велики број субјеката

⁸⁴ Исто, стр. 48.

који доносе безбедносне процене и планове безбедности, али је веома важно да различити нивои менаџмента, и вертикално и хоризонтално, у оквиру једне организације врше процене на јединствен начин. Јединственост методологије израде безбедносне процене огледа се у факторима које је сваки менаџер, или група, дужна да оцени приликом израде безбедносне процене. У квалитативном погледу, процена сваког од наведених фактора ствар је талента и искуства менаџера који врше процене, и само време и догађаји на које се процена односи могу да дају релевантну оцену квалитета процене. „Државне организације које доносе процене безбедности углавном прописују методологију израде процене, и обавезну структуру које се морају придржавати сви који раде на изради безбедносне процене.“⁸⁵ Иако су методологије за израду безбедносне процене у суштини различите, свака безбедносна процена мора да садржи безбедносне задатке за све организационе јединице једне организације или субјекте шире или уже друштвене заједнице. Безбедносни задаци које садржи безбедносна процена представљају само подручја рада која се у области безбедности одређују свакој организационој јединици неке организације у зависности од природе њене основне делатности и природе безбедносних ризика изазова и претњи тој организацији. Безбедносни задаци се кроз планове безбедности конкретно разрађују и најчешће се прописују као „систем безбедносних мера и процедура које се стављају у одговорност свакој организационој јединици“⁸⁶.

У оквиру фазе планирања, један од основних корака представља и процена ризика. Управљање ризиком се пре свега односи на анализу ризика. Процес анализе ризика омогућава да се: изврши идентификација имовине коју треба заштити, одреде претње које могу довести до губитка имовине, процени вероватноћа да дође до претње, процени утицај претње, фреквенција дешавања и могућности за управљање претњом, као и да се утврде контрамере претњи.⁸⁷ Основни циљ процене ризика јесте да се процене потенцијални губици и да се на време предузму акције да се ти губици избегну или умање. Тај процес подразумева примену различитих техника.

⁸⁵ Исто, стр. 49.

⁸⁶ Исто, стр. 52.

⁸⁷ Више о томе: Фау, Ј. Ј., исто.

Следећа фаза у оквиру планирања је доношење одлуке. Процес доношења одлуке је мисаони процес који укључује знање, искуство, рационално промишљање конкретне безбедносне ситуације, али и интуицију и инстинктивно реаговање менаџера, нарочито у кризним ситуацијама праћеним великим степеном неизвесности и мањком информација. Квалитет донете одлуке, брзина којом се одлуке доносе и начин на који се одлуке спроводе од изузетне је важности за успех сваке организације. Према речима Френка Харисона „Успешне организације побеђују своје противнике на најмање три начина: Они доносе боље одлуке; Они одлуке доносе брже; и Они више и боље примењују одлуке које су донели.”⁸⁸. Сви нивои менаџмента топ, средњи или најнижи ниво менаџмента, свакодневно доносе велики број одлука које немају исти ниво важности. Најважније одлуке доноси топ менаџмент и оне су, по правилу, од виталног значаја за дугорочну стратегију организације и избори које направи топ менаџмент пресудно утичу на судбину организације. Одлуке које доноси средњи ниво менаџмента углавном су концентрисане на управљање најважнијим административним центрима организације. Менаџери рутинске одлуке доносе у оквиру процеса који се одвија на системски начин са јасно дефинисаним елементима и компетенцијама сваког нивоа менаџмента. Процес доношења рутинских одлука нарочито јасно је дефинисан у државним безбедносним службама, као што су војска и полиција. Доношење одлука у војсци веома јасно је дефинисано, и сваки старешина има право да доноси одлуке у складу са местом које заузима на хијерархијској лествици. “У сваком послу се одлучујемо за нешто после анализе одређеног проблема. Предлог неког органа команде је одлука о предлогу. После командантове одлуке, начелник истог органа доноси одлуку у циљу реализације одлуке команданта. То значи да и други органи руковођења доносе одлуке које су везане, односно којима се спроводи одлука старешине јединице. Дакле, остали органи команде, односно други носиоци руководствених функција у оквиру команде имају двојаку улогу у процесу руковођења: 1. као учесници у анализи (процени ситуације) и предлагању одлуке за

⁸⁸ Harrison, F. E., *The Managerial Decision-Making Process*, 5th ed., Houghton Mifflin, Boston, 1999., стр. 12.

употребу јединице и 2. као доносиоци одлука за подручје своје организационе зоне. То је карактеристика читаве структуре руковођења у војној организацији.”⁸⁹

Војна организација која, по својој природи, захтева чврсту организациону структуру и јасну поделу надлежности, не оставља много простора старешинама на нижим нивоима руковођења да самостално доносе одлуке, а најчешће њихове одлуке служе да се омогући спровођење одлуке виших нивоа командовања. Слични модели руковођења и доношења одлука постоје и у полицији, нарочито у централизованим и милитаризованим полицијским структурама, каква постоји у Србији⁹⁰. Процес доношења одлука у приватном безбедносном менаџменту, не подлеже тако строгим правилима, осим у већим компанијама које се баве производњом, или пружањем услуга, које су од већег значаја за безбедност шире заједнице.

Процес доношења стратешких одлука представља посебно поље безбедносног менаџмента и оно је у јавном безбедносном менаџменту најчешће везано за највише органе извршне или законодавне власти, док је у приватном безбедносном менаџменту то одговорност топ менаџмента. Начин на који се доносе стратешке одлуке у јавном безбедносном менаџменту, углавном је дефинисан уставима и законима, односно дефинисане су надлежности појединих државних органа да одлучују о одређеним питањима везаним за безбедност, а сам начин на који се одлуке доносе дефинисан је пословничким документима. У приватним безбедносном менаџменту стратешке одлуке доноси топ менаџмент и не постоје општа правила када је у питању надлежност за доношење појединих одлука везаних за безбедност, нити постоји општеприхваћена процедура у којој се доносе одлуке од значаја за безбедност приватних организација. У већини савремених држава постоје законски прописи који регулишу обавезе приватних субјеката у погледу безбедности, али они дефинишу само одговорности одређених органа унутар организације, али не дефинишу надлежности за доношење одлука, јер би то било мешање државе у слободу предузетништва, што је директно супротно демократским тековинама савремене цивилизације. „Сам процес доношења одлуке се састоји од више фаза и то:

⁸⁹ Јовановић, Б., *Руковођење ОНО и ДСЗ*, Привредапублик, Београд, 1988., стр 182.

⁹⁰ Више о томе: Стевановић, О., *Руковођење у полицији*, ПА, Београд 2002.

одређивање оквира у коме мора бити донета одлука о питању о коме се одлучује, прикупљање информација које су релевантне за доношење одлуке, доношење одлуке и праћење спровођења одлуке и оцена повратних информација.“⁹¹ Дobar менаџер безбедности треба да пронађе одрживе моделе деловања и достизања потребног стандарда безбедности, који неће задовољити максималне стандарде безбедности, али ће омогућити нормално одвијање основних делатности организације, наравно осим у ситуацијама где постоји нулта толеранција према извору угрожавања, тада се потпуна безбедност угроженог добра претпоставља свим осталим захтевима. У складу са допустивим толеранцијама у стању безбедности морају бити постављени и критеријуми за оцену одлуке, јер у супротном би се добили критеријуми који су нереални и као такви потпуно бескорисни у оцени стања квалитета одлуке. Добра одлука мора да има неопходне карактеристике, да би могла да производи жељене последице у пракси. Основне карактеристике добре одлуке су: благовременост, целисходност и ефективност.⁹²

Коначна фаза у планирању јесте фаза израде планова. Ова фаза подразумева административно-техничко уобличавање планске одлуке и њено представљање кроз један или више планских докумената. У планове се уносе сви елементи одлуке, као што су циљеви, задаци, снаге, средства, простор, рокови, мере безбедности, начин руковођења и сл. План је инструмент процеса планирања којим се квантитативно и квалитативно изражава задатак организације који треба остварити у наредном периоду. Планом се мора предвидети и могућност промене планских задатака, уколико дође до битних промена околности у којима организација обавља своју делатност. Зато се процес планирања не завршава доношењем планског документа, већ се планирање обавља континуално. Планом се одређују и неопходна материјална средства и кадрови за остварење предвиђеног циља. „Уколико постоји велики несклад између средстава и кадрова којима располаже организација и оних која су

⁹¹ Драгишић, З., исто, 71.

⁹² Више у: Драгишић, З., исто.

неопходна за остварење предвиђеног циља, планом се предвиђа начин на који се може доћи до недостајућих кадрова и средстава, како би се остварило циљ.“⁹³

Треба имати у виду да се планови, када је у питању јавни и приватни безбедносни менаџмент, битно разликују. У области јавног безбедносног менаџмента постоје прописана правила у погледу начина израде и садржаја планова. Методологија израде планова у војсци и полицији је веома слична и заснива се на истим принципима. Разлике између војних и полицијских планова проистичу из разлике која постоји у мисијама ове две организације и разлика које су последица конкретних задатака које ове две организације извршавају. Планови који се израђују у приватном безбедносном менаџменту веома често личе на полицијске или војне планове, што је с једне стране последица сличних задатака (обезбеђење јавног скупа, обезбеђење објекта, транспорт драгоцености, обука, набавка опреме и сл.), а са друге стране флукуације кадрова из јавног у приватни сектор и истоветног образовања менаџера безбедности. Направити класификацију планова који се израђују у оквиру приватног сектора безбедности је веома тешко и морало би да укључи веома велики број критеријума, уз реалан ризик да велики број планова не буде обухваћен том класификацијом. Поред тога, за највећи број приватних субјеката не постоји обавеза да израђују планове, а самим тим ни прописана методологија израде планова. Општи принципи планирања које примењују државни органи представљају добру основу за израде планова у приватном сектору, уз наравно, уважавање специфичности сваке делатности. Планови безбедности у приватном сектору углавном чине саставне делове ширих планова који се односе на основну делатност организације која се штити, и морају, поред захтева безбедности, поштовати захтеве техничко-технолошког процеса организације која се штити.

Треба напоменути да се безбедносне мере и активности које се спроводе у некој организацији или заједници, увек морају кретати у задатом финансијском оквиру, који представља основни плански документ јер одређује оквир у коме се могу планирати све остале мере и активности.

⁹³ Драгишић, З., исто, стр. 82.

2.3.2. Организовање као функција безбедносног менаџмента

Организовање подразумева уређивање активности на такав начин који ће систематски доприносити постизању циљева организације. „Организација се састоји од људи који поседују специјалистичка знања, чија координација доприноси постизању циљева организације.“⁹⁴ Из овог Деслеровог одређења видљиво је да организација представља део менаџмент процеса који се односи на одређење оптималног распореда снага и средстава ради постизања циљева организације. Организација није само последица организовања као посебног дела менаџмент процеса, већ последица целокупног менаџмента једне организације.

Појам организације схвата се двојачко, као функционална група или институција (држава, предузеће, полиција, војска, војна јединица, полицијска станица и сл.) и као процес организовања. Процес организовања подразумева креирање организационе структуре у оквиру које се делегирају послови на чланове организације.⁹⁵

Организација представља инфраструктуру за обављање послова једне институције или функционалне групе, која је прилагођена постизању циљева институције или групе која ствара организацију. Организација мора бити тако избалансирана да, са једне стране, омогући стабилност акцијама својих чланова што омогућава да институција или функционална група могу да у дужем временском периоду планирају достизање стратешких циљева, а са друге стране да буде довољно флексибилна да омогући прилагођавање променама којима је свака организација изложена. Промене су саставни део живота сваке организације, и уколико је организација спремнија да се брже прилагођава шансе да оствари своју мисију су много веће. Историја је пуна примера различитих организација, од држава, политичких покрета па до предузећа која су нестала због тога што нису успела да се прилагоде.

Већина организација развија се постепеним прилагођавањем на одређене факторе. Фактори који пресудно утичу на сваку организацију су: природа делатности

⁹⁴ Dessler, G., исто, стр. 190.

⁹⁵ Више о томе: Тодоровић, Ј., и други аутори, исто, стр. 84.-104.

којом се организација бави, техничко-технолошка развијеност, организациона култура и стил управљања. Модерне организације настају као последица “покушаја и грешака”, и веома тешко је успоставити један најбољи модел организовања који је применљив на све организације, или бар на оне које имају исту делатност.⁹⁶

Уобичајени начин за приказивање организације је *шема организације*. Шема организације нам показује организациону структуру, и сваку менаџерску позицију у оквиру организационе структуре. На основу шеме организације јасно се могу видети линије одговорности, ко коме одговара и који је менаџер одговоран за коју област рада. Овај садржај организационе шеме у америчкој теорији организације назива се и „ланац командовања или линија ауторитета“⁹⁷. Линија ауторитета показује пут који директива треба да прође од топ менаџмента до најнижих позиција у организацији, и обрнуто пут који повратна информација треба да пређе од запослених који се налазе на дну организационе лествице до топ менаџмента који доноси одлуке на основу тих повратних информација, и враћа их назад до свих организационих целина.

У приватним корпорацијама, власници, начелно, бирају борд директора који треба да репрезентују њихове интересе, што значи да се борд налази на челу ланца командовања. Главне функције борда су избор најважнијих менаџера у организацији који су носиоци извршне функције, доношење стратешких и дугорочних планова и контрола свих аспеката пословања, како би интереси власника капитала у организацији били заштићени.

Међутим, поред формалне организације коју приказује организациона шема постоји и неформална организација, коју организациона шема не приказује, нити је може приказати, јер је она последица неформалних односа унутар једне организације. За менаџера безбедности неформална организација је често много значајнија од формалне, јер неформална организација почива на истинској моћи и истинском положају чланова организације, насупрот формалне организације која не мора увек да изражава истинску моћ. Неформална организација развија се личним неформалним контактима, неформалним каналима комуникације и начинима да се

⁹⁶ Више о томе: Драгишић, З., исто, стр. 87-90.

⁹⁷ Dessler, G., исто, стр. 190.

обаве неки послови који се развијају од стране самих запослених у некој организацији, а који се не подударају са официјелним процедурама, уколико оне постоје. Чести су примери у пракси да, рецимо, секретарица директора није само особа која подиже телефонску слушалицу и планира састанке, већ она има и улогу неформалног саветника директора, поготово ако је у организацији дуже него директор, она, у правилу, постаје неформални саветник за кадровска питања, јер боље од директора познаје запослене у организацији, чиме се у рукама секретарице, која нема никакву формалну моћ, може наћи огромна количина моћи и утицаја. Менаџери безбедности се у већини организација налазе у врховима ланаца командовања, па је самим тим и њихова формална моћ велика, међутим какав год да је формални положај менаџера безбедности њихов неформални утицај је увек велики због природе посла којим се баве. Сматра се да саветници за безбедност у већини организација представљају “сиву еминенцију”, и да је њихов утицај увек огроман, јер, у најмању руку, уживају потпуно поверење власника, или најважнијих чланова борда.⁹⁸

Како истиче Харисон⁹⁹, циљеви организације су најважнији фактор који утиче на обликовање организације, односно, избор најрационалнијег организационог модела, због чега се дефинисању циљева организације мора посветити посебна пажња. Циљеви организације морају бити јасни јер се око њих као мотивационих фактора окупљају сви чланови организације; остварљиви јер се морају рашчланити на конкретне задатке који се морају остварити у одређеном времену и простору и ранжирани по приоритету.

У свакој организацији постоји темељни циљ због кога је организација основана, парцијални циљеви појединих организационих јединица и појединачни циљеви појединих менаџера, радника или тимова у оквиру организације. Темељни циљ сваке организације је успостављање оптималне организације, односно, успостављање најрационалнијег организационог модела у конкретним условима.

⁹⁸ Видети: Драгишић, З., исто, стр. 89.

⁹⁹ Видети: Harrison, F. E., исто., стр. 356.

Оптималном организацијом се постижу циљеви организације уз што мање трошење ресурса.

Поред тога Харисон истиче три темељна циља организације: „подела рада, деловање појединих организационих јединица у функцији остваривања циљева организације, планирање, руковођење и спровођење мора бити такво да осигура максималну делотворност“¹⁰⁰.

Многи аутори од Тејлора до данас су покушавали да систематизују начела организације. Прву озбиљну систематизацију начела организације извршио је Фајол који је набројао четрнаест начела организације и то: подела рада; ауторитет; дисциплина; јединство награђивања; јединство управљања; потчињавање појединачних интереса општим интересима; награђивање; централизација; хијерархија; наређивање и ред; правичност; сталност особља; иницијатива; удруживање уједињавање и изједначавање особља.

Под утицајем Фајола многи каснији аутори предлагали су сличне класификације, које су обухватале различит број начела, која су најчешће настајала као резултат спајања или раздвајања начела која је систематизовао Фајол.

Међутим сви покушаји систематизације начела организације укључују неколико основних начела која истичу сви аутори и то су: начело поделе рада и специјализације; начело повезивања ресурса организације и начело координације. Ова три начела су од посебног значаја када је безбедносни менаџмент у питању јер „без поштовања ових начела није могуће на ваљан начин организовати одвијање послова безбедности у оквиру организације“¹⁰¹.

У обликовању организација користе се практично све методе које се користе у друштвеним наукама, јер свака организација представља мање или више сложен друштвени систем. Посебан значај имају методе, односно групе метода, које су развијене само за успостављање и обликовање организација, као и приликом реорганизовања и сличних поступака. У пракси постоје две групе метода и то: методе за обликовање организација и методе за оцену и вредновање организација.

¹⁰⁰ Исто.

¹⁰¹ Драгишић, З., исто, стр. 91.

Приликом употребе ових метода истичу се два приступа емпиријски и теоријски. Код примене емпиријског метода користе се властита и туђа искуства у решавању организационих проблема, што је нерационално, парцијално и непотпуно па се применом ових метода не могу решавати озбиљни организациони проблеми. Теоријски приступ решавању организационих проблема подразумева примену научно потврђених законитости, што овај приступ чини много погоднијим за решавање сложенијих организационих проблема. „Теоријски приступ у решавању организационих проблема у области безбедносног менаџмента полази од законитости наука безбедности, организационих наука али и свих других друштвених наука, пре свега права и социологије, које имају веома велики значај у проучавању проблема безбедности, па самим тим и решавању организационих проблема у овој области.“¹⁰²

Међу методама за обликовање организације најчешће се користи комплексна матрична метода која има следеће етапе:

- груписање послова са становишта задатака, простора, корисника и слично уз дефинисање радних места на извршном и руководећем нивоу,
- обликовање организационих јединица,
- пројектовање међусобних веза и односа и комуникационог система унутар организације и организације са околином,
- пројектовање модела организације, креирање документације и процедура за њено кретање унутар организације и заштиту тајности садржаја поверљиве документације.

Међу посебним методама за анализу и оцењивање организације користе се најчешће две групе метода и то:

- комплексна аналитичка метода која се заснива на рашчлањивању свих послова, утврђивању утицаја и међузависности свих фактора који утичу на рад организације и на крају утврђивање потенцијала организације и поређење са постојећим стањем организације.
- метода оцењивања по процесним функцијама.

¹⁰² Исто.

Методе за оцењивање и анализу организација нарочито су важне за процес контроле над организацијама које се баве безбедношћу. У јавном безбедносном менаџменту се питање контроле поставља као једно од кључних питања демократског процеса у друштву, познато под називом “цивилна и демократска контрола сектора безбедности”, која се врши од стране државних институција, међутим у нашој земљи нису довољно развијени методи за оцену стања организација које се баве питањима безбедности. Важно је напоменути да се овим методама контролише квалитет успостављене организације, а не законитост или целисходност рада, мада се мора нагласити да је „квалитетно успостављена организација основни предуслов за законито и ефикасно деловање служби које се баве националном безбедношћу“¹⁰³.

Организациона структура настаје као последица процеса организовања, и она уређује везе и односе који постоје у једној организацији између различитих организационих целина те организације, као и везе и односе које постоје унутар самих организационих јединица. Поред уређивања веза и односа, организационом структуром се врши подела надлежности унутар организације, што је веома значајно ради ефикаснијег и ефективнијег рада. Постојање организационе структуре омогућава стабилност и континуитет у раду организације, без обзира на кадровске промене.

Организациона структура указује на: „начин повезивања процеса и функција, степен поделе рада, расподелу ауторитета и начин контроле“¹⁰⁴. Обављање сличних послова на једном месту доводи до стварања организационих јединица. Организационе јединице представљају прву организациону последицу поделе рада. Ефикасност организације зависи од поделе рада у оквиру радних јединица, док ефективност зависи од интеграције радних јединица.

Организациона структура представља се графички помоћу организационе шеме, која приказује односе између организационих јединица и радних места. Без обзира на величину организационе шеме она садржи само три симбола квадрате,

¹⁰³ Исто.

¹⁰⁴ Годоровић Ј., и други, исто, стр. 84.

вертикалне линије и хоризонталне линије. Квадрати представљају организационе јединице и радна места, а често и једно и друго, и у квадрате се уписују називи организационих јединица. Вертикалне линије представљају правце простирања ауторитета и одговорности. Највећи ауторитет и одговорност је на врху организационе шеме, а најмањи на дну, ауторитет се простире одозго на доле, док се одговорност простире одоздо на горе. Одговорност по радним местима најмања је на дну шеме, а највећа на врху. Хоризонталне линије представљају везу обавезне сарадње у организацији. Радна места која се налазе на истој хоризонталној линији морају се обавезно договарати, сарадња је могућа и по дијагонали али није обавезна. Дубина организационе шеме одређена је бројем нивоа у организацији. Организациона шема описује пет битних елемената организационе структуре. Прво, поделу рада. Сваки правоугаоник говори о одговорности за конкретни радни задатак. Друго, однос менаџера и подређених. Линије између правоугаоника приказују канал комуникације на чијим крајевима се налазе информације о томе ко извештава и коме се подносе извештаји. Треће, тип посла који се обавља. Ознаке у квадратићима означавају различите активности и области одговорности. Четврто, критеријуме груписање послова. Увид у целину организационе шеме показује на бази чега је извршена подела организације. Пето, управљачке нивое. Организациона шема указује не само на појединачне менаџере и њихове подређене, већ и на целокупну линију командовања и контроле. „Сви запослени који подносе извештај истој особи налазе се на истом хијерархијском нивоу без обзира на њихово место у организационој шеми“.¹⁰⁵

Велике организације имају често толико сложену организациону структуру која се не може графички представити, зато се за представљање организације поред организационе шеме користи и организациони модел. Организациони модели представљају упрошћену слику реалне организације. Суштину организационог модела чине критеријуми диференцирања послова на организационе делове и начин њихове интеграције у целину. Постоји неколико организационих модела, али су за

¹⁰⁵ Годоровић, Ј., и други, исто, стр. 85.

безбедносни менаџмент најважнији линијски, линијско-штабни, функционални, дивизиони, хибридни и матрични.¹⁰⁶

2.3.3. Координација као функција безбедносног менаџмента

Под појмом координације подразумева се активност која је усмерена на довођење елемената структуре неке организације у складан однос, као и усклађивање активности у једном процесу. Координација се као функција безбедносног менаџмента јавља се у свим осталим фазама менаџмент процеса, односно осталим функцијама менаџмента. Планирање, организовање, вођење и контрола, прожети су координацијом која је неопходна за стварање складних односа у организацији. Појам координације блиско се везује за појмове интеграције и организационог усмеравања, и она је неопходна да би људи у оквиру неке организације у сваком тренутку били свесни своје праве улоге у остваривању планираних задатака, и остварењу мисије организације којој припадају.¹⁰⁷

Сваки појам из домена интеграције, кооперације, централизације, децентрализације, концентрације и деконцентрације односно сви процеси организационог усмеравања везани су за функцију координације. То је активност усклађивања више учесника у једном процесу, односно карактеристика сваке интеракције.

Потреба за координацијом је последица поделе рада и специјализације, које омогућавају организацијама да ефикасно користе ограничене ресурсе. Без координације појединци и организациони делови губе улоге или добијају погрешне улоге у организацији и често покушавају да остваре своје појединачне интересе на рачун организационих циљева. Координација је одговорност менаџера, и сваки менаџерски ниво треба да остварује координацију и по вертикали и по хоризонтали, али и латералну координацију. Координација се обавља на бази информација које се

¹⁰⁶ Више о томе: Драгишић, З., исто.

¹⁰⁷ Стевановић полази од интеграције као битног обележја координације, и цитира став Џејмса Мунеја, који координацију поистовећује са интрграцијом (Стевановић, О., исто, стр. 202.).

преносе писаним путем, а могу се преносити и путем информационог система. „Информације на основу којих се врши координација морају да доведу до акције.“¹⁰⁸

Према схватању Ј. Тодоровића, „потреба за координацијом проистиче из разлика у ставовима“¹⁰⁹ међу члановима организације. Према овом аутору постоје четири извора разлике у ставовима међу члановима исте организације.

Прво, разлике у оријентацији у односу на циљеве. Оваква разлика испољава се као тежња сваког дела организације или сваког појединца у организацији да наметне циљеве своје организационе јединице или своје струке као доминантне организационе циљеве.

Друга разлика проистиче из различитог односа према времену. Неки менаџери у организацији захтевају тренутна решења која ће одмах донети ефекте, док други инсистирају на дугорочним решењима и баве се проблемима који имају дугорочније ефекте. Оваква разлика је последица природе посла којима се поједини менаџери баве. Бављење различитим пословима развија две различите филозофије и два различита приступа, оба веома важна за успех и развој сваке организације. Одсуство првог приступа учинило би организацију неефикасном и неоперативном, а одсуство другог приступа учинило би је бесперспективном. Задатак координације је да помири ова два приступа и организацији понуди и ефикасна решења којима се обављају дневне активности и визију будућности, без које нема перспективе и развоја.

Трећа разлика се односи на разлике у интерперсоналним односима. На пример код обављања одређених безбедносних задатака, нарочито у војсци и полицији, комуникација се базира на брзој размени информација и аутоматском доношењу и извршавању одлука. Код планско-аналитичких и развојно-истраживачких послова комуникација је спорија и захтева интерактиван однос, уважавање креативности и сагледавања проблема из различитих углова. У оваквим пословима „*brainstorming*“ анализе и панел дискусије, које захтевају више времена за дугачке разговоре, представљају неопходан услов за успех организације. За менаџере навикнуте на први модел интерперсоналних односа анализирање се доживљава као губитак драгоценог

¹⁰⁸ Драгишић, З., исто, стр. 101.

¹⁰⁹ Тодоровић, Ј., и други аутори, исто, стр. 91.

времена, док код менаџера који се баве планско-аналитичким делатностима брзо доношење одлука, без анализе, се доживљава као површност. „Овај сукоб гледишта разрешава се тако што сваки сегмент организације ради на свој начин, без међусобног преузимања модела, а временску координацију међу њима врше менаџери који се у организационој шеми налазе на непосредно вишем нивоу.“¹¹⁰

Четврта разлика проистиче из степена формализације. Свака организациона јединица има различите стандарде у оцени степена достигнутих циљева. Разлике су често последица различитих делатности које се обављају у различитим организационим јединицама. Неке организационе јединице баве се лако мерљивим пословима где није тешко успоставити стандарде квалитета, на основу којих је могуће објективизирати контролу, док се друге баве флуидним пословима где је објективизација контроле често немогућа. У области безбедносног менаџмента, објективна контрола често је немогућа јер су послови које обављају делови организације задужени за безбедност немерљиви. Оваква природа посла организационих јединица које се баве питањима безбедности, често као последицу има, да се у другим организационим јединицама поставља питање сврсисходности постојања службе обезбеђења која „не ради ништа“¹¹¹, што као последицу има незадовољство запослених у другим организационим јединицама који имају осећај да издржавају службу обезбеђења која не зарађује своју плату и нико их ништа не пита, док запослени у служби безбедности имају осећај да се њихов рад не цени довољно.

Запослени у одређеним организационим деловима настоје да развију сопствени приступ циљевима организације и начинима како да их достигну. Подела рада и специјализација не утичу само на разлике у одређеним пословима, већ и на разлике у начину гледања на одређену организацију, начину сагледавања сопствене улоге као и начину успостављања односа са другим члановима организације и другим организационим деловима. Према Мунеју уместо термина „координација“, у

¹¹⁰ Драгишић, З., исто, стр. 102.

¹¹¹ Исто.

овом смислу, треба користити термин „интеграција” да би се означио степен у коме чланови различитих организационих делова раде на остварењу истих циљева.¹¹²

Да би се постигла ефикасна координација неопходно је стално комуницирање између елемената система и елемената система и окружења. У безбедносном менаџменту координација је незамислива без размене безбедносних података. Уколико се задатак обавља у условима веће неизвесности потреба за разменом информација и координацијом је већа. Добро комуницирање је основа за добру координацију.

Постоје три основне врсте координације унутар једне организације: вертикална, хоризонтална и латерална (побочну). Вертикална димензија координације је карактеристична за размену информација између различитих хијерархијских нивоа. Хоризонтална димензија координације је карактеристична за размену информација између субјеката који се налазе на истом хијерархијском нивоу. Латерална димензија координације је карактеристична за размену одређене групе информација усмерене за остварење одређеног пројектног задатка. Која ће димензија координације бити доминантна зависи, пре свега, од потребе за координацијом.

Поред овог критеријума координација се може поделити и према организационим и формалним карактеристикама. У организационом смислу координација може бити интерна и екстерна. Интерна координација се остварује између унутрашњих елемената организације, док се екстерна остварује између унутрашњих елемената организације и окружења. У безбедносном менаџменту „потреба за екстерном координацијом често је веома велика и од ње зависи успех задатка“¹¹³. Приватне службе безбедности и полиција веома често раде на остварењу истог задатка, полиција и војска у сложенијим операцијама увек учествују заједно, готово редовно се у извршењу сложенијих безбедносних задатака појављује више организација које заједничким деловањем треба да отклоне неку опасност или да санирају последице неког штетног безбедносног догађаја. Тако се у санирању

¹¹² Видети: Моонеу, J. D., *The Principles of Organization (Rev. ed.)*, Harper, New York 1947.

¹¹³ Драгишић, З., исто, стр. 103.

последица неке елементарне непогоде најчешће на истом задатку налазе војска, полиција, јединице цивилне заштите, приватне службе обезбеђења, ватрогасне јединице, привредне организације, хитна медицинска помоћ и самоорганизовани грађани. Јасно је да у тако сложеној ситуацији од квалитета екстерне координације зависи успех заједничког подухвата, што је задатак сложенији и неизвеснији, потреба да се успостави чврста координација, и интерна и екстерна, је већа. Интерна координација се, у правилу, много лакше успоставља јер постоје јасно дефинисане надлежности појединих менаџера, и различитих менаџерских нивоа. Посебно су међусобни односи јасно дефинисани у државним безбедносним службама као што су војска и полиција, где се односи дефинишу посебним правилима која имају апсолутно обавезујући карактер за све припаднике војне и полицијске организације. У приватним безбедносним организацијама које нису толико чврсто структуриране и где не постоји толики степен дисциплине која је гарантована правним регулативама, координацију је теже постићи. Међутим, правилним организационим решењима и добром селекцијом и обуком кадрова стварају се услови за успостављање добре координације. Успостављање добре екстерне координације је најзахтевнији посао када је координација у питању. Складан однос у активностима у којима учествују различите организације, са различитим унутрашњим односима, са различитом филозофијом рада, често и различитим циљевим може изгледати као неостварљив задатак. Неопходан услов да би се у оваквој ситуацији успоставила нормална координација је добра комуникација уз инсистирање да свако обави онај део посла за који је најстручнији.

Према формалним карактеристикама координација се појавити као: усмеравање рада, сарадња, обједињавање рада, заједнички рад, испомоћ и садејство. „Обједињавање рада и испомоћ спадају у вертикалну димензију координације, коју реализују виши нивои менаџмента према нижим нивоима. Усмеравање рада је најчешће хоризонтална или латерална димензија координације, док сарадња,

заједнички рад и садејство спадају у чисто хоризонталну димензију координације, мада готово редовно проистичу из одлука виших нивоа менаџмента.“¹¹⁴

„Суштину процеса координације чини повезивање потребе за координацијом са капацитетом координације.“¹¹⁵ Постоје три приступа за постизање успешне координације: коришћење основних принципа менаџмента, раст потенцијала координације и смањење потребе за координацијом.

Основни принципи менаџмента су поштовање хијерархије, поштовање прописаних поступака и процедура и принцип планирања. Коришћење ових принципа ради постизања успешне координације је могуће у организацијама са релативно малим потребама за координацијом. У сложенијим моделима организације организациони делови повећавају степен своје независности у односу на целину, повећавају величину или проширују функције, па је за успешну координацију потребна много већа количина и много бржи проток информација. Уколико се применом основних принципа менаџмента не постиже довољан ниво координације, неопходно је применити друге поступке и принципе како би се постигао потребни проток довољног броја информација за успешну координацију.

Потенцијал координације повећава се растом броја вертикалних и латералних информација. Вертикалне информације преносе се изнад и испод организационих нивоа, при чему се координација остварује унутар канала комуникације. Латералне информације се добијају кроз непротоколисану размену. Латералне информације се често добијају кроз размену између појединаца који деле исту ситуацију или исти проблем, чиме се избегава дизање проблема на виши ниво, односно арбитража, чиме се проблем усложњава и пут до његовог решења постаје много дужи и тежи, што захтева ангажовање додатних ресурса. Уколико се ова комуникација не одвија на жељеном нивоу, друга могућност је проширење одговорности. Одговорност се може проширити увођењем послова који подразумевају стварање везе између делова организације са учесталим односима и поверавање тих послова тачно одрешеним појединцима. Трећа могућност је преко успостављања интеграције преко одређених

¹¹⁴ Исто.

¹¹⁵ Годоровић Ј., и други аутори, исто, стр. 91.

појединаца у пословима који тангирају већи број организационих јединица, а није неопходно или целисходно да се интеграција остварује преко организације као целине. Уколико ни један од ових модела не да одговарајући ниво координације, последња могућност је повезивање менаџера, путем успостављања функције менаџера за везу. Менаџер за везу има формални ауторитет над свим организационим јединицама укљученим у пројекат. Тај ауторитет се обично јавља у форми „снажних контролних овлашћења која има менаџер за везу, уз свакако, најзначајније контролно овлашћење - контролу буџета сваке организационе јединице која је укључена у пројекат“¹¹⁶.

Потреба за координацијом се смањује путем повећања самосталности организационих јединица и њиховим оспособљавањем да обављају своје активности независно од других организационих јединица у организацији.

Успостављање веза и односа у обављању неког посла везани су за простор и време. У времену и простору се обавља координација свих материјалних, људских и информационих ресурса неопходних за обављање неког процеса рада, које је неопходно координирати да би делатност сваког од њих била усмерена ка достизању организационих циљева. Координацију свих ресурса треба успоставити у простору и времену па можемо говорити о „просторној и временској димензији координације“¹¹⁷.

Као што је већ речено, координација као функција безбедносног менаџмента прожима све остале функције, и она је саставни део сваке фазе менаџмент процеса. Координација се налази у фази планирања, али се и сама планира. Просторна димензија координације се планира када више организационих јединица извршава исту активност у истом времену на различитом простору, чиме се постиже да они своју активност обаве правовремено на различитим тачкама простора. Временска димензија координације планира се када више организационих јединица треба да при обављању своје активности користе исти простор у различитом времену, без међусобног преклапања и ометања у простору. Планирање временске димензије

¹¹⁶ Драгишић, З., исто, стр. 105.

¹¹⁷ Исто.

координације је такође веома значајно када „активност једне организационе јединице зависи од завршетка активности друге организационе јединице и када је потребно да се у одређеној фази неке активности укључи и друга, или друге организационе јединице“¹¹⁸.

2.3.4. Вођење као функција безбедносног менаџмента

Вођење представља извршну фазу менаџмент процеса, јер оно што је планирано, организовано и координисано треба спровести у дело. Свака активност у организацији извршава се преко чланова те организације, односно запослених у њој. Способност менаџера да мотивише људе да ефикасно обаве свој посао од есенцијалне је важности да би неко могао да буде добар менаџер. Бити менаџер не значи истовремено бити и вођа односно лидер, ове две улоге битно су повезане, али међу њима постоји и разлика. Деслер сматра да је разлика између менаџера и вође у томе што менаџер ствари ради на прави начин, а вођа ради праве ствари. Веома је важно, „да се у једној личности нађу и менаџер и вођа“¹¹⁹.

У пракси се често мешају појмови руковођење, менаџмент, вођење и управљање. Ове појмове није могуће до краја јасно раздвојити, поготово што није могуће увек прецизно одредити о чему се у конкретном случају ради. Поред тога, пословима безбедности се баве веома различите организације у друштву, од војске, полиције, обавештајних и безбедносних служби, па до приватних служби обезбеђења. Свака организација која се бави привредним или другим делатностима предузима одређене мере ради заштите свог пословања. Послови безбедности који се предузимају од стране вандржавних организација, обављају се од стране посебних организационих јединица које се образују у оквиру организације или, уколико се такве организације не формирају, од стране менаџмента, у оквиру редовних менаџмент активности. Шароликост организација које се баве безбедношћу ствара додатне тешкоће у јасном разграничавању појмова менаџмента, руковођења, вођења и управљања. Поједини од ових појмова не могу се применити на неке организације

¹¹⁸ Исто, стр. 109.

¹¹⁹ Исто, стр. 111.

јер су супротни основној мисији и природи организације. „На пример, руковођење и командовање је примерено војним и полицијским организацијама, док је у случају организација из области образовања, културе, а посебно медија такав вид вођења организације потпуно непримерен, иако свака од наведених организација спроводи одређене активности из области безбедности.“¹²⁰ Ако нисмо у стању да их прецизно дефинишемо, било би неопходно покушати ове појмове бар разграничити.

„Вођество или вођење се може дефинисати двојачко: као процес издавања директива и утицања на активност запослених у организацији или њених припадника, ради постизања циљева организације и као способност одређене личности да утиче на понашање људи, на усмеравања њихових жеља, ставова и активности у правцу остваривања циљева лидера и организације на чијем челу се лидер налази.“¹²¹ Лидерство се представља „људски део менаџмента“, и оно се пре свега може сматрати вештином. Лидерство се заснива на претпоставци да је ефикасност пословања у великој мери зависна од мотивације, способности и напора запослених у једној организацији. Оваква претпоставка потврђена је у многим теоријама „научног“ управљања. Данас је уврежено схватање да је успех организације директна последица односа чланова организације према циљевима које је та организација поставила пред себе.

Менаџмент и вођење, се у великој мери разликују. Менаџмент је шира активност од вођења и она у себе укључује не само људе и рад са њима већ и читав низ других активности у организацији, које су у вези са финансијским средствима, логистиком, тржишним активностима, технолошким иновацијама, управљањем променама, информационим процесима и др. Менаџери су најчешће и лидери, мада не мора бити тако. Менаџер може бити веома успешан у обављању техничког дела свог посла, који може бити везан за технолошки процес, набавку материјала, финансијско пословање, планирање или слично, а да при томе нема контакте са запосленима, нити на њих врши било какав утицај. У безбедносном менаџменту постоје веома добри аналитичари, планери и менаџери који се веома успешно баве

¹²⁰ Исто.

¹²¹ Исто, стр. 112.

проценама, а да при том немају вештину вођења људи, нити успевају да се наметну као ауторитети. „Овакви менаџери задржавају свој формални статус у организацији без обзира на недостатак лидерских способности, док неки радник у организацији који нема никакав формални менаџерски статус може да се наметне као одличан вођа групе. О оваквим припадницима организације посебну пажњу треба да воде менаџери задужени за управљање људским ресурсима и да их распореде на одговарајућа радна места где ће њихове лидерске способности највише доћи до изражаја.“¹²²

Менаџерско вођење сваке организације је веома важно јер постоје велике празнине у организационим шемама сваке организације, које се не могу попунити без доброг менаџерског вођења. Неформални односи који се развијају унутар организације могу организацији користити и учинити је флексибилнијом и способнијом да се брже прилагођава ситуацији у окружењу, али је могу у потпуности разорити и онемогућити нормалне канале комуникације, увести хаос у унутрашње односе у организацији и на тај начин је довести до сигурног краја. Да ли ће постојање неформалних односа у организацији бити од користи или штете зависи искључиво од вођења и способности менаџера да се наметне као истински лидер.¹²³ Ниједно планирање не може да предвиди све промене у окружењу којима се организација мора прилагођавати. Вође у организацији треба да осете те промене и да људе наведу да се прилагоде. „Вођењем се постиже интеракција међу припадницима организације, постиже се заједнички дух и елан по коме се успешне организације разликују од неуспешних.“¹²⁴

Управљање се у начелу схвата као функција одређивања циљева организације, па је то функција која углавном припада власницима или топ менаџменту, односно највишим државним институцијама ако је реч о војсци, полицији, обавештајним или безбедносним службама. Носиоци управљања имају задатак да донесу стратегијске одлуке којима ће одредити циљ организације, да тај циљ операционализују кроз глобалне и парцијалне задатке и поставе стратегију за извршавање задатака и

¹²² Исто.

¹²³ О значају социјалне интелигенције менаџера види шире: Harrison, F. E., исто, стр. 281-288

¹²⁴ Драгишић, З., исто.

достизање циљева организације. Са становишта безбедносног менаџмента ово одређење је прихватљиво и изражава „основну разлику између делатности највиших државних органа и војних команди“¹²⁵, на пример.

„Руковођење се дефинише као систем метода, техника и начела којима се регулишу све активности једне организације ради постизања циљева који су постављени организацији.“¹²⁶ Процес руковођења нужно је везан са ауторитетом руководиоца, стилем и методама руковођења, одговорношћу, хијерархијом и организационом моћи, што све заједно чини систем руковођења.

Војно руковођење из кога су настале сви каснији облици руковођења, дефинише се у домаћој теорији као „делатност старешина и команди (штабова, управа) на усмеравању организационих јединица и појединаца у процесу остваривања циљева постављених војној организацији“¹²⁷.

Међу ауторима који се баве питањима безбедности и питањима менаџмента постоји неусаглашен став око постојања војног и полицијског менаџмента. Већина аутора сматра да у војсци и полицији постоји само руковођење док је менаџмент више окренут цивилним безбедносним организацијама, мада се у војној логистици, као и у полицијској, може говорити о менаџменту. Према Јурини, да би се могло говорити о полицијском менаџменту неопходно је да се „промени окружење у коме полиција делује, да дође до промена у самој полицијској организацији и да се радикално промени систем руковођења“¹²⁸.

Постоји неколико основних предуслова који су неопходни да би вођство уопште било могуће¹²⁹. Прво, вођство постоји уколико постоје подређени који су спремни да следе вођу, и који прихватајући директиве вође процес вођења чине могућим. Друго, вођење подразумева расподелу моћи између вође и чланова групе. Вођа има формални ауторитет да подређенима издаје директиве, али утицај тих директива на чланове групе није увек, и код свих чланова, исти. Треће, поред

¹²⁵ Исто, стр. 113.

¹²⁶ Исто.

¹²⁷ Јовановић, Б., исто., стр. 8

¹²⁸ Јурина, М., *Елементи организације полиције*, МУП Републике Хрватске, Загреб, 1995., стр. 224.

¹²⁹ Видети: Тодоровић Ј., и други аутори, исто, стр. 113.-128.

формалне моћи издавања директива, вођа може и на друге начине остварити утицај на подређене и обезбедити њихову лојалност.

У одређивању суштине вођства постоје три приступа: „приступ персоналних карактеристика вође, бихејвиористички приступ и ситуациони приступ“¹³⁰.

Карактеристике личности вође се могу анализирати на два начина. Прво, поређењем карактеристика личности вође са карактеристикама личности подређених чланова организације. Друго, поређењем карактеристика личности успешних и неуспешних вођа.

Већина истраживања карактеристика личности вође спада у прву групу истраживања. Поређење личности вође са личностима подређених у организацији показује да су вође отвореније, интелигентније, предузимљивије и самопозданије особе од оних који их следе. Међутим, сви интелигентни и предузимљиви људи не постају вође, као што неке потврђене и доказане вође нису имале ове карактеристике. Мерење особина личности вође психолози могу да изведу на веома егзактан начин и та мерења показују да већина вођа нема комбинацију карактеристичних особина вође, која би их издвојила од особа које се не идентификују као вође, ни по карактеристикама личности ни по формалном положају. Што се тиче истраживања која пореде карактеристике личности успешних и неуспешних вођа, општи је закључак да таква истраживања нису успела да „јасно изолују карактеристике личности које одвајају успешне од неуспешних вођа“¹³¹.

Бихејвиористички приступ је фокус проучавања са карактеристика личности вође преместио на понашање вође, јер је уочено да вође не поседују неке особине личности које их издвајају од остале популације. Истраживања представника овог приступа траже одговор на питање шта успешне вође раде, односно како се понашају? Посебан нагласак је на проучавању начина на који вође комуницирају са подређеним члановима организације, начинима на које вође мотивишу подређене, на који делегирају овлашћења и сл. За разлику од карактеристика личности, понашање је подложно процесу учења, па се може закључити да се појединац може обучити

¹³⁰ Драгишић, З., исто, стр.113.

¹³¹ Исто, стр. 114.

ефикасном вођењу и да се путем процеса образовања може доћи до успешних вођа на различитим нивоима менаџмента. Међутим, истраживања су показала да „не постоји тип понашања који ће дати добре резултате у свим ситуацијама“¹³².

Бихејвиористички приступ проучава два аспекта вођства: функције вођства и стилове вођства. Први приступ вођству подразумева проучавање функција које вође имају у организацији. Вођа обавља две врсте функција у организацији, пословне и социјалне функције. Пословне функције вођа обавља у циљу решавања проблема и он у том смислу сугерише решења, нуди релевантне информације и алтернативна решења. Социјалне функције вође односе се на одржавање групе и обухватају све активности које доприносе да организација функционише ефикасно. Ефикасне организације веома често имају неформалну структуру која обавља социјалну функцију, док се менаџер, односно формални лидер бави решавањем проблема.

Менаџери безбедности често обављају социјалну функцију у организацији, или воде рачуна како се она обавља, пошто је стање односа унутар групе веома важан предуслов успешног функционисања организације. Социјални односи унутар организације представљају веома важан безбедносни податак, јер многи извори угрожавања организације проистичу управо из лошег стања односа између запослених, односно између запослених и менаџмента. Треба имати у виду да је нарушавање социјалне равнотеже унутар организације један од често примењиваних метода за нарушавање ефикасности, а често и за потпуно уништење организације. Менаџер безбедности мора непрекидно да процењује стање односа у организацији. Приликом израде процене стања социјалних односа у организацији, „менаџер безбедности, мора:

- да добро уочи социјалне односе,
- да дефинише истинску организациону шему организације, односно да уочи ко су стварни носиоци моћи у једној социјалној групи,
- какви су односи међу различитим социјалним групама и на чему се ти социјални односи заснивају?,
- постоје ли кланови унутар колектива и ко су вође кланова?,

¹³² Исто, стр. 115.

- каква је формална позиција вођа кланова?,
- каква је структура чланова клана?,
- каква је повезаност клана са структурама изван организације?,
- ко су главни покретачи сукоба унутар групе и између различитих група?,
- какви су декларисани разлози за сукобе?,
- какви су стварни разлози сукоба?,
- колика је разлика између декларисаних и стварних разлога за сукобе?,
- колико су разлози због којих долази до сукоба на релацији запослени менаџмент оправдани?,
- коме иду у прилог сукоби?,
- како се могу развијати латентни сукоби који постоје унутар организације?,
- каква је могућност да дође до насилних сукоба у организацији и ко су потенцијални носиоци сукоба?¹³³

Процена стања социјалних односа у организацији је веома важан показатељ топ менаџменту за креирање мера којима би се социјални односи унапредили или задржали на постојећем нивоу, уколико он одговара захтевима ефикасности организације. Лоше стање социјалних односа је први индикатор да се према организацији спроводи субверзивна делатност. Уколико се региструје значајно погоршање социјалних односа, то наравно, не значи аутоматски да нека друга организација или појединци спроводе субверзију према организацији, али је то могућност која се мора сматрати веома вероватном, док се год не утврде прави узроци погоршања социјалних односа.

Иако постоје различите поделе стилова вођења, могу се уочити два основна стила¹³⁴: аутократски и либерални стил вођења.

¹³³ Исто, стр. 115.-116.

¹³⁴ Б. Јовановић стилове вођења дели на аутократске, демокретске, либералне, опште и посебне стилове руковођења. О. Стевановић преузима поделу на уздржани стил руковођења, ангажовани стил руковођења, прегалачки стил руковођења и интегрисани стил руковођења. Треба имати у виду да се ова два аутора баве руковођењем у војсци и полицији, као специфичним организацијама у којима се издваја више стилова руковођења и неопходно је направити финију класификацију која би обухватила све стилове којима се служе војне и полицијске старешине у вођењу својих јединица. Са аспекта безбедносног менаџмента који обухвата и војно и полицијско руковођење сматрамо да је боље

Аутократски стил вођења се заснива на стриктној контроли подређених чланова групе како би се у потпуности оствариле замисли вође, односно менаџера. Менаџери који прибегавају оваквом стилу вођења више су заинтересовани да се посао заврши, него да дође до сатисфакције запослених и да се развије добра атмосфера у организацији. За разлику од ауторитарног у либералном стилу вођења пажња се уместо контроли поклања мотивацији. Овакав стил руковођења „подстиче чланове организације на обављање активности кроз учешће у доношењу одлука, и делегирању одговорности на чланове организације за обављање својих послова“¹³⁵.

На избор стила вођења утичу три групе фактора: „карактеристике менаџера, карактеристике подређених и ситуациони фактори“¹³⁶.

Карактеристике менаџера (образовање, систем вредности, искуство и сл.) примарно утичу на стил вођења. Менаџери који више уважавају циљеве појединца и који прихватају демократске вредности опредељују се чешће за либерални стил вођења, док менаџери који у први план стављају брзо и ефикасно обављање посла више се опредељују за аутократски стил вођења. Боље образовани менаџери који имају више самопоуздања, лакше се опредељују да препусте више дискреције запосленима, они само одређују лимите у оквиру којих запослени сами доносе одлуке.

Карактеристике запослених су други фактор који битно утиче на стил вођења. Партиципативни менаџмент се примењује када подређени испољавају независност и слободу акције, када показују интерес за преузимање одговорности за доношење одлука, када се идентификују са циљевима организације, када имају довољан ниво компетентности да би могли да доносе одлуке и када имају искуство са партиципацијом. Уколико ови услови нису испуњени менаџер бира ауторитарни стил вођења који у оваквој ситуацији даје много боље резултате. Веома је опасно препустити иницијативу подређенима који немају интерес или компетентност да учествују у доношењу одлуке, нити да је самостално и у правој мери спроведу у дело.

прибећи грубој подели стилова руковођења пошто их није све могуће детаљније описати због ширине организација и делатности које спадају под безбедносни менаџмент.

¹³⁵ Драгишић, З., исто, стр. 117.

¹³⁶ Исто.

У таквим ситуацијама аутократски стил вођења даје много боље резултате и обезбеђује већу безбедност пословања.

Избор стила вођења зависи и од ситуационих фактора као што су култура организације, карактеристике групе, природа посла, временски фактор и фактор средине.

Поред тога, постојање неформалних група утиче на избор стила вођења. Група која добро функционише и која је у стању да сама реши проблеме захтева отворену и слободну атмосферу у односу на стриктну контролу. У великој групи и групи која је географски дислоцирана партиципативни менаџмент се тешко примењује.

Међутим, чисти стилови руковођења у пракси се веома ретко срећу. Сваки менаџер примењује различите стилове вођења у истој организацији у различитим ситуацијама. „Најбољи модел вођења је онај који води рачуна подједнако и о ефикасности обављања посла и о односима унутар организације, дајући предност једном или другом у зависности од конкретне ситуације, али не запостављајући ни један ни други“¹³⁷.

Истраживања вођства показала су да не постоји универзалан приступ који обезбеђује ефикасно вођство. Због тога су истраживања усмерена у правцу проналажења и проучавања ситуационих фактора који утичу на ефикасност вођства. Теоретичари ситуационог приступа покушавају да идентификују различите факторе који утичу на понашање вође. Чермес¹³⁸ тако наводи следеће ситуационе факторе као битне за ефикасно вођство: претходно искуство и амбиције вође, очекивања и понашање надређених, карактеристике послова који се обављају у организацији, карактеристике и понашање подређених, очекивање и понашање колега, култура и политика организације. Такође, ситуациони приступ покушава да утврди који су од тих фактора најважнији за дати скуп околности као и да одреди стил вођења који ће бити најефикаснији за дате околности. У покушају да се одговори на ова питања развијени су Херсеј-Бланшаров и Фидлеров модел.¹³⁹

¹³⁷ Исто.

¹³⁸ Видети: Chermes, M., *The social, organizational and Cultural context effective leadership*, Harvard business review, 1984.

¹³⁹ О моделима види шире: Тодоровић Ј., и други аутори, исто, стр. 116.-119.

Херсеј–Бланшаров модел полази од претпоставке да зрелост, искуство, жеља за резултатима и спремност да се прихвати одговорност од стране подређених утиче на ефикасност вођења. Циљеви и знање чланова организације који следе вођу су битне варијабле које одређују стил вођења. Према овом моделу однос између менаџера, односно вође и подређених пролази кроз три фазе. У првој фази у којој подређени улазе у организацију менаџер је више усмерен на ефикасно обављање посла и склонији ауторитативном стилу вођења. Подређени, приликом уласка у организацију, треба да се обучи за успешно обављање послова којима ће се бавити у организацији и да прихвати правила понашања која су део културе организације. У овој фази неауторитативно вођење може изазвати конфузију, тако да партиципативни менаџмент у овој фази развоја односа још увек није актуелан, пошто се нису развили колегијални односи између запослених. У другој фази подређени још увек уче о пословима које обављају, тако да још нису спремни за прихватање одговорности, тако да је ауторитативно вођење у овој фази још увек актуелно, мада уверење и подршка подређенима расте. У овој фази расту капацитети за примену партиципативног менаџмента. У трећој фази способност и мотивација подређених расте што доводи до повећавања спремности за прихватање одговорности менаџери све мање примењују ауторитативан стил вођења и пружају већу подршку подређенима у прихватању одговорности. У мери у којој расте одговорност и самосталност подређених, престаје потреба за директним односом између менаџера и подређених. Овај модел губи из вида чињеницу да сви менаџери нису подједнако флексибилни и способни да мењају стил вођења. Уколико је менаџер флексибилан или добро обучен да стил вођења прилагођава ситуацији, може се очекивати да ће бити ефикасан у великом броју ситуација. Међутим, ако је менаџер нефлексибилан може се очекивати да ће „његов стил вођења бити ефикасан у одређеном броју ситуација, у којима његов стил одговара конкретној ситуацији“¹⁴⁰.

Фидлеров модел полази од става да нема еволуције у стиливима вођења поготово ако су менаџери имали успеха приликом примене једног стила вођења. То је разлог због кога покушај промене стила вођења, како би се прилагодио новој

¹⁴⁰ Драгишић, З., исто, стр. 119.

ситуацији, не даје резултате. Пошто су стилови вођења нефлексибилни и пошто се у једној ситуацији може применити више стилова вођења, ефикасно вођење се постиже избором менаџера који одговарају одређеној ситуацији или промени ситуације.

Овај модел предвиђа специфично мерило стилова вођења. Стил вођења одређује се према ЛПЦ мерилу, које одређује степен задовољства најмање прихваћеним колегом. Уколико већина запослених оцењује најмање прихваћеног колегу на релативно позитиван начин, можемо закључити да вођа води рачуна о социјалним односима, у супротном ако запослени најнеприхваћенијег колегу описују на негативан начин, у питању је ауторитаран стил вођења који не поклања пажњу социјалним односима и базира се на стриктној контроли. Менаџери који имају висок ЛПЦ имају добре односе у својој организацији, што за последицу има општу ефикасност вођења организације.

Фидлеров модел користи три ситуационе варијабле. Прво, однос између менаџера и чланова групе. Квалитет овог односа има највећи утицај на моћ и ефективност менаџера. Уколико менаџер има добар однос са члановима групе, уколико они поштују његову личност, карактер, знање, цене његове потезе, менаџер неће морати да троши свој формални ауторитет у обављању послова и за таквог менаџера с правом можемо рећи да је вођа. У супротном менаџер мора да користи свој формални ауторитет и да са члановима групе комуницира путем директива, што за последицу има мање ефикасно обављање послова, веће незадовољство чланова групе, мању мотивисаност и сл. Друга варијабла је структура послова. Код високо структурираних послова постоје прецизне инструкције и поступци за обављање послова тако да запослени знају веома прецизно шта се очекује да раде. Менаџери у овој ситуацији имају висок ниво ауторитета пошто постоје прецизна мерила резултата. У супротном, ако послови нису структурирани, улога чланова групе није јасна а моћ менаџера је много мања, пошто се запослени увек могу супротставити њиховим инструкцијама или оценама. Треће, моћ положаја вође је последња ситуациона варијабла. Одређени положаји носе висок степен моћи, рецимо генерал у војсци, председник компаније, генерални менаџер и сл. Моћ и ауторитет који носи високи положај олакшава утицај менаџера на подређене. Фидлер је закључио да вође

са ниским ЛПЦ, које су оријентисане на посао и мало пажње поклањају социјалним односима показују највише ефикасности у екстремним ситуацијама, поготово ако је реч о високоструктурираним пословима. „Вође са високим ЛПЦ-ом су најефикасније у ситуацији када имају осредњу моћ и утицај, у условима неструктурираних послова“¹⁴¹.

Савремене теорије вођења истичу два теоријска правца вођења, тзв. харизматског или „трансформационог вођу“ и теорију самовођења. Харизматски вођа назива се трансформациони јер он тежи да трансформише организацију. Супротно трансакционом вођи који прецизно дефинише шта подређени треба да ураде како би се остварили циљеви организације, трансформациони вођа има задатак да подстакне самоактуелизацију, како би подређени чланови групе остварили више него што се од њих очекује. Да би то постигли вође користе личну визију и енергију. Теорија самовођења не негира вођство као социјалну функцију менаџера. Висока технологија не искључује раније развијене менаџмент методе, већ их само модификује, под одређеним условима. Да би самовођење било могуће неопходно је да постоје следећи услови: да постоје високообразовани извршиоци који су способни да својим вештинама и знањима обављају самостално послове групе. Друго, да извршиоци имају моћ да одреде метод и програм обављања послова и одговарајућу алокацију ресурса. Треће, да постоји веза између успеха групе и система награђивања. Самовођење спаја иницијативу и креативност подређених са стриктним принципима менаџмента.¹⁴²

2.3.5. Контрола као функција безбедносног менаџмента

Контрола је једна од пет интегралних фаза менаџмент процеса. Контрола се често истиче као последња фаза у процесу менаџмента којом се даје одговор на питање да ли је све што је планирано и урађено на задовољавајући начин. Овакав приступ је у основи погрешан јер контрола временски не долази на крају, већ је укључена у све фазе одвијања неког посла. Циљ контроле је да открије одступања од

¹⁴¹ Драгишић, З., исто.

¹⁴² Видети: Годоровић Ј., и други аутори, исто, стр. 113-118.

планираних величина у раним фазама и да омогући њихову корекцију пре него што посао буде завршен.

Основна сврха контроле је да се обезбеди да постигнути резултати неке организације одговарају планираним. Контрола је веома блиско повезана са планирањем, којим се дефинишу циљеви организације и начин постизања тих циљева. У том смислу контролу можемо одредити као процес којим се мери степен реализације планираних циљева, утврђивање степена одступања реализованих од планираних величина и стварање услова за благовремено и адекватно предузимање корективних активности.

Када би менаџери били сигурни да ће се сваки план који су сачинили, односно сваки циљ који су поставили, до краја и у потпуности остварити, тада контрола не би била потребна. Сви резултати били би онакви какви су планирани, без непријатних изненађења. Међутим, ствари у реалном животу веома ретко иду глатко и без проблема, јер сваки план, треба да спроведу људи, који у сваку активност уносе људска ограничења на која менаџер увек мора да рачуна. Поред тога промене у савременим околностима су толико брзе да нико није у стању да тврди да план који је данас сачињен већ за пар дана неће бити застарео. Због тога је неопходно да сваки план, и циљеви који су тим планом предвиђени, буду стално надзирани, контролисани и кориговани.

Потреба за контролом се повећава што је организација сложенија, и што је већи број нивоа менаџмента на који се делегирају овлашћења. Менаџери у сложеним организацијама делегирају своја овлашћења на сараднике, али и даље задржавају пуну одговорност за постигнуте резултате, што сталну контролу рада сарадника чини неопходним условом успеха самог менаџера.

У складу са тим, разлоге због којих долази до одступања реалних од планираних величина и учинака можемо систематизовати у неколико група.¹⁴³

Прво, промене у окружењу које могу бити економске, политичке, технолошке, безбедносне, или сличне, су веома честе, поготово у нестабилним друштвима какво је наше. Настанак оваквих промена је немогуће предвидети, а њихов утицај на

¹⁴³ Видети: Драгићић, З., исто, стр. 129.-146.

постизање планираних циљева може бити пресудан. Због тога је важно да се сталним праћењем и процењивањем ситуације у организационом окружењу овакве промене благовремено уоче, процени њихов утицај и креирају корективне акције.

Друга група разлога везана је за психолошке карактеристике запослених. Људи веома често нису у стању да схвате шта се од њих очекује, нису довољно стручно оспособљени за посао који обављају, у одређеним тренуцима попушта им пажња, оптерећени су другим обавезама и сл. Психолошка ограничења или слабости запослених често се појављују као проблем управо у безбедносном менаџменту, где је висок ниво концентрације код релативно досадних послова, услов успеха примене одређених безбедносних процедура. Због ових проблема у пракси веома често долази до одступања постигнутог од планираних циљева.

Трећа група разлога везана је за лојалност запослених. Неке групе запослених могу имати личне циљеве који нису подударни са циљевима које је организација поставила пред себе, или немају одговарајући ниво безбедносне културе, што може изазвати да они свесно, или несвесно, раде против интереса организације. Нелојалност запослених нужно ће довести до немогућности организације да оствари своје циљеве, па је основни задатак контроле коју менаџери спроводе да утврде у којој мери су запослени лојални и колико примењују безбедносне процедуре које су прописане.

Четврта група разлога због којих долази до немогућности постизања планских циљева односи се на грешке које су учињене приликом израде планова. Главна грешка у изради планова потиче од лоше урађених процена безбедности којима се превиде неки важни безбедносни проблеми, прецене, се или потцене, властите могућности и могућности носилаца безбедносног угрожавања, пропишу се неадекватне безбедносне мере и процедуре, што све нужно, доводи до немогућности да се остваре плански циљеви.

Према Деслеру „све што менаџери раде је повезано са контролом. Основни циљ сваког менаџера је да избегне непријатна изненађења и да буде сигуран да ће

увек моћи да предузме правовремену акцију¹⁴⁴. Да би менаџери били у стању да увек предузму правовремену корективну акцију потребно је да имају правовремене информације да постоје одступања од планираних величина.

Уз помоћ информација које се добијају контролом свака организација покушава да смањи неизвесност и да повећа предвидивост резултата својих активности у будућности. Помоћу информација до којих се долази спровођењем контроле, могуће је на време уочити правце промена које се дешавају у окружењу и на време предвидети мере којима се могу избећи штетни а повећати повољни утицаји из организационог окружења.

Да би информације имале употребну вредност у праћењу остварених резултата и предузимању корективних акција оне морају бити квалитетне, релевантне, свеобухватне и правовремене.

Квалитет информације огледа се у могућности да се на основу ње донесу исправни закључци о остваривању резултата који су планирани. Квалитет информације зависи од начина на који је прикупљена и од квалитета извора из кога су информације прикупљене. Лоша методологија прикупљања информација и непоздани извори увек ће дати лош квалитет информације. Информације се могу прикупљати на различите начине: путем увида у јавне евиденције, статистике, спровођењем различитих врста емпиријских истраживања, интервјуима, мерењима и сл. Веома је важно користити оне начине путем којих се добијају најпрецизнији подаци који су лако мерљиви и упоредиви. Сваки извор информације мора бити процењен са аспекта његове поузданости. По правилу, најпоузданији извори информација су јавне евиденције и статистички подаци који се воде и обрађују од стране непристрасног субјекта. Најнижи ниво поузданости имају информације које се прикупљају од стране запослених који су лично заинтересовани да своје резултате представе у што бољем светлу.

Релевантност информације зависи од њеног садржаја. Релевантним информацијама можемо сматрати оне на основу којих можемо закључивати битне чињенице о предмету контроле. Информација може бити тачна, поуздана и

¹⁴⁴ Dessler, G., исто, стр. 454.

квалитетна, али небитна за предмет контроле. У безбедносном менаџменту велики проблем представљају информације које се чине интересантним али немају много везе са предметом рада менаџера безбедности. Релевантност сваке информације до које се дође у процесу контроле треба добро проверити да би закључци били исправни.

Свеобухватност информација односи се на њихове квантитативне карактеристике. Добри закључци се не могу доносити уколико не постоји довољна количина информација које, уколико је могуће, покривају све сегменте рада који се контролишу. Приликом планирања контроле потребно је испланирати прикупљање свих релевантних информације на основу којих се може донети закључак о степену остваривања планираних циљева и разлозима због којих је дошло до евентуалних девијација у постизању циљева.

Правовременост је неопходан услов да би се нека информација уопште могла узети у разматрање. Да би се обезбедила правовременост информација неопходно је да систем контроле буде добро испланиран да би се избегла непријатна изненађења. Уколико постоје озбиљна одступања у остваривању планираних циљева веома је важно да се то на време открије, јер је само тако могуће избећи негативне последице грешака до којих се долази у току рада.

„Око 80 процената сметњи у функционисању предузећа настаје услед проблема у комуницирању. Лоше комуницирање је последица недовољног броја потребних или великог броја непотребних информација. Информације представљају пословни ресурс број један модерног предузећа. Информације омогућавају обављање менаџмент процеса, посебно фаза планирања и контроле.“¹⁴⁵

Информације до којих се долази у процесу контроле представљају основ за оцењивање у којој мери се остварују планирани циљеви, али и повратне информације које се користе у процесу израде планова. Информације које се добијају путем контроле покрећу нови циклус менаџмент процеса.

Контрола, као веома важна фаза менаџмент процеса мора бити добро организована. Добра организација контроле подразумева да се контрола врши на

¹⁴⁵ Годоровић, Ј., и други, исто, стр 129.

такав начин да обезбеди правовремено откривање одступања од планираних циљева и да се омогући отклањање одступања пре него што се заврши одређена фаза планираних активности. Поред тога контрола не сме да омета нормално одвијање посла.

Контрола код запослених често изазива негативне реакције и њена перцепција није у складу са правима значајем који контрола има за функционисање организације. „Контрола, обично, има негативне конотације јер се њоме угрожава дискреција појединаца или група у доношењу одлука“.¹⁴⁶ Овакав став о контроли настаје као последица стриктне и честе контроле, која појединцима или групама, не оставља довољно простора да искажу своје стручне и личне потенцијале. Превише честа и стриктна контрола спутава креативност, што утиче на пад мотивације и изазива смањивање ефективности групе. Када су контроле превише стриктне и честе, запослени много више размишљају како да задовоље „контролоре“, него како да постигну боље резултате, што уз нејасне критеријуме по којима се контрола врши, неизбежно доводи до штетних последица по организацију. У безбедносном менаџменту, стриктне и честе контроле су неопходне због врсте послова којима се баве менаџери безбедности, али добро организован систем контроле чини да се избегну штетни ефекти оваквог начина контроле.¹⁴⁷

Са друге стране, недовољна контрола доводи до неефикасности у испуњавању планираних циљева, конфузије и хаоса. Један од главних циљева рационалног система контроле треба да буде успостављање баланса између потребе да се успостави пуна контрола над свим активностима које се одвијају у оквиру једне организације и поштовања дискреције појединца и развијања индивидуалне и групне креативности. Због тога је важно да се контрола организује као систем, који мора

¹⁴⁶ Исто, стр, 130.

¹⁴⁷ Одређивање индикатора контроле и нормирање стандарда се поставља као есенцијално питање за успех система контроле у безбедносном менаџменту. Грешке које се у том погледу направе могу штетно утицати на целокупно одвијање посла. Уколико, на пример, полицији као индикатор контроле поставимо број поднетих кривичних и прекршајних пријава у временском периоду на који се односи контрола, то ће се негативно одразити на квалитет полицијског рада. Иако постављање овог критеријума делује наизглед мотивишуће, претерана трка полицајаца да поднесу што више кривичних и прекршајних пријава лоше ће се одразити на квалитет тих пријава, а може утицати лоше и на однос полиције и грађана. Промена кривичнопроцесног законодавства у Србији је ублажила штетне последице овако постављених стандарда контроле, али је пример веома индикативан.

бити јасан, прецизан, експлицитан и заснован на недвосмисленим принципима. Сваки систем контроле састоји се од елемената контроле, од различитих врста контроле и принципа контроле.

Елементи система контроле дефинисани су Моклеровом дефиницијом контроле¹⁴⁸, према којој је основни циљ контроле да се плански циљеви преточе у стандарде контроле, да се дефинише повратне спрега, да се пореде постигнути резултати са претходно дефинисаним стандардима, да се одреди величина и значај одступања и да се предузму корективне акције како би се евентуална одступања довела у склад са стандардима.

Систем контроле се састоји од четири фазе које представљају елементе овог система:

1. дефинисање стандарда и метода мерења резултата,
2. мерење резултата,
3. поређење резултата са стандардима,
4. предузимање корективне акције.

Дефинисање стандарда и метода мерења резултата представља прву фазу процеса контролисања. Стандарди се дефинишу на основу планираних циљева и уједно се одређују менаџери унутар организације који су одговорни за остваривање планираних резултата, као и методе на основу којих се ти резултати мере. Стандарди морају бити разумљиви, реални и прихватљиви онима који су обухваћени системом контроле. Методе за мерење резултата морају бити поуздане. Да би плански циљ могао постати стандард контроле уз њега се морају дефинисати одговарајућа мерила резултата.

Стандарди морају бити добро дефинисани, јер у одсуству стандарда менаџери могу претерано реаговати на мала одступања или пропустити да реагују на битна одступања од планираних циљева. Стандарди контроле имају две битне функције: мотивациону и функцију „прага“ поређења. Достижање стандарда мотивише људе, међутим, уколико су стандарди превише високо постављени они могу деловати

¹⁴⁸ Наведено према: Тодоровић, Ј., и други аутори, исто.

демотивишуће, пошто су запослени унапред свесни да неће моћи да их достигну. Уколико се стандарди ниско поставе то такође демотивише запослене пошто их могу постићи без много напора, и чини да ефикасност рада буде много испод реалних могућности организације.

Стандарди су величине које се мењају у зависности од фактора који на њих утичу. Рецимо уколико се набави нова безбедносна опрема, стандардизоване процедуре ће морати да се прилагоде могућностима нове технологије, уколико дође до пораста стопе криминала или промене доминантних кривичних дела у једној средини, стандарди ће се прилагодити новонасталим околностима итд. Стандарди се морају мењати сваки пут када фактори који утичу на дефинисање стандарда, поштујући при том основна правила која се односе на прецизност, реалност и прихватљивост стандарда.

Стандарди могу бити класификовани на више начина у зависности од критеријума који се користе. „Стандарди могу бити изражени у новцу, времену, квантитету, квалитету, комбинацији ових стандарда или „неопипљивим“ стандардима. Без обзира на категорију стандарда која се користи, новац, квалитет или квантитет, уобичајена је процедура да се прво одабере штап за мерење. На пример за трговца то може бити да прода робу у вредности од 8000 долара за недељу дана, ако је критеријум стандарда новац, или да прода 10 јединица производа дневно, ако је критеријум стандарда квантитативан“.¹⁴⁹

Стандарди контроле могу бити физички, који се изражавају физичким јединицама мере и они се у безбедносном менаџменту користе приликом контроле рада полиције, рецимо колико је кривичних дела и прекршаја расветљено у одређеном временском периоду, колико је спроведено контрола возача и др. У контроли приватних безбедносних организација ова врста стандарда је веома коришћена за утврђивање броја интервенција, броја пружених услуга и сл.

Стандарди трошкова изражавају се у новцу. У јавном безбедносном менаџменту ови стандарди се увек користе код контроле утрошка буџета. На основу

¹⁴⁹ Dessler, G., исто, стр. 457.

контрола које се спроводе применом ових стандарда планирају се буџети за наредни временски период.

Стандарди капитала представљају вредносно изражене нормативе инвестираног капитала, односно остварени профит у односу на инвестирани капитал. Ова врста стандарда користи се у приватном сектору безбедности ради оцене успешности предузећа и за процену финансијске ефикасности улагања у систем безбедности.

Стандарди прихода се изражавају новчаним јединицама и односе се на приходе остварене продајом роба или услуга. Користе се за контролу пословања приватних предузећа која се баве пружањем услуга безбедности, али и јавном безбедносном менаџменту када организације као што су војска и полиција приходују од пружања услуга трећим лицима.

Стандарди програма се изражавају углавном временом у коме је планирано да неки пројекат буде спроведен у дело. Овај стандард се односи на норме учинка и зато се најчешће изражава у временским јединицама.

Неопипљиви стандарди представљају одређена правила и процедуре којих се запослени морају придржавати. Ови стандарди се односе на појмове који се не могу егзактно измерити нити изразити одређеним јединицама мере. Ови стандарди се односе на домен безбедносне културе, пословне етике, односа са јавношћу и сл. Постављање неопипљивих стандарда се може вршити на основу коришћења упитника, интервјуа и сл. Неопипљиви стандарди се често користе у безбедности, пошто је сам појам безбедности веома тешко одредити, а готово немогуће измерити. Ниво утицаја који на стање безбедности неке организације, заједнице или пословног пројекта остварују безбедносне мере које се примењују на основу плана безбедности, представља основни предмет контроле. Стање безбедности може се контролисати применом различитих врста стандарда, али примена ни једног објективног стандарда не може до краја одговорити на битна питања без којих не можемо дати оцену стања безбедности. Процена нивоа безбедносне културе запослених може се проценити само применом неопипљивих стандарда који задиру у људске мотиве, ставове и очекивања. Квалитет безбедносне процене можемо проценити ако сами оценимо

елементе који су у процени, која је предмет безбедносне процене, узети као релевантни, односно, ако сагледамо и оне елементе које менаџери који су израдили безбедносну процену нису узели у обзир.

Успешна контрола подразумева да и неопипљиви стандарди морају бити у највећој могућој мери објективизирани, као би се избегла самовоља менаџера који контролишу стање безбедности и спровођење безбедносних мера на основу неопипљивих стандарда.

Стандарди могу бити утврђени на више начина, али већина аутора указује на: историјски, компаративни, технички и субјективни.

Историјски метод за утврђивање стандарда користи претходна искуства и резултате остварене у прошлости као основу на којој се утврђују стандарди. Предности ове методе огледају се у реалном сагледавању могућности запослених и организације, као и реалних потреба у области безбедности. Као стандарди, приликом коришћења овог метода, узимају се просечни резултати остварени у претходном периоду. Немогућност антиципације промена представља главну слабост овог метода за одређивање стандарда контроле.

Компаративним методом стандарди се одређују на основу резултата које су постигле друге организације које се баве истоврсним послом. До сазнања о резултатима које су постигле друге организације долази се директним увидом, разменом података или увидом у стручне публикације које објављују овакве податке. Организације које се баве безбедношћу веома често податке који се односе на њихово пословање чувају као пословну тајну, а државне безбедносне организације такве податке штите као државну и војну тајну, што прикупљање ових података чини изузетно отежаним. Поред тога, ови подаци имају веома мали ниво поузданости пошто никада не можемо бити сигурни који су фактори били пресудни да одређене безбедносне организације постигну добре или лоше резултате. На пример, тешко можемо узети као стандард резултат организације која има одличну техничку опрему и велики буџет за организацију која располаже застарелом опремом, необученим кадровима и ниским буџетом. Код успостављања стандарда коришћењем овог метода мора се имати у виду целокупан контекст резултата који је нека организација

постигла да би се ти резултати могли узети као стандард контроле за организацију коју контролишемо.

Технички стандарди се одређују на основу претходно утврђених стандарда за одређени тип посла. Овај метод се може користити за контролу експлоатације и одржавања одређених техничких средстава. Технички стандарди имају веома велики ниво поузданости и објективности, али је њихов домет у безбедносном менаџменту ограничен.

Субјективни метод се ослања на искуство менаџера. Тако на пример менаџер безбедности може да постави одређене стандарде у приватној служби обезбеђења на основу искуства које је стекао радећи ту врсту посла у као војни или полицијски старешина. Овај метод има веома велику примену у безбедносном менаџменту, али приликом његовог коришћења треба испунити све захтеве који произилазе из основних начела контроле, како би се избегла самовоља менаџера. Субјективно постављени стандарди морају бити јасни, објективизирани и унапред познати свима на које се односе. Једном успостављени ови стандарди се, без објективних разлога, не могу често мењати, јер то може демотивисати запослене.

Када се стандарди успоставе они се морају односити на све менаџере у једној организацији. На тај начин сваки менаџер се чини одговорним за свој рад, односно рад организационе јединице којом руководи. Овакав приступ је неопходан јер се на тај начин прецизно лоцира одговорност за одступања од стандарда, и омогућава да се прецизно установе разлози за одступања и лакше одреде неопходне корективне активности. Поред тога стандарди се успостављају по стратегијским активностима организације, како би се омогућило да се контролишу све битне активности. Тако успостављен систем контроле треба да буде што је могуће једноставнији и ефикаснији, као би се корективне активности могле предузети благовремено. Стандарде контроле треба везати за центре одговорности, како би сваки центар био одговоран за активности који се налазе у домену његових функција.

Мерење резултата је друга фаза у систему контроле без које није могуће поредити остварене са планираним резултатима. Мерење резултата захтева постојање

повратне спреге. Резултати мерења достављају се назад доносиоцима одлука, чиме целокупан менаџмент процес добија облик круга.

Мерење резултата је активност која се непрекидно понавља, а фреквенција тог понављања зависи од природе активности чији се резултати мере. Топ менаџмент одређује које се акције мере, стандарде резултата за све делове организације и све активности које се мере, пошто све активности немају исти ниво значајности, нити су резултати свих активности мерљиви. Поред тога ни сви резултати мерења не иницирају нове активности, било корективне, било активности које подразумевају покретање новог планског процеса.

Нижи нивои менаџмента такође могу одредити, у оквиру свог домена деловања, које ће се активности мерити, како би остварили потпуни увид у остваривање планираних циљева.

Фреквенција мерења, односно временски интервал у коме се врши мерење резултата зависи од природе активности чији се резултати мере. У кратким временским интервалима мере се резултати једноставнијих активности чији се резултати могу лако квантификовати. На пример, у полицији се дневно и недељно мери учинак полицајаца, у приватним предузећима за безбедност рад радника на одређеним радним местима, такође се дневно, недељно и месечно мери и резултате мерења доносиоци одлука примају у кратким временским интервалима. Укупан резултат организација који се односи на ефикасност и ефективност њиховог пословања, било да је реч о приватним или јавним безбедносним организацијама мери се на тромесечном, шестомесечном и годишњем нивоу. Јавне безбедносне организације имају законску обавезу да резултате свог рада најмање једном годишње презентују парламентарном одбору за безбедност, што представља веома важан вид дугорочног мерења резултата рада, о коме ће касније бити више речи.

Да би мерење резултата рада било ефикасно и ефективно оно мора да буде директно везано за стандарде. Уколико мерење није директно везано за стандарде информације до којих се дође таквим мерењем биће ирелевантне и из тих резултата нећемо добити информације које су нам неопходне да би стекли прави увид у ниво остварења планираних циљева организације. Данас је често присутан проблем

сувишних мерења, која су скупа и дају нам податке који могу бити веома детаљни, али безначајни. Са друге стране, постоје резултати који су веома важни, али се до њих може доћи само посредним мерењем неопипљивих стандарда. Ниво безбедносне културе у једној организацији није могуће егзактно измерити, али се до тог резултата може доћи посредно на основу података о кашњењу на посао, боловања, сукоба на радном месту, флукуације запослених, броја жалби запослених и сл.

Узорак на коме се врши мерење мора да буде репрезентативан за целу популацију. Веома често нисмо у могућности да меримо све аспекте пословања неке организације, па се због тога мерења обављају само на делу пословања, или на појединим случајевима или узорцима. Веома је важно да узорак на коме се врши мерење одсликава стање целине активности која је предмет контроле.

Мерење мора да буде поуздано и валидно. Поузданост упућује на стабилност резултата мерења током времена. Исти услови треба да доведу до истих резултата у два узастопна мерења. Валидност мерења је захтев да се заиста мери оно што имамо намеру да меримо, а не нешто друго. Мерни инструменти који се користе морају да нам дају податке о величинама на основу којих вршимо контролу. Ако желимо да истражимо ниво безбедносне културе запослених у једном предузећу, то можемо учинити путем упитника, односно скале ставова. Упитници морају бити тако сачињени да одсликавају ставове запослених битне за утврђивање нивоа безбедносне културе, а не нешто друго. Уколико желимо да измеримо успешност полиције у локалној заједници, морамо бити сигурни да су питања у упитнику постављена на тај начин да ће одговори на њих одсликавати однос грађана према локалној полицији а не рецимо, према политичкој ситуацији у општини или раду локалних комуналних служби.

Уколико користимо непоуздане и невалидне мерне инструменте, доћи ћемо до потпуно погрешних података о нивоу остварења планираних циљева. На основу погрешног мерења можемо доћи до податка да се планирани циљеви остварују у потпуности, а да у реалности постоје значајне девијације, или можемо доћи до закључка да постоје битне девијације, које заправо не постоје. Поред тога, лоши мерни инструменти, уколико установимо да постоје девијације, које заиста постоје,

даће нам лажну слику о стварним узроцима због којих је дошло до девијација. У сваком случају лоше мерење ће довести до лоше контроле, а лоша контрола ће се негативно одразити на процес планирања, што ће изазвати битне промашаје у целокупном менаџмент процесу.

У следећој фази контролног процеса пореди се оно што је постигнуто са оним што је требало да буде постигнуто. Да би се ова фаза контролног процеса спровела на квалитетан начин важно је да претходне две фазе буду добро спроведене. Уколико постоје тачно одређени стандарди, односно вредности за које се очекују да буду остварене и добро измерени подаци о оствареним учинцима, менаџери поређењем ове две групе величина могу лако доћи до сазнања колико су остварени учинци у складу са очекивањима.

Поређењем ових група величина установљавају се одступања остварених од планираних учинака. У безбедносном менаџменту ти учинци могу бити веома различити и они се односе на све аспекте функционисања безбедносних организација, од остваривања превентивне заштите, постигнутих резултата у спровођењу безбедносних мера, до финансијских аспеката пословања, који су битно различити за јавне безбедносне организације које се финансирају из буџета и приватне организације које послују на тржишту и у том погледу су сличне било ком услужном предузећу. Веома је важно да се установе девијације за сваки центар одговорности унутар једне безбедносне организације, како би се корективна акција могла правилно усмеравати.

Пракса показује да одступања од стандардних учинака увек постоје, тако да се главна пажња менаџера не усмерава на постојање девијација, већ на толерантне границе у којима се крећу девијације. Граница толеранције треба да се утврди приликом утврђивања стандарда, за сваку делатност и за сваку центар одговорности унутар безбедносне организације. Постојање границе толеранције је важно јер менаџери не треба да реагују на мала и безначајна одступања, која не могу довести до штетних последица по вредности које се штите, нити могу угрозити мисију организације. Превише корективних акција ради исправљања небитних девијација би превише оптеретило менаџере и довело до штетних последица у социјалној клими

организације. Да би овај приступ контроли могао да функционише, неопходно је утврдити дозвољену границу одступања од стандарда. Сва одступања која излазе из оквира предвиђених стандардима имају карактер „непожељних одступања“¹⁵⁰, која захтевају посебну менаџерску пажњу и контролу.

Посебну пажњу треба посветити одступањима од неопипљивих стандарда, јер је веома тешко мерити учинке који се постижу у остваривању ових стандарда, а поготово је тешко прописати прецизно колика су дозвољена одступања од ових величина. Квалитативни показатељи који се односе на морал, ставове, мотивацију, имају изузетан значај за безбедносни менаџмент и не може бити праве контроле функционисања безбедносних организација уколико се наведене величине на неки начин не стандардизују и држе под контролом.

У области безбедности постоје делатности које имају тзв. “нулту толеранцију”¹⁵¹, тј. ни најмања одступања од стандардних величина нису дозвољена. Такве делатности морају бити унапред дефинисане и на њих се примењује систем непрекидне контроле, где се одступања од стандардних процедура одмах региструју и одмах коригују. Такве активности су на пример контрола на аеродромима, приступна контрола у постројења која садрже екстремно опасне силе, контрола уласка у важне институције и све друге безбедносне активности где би одступање од стандарда могло да изазове катастрофалне последице.

Предузимање корективне акције као четврта фаза контроле, за разлику од претходне три фазе, не предузима се увек у оквиру контролног процеса. Када се установљене девијације крећу у границама толеранције, односно када су девијације мале, оне се не анализирају нити захтевају корективну акцију већ се просто занемарују.

Често су, међутим, одступања од стандарда значајна и захтевају корективну акцију, која је завршна фаза контролног процеса. Када се установе одступања, приступа се анализирању узрока због којих је дошло до девијације од стандарда, да би се ти узроци отклонили одмах или у наредном временском периоду. „Отклањање

¹⁵⁰ Види шире: Бабић, М., Ставрић, Б., *Менаџмент*, КИЗ Центар, Београд, 1999., стр 298-301

¹⁵¹ Драгишић, З., исто, стр. 139.

узрока врши се путем корективне акције, која се предузима након што се узроци настанка одступања детаљно анализирају и установи њихова права природа и димензије¹⁵².

Корективна акција укључује спровођење многих мера, од обуке људства, набавке нове безбедносне технике, премештања неких запослених, појачавање превентивних мера и сл.

Веома често узроци девијација се налазе у лошим безбедносним проценама, лошим плановима, лошој организацији и другим пропустима у фази планирања. Приликом анализирања узрока одступања од планираних циљева, потребно је целокупан менаџмент процес „враћати уназад“¹⁵³, како би се дошло до правих узрока девијације. Уколико се установи да су узроци девијације лоши планови, неопходно је да корективна акција обухвати промене безбедносних процена, понекад треба променити и саму методологију по којој се израђују безбедносне процене, ревизију планова, циљева организације, процедура, политика и др.

Наведене фазе контролног процеса треба третирати као међузависне делове система контроле. На основу података до којих се дође током процеса контроле коригују се планови или израђују нови, евалуирају се методологије за израду процена безбедности и планова, другим речима почиње нови круг менаџмент процеса.

Контрола се може класификовати према великом броју различитих критеријума. Према пословној функцији која се обавља контрола може бити: контрола финансијског пословања, управна контрола, контрола законитости пословања, контрола производње, контрола безбедносних мера и сл. Према начину на који се обавља, контрола се може бити: „водећа контрола, „да-не“ контрола и постакциона контрола“¹⁵⁴.

Основна карактеристика водећег модела контроле ја да се контролна акција предузима пре него што се операција или пројекат који се контролишу заврше. Контролна акција се предузима још у фази припреме операције или пројекта ради предвиђања могућих узрока одступања и предвиђања потребних ресурса да се

¹⁵² Исто.

¹⁵³ Исто.

¹⁵⁴ Драгишић, З., исто, стр. 139.

отклоне узроци који могу довести до одступања, односно да се отклоне штетне последице пре него што угрозе успешан довршетак операције или пројекта. Овај модел контроле подразумева да контролна акција траје сво време операције или пројекта. На тај начин се обезбеђује правовремено предузимање корективне акције и успешан довршетак започете активности.

Контролисање остварених резултата, по овом моделу контроле, постиже се и помоћу постављања „контролних тачака“, односно спровођењем контроле у одређеним временским размацама или контролисањем сваке фазе остварења активности, на тај начин се проверава напредак у остварењу планских циљева много пре него што се активност заврши. Корективна акција се код овог модела контроле спроводи одмах након обављене контроле, без посебних анализа узрока због којих је дошло до одступања. Анализа узрока девијације, и самих девијација, врши се након завршене активности, добијени резултати се користе као основа за нови циклус планирања.

Водећа контрола се предузима у случајевима посебно осетљивих активности код којих је могућа појава великог броја узрока који могу угрозити пројекат или операцију или се кризне ситуације могу појавити неочекивано. Водећи модел контроле примењује се веома често у безбедносном менаџменту, посебно у осетљивим војним или полицијским операцијама, које се предузимају у условима велике неизвесности. Такве су рецимо акције ослобађања таласа, обезбеђивања великих скупова на којима се појављују посебно значајне личности и друге активности које захтевају посебно строг режим контроле.

Контрола по „да-не“ моделу, врши се на контролним тачкама процеса, али она не подразумева постојање корективне акције већ се започети посао прекида уколико нису испуњени плански циљеви, и обрнуто уколико се плански циљеви остваре на том нивоу активности посао се наставља. Модел „да-не“ контроле се често користи као допунски модел за водећу контролу када није могуће предвидети све узроке девијација, а девијације имају толики ниво значајности да доведу у питање исплативост или безбедност целокупне активности или пројекта. Овај модел контроле користи се за пројекте истраживања и развоја, који се прекидају ако се, на

основу контроле перформанси у одређеним фазама пројекта, установи да резултати пројекта неће бити такви да оправдају даља улагања. Овај модел контроле користи се код свих пројеката где је сигурност критичан фактор или код пројеката који изискују већа материјална или финансијска улагања.

„У безбедносном менаџменту, ова врста контроле се такође користи за оцену вредности истраживачких и развојних пројеката и ради оцене исплативости пројеката техничке заштите. У сектору јавног безбедносног менаџмента, овај модел контроле се често користи у акцијама заштите и спасавања, у неким војним или полицијским операцијама.“¹⁵⁵

Коришћење „да-не“ модела контроле је блиско повезано са cost/benefit анализама. На пример, у акцијама заштите и спасавања увек се поставља питање да ли је исплативо и морално оправдано угрозити животе неколико спасилаца ради покушаја да се спасе једно лице, у ситуацијама високог ризика и без великих шанси да се угрожено лице, или лица, стварно и спасу. Одговор подразумева детаљну контролу свих мера које је организација цивилне заштите до тада предузела као и процену реалног стања угрожености, на основу којих би се донела одлука о даљем наставку акције. Оваква одлука подразумева велику моралну дилему и она никада није чисто менаџерска одлука. Међутим, менаџери безбедности се морају припремити на тешке моралне одлуке и на преузимање одговорности за сваку своју одлуку.

Постакциони модел контроле подразумева мерење резултата и њихово поређење са стандардима контроле након што пројекат буде завршен. Овим моделом контроле се утврђује одступање и разлози одступања вредности постигнутих резултата од стандарда који су предвиђени планом. Овај вид контроле се најчешће користи у свим областима менаџмента. Основни проблем пост-акционе контроле је немогућност да се предузме корективна акција пре него што целокупан пословни циклус буде завршен. Резултати ове контроле могу се „констатовати, анализирати и предузети корективна акција *pro futuro*“¹⁵⁶, односно, девијације које су се појавиле у

¹⁵⁵ Драгишић, З., исто, стр. 140.

¹⁵⁶ Исто, стр. 141.

једном пословном циклусу могу бити исправљене тек у следећем. Резултати који се добијају овим моделом контроле су добра основа за планирање и они представљају спону између два циклуса менаџмент процеса.

Предности модела постакционе контроле огледају се у његовој комфорности за запослене и већем степену слободе акције нижих нивоа менаџмента и непосредних извршилаца, што подстиче њихову креативност и утиче на побољшање интерперсоналних односа. Постакцијом контролом могу се поставити стандарди за награђивање запослених у зависности од резултата које су постигли у раду. Овај модел стимулације познат још код Тејлора, у својим модификованим облицима, примењује се и данас због својих стимулационих ефеката и утицаја на ефективност рада запослених.

Буџетска контрола представља најбољи пример за пост акциону контролу. Надлежни органи, преко контроле остварења буџета контролишу рад безбедносних служби на веома експлицитан начин. Буџет представља план расхода и прихода, путем кога се одређује оквир за рад свакој служби. Све девијације у остварењу расхода и прихода се, по буџетским ставкама, веома јасно виде, што представља веома добре показатеље за планирање буџета за наредну годину. Девијације у остварењу буџета показују и девијације у остварењу других делова плана тако да контрола буџета има много шире контролне домашаје од пуке финансијске контроле.

Наведени модели контроле представљају пре дидактички уобличену слику о контроли, него што се у пракси појављују у чистом облику. Различити модели контроле се комбинују, међусобно преплићу и допуњавају у циљу постизања пуне контроле над свим активностима које се предузимају у оквиру једне организације.

Контрола у сваком систему мора да одговори основним захтевима који се постављају пред ову фазу менаџмент процеса. Да би контрола била сврсисходна она мора да буде ефикасна и ефективна. Односно, она мора бити рационална и мора обухватити све битне параметре помоћу којих се може контролисати у којој се мери остварују планирани циљеви у једној организацији. Да би се постигла ефикасност и ефективност система контроле он мора бити заснован на одређеним принципима. Принципима контроле различити аутори приступају на различите начине, међутим,

имајући у виду карактеристике менаџмента безбедности, чини се да поштовање следеће групе принципа омогућава да се контролом постигну очекивани ефекти.

Информације на основу којих се врши контрола морају бити потпуно поуздане, јер се на основу тих информација предузимају корективне акције и планира нови менаџмент циклус. Основни садржај поузданости информације чини њена истинитост и свеобухватност. Информације које садрже податке који не одговарају реалном стању ствари и које само делимично покривају предмет контроле, не могу бити основа за предузимање корективних акција и отпочињање новог менаџмент циклуса. Корективне акције које би се предузеле на основу непоузданих информација могле би само да погоршају постојеће проблеме или да проузрокују нове. Оцена поузданости информација на основу којих се доносе различите врсте одлука у безбедносном менаџменту представља један од најважнијих задатака сваког менаџера безбедности. Свака информација би требало да буде проверена из више извора и оцењена у контексту информација чија је поузданост већ утврђена.

Правовременост информација је неопходан услов да би нека информација била узета у разматрање приликом вршења контроле. Информације на основу којих се врши контрола морају бити на време прикупљене, оцењене и класификоване. Уколико се информације не прикупљају и обрађују правовремено контрола ће се обављати „напамет“¹⁵⁷ или ће се закаснило реаговати, што увек доводи до штетних последица. Поштовање овог принципа је блиско повезано са систематским прикупљањем и обрадом свих врста података који су битни за безбедност неке организације и заједнице, груписањем и обрадом релевантних података добијају се информације на основу којих се доносе одлуке. Такве информације, које су благовремено прикупљене и обрађене, представљају добру основу за контролу јер се у сваком тренутку на основу њих може извршити „пресек стања“, и утврдити у којој мери постигнути резултати одступају од планираних циљева. Уколико се информације систематски прикупљају и обрађују свако значајније одступање од планираних циљева биће правовремено примећено, што оставља довољно времена да се предузме корективна акција и избегну неповољни безбедносни догађаји.

¹⁵⁷ Исто, стр. 142.

Критеријуми који се користе у систему контроле морају бити објективни и разумљиви. Сваки запослени мора унапред знати шта се од њега очекује, који се резултати сматрају успехом а који неуспехом, и на основу којих информација ће се процењивати свачији успех. Јасни критеријуми контроле мотивишу запослене и доприносе остварењу циљева организације. Уколико се систем контроле ослања на објективне критеријуме, без превише простора за субјективне процене носиоца контроле, веће су шансе да доносиоци одлука добијају квалитетније информације на основу којих ће се предузимати ефикасне и ефективне корективне акције. Систем контроле који се ослања на субјективне оцене носилаца контроле и који је неразумљив, фрустрира запослене и доводи до конфузије, што нарушава мотивацију запослених и ствара простор за злоупотребе менаџера. Нејасан и необјективан систем контроле не би угрозио само контролу као фазу менаџмент процеса, већ би могао да доведе до много дубљих конфликта у једној организацији и да, уместо стварања услова да систем контроле допринесе стабилности организације, доведе до озбиљних проблема који могу проузроковати озбиљне проблеме у функционисању организације, па чак и њен крај.

Систем контроле мора бити усмерен на битна питања, односно на оне послове од којих у највећој мери зависи остваривање мисије организације. У безбедносном менаџменту посебну пажњу треба посветити стратешким питањима, односно спровођењу оних планова, и делова планова, који се директно рефлектују на достизање стратешких циљева организације. Фокусираност на битна питања доприноси ефикасности и ефективности контроле јер се енергија и ресурси усмеравају на она питања где би значајније одступање од планираних циљева имало најтеже последице. У одређивању приоритетних питања у систему контроле треба поћи од општег ка појединачном, односно од оних циљева који су за безбедност неке организације најважнији и где би одступања од планова могла донети највећу штету организацији. „Предузимање корективних акција, када је одступање од стратешких циљева у питању, благотворно делује и на остваривање тактичких циљева, који у безбедносном менаџменту увек представљају саставни део веће стратешке целине. Фокусирањем на споредна питања губи се драгоцено време, ресурси и енергија, а

корективна акција на нивоу тактичких циљева не може да доведе до спречавања неповољних безбедносних трендова који се одвијају на стратешком нивоу.¹⁵⁸ Одређивање битних питања на која се фокусира систем контроле врши се на основу анализе утицаја претње, односно на основу штетних учинака до којих могу да доведу одступања од планираних циљева у одређеној области безбедности организације.

Систем контроле мора да буде економичан, односно трошкови система контроле не смеју да пређу користи које систем контроле доноси. Најбољи начин да се избегну непотребни трошкови у систему контроле је дефинисање минималног нивоа праћења активности који утичу на остварење циља. На пример није потребно дневно контролисати спровођење неке безбедносне процедуре која се дневно одвија по више десетина пута, довољно је једном недељно, или ређе у зависности од нивоа утицаја претње, извршити увид у спровођење процедуре, јер би свако чешће контролисање било скупо и стварало би незадовољство службеника који спроводе процедуру, а не би довело до повећања ефикасности контроле.

Систем контроле мора да одговара свим специфичностима организације, од врсте посла којим се организација бави па до организационе структуре. Врста посла којом се нека организација бави представља полазну основу за успостављање система контроле у безбедносном менаџменту. Систем контроле безбедносних мера и процедура полази од њихове важности за опстанак и раст организације, посебна пажња и строжији систем контроле примењују се код оних мера и процедура чије би пропуштање могло довести до тешких последица по опстанак и раст организације, док се блажи систем контроле примењује код мера и процедура чије би пропуштање имало лакше последице које организација може да амортизује. Усклађивање система контроле са карактеристикама организације доприноси ефикасности и ефективности контроле јер се контролне мере усмеравају према најважнијим циљевима организације, од чијег остваривања зависи достизање мисије организације.

Систем контроле треба прилагодити и организационој шеми, односно контролне активности менаџмента безбедности треба усмерити према најодговорнијим људима у организацији, односно према оним деловима организације

¹⁵⁸ Исто, стр. 143.

који имају највећу моћ и утицај и чије би грешке, или лоше намере, довеле до озбиљних безбедносних проблема. Посебну пажњу треба посветити неформалној организационој шеми, односно открити постојање неформалних центара моћи, и уколико они постоје, неопходно је остварити контролу над њиховим радом. Контрола над радом важних људи у једној организацији и над неформалним центрима моћи често није могућа коришћењем уобичајених контролних механизма, због тога је веома важно развити механизме којима се може контролисати рад ових особа, или група, унутар организације. У сврху ове контроле најчешће се користе контроле преко резултата које постижу, рачуноводствених извештаја, одређене социометријске технике и други методи који могу указати на одступања од планираних циљева који настају као последица лошег рада важних руководиоца или неформалних група унутар организације. Да би се оваква контрола могла спроводити неопходна је пуна подршка топ менаџмента менаџерима безбедности, уз унапред јасне циљеве, методе и критеријуме контроле, јер би се оваква контрола у супротном могла претворити у обично шпијунирање.

Флексибилно постављен систем контроле омогућава да се благовремено реагује на одступања од планираних циљева и на промене у организационом окружењу. Флексибилност контроле постиже се кроз флексибилно постављене контролне механизме и кроз флексибилно организовану фреквенцију контроле. Уколико се инсистира на унапред постављеним механизмима контроле и на спровођењу контроле у тачно утврђеним временским размацама, контрола се претвара у рутину што може неповољно утицати на ефикасност и ефективност контроле. Поред тога, промене које се дешавају у организационом окружењу утичу на промене природе безбедносних претњи које се могу изненадно појавити. Систем контроле служи да спречи непријатна изненађења. Уколико систем није флексибилан у смислу механизма и у смислу фреквенције контроле, могућност да се непријатна изненађења догоде расте, без обзира на постојање система контроле. Неповољан безбедносни догађај ће се десити на начин који није обухваћен механизмом контроле и у време које фреквенција контроле не покрива, што може изазвати озбиљне последице по опстанак и раст организације. Да би се избегла непријатна изненађења,

систем контроле треба да зависи од безбедносне процене. Уколико се безбедносном проценом предвиди промена природе безбедносне претње, њен раст или опадање и могућност појављивања у одређеном времену, неопходно је да се систем контроле безбедносних мера прилагоди стању безбедности које је установљено проценом безбедности. Резултати до којих се дође у процесу спровођења контроле представљају полазну основу за израду нове процене безбедности, чиме се успоставља међузависност процеса израде безбедносних процена и система контроле, што чини један од најважнијих механизма за успешно функционисање безбедносног менаџмента.

Контрола мора бити конструктивна. Овај принцип захтева да резултати контроле имају практичну примену. Контрола, поред утврђивања одступања у остваривању планираних циљева организације, мора и да предложи одговарајућу корективну акцију. То значи да механизми контроле морају бити тако осмишљени да се њима долази до информација које иницирају адекватну акцију којом ће уочени недостаци бити отклоњени. Основна слабост система контроле огледа се у превеликом поклањању пажње информацијама до којих се лакше долази и онима које се лакше мере, без обзира на њихову практичну примењивост и релевантност за систем контроле. Због тога се често дешава да постоји „превише небитних информације и премало информација на основу којих се могу доносити квалитетне одлуке“¹⁵⁹. Контрола представља фазу безбедносног менаџмента на основу које се отпочиње нови циклус планирања, што подразумева да информације до којих се дође у процесу контроле морају имати такав квалитет да се на основу њих могу доносити планске одлуке. Систем контроле, односно механизми контроле и предмет контроле морају бити тако планирани и спроведени да се добију релевантне и употребљиве информације.

Контрола треба да буде прихваћена и спроводива. Систем контроле треба да буде креиран тако да буде прихватљив за запослене. Контрола не треба да буде лов на грешке запослених, већ као што је то речено, начин да се дође до информација о одступањима од планираних циљева. Уколико је систем контроле усклађен са

¹⁵⁹ Исто, стр. 145.

интересима и циљевима запослених он ће бити искрено прихваћен и спроводиће се без отпора унутар организације. Међутим, треба имати у виду да ће запослени веома често ометати систем контроле у намери да резултате рада представе бољима него што они заиста јесу, како би себи обезбедили бољи положај у организацији. „Објективизација система контроле омогућава да се дође до релевантних информација без обзира на евентуалне опструкције запослених. Уколико се систем прикупљања информација у оквиру процеса контроле ослања искључиво на извештаје запослених, неће бити поуздан и на основу таквих информација тешко се могу предузимати адекватне корективне акције.“¹⁶⁰

У безбедносном менаџменту контрола има изузетно важну функцију због великог значаја који за опстанак и развој организација и заједница које се штите имају мере које се предузимају у оквиру менаџмента безбедности. Пропусти у планирању или примени ових мера могли би имати катастрофалне последице, било да је реч о привредним организацијама које би могле доживети уништење на тржишту, или да је реч о примени мера безбедности од стране јавних безбедносних организација које се односе на заштиту шире друштвене заједнице, где би пропусти могли имати катастрофалне последице ширих размера. Поред тога, безбедносне организације, поготово државне, имају веома широка овлашћења чија би злоупотреба могла довести до озбиљног кршења основних људских права и слобода. Овакве злоупотребе могле би имати озбиљне последице по функционисање политичког система земље и нарушити демократију, а у тежим облицима чак и довести до различитих облика диктатуре.

Због тога је, када је реч о безбедносном менаџменту, оправдано говорити о два система контроле. Систем контроле који се успоставља унутар безбедносних организација ради контроле спровођења циљева организације и постизања планираних резултата сличан је контроли која постоји у већини других организација и њиме се, мање–више, контролише квалитет постигнутих резултата у пословању, било да је реч о приватном или јавном безбедносном менаџменту, јер су циљеви те

¹⁶⁰ Исто.

контроле идентични, утврђивање одступања фактичког од планираног стања и предузимање корективних мера.

У приватним организацијама које се баве пружањем услуга безбедности систем контроле се не разликује битно од контроле било ког другог предузећа, према циљевима и начину вршења. Ову контролу у безбедносном менаџменту можемо назвати унутрашња или интерна контрола.

Контролу коју над радом државних и приватних безбедносних организација врше органи државне власти ради утврђивања уставности и законитости рада и утрошка планираних буџетских средстава називамо спољашња или цивилна контрола. У домаћој и страној литератури која се бави цивилно-војним односима користе се изрази „цивила и демократска контрола“, који више говоре о политичкој природи те контроле. Контрола коју органи државне власти врше над радом државних безбедносних организација је цивилна према врсти носиоца контроле. Да ли ће бити и демократска зависи од врсте политичког поретка у којој се та контрола обавља. Познати су примери многих диктаторских режима где је постојала стриктна контрола над оружаним снагама и другим деловима система националне безбедности од стране цивилних органа, али би ту контролу веома тешко могли назвати „демократском“¹⁶¹, пошто органи који су вршили контролу, иако цивилни, нису имали никакав демократски легитимитет.

Спољашња (цивилна, демократска) контрола над радом државних безбедносних организација, може се према носиоцима и врсти контроле поделити на парламентарну, управну (контролу система националне безбедности од стране извршне власти) и судску контролу.

¹⁶¹ Исто, стр. 146.

3. СИСТЕМ БЕЗБЕДНОСНОГ МЕНАЏМЕНТА

Многе организације које данас послују имају неке планове безбедности, али постоје и оне које их уопште не праве. Ти планови се састоје од заштитних мера, планова за ванредне ситуације¹⁶², и безбедносних прописа, који могу бити од користи као водиле безбедности. Треба напоменути, да иако је физичко обезбеђење у великој мери превазиђено, оно је и данас основни задатак, односно „основна мера система безбедносног менаџмента“¹⁶³.

Данашње организације морају да раде у сложенем окружењу где постоје различите оперативне и техничке мреже које омогућавају рад али и представљају ризик. Ове мреже се стално мењају и еволуирају, повећавају изложеност организације, мада представљају потенцијал за раст. Са том врстом проблема се не суочавају само велике организације. Безбедност прожима све аспекте рада организације: односи се на операције, на промене у окружењу, ток информација, запослене (од запошљавања и обуке до прављења тимова), финансирање и тако даље. Вечно присутно питање је: како се може спровести интеграција безбедности на свим нивоима менаџмента у организацији? Данас се безбедност пословног процеса дефинише као „заштита људи и имовине од периодичних и катастрофалних инцидената који могу бити последица непланираних или неочекиваних одступања у стањима процеса“¹⁶⁴. То значи да безбедност пословног процеса представља значајан елемент организације у избегавању људских жртава и финансијских губитака. С тим у вези, управљање безбедношћу пословног процеса¹⁶⁵ се може дефинисати као

¹⁶² Планови за ванредне ситуације садрже елементе који обухватају: процену ризика, начине за избегавање и ублажавање ризика, одговор на претње и мере за опоравак у случају да се претња испољи. Видети: Haddow, G. D., Bullock, J. A., Coppola, D. P., *Introduction to Emergency Management*, 3rd ed., Elsevier, Burlington, 2008.

¹⁶³ Fennelly, L. J., *Effective Physical Security*, 3rd ed., Elsevier Inc., Burlington, 2004., стр. 101.

¹⁶⁴ The Center for Chemical Process Safety, *Guideline for Safe Automation of Chemical Processes*, AIChE, New York, 1993.

¹⁶⁵ Управљање радним процесом је менаџмент приступ који организацију предузећа посматра као свеукупан скуп међусобно повезаних активности који имају за циљ да мапирају, побољшају и ускладе процесе у организацији. Према стандарду ISO 9001:2000, управљање радним процесом има нарочит значај у задовољавању интереса свих заинтересованих страна и промовисању интеграције организационих функција. - Biazzo, S., Garengo, P., *Performance Measurement with the Balanced*

„систем научног безбедносног менаџмента који подразумева извештавање о елементима пословног процеса као што су планови безбедности рада, инсталација, и сл., у случају да се уводе нове инсталације, трансфер или модификација опасних постројења ради превенције озбиљних ванредних догађаја“.¹⁶⁶

Планови безбедности обично делују одвојено од планова процеса рада и често постају статички документ, одвојен од операција или од активности стратешког менаџмента и далеко су од динамичног приступа који захтева безбедност. Али, постојање таквих планова може створити утисак да се спроводе добри поступци у безбедности што може спречити организације да заузму неопходан холистички став. Другим речима, „планови безбедности могу бити препрека за постизање одговарајућег нивоа безбедности“¹⁶⁷. Да би се то избегло, безбедносни менаџмент и стратегија безбедности морају бити довољно динамични да одрже корак са организационим и технолошким променама. Безбедносни менаџмент мора да подржи организацију у напорима да буде флексибилна и да се прилагођава околини и да да мерљив допринос укупној и дугорочној еластичности организације. „Еластичност организације је способност да издржи систематичне прекиде пословања и да се прилагоди новим ризичним срединама.“¹⁶⁸

За решавање многих од ових питања, потребно је управљати безбедношћу на ефикасан и ефективан начин. У том циљу, последњих година се у савременом свету развија систем безбедносног менаџмента. Током седамдесетих и осамдесетих година прошлога века у многим европским земљама су се појавили нацрти законске регулативе који су „довели до стварања јединствене европске регулативе (*European Community*, 1989)“¹⁶⁹. Таква регулатива је померила нагласак са техничких питања на питања одлучивања и менаџмента која се формулишу унутар безбедносне политике. Овакав тренд је појачан низом званичних извештаја о великим катастрофама. Главни

Scorecard: A Practical Approach to Implementation within SMEs, Springer-Verlag, Heidelberg, 2012., стр. 61.

¹⁶⁶ Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

¹⁶⁷ www.jha.ac/articles/a060.pdf

¹⁶⁸ Caralli, R. A., Wilson, W. R., исто.

¹⁶⁹ Hale, A. R., Heming, B. H. J., Catfhey, J., Kirwan, B., *Modelling of safety management Systems*, *Safety Science*, Vol. 26, No. 1/2, 1997, pp. 121-140.

закључак који намећу ови извештаји је да менаџмент није у могућности да обезбеди да се несметано одвијају планиране активности. Многе директиве које се доносе у развијеним земљама се односе на увођење система безбедносног менаџмента (СБМ) у организације које могу бити потенцијално опасне за животну средину и које могу угрозити велики број људских живота. Такође, владе многих земаља су усвојиле међународне стандарде квалитета које се користе као основа за осмишљавање стандарда за СБМ или повезаних менаџмент система (*British Standards Institution, 1992, British Standards Institution, 1996*). Ово доводи до потребе да се развијају и користе „системи за контролу и процену адекватности и начина побољшања система безбедносног менаџмента“¹⁷⁰.

Витингам и Холоивел¹⁷¹ сматрају да ефективан СБМ треба да буде формализована верзија постојећег система управљања како безбедношћу, тако и производњом. Штавише, „ефективан безбедносни менаџмент је резултат комбинације структуре система безбедносног менаџмента и организационе безбедносне културе“¹⁷². Истраживање које је спровео Кандола потврђује да „менаџмент систем мора да омогући процену ризика и имплементацију адекватних мера за смањење ризика, као и одговарајуће механизме повратне везе ради будућих побољшања“¹⁷³. Као што тврди Ризон¹⁷⁴, ефективан безбедносни менаџмент значи активно управљање безбедношћу да би се достигла зона максималне отпорности. Директива Савета 96/82/ЕЦ позната као SEVESO II, дефинише СБМ као „укључивање организационе структуре, одговорности, пракси, процедура, процеса и ресурса у утврђивању и имплементацији политике за превенцију већих акцидентата“¹⁷⁵. Коначно, безбедносни менаџмент је аспект укупне менаџмент

¹⁷⁰ Исто.

¹⁷¹ Видети: Whittingham, B., Holloywell, P., Ensuring you take credit for an effective safety management system, *Incorporating the Human Factors into Offshore Safety Cases Conference*, Aberdeen, 1 March 1994.

¹⁷² Santos-Reyes, J., Beard, A. N., Assessing safety management systems, *Journal of Loss Prevention in Process Industries*, Vol. 15, Issue 2, March 2002, Pages 77-95.

¹⁷³ Kandola, B. S., Risk based approach to fire safety engineering, *Fire Engineers Journal*, 1997, Pages 21–26.

¹⁷⁴ Видети: Reason, J., *Managing the risks of organisational accidents*, Ashgate, Aldershot, 1997.

¹⁷⁵ Mitchison, N., Porter, S., *Guidelines on a major accident prevention policy and safety management system, as required by Council Directive 96/82/EC, SEVESO II*, EUR 18123 EN, European Commission, DG JRC, Ispra, 1988.

функције која одређује и имплементира организациону безбедносну политику. Она укључује низ активности, иницијатива и програма, који се фокусирају на техничке, хумане и организационе аспекте и односи се на све индивидуалне активности у организацији. Ове активности су повезане са концептом континуираног побољшања преко „контролних кругова“¹⁷⁶, који подразумевају следеће кораке: планирање, организовање посла, имплементацију планова, евалуацију, проверу резултата у односу на план и предузимање корективних мера.

Поред тога, да би био ефикасан, безбедносни менаџмент мора да промени приступ од реактивног ка проактивном, јер је то предуслов за решавање питања људске грешке. Међутим, кључни узроци ванредних догађаја су обично састављени од многих сложених, међусобно повезаних фактора унутар и изван организације, а не само од људске грешке, тако да је управљање организационим и менаџмент факторима постало веома значајно. Ипак мало је пажње посвећено дефинисању шта је то што утиче на успешан СБМ и који су односи међу тим факторима. После детаљне анализе, група аутора¹⁷⁷ је дошла до закључка да су основни фактори који утичу на СБМ:

1. стратегија и политика која укључује комисију за безбедност, безбедносну политику и правила, као и владине прописе. Правила која постави безбедносна комисија морају бити у складу са нормативним актима државе;
2. имплементација, која се односи на документацију, алате, фабрике, одржавање, сервисирање, спремност у случају непредвиђених догађаја и остале активности које директно утичу на безбедносни ниво организације;
3. људски фактор, који обухвата проблеме у комуникацији, управљање људским ресурсима, управљање одржавањем ресурса, безбедносну културу, почетну и сталну обуку, компетентност појединаца;
4. мониторинг и повратна веза, који обухватају управљање безбедносним ризицима и истраживање и анализу ванредних догађаја.

¹⁷⁶ Mitchison, N., Papadakis, G. A., Safety management systems under Seveso II: implementation and assessment, *Journal of Loss Prevention the Process Industries*, 12 (1999), pp. 43–51.

¹⁷⁷ Видети: Liou, J. J. H., et al., *Building an effective safety management system for airlines*, *Journal of Air Transport Management* 14, (2008), стр. 20.

Поједини фактори су испитани и груписани према степену значајности. Показало се да највећи значај имају политика и стратегија безбедности. Они имају већи утицај на остале факторе, чиме се указује да они треба да имају „највећи приоритет приликом увођења промена и побољшања“¹⁷⁸.

3.1. Директиве „Seveso“

У току 1982. године Европска комисија је „усвојила Директиву Савета 82/501/ЕЕЦ о опасностима од великих катастрофа појединих индустријских активности (*Council Directive 82/501/EEC on the major-accident hazards of certain industrial activities - OJ No L 230 of 5 August 1982*)“¹⁷⁹ – такозвану SEVESO Директиву.¹⁸⁰ Ова директива је више пута допуњавана и то 1987. и 1988. године (*Directive 87/216/EEC of 19 March 1987 - OJ No L 85 of 28 March 1987* и *Directive 88/610/EEC of 24 November 1988 - OJ No L 336 of 7 December 1988*), као последица великог броја катастрофалних акцидентата, попут оног у Бопалу 1984. и у складишту Сандоза у Базелу 1986. године¹⁸¹. Обе ове допуне су имале за циљ да се прошири опсег директиве, да би се у њу укључила и складишта опасних супстанци.

На основу предлога из 1994. године, у децембру 1996. године, усвојена је Директива Савета 96/82/ЕЦ о контроли опасности од катастрофалних акцидентата (*Council Directive 96/82/EC on the control of major-accident hazards*), такозвана „Seveso II“ директива. Нова директива се заснива на члану 130s Уговора о оснивању Европске заједнице. Државе чланице су имале рок од две године да донесу националне законе, регулативе и административне одредбе који су у сагласности са директивом. Било је дозвољено да се примењују и строжа правила од оних који су наведени у директиви, међутим то би могло да утиче на компетитивност индустрија на које се директива односи. Од 3. фебруара 1999. године, Директива је постала обавезујућа за

¹⁷⁸ Исто, стр. 6.

¹⁷⁹ Kirchsteiger, C., Review Of International Industrial Safety Management Frameworks, *Trans IChemE, Vol 80, Part B, September 2002, pp. 235-244.*

¹⁸⁰ Више на: <http://ec.europa.eu/environment/seveso/index.htm>

¹⁸¹ У Индији је 1984. год. дошло до цурења метил изоцијанида, што је довело до смрти више од 2500 људи, а у Швајцарској је 1986. год. дошло до загађења живом реке Рајне и помора пола милиона рибе.
- Kirchsteiger, C., исто.

индустрију, као и за јавне власти чланица које су одговорне за имплементацију и спровођење ове директиве.

Обавезујуће регулативе имају различите утицаје на постојећу индустрију која потпада под директиву „Seveso II“ и то по питањима као што су: документација, одговорност за животну средину, планирање коришћења земљишта и сл. Такође, разлике утичу на то да неке државе или региони буду више или мање привлачни за раст постојећих или оснивање нових локација, тако да се одређена поља активности концентришу на начин који онемогућава да се даље развијају постојеће локације у другим државама или регионима. Највећи практични значај безбедносног извештаја у директиви „Seveso II“ је објашњење сценарија акцидента. „Дефинисањем сценарија се изриче најрепрезентативнија ситуација која може довести до акцидента великих размера“.¹⁸²

Члан 1. Директиве „Seveso II“ тврди да је „основни циљ директиве превенција акцидента већих размера које укључују опасне материје, и ограничавање последица таквих акцидента на људе и животну средину, са изгледима да се обезбеде високи нивои заштите широм заједница на конзистентан и ефективан начин“¹⁸³. Опсег директиве „Seveso II“ је проширен и поједностављен у исто време. Она се односи на присуство опасних материја у објектима. При томе, „присуство опасних материја“ се дефинише као стварно или предвиђено присуство таквих супстанци или присуство супстанци које могу настати уколико дође до губитка контроле у индустријском процесу, као што су нпр. тетрахлордобензопарадиоксин. Тако се постиже да „опсег покрива индустријске активности али и складиштење опасних хемикалија“¹⁸⁴.

Основне измене нове директиве у односу на „Seveso I“ директиву се могу сагледати у две основне ставке:

1. првобитна директива је садржала списак постројења која су описана преко низа одређених активности. Нова директива не садржи такав списак. Стога је сувишна

¹⁸² Pey, A., Lerena, P., Suter, G., Campos, J., Main differences on European regulations in the frame of the Seveso Directive, *Process Safety and Environmental Protection*, Volume 87, Issue 1, January 2009, Pages 53–58.

¹⁸³ Directive 96/82/EEC, 1996.

¹⁸⁴ Kirchsteiger, C., исто.

потреба да се дефинише појам индустријске активности. Док се старија директива примењивала на постројења, нова се односи на предузећа која се дефинишу као „целокупна област коју контролише Оператер, а на којој су присутне опасне материје у једном или више постројења, укључујући заједничке инфраструктурне објекте или активности“¹⁸⁵. Ова битна промена у приступу уклања двосмисленост, у погледу тумачења директиве по којој постоје разлике између производних активности и постројења за складиштење, због које би могло доћи до избегавања законских обавеза.

2. Списак именованих супстанци је смањен са 180 на отприлике 50 материја у корист повећаног и систематичнијег списка који садржи генеричке категорије као што су токсичне, експлозивне и запаљиве супстанце. Што се тиче дефиниције ових категорија, директива се позива на директиве које се односе на класификацију, паковање и означавање опасних материја, препарата и пестицида. Слично претходним директивама, „Seveso II“ покрива двослојни приступ, који значи да за сваку именовану супстанцу и за сваку генеричку категорију супстанци и препарата, постоје два различита количинска нивоа (нивои прага) и то доња и горња вредност. Претпоставља се да ризик од појаве акцидента већих размера расте када је у предузећу присутна већа количина опасних материја. Према томе, директива намеће више обавеза предузећима која користе веће количине ових материја. Заправо, ова директива се може посматрати као пропорционални трослојни контролни механизам, где веће количине значе више контроле. Предузећа која користе количине опасних материја које су испод доње границе прописане у директиви, не подлежу њеним обавезама, већ су пропорционално контролисана од стране општих прописа који се односе на здравље, безбедност и заштиту животне средине. Предузећа која користе количине опасних материја које су изнад доње границе одређене директивом, подлежу обавезама које се односе на нижи ниво контроле. За предузећа која користе количине опасних материја које су изнад горње границе прописане директивом, су обавезни сви прописи који су дати у директиви.

¹⁸⁵ Исто.

Важне области које су искључене из опсега директиве „Seveso II“ су нуклеарна безбедност и транспорт опасних материја путем цевовода. Међутим, постоје захтеви пред Европским Саветом да се истражи потреба за предузимањем активности у областима транспорта као што су луке и железничка складишта, као и пренос опасних материја путем цевовода. Уочено је да превоз опасних материја има значајан потенцијал у изазивању акцидентата већих размера. Превоз до и од предузећа може представљати већи ризик од оног који постоји у самом предузећу. Број људи који је под могућим утицајем опасних материја током транспорта кроз насељена места, или током привременог складиштења близу тих места, је много већи него у постројењима где се те материје производе, користе или складиште. Тренутно се ради на повезивању са транспортним сектором да би се усагласиле политике у овој области.

Најважније обавезе које прописује директива „Seveso II“ су:

1. Обавештавање.

Оно се односи на опис предузећа и постројења и процеса који се у њима одвијају, укључујући и географску локацију. Ту спада и усвајање Политике за Спречавање Акцидентата великих размера (Major Accident Prevention Policy - MAPP) и Система Безбедносног Менаџмента (Safety Management System - SMS).

2. Систем Безбедносног Менаџмента.

Добар систем управљања је неопходан када је реч о безбедности, иако није довољан. Међутим, наглашено је да у већини акцидентата који су пријављени систему Европске Комисије највећу улогу су одиграле грешке у систему управљања. Директива „Seveso II“ одређује потребу за успостављањем система безбедносног менаџмента, а одређује и области које она одређује (укључујући и процену ризика).

3. Безбедносни извештај.

Циљ безбедносног извештаја је да „укаже на:

- то да су идентификоване опасности од акцидентата већих размера,
- мере које су предузете за спречавање таквих акцидентата и ублажавање њихових последица,
- то да постоје планови за ванредне ситуације у оквиру предузећа,

- то да су обезбеђене адекватне информације властима да би се могле одредити политике за коришћење околног земљишта и успоставити спољашњи план за ванредне ситуације.“¹⁸⁶

Заједнички аспект свих система извештавања у области акцидента великих размера је да се мора јасно указати на то да су предузете акције за спречавање акцидента, али и да су последице ограничене и постигнут висок ниво заштите. Зато су потребни одређени технички критеријуми ради процене последица, нивоа заштите и прихватљивости резултата. Овде настају проблеми због недостатка дефиниције и јасне методологије за прагове ризика широм ЕУ и прихватљивости и толеранцији последица. То доводи до различитих начина на које се директива примењује у различитим земљама или регионима у оквиру земаља у Европској Унији. Последице тога су то да се користе различите методе за идентификацију сценарија акцидента већих размера. Затим, користе се различити критеријуми за дефинисање идентификованих сценарија, а користе се и различити прагови толеранције за процену последица ових сценарија. Коначно, користе се различити критеријуми за одређивање „прихватљивог ризика за последице које проузрокују индустријске активности по становништво и животну средину“¹⁸⁷.

У Холандији, нпр. постоји обавеза да се у безбедносном извештају да пробабилистичка анализа ризика. У Холандији је јасно дефинисана политика максималног нивоа прихватљивог ризика када се доносе одлуке о коришћењу земљишта. У Великој Британији се фаворизује употреба пробабилистичког приступа анализи ризика, али квантитативни критеријуми ризика се само односе на контролу коришћења земљишта у непосредној близини индустријских постројења. У Немачкој, детерминистички приступи се користе за хемијску процесну индустрију да би се указало на квалитет предузетих мера за избегавање ризика унутар и изван постројења. Потенцијал за опасности се примарно одређује ударним опсегом материјала и емитоване енергије на основу појединих инцидената и номограмске технике. Вероватноћа догађања се углавном може одредити на основу осетљивости

¹⁸⁶ Kirchsteiger, C., исто.

¹⁸⁷ Pey, A., Lerena, P., Suter, G., Campos, J., исто.

самих опасних материја. „Процена је могућа једино на основу општих изјава о вероватноћи, а овај приступ је установљен и често се користи у пракси, посебно за класификовање контроле процеса инжењерских система, као што су функционисање, мониторинг, системи за минимизацију оштећења и безбедност, одржавање и инструментација.“¹⁸⁸

4. *Обавезе власти.*

Према директиви „Seveso II“, компетентне власти у државама чланицама треба да – бар када су у питању већа предузећа од којих се захтева безбедносни извештај – прегледају извештај и пренесу закључке оператеру. Општије, од власти се захтева да забране коришћење постројења чије су безбедносне мере озбиљно изнад захтеваних прописа.

5. *Захтеви за обезбеђивањем информација.*

Државе чланице ЕУ треба да обезбеде информације о безбедносним мерама и о обавезном понашању у случају када дође до акцидента, без посебног захтева за њима, и то особама које могу бити под утицајем акцидента већих размера који настаје у предузећима која спадају у горњи слој контролног механизма. Чланице морају да обезбеде информације Европској Комисији одмах по настанку акцидента већих размера. Комисија треба да успостави и стави на располагање информациони систем који се односи на информације о таквим акцидентима (*the MARS system*).

6. *Инспекцијски надзор.*

Директива захтева инспекцијски надзор и одређује области које морају да буду покривене у области контроле опасности, не само прегледањем техничке опреме. Штавише, постоје експлицитни захтеви за извештавањем оператера о резултатима ових надзора, да би се омогућило да се сви недостаци правовремено и у најбољој могућој мери исправе.

7. *Провера планова за ванредне ситуације.*

Директива „Seveso II“ захтева да интерни и екстерни планови за ванредне ситуације буду проверени да би се осигурало да ће они функционисати правилно у случају да дође до акцидента.

¹⁸⁸ Kirchsteiger, С., исто.

8. Планирање коришћења земљишта.

Акцидент у Бопалу је дао стравичан доказ да насељене области треба да буду на безбедној дистанци од извора главних опасности. Планирање коришћења земљишта је уграђено у административне праксе чланица ЕУ, и могуће је да је због тога Европски Парламент одбио предлог Европске Комисије да се развију хармонизовани критеријуми за узимање у обзир великих опасности приликом израде планова за коришћење земљишта. Међутим, такав принцип је усвојен, а „Seveso II“ захтева да техничко саветовање о већим опасностима буде доступно када се доносе одлуке о планирању у вези коришћења земљишта. Заправо, критеријуми, средства и методе које се користе за процену индустријских ризика су још увек далеко од хармонизације у различитим државама чланицама. На пример, коришћење пробабилистичких или детерминистичких процена ризика у суштини се разликује од места до места. Ове разлике су настале због историјских разлога и зато што су различити приступи развијани независно једни од других. Ово је много значајније од разлика у технологији или природи проблема и не постоји разлог зашто различите индустрије или различите земље не би користиле исти општи приступ. Главни проблем који се јавља због ових различитих приступа у процени ризика не лежи толико у сагласности, колико од транснационалних операција. На пример, компаније које имају постројења у различитим земљама Европске Уније треба да усагласе своје унутрашње безбедносне политике и да воде рачуна да би избегле неспоразуме са различитим националним законодавствима. „Заједно са хармонизованим процедурама, процена ризика би била трошковно ефикаснија и значајно би повећала разумевање одлука које се доносе у другим земљама или другим областима функционисања. Ово би утицало на транспарентност процеса одлучивања у којем би све заинтересоване стране могле лакше да буду укључене и тиме повећале друштвену прихватљивост технолошких ризика.“¹⁸⁹

9. Информације и транспарентност.

Када је реч о транспарентности, директива „Seveso II“ захтева да информације буду доступне сваком човеку или правном лицу на захтев. Ово указује на већу

¹⁸⁹ Kirchsteiger, С., исто.

транспарентност и слободу информација. Постоје изузеци који се односе на личне податке, питања од јавне безбедности и комерцијалне поверљивости. Наравно, ово се односи не само на јавне информације и транспарентност, већ и на учешће јавности у доношењу одлука. „Јавност треба да буде омогућена да да своје мишљење о новом предузећу или модификацији постојећег, као и о развоју у области, а јавност се мора консултовати по питању спољних планова за ванредне ситуације.“¹⁹⁰

3.1.1. Анализа ризика и израда сценарија према директиви „Seveso II“

У односу на припремање безбедносног извештаја и у току идентификовања опасности које настају због индустријских активности, коришћење технике за анализу ризика је основни захтев свих регулатива. Тешко је дефинисати која ће се специфична техника или методологија користити, будући да тај избор „зависи од постојећих знања, организационих процедура, система безбедносног менаџмента и сл.“¹⁹¹

У „Упутству за припрему безбедносног извештаја да би се задовољила директива Савета 96/82/EC“ (*Guidance on the preparation of a Safety Report to meet the Requirements of Council Directive 96/82/EC*) је дат дугачак референтни списак.¹⁹²

Обично, уколико се добро примењују у смислу погодности за постројења и процесе, различите технике могу да добро идентификују опасности. Због тога се обично не поставља питање неслагања око најбоље технике или методологије у овој области. Али, због тога се опасности морају исказати у виду сценарија акцидентата и уобичајено је да се „у регулативама нађу изјаве као што су:

- реалистичан сценарио најгорег могућег случаја,
- студија хазарда треба да буде пропорционална са обимом опасности које постоје у постројењима и њиховим предвидивим последицама,
- хипотеза о акциденту треба да докаже да се може одбацити најудаљенија вероватноћа настанка акцидента,

¹⁹⁰ Исто.

¹⁹¹ Видети: Peu, A., Lerena, P., Suter, G., Campos, J., исто.

¹⁹² Видети: Papadakis, G. A., Amendola, A., *Guidance on the Preparation of a Safety Report to meet the Requirements of Council Directive 96/82/EC*, Joint Research Center, European Commission (1997).

- прихватљиво објашњење одабира сценарија опасности.¹⁹³

Поред тога, док се дефинишу сценарија акцидента, регулативе траже да се узму у обзир питања попут:

- последица које настају услед неауторизованих активности на локацији,
- неуспех да се задржи опасна материја у контролисаним условима,
- неисправно функционисање или технички проблеми са опремом и системима,
- грешке на у систему за издавање радних дозвола.

У овом кораку, могу се јавити велике разлике у безбедносним извештајима различитих држава или региона, као последица прошлих догађаја везаних за акциденте, евалуационе процедуре, стања које се односи на извештаје везане за традицију и сл., због „разлика у формулацији између детерминистичких и пробабилистичких сценарија“¹⁹⁴.

У истом упутству, може се наћи јасна изјава која се односи на ову чињеницу, с обзиром да је избор квалитативног или квантитативног приступа под јаким утицајем специфичне безбедносне културе и филозофије која је доминантна у појединој држави чланици и да „не постоји јединствен приступ који се односи на тип мера које треба предузети за одабир сценарија“¹⁹⁵.

Обично се усваја детерминистички приступ за позиционирање сценарија акцидената. Детерминистички приступ се може добро представити и узети у обзир неуспехе организационих и техничких безбедносних мера, кварове опреме, грешке у процедурама, плановима и сл. То подразумева, да док год постоји потенцијална опасност претпоставља се да ће се она развити пре или касније, као да се неће предузети никакве техничке мере. Главни проблем је то што овај тип приступа не приказује безбедносне мере које су усвојене у циљу превенције дешавања ових сценарија. Стога, сценарио се може оценити као нереалистичан, премало вероватан, неприхватљив, итд. Алтернативно решење је да се овај екстремно апокалиптични

¹⁹³ Реу, А., Lerena, P., Suter, G., Campos, J., исто.

¹⁹⁴ Исто.

¹⁹⁵ Исто.

детерминистички сценарио до одређене мере подвргне пробабилистичким принципима, током развијања, односно описивања сценарија. Али, онда настаје проблем који се односи на „недостатак података о вероватноћи настанка квара у систему контроле, цевоводима, људске грешке и сл.“¹⁹⁶

Индустријско искуство, чак иако је веома дуго, у суштини је јако кратко да би се на прави начин на техничким основама могле проценити фреквенције дешавања акцидента када се ради о догађају у једном, десет или стотину милиона година, а понекад су то временске скале на којима се сценарио мора поставити да би се за неки догађај могло рећи да је превише мала вероватноћа његовог настанка. Такође, јако је тешко проценити утицај техничких мера као што су заштитни уређаји или безбедносни фактори у односу на вероватноћу настанка или фреквенцију велике опасности. Искуство показује да је у многим случајевима, када се дају правилна објашњења о постојећим безбедносним мерама, могуће пронаћи техничко оправдање да се не рачунају сценарија са највећим последицама ван фабрике. Ове безбедносне мере се обично користе у време планирања постројења, због поштовања постојећих стандарда, корпорацијских упутстава, најбољих пракси и сл., или могу бити дефинисане и имплементиране на основу анализе ризика која се спроводи у фабрици. Зато, процена ризика може да оправда одбацивање „најгорег могућег сценарија“ и да дефинише „најгори прихватљиви сценарио“, који обично није толико катастрофалан. Сценарио који подразумева реалистичну перцепцију опасности, а при том има средњу или високу вероватноћу дешавања, обично има мале или никакве последице ван постројења када се њим правилно управља. У већини сценарија „равнотежа се налази између кварова и грешака који покрећу дешавања и безбедносних техничких мера које ће се примењивати и неће отказати када сценарио почне да се развија“¹⁹⁷.

¹⁹⁶ Реу, А., Lerena, P., Suter, G., Campos, J., исто.

¹⁹⁷ Исто.

3.1.2. Предлози за побољшање директиве

Ревизија директиве „Seveso II“ је завршена током 2010. године, а у децембру исте године Европска Комисија је усвојила Предлог за нову директиву која би заменила постојећу до јуна 2015. године.¹⁹⁸

Главне предложене промене се односе на:

- усаглашавање Анекса I о дефинисању материја које су у оквиру опсега директиве са системом класификације опасних материја који је усвојен у ЕУ;
- укључивање корективних механизма за прилагођавање Анекса I да би се могао користити у будућим ситуацијама где су опасне материје укључене или искључене и које представљају или не представљају опасност за изазивање већих акцидентата;
- јачање одредби које се односе на јавни приступ безбедносним информацијама, партиципацију у доношењу одлука и приступ правосуђу, побољша начин прикупљања, управљања, стављања на располагање и дељење информација;
- увођење строжих стандарда за инспекцијски надзор постројења да би се обезбедила ефективна имплементација и примена безбедносних правила.

Остале измене се односе на мање техничке модификације ради разјашњења и ажурирања одређених одредби, укључујући симплификацију и растерећење преобимног административног апарата.¹⁹⁹

3.2. Концептуални оквир система безбедносног менаџмента

Академски и правни кругови, као и индустријалци су уложили много труда да би истражили и развили начине за решавање проблема везаних за заштиту од пожара, безбедност и заштиту животне средине. „Неке организације су осмислиле своје системе безбедносног менаџмента на основу стандарда за заштиту животне средине као што је стандард ISO 14001 EMS (*Environmental Management System*) из 1995.

¹⁹⁸ Више на: <http://ec.europa.eu/environment/seveso/review.htm>

¹⁹⁹ Видети исто.

године“.²⁰⁰ Тај стандард је формализовани метод за утврђивање и задовољавање циљева везаних за животну средину. Састоји се од политике, планирања, имплементације и активности, мерења и процене, као и ревизије и побољшања. Политика означава посвећеност организације питањима животне средине и обезбеђивање ресурса за њену имплементацију. Планирање подразумева идентификацију потенцијалних ефеката које производи, услуге и уопште активности организације имају на животну средину, али и одређивање стратегије која наглашава значајне аспекте у систему за управљање животном средином. Ово укључује идентификацију специфичних мерљивих циљева. Имплементација и функционисање подразумевају средства и методе за постизање политике према утврђеном плану. Мерење и процена се односе на средства за праћење напретка да би се утврдило да ли се циљеви испуњавају, као и процедуре које се користе за исправљање могућих недостатака. Коначно, ревизија и побољшање обезбеђују средства за периодичну ревизију и континуирано увођење побољшања у систем управљања животном средином. Планирање, организовање, имплементација и контрола, такође, треба да буду основне функције СБМ. Планирање подразумева развијање политике и дугорочних и краткорочних циљева организације. Организовање подразумева успостављање организационе структуре и доделу улога, одговорности, ауторитета и одговорних лица за постизање циљева. Имплементација обезбеђује механизме за извршење политике. Коначно, контролна функција укључује мерење, процену и корекцију перформанси. Према Бенлију и Соклију²⁰¹, СБМ се састоји од разумевања опасности преко Анализе управљања опасностима (*hazard management analysis* - НМА). Ова Анализа се састоји од процеса идентификације, процене, контроле и опоравка. Тако се лакше идентификују критичне активности. Потоме се за сваку од тих активности успоставља скуп докумената, такозвани Каталог СБМ, који описује и показује како се управља безбедношћу у организацији. На крају се посвећеност и подршка организације обрађују у посебном документу који се назива Упутство за СБМ, а који показује безбедносне циљеве организације и средства која се користе за

²⁰⁰ Santos-Reyes, J., Beard, A. N., исто.

²⁰¹ Видети: Bentley, P. D., Sockley, J. D., Hazard management and safety management systems: a structured approach, *Offshore Technology Conference (OTC) Proceedings*, May 1992, pp. 471–476.

њихово остварење. Ове контроле укључују извештавање о инцидентима, индикаторе перформанси, процене и ревизије, непрекидан надзор, процену и побољшање перформанси активности и операција. Друге организације, попут Европског Центра за Безбедност Процеса (*European Process Safety Centre - EPSC*) су развиле упутства која се састоје од политике, организације, праксама и процедурама за управљање, надзор и процену, као и ревизију менаџмента. Слично, Форум за Истраживање и Производњу (*Exploration and Production Forum*) нуди решење које се састоји од вођства и посвећености (*top-down* посвећеност и сл.), политике и стратешких циљева, организације, ресурса и документације, процене и управљања ризиком, планирања, имплементације и мониторинга, као и процене и ревизије. Неки аутори (нпр. Минг, Бентли и др.²⁰²) сматрају да се СБМ састоји од постављања циљева, организовања и алоцирања ресурса, успостављања стандарда перформанси, имплементације плана, процене и ревизије система ради утврђивања сагласности и одређених побољшања. Минг²⁰³ наглашава да је сврха СБМ да обезбеди неопходну заштиту свих људи који су под било каквим утицајем организације, као и да штити животну средину и имовину организације. Директиве Асоцијације за Офшор Операције Уједињеног Краљевства (*The United Kingdom Offshore Operators Association - UKOOA*) из 1995. године имају за циљ да охрабре интегрисани приступ менаџменту заштите од пожара и експлозија. Ове директиве укључују животни циклус управљања опасностима, процену могућности дешавања појединих опасних догађаја, уграђену безбедност, селекцију и спецификацију система за детекцију пожара и експлозија, контролу и ублажавање, као и имплементацију. Директива за Здравље и Безбедност (*The Health and Safety Executive - HSE*) из 1997. године, предлаже приступ безбедности у односу на управљање здрављем и безбедношћу. Овај процес се састоји од политике, организовања, планирања и имплементације, мерења и ревизије перформанси, као и процене да би се могла искористити досадашња искуства. Канадска Асоцијација за

²⁰² Видети: Bentley, P. D., Mundhenk, D.L., Jones, M.G., Geert de Jong, Visser, J. P., Development and implementation of an HSE management system in E&P companies, *Journal of Petroleum Technology (JPT)*, 1 (1995), pp. 54–60.

²⁰³ Видети: Ming, K. T., Application of a quality management system approach to health, safety and environment, *Offshore South East Asia, Proceedings of the 10th Conference and Exhibition World Trade Centre*, Singapore, 6–9 December 1994, pp. 739–745.

Дрво и Папир (*The Canadian Pulp and Paper Association*) је развила скуп принципа за управљање здрављем и безбедношћу на раду (*occupational health and safety* - ОН&S). Ови принципи наглашавају да систем власништва, циљева и процедура, мерења перформанси, ревизије мера и корективних активности представљају кључне компоненте СБМ које морају бити у најбољем реду.

Истраживање које су спровели Дегани и Винер²⁰⁴, предложени оквир интегрисане организационе филозофије, политике и стандардне процедуре за управљање кокпитом. Аутори сматрају да у је високоризичном окружењу од суштинске важности да процедуре буду беспрекорне, зато што је грешка неприхватљива. Организациона филозофија укључује одређивање начина на који организација спроводи пословање. Политике су широк спектар спецификација начина на који менаџмент очекује да се послови обављају, пре свега обука, одржавање, понашање и сл. Да би се подржале политике, успоставља се скуп оперативних процедура који се додељује свим запосленим. Процедура има за циљ да недвосмислено опише задатак, време и редослед њеног обављања, активности и начин на којих их треба обавити, особе које треба да их обаве и који тип повратне информације мора да се обезбеди осталим запосленим.

Безбедност и заштита од пожара су од великог значаја и у поморској индустрији. Међународна Поморска Организација (*The International Maritime Organisation* - ИМО) је усвојила низ иницијатива који имају за циљ да побољшају заштиту од пожара, безбедност и превенцију загађења, посебно на пловилима и бродовима. Родрикс²⁰⁵ описује СБМ за управљање заштитом од пожара на путничким бродовима. Овај СБМ укључује четири главна аспекта, као што су комуникација, графички дисплеј, командовање и контрола и процедуре за гашење пожара. Неки аутори сматрају да се систем заштите од пожара састоји од „комбинације два подсистема и то *hardware* и *software* система“²⁰⁶. Подсистем

²⁰⁴ Видети: Degani, A., Wiener, E.L., Procedures in complex systems: the airline cockpit, *IEEE Trans. on Systems, Man and Cybernetics—Part A: Systems and Humans*, 27 (3) (1997), pp. 302–312.

²⁰⁵ Видети: Rodricks, B., A system for managing fire safety on passenger vessels, *Fire Prevention*, 260, 1993, pp. 24–28.

²⁰⁶ Xiao, X., Marchant, E., Griffit, A., Assuring the quality of fire safety systems in buildings, *Fire Prevention*, 261, 1993, pp. 27–31.

“софтвера“ укључује менаџерске мере које се тичу заштите од пожара, попут обуке, функционисања и одржавања опреме, планова за ванредне ситуације и сл. Други, „хардверски“ подсистем се састоји од неколико компоненти, као што су пасивни систем заштите од пожара, детекције пожара и алармног система, система за сузбијање пожара, евакуацијског система, система за контролу дима и система за осветљење у случају ванредне ситуације.

На основу свега наведеног, систем безбедносног менаџмента се може схватити као скуп политика, стратегија, поступака, процедура, улога и функција повезаних са безбедношћу. То је механизам који се интегрише у организацију и има за циљ да контролише опасности²⁰⁷ које могу утицати на здравље и безбедност запослених, производа и услуга, али и на окружење и опстанак самог предузећа. У исто време, овај систем омогућава да се организација лакше прилагоди законској регулативи. Да би систем безбедносног менаџмента био ефикасан и ефикаван мора бити прихваћен и примењен од стране запослених. Дакле, овај систем мора промовисати позитивну безбедносну климу, односно културу²⁰⁸. Због тога је потребно да „сви нивои управљања, а нарочито „топ менаџмент“, подржавају и промовишу систем безбедносног менаџмента“²⁰⁹.

²⁰⁷ Опасност је нешто што може угрозити здравље људи, нанети штету опреми и ресурсима. Видети: <http://www.hse.gov.uk>

²⁰⁸ Безбедносна клима одражава симболичке (нпр., плакати на радном месту, изјаве основних принципа и сл.) и политичке (нпр., менаџери који изражавају своју посвећеност безбедности, алокација финансијских средстава за сектор безбедности и сл.) аспекте организације који чине пословно окружење. Безбедносна клима може, али и не мора да буде опипљива манифестација прихваћених веровања и вредности које су отелотворене у безбедносној култури организације, иако треба да буде повезана са њима. Сама безбедносна култура је састављена од сазнања (нпр., процесирање информација и процена која се врши пре доношења одлуке или извршавања активности) и емоције (нпр., да ли су људи задовољни или узнемирени због нечега) што одређује карактер групе или организације. Безбедносни менаџмент и безбедносна клима могу бити резултат реакције на одређену ситуацију, док безбедносна култура представља стабилну и трајну карактеристику организације. – Willis, A., Watson, B., Biggs, H. C., Comparing safety climate factors as predictors of work-related driving behavior, *Journal of Safety Research, Volume 37, Issue 4, 2006, Pages 375-383.*

²⁰⁹ Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., Safety management system: Development and validation of a multidimensional scale, *Journal of Loss Prevention in the Process Industries, Volume 20, Issue 1, January 2007, Pages 52-68.*

3.3. Модел система безбедносног менаџмента

Експлицитан модел система безбедносног менаџмента, који може представити динамичну природу процеса безбедносног менаџмента, може да да добру основу за његову процену. Развијање курса за саветнике о питањима безбедности и менаџере безбедности има стимулативан ефекат за сређивање тема које треба подучавати. Померање схватања о програмима образовања у многим земљама на питања безбедносног менаџмента је довело до потребе да се свеобухватно и конзистентно обликује модел СБМ, у оквиру којег је неопходно познавање начина развијања, процене и побољшања самог модела. Једино се у таквом оквиру може довести у ред фрагментирана литература, тако да се могу извући закључци о томе шта представља прихваћено сазнање и где постоје изазови у истраживању и пракси. Истраживање у Делфту²¹⁰ је имало за циљ да направи такав оквир. Основа за успостављање модела безбедносног менаџмента, лежи у прописима Директиве „Seveso“.

Истраживање које је спроведено у Делфту „има за основу принцип циклуса решавања проблема, који је већ коришћен у различитим истраживањима“²¹¹. Циљ овог истраживања је био да се обезбеди систематичан и комплетан опис елемената који би требало да чине СБМ и како они треба да буду повезани између себе. Такође, било је потребно да се обелодане везе између ризика и директних мера заштите и контроле са једне, и организационих и менаџмент процеса који омогућавају увођење и функционисање тих мера, са друге стране. Сврха је да се укаже на то који су менаџмент фактори који могу да се укључе или побољшају да би се побољшала ефикасност СБМ. Дакле, основни задатак овог истраживања се односио на то да се пронађе начин за процену и побољшање постојећег и за дизајнирање потпуно новог система безбедносног менаџмента. Такође, од великог значаја представља и обука стручњака и менаџера за безбедност да би се схватила њихова улога у том систему²¹².

²¹⁰ Видети: Hale, A. R., at al., исто.

²¹¹ Исто.

²¹² „Многи менаџери се слажу да је основна полука успеха сваке организације добра обука и добре вештине запослених.“ - Rothwell, W. J., Lindholm, J. E., Wallick, W. G., *What CEOs Expect from Corporate Training*, AMACOM, New York, 2003., стр. 28.

Безбедносни менаџмент је сложен процес. Он се односи на све делове организације и све фазе њеног животног циклуса. У терминологији теорије система, СБМ представља аспектни систем, који се односи на испуњавање скупа циљева целог система, односно организације. Аспектни систем укључује већину елемената од којих је састављен цео систем, али не укључује све везе између њих. У овом случају, фокус је на односима који имају утицај на безбедност. Да би се конципирао модел, „потребно је да су испуњени следећи захтеви:

- 1) он треба да одражава комплексан, динамичан систем у којем СБМ постоји;
- 2) мора бити способан да се фокусира на елементе система без губљења веза са целим моделом;
- 3) мора обезбедити јединствен језик за описивање и моделовање свих аспеката система;
- 4) мора бити компатибилан са постојећим идејама и принципима безбедносног менаџмента, менаџмента квалитета и идејом организације која учи;
- 5) мора обезбедити везе са стандардним концептима који се користе у литератури о менаџменту, на пример, дефинисана разлика између политике, процедура и наредби;
- 6) мора моделовати и примарне (технолошке) процесе са њиховим ризицима и менаџмент одлуке које их контролишу.²¹³

Примарни процеси се могу посматрати као токови енергије који морају бити каналисани. У ширем контексту токови се могу односити на материјале, као што су отровне супстанце које могу утицати на здравље или животну средину. Техника моделовања осмишљена за производне процесе, обезбеђује основу за обликовање модела за такве токове и контроле²¹⁴ које спречавају настанак грешака. Међутим, таква техника није прилагођена за токове информација и одлучивање, који представљају основне процесе менаџмент система. Информациони токови су од велике важности и за „производне процесе“ непроизводних предузећа као што су

²¹³ Hale, A. R., at al., исто.

²¹⁴ Треба напоменути, да „контрола подразумева да процеси који се дешавају у систему, као и сви захтеви који се постављају пред систем, у потпуности разумљиви“ - Gupta, P., *Six Sigma Business Scorecard*, McGraw-Hill, New York, 2004., стр. 9.

банке или консултантске компаније, чији СБМ би такође био обухваћен јединственим моделом. Због тога су аутори одабрали технику структурне анализе и дизајнирања (SADT - *Structured Analysis and Design Technique*), која потиче из поља софтверског инжењеринга, али се више користи у моделирању активности доношења одлука.²¹⁵

Основна структура (слика 1.) се састоји од активности које контролишу три аспекта, што заједно даје излаз. Логика моделовања је да улази (инпути – I) морају бити неопходни и довољни да би се добили излази (аутпути - O), дати ресурси (R) и критеријуми контроле (C). *Улази* се додају активностима и или се трансформишу или користе током времена да би се добили излази. Улази су углавном информације или документација (планови, нацрти, израчунавања, процене и тако даље). Временом је потребно моделовати активности као што су обуке, где су људи улази, или производ испитивања, а у којој хардвер може бити улаз. Када се моделира главни производни процес инпути могу бити материјали или енергија, а излаз може бити избегнут путем примене СБМ-а, као смањење ризичне ситуације која је одређене безбедносним критеријумима.

Излази су жељени производи, нуспроизводи и нежељени резултати. Излази морају да задовољавају одређене критеријуме безбедности, у апсолутном смислу и у односу на околности у којима се користе као улази или ресурси за остале делове процеса.

Ресурси су неопходна средства за обављање активности, али која нису промењена нити укључена у њих, бар не краткорочно. То су хардвер (на пример, инструменти за мерење) или људи. Ако се активношћу лоше управља, или се она одвија дуже времена, ресурси се могу деградирати (хабати и кидати, застарети, повредити или оштетити) и мора постојати циљна активност која укључује избегавање деградације или њено ограничење на прихватљиви ниво оштећења. Ресурси су подређени процесу спецификације, селекције, набавке, коришћења, надгледања и одржавања, који може бити моделован као активност, а у оквиру те активности се може инкорпорисати и ризик од неприхватљивог оштећења.

²¹⁵ Видети: Hale, A. R., at al., исто.

Контроле или *критеријуми* се користе као стандарди да би се проценило да ли је активност успешна. Ово укључује законе и предложене или уведене стандарде безбедности²¹⁶. Такође се могу моделовати и стандарди квалитета за излазе активности. Стрелица која указује на контроле се приказује као да улази на средину активности. Заправо би требало да се примењује на другим тачкама: - на стрелицу која показује улаз, да би се проверило да ли су улази одговарајућег квалитета и потпуности да би се могли трансформисати у жељене излазе; - на стрелицу ресурса, да би се проверило дали су ресурси довољни у квантитету и квалитету да би обављали захтевану трансформацију; - на сам процес трансформације, да би се проверило да ли су процеси у складу са дефинисаним критеријумима и - на стрелицу излаза, да би се проверило да ли задовољава одређене спецификације, пре него што се проследи за следећи процес.

У овом систему се разликују три нивоа активности који одговарају класичној подели менаџмента између политике, планирања и контроле и извршавања. Овде спадају структура система (S), планирање, организација и процедуре (P), извршавање (E - *execution*). Ови нивои морају функционисати у свакој од фаза животног циклуса. Животни циклус се односи на технологију, материјале или производе и у великој мери је повезан са заштитом животне средине.

На пример, Европски машински стандард (CEN, 1991) укључује животни циклус у процену ризика. Постоји шест основних фаза животног циклуса: - планирање (концептуално моделовање, прелиминарни инжењеринг, детаљан план), - конструкција, - израда, - оперативна фаза (покретање, нормално функционисање, гашење), - одржавање и модификација, - демонтажање и уништавање. Овај процес поделе на фазе животног циклуса се може наставити бесконачно. Свака фаза циклуса има свој основни процес, а свака има и своје опасности и потенцијална одступања. Свака од фаза се повезује са свим осталим процесима у моделу. Производ (излаз) једне фазе, представља улаз у другу и стога је безбедност следеће фазе делимично

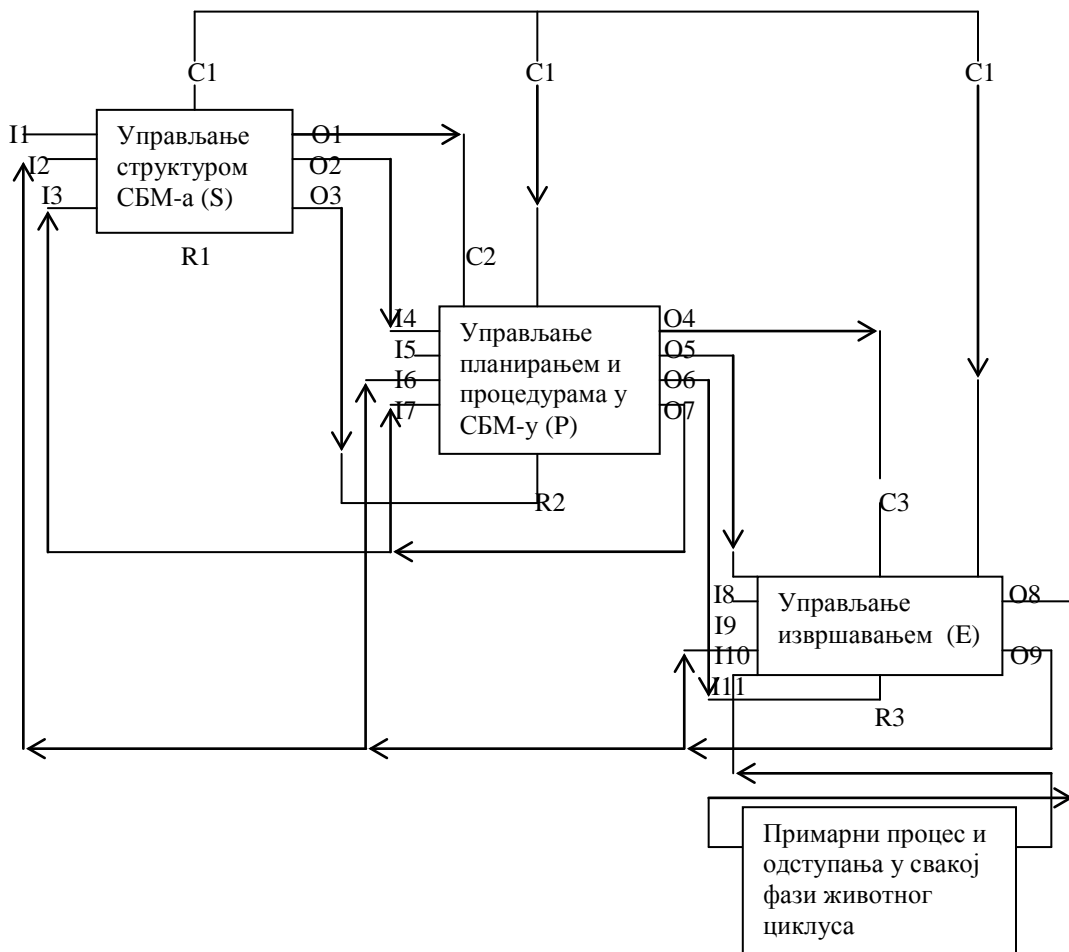
²¹⁶ У принципу, може се рећи да стандарди безбедности имају за циљ да организациони систем учине објективно безбеднијим. Међутим, мерење доприноса неког стандарда безбедности је практично немогуће, зато што на безбедност утиче огроман број фактора и сл. - McDermid, J., Rae, A., *Goal-Based Safety Standards: Promises and Pitfalls, Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 259.

одређена безбедношћу тог производа. Коначан план представља улаз у фазу конструкције, фаза одржавања обезбеђује улаз у оперативну фазу. Према томе, могу се уочити две врсте безбедности којима СБМ мора да управља у свакој од фаза: безбедност процеса и безбедност производа.

На *извршном нивоу* (Е) активности оних који су директно укључени утичу на појаву и контролу опасности (одступања): то су проблеми који се решавају. Првенствено се води брига о већ познатим опасностима (И11) и избору имплементације већ научених активности за њихово елиминисање, смањивање или контролу (О8). Степени слободе који постоје на овом нивоу су ограничени и повратна веза и циклус корекције (О9/И10) се првенствено бави исправљањем одступања од договорених процедура и враћања активности на те стандарде. Чим се ситуација схвати као неодговарајућа за постојеће норме, активира се следећи ниво (И6). Циклус решавања проблема за откривање и уклањање опасности на извршном нивоу у току фазе планирања прилично личи на ниво планирања.

Ниво планирања, организовања и процедура (Р) се бави осмишљавањем и формализовањем активности које треба да изврши Е ниво у зависности од читавог низа очекиваних опасности. Ниво планирања се може наћи у многим приручницима о безбедности где се постављају одговорности, процедуре, линије извештавања, итд. Обезбеђује непрекидност у СБМ, збирку лекција које су научене из успеха и неуспеха у функционисању извршног нивоа. Активира се да би осмислио или променио ниво Е (О4/С3, О5/И8), али то ради у оквиру укупне филозофије и стила који се развијају из структурног системског нивоа. Он омогућује прелаз са апстрактних принципа (И4) на расподелу и имплементацију конкретних задатака (О5, О6). То је ниво који је стално у току и развија нове процедуре за опасности које су нове за организацију (И5) и модификује постојеће процедуре да би биле у току са новим схватањима или стандардима (С1) и решењима која се односе на опасности. Стога је у вези са циклусом побољшања која су потребна у системима управљања квалитетом. Проблем на овом нивоу је сигнал да нижи ниво не ради довољно добро (И6), или да виши ниво (S) жели да уради неку промену (С2), или из окружења о новој опасности или стандарду (И5). Кораци у овој фази покривају спектар средстава

доступних науци, од ревизије планова и статистике о ванредним догађајима (признавање проблема), кроз анализу трошкова и користи (одабир решења), до контроле (мониторинга²¹⁷) и пружања прве помоћи (планирање за ванредне ситуације).



Слика 1. Однос између нивоа система безбедносног менаџмента (Hale, A. R., Heming, B. H. J., Catfhey, J., Kirwan, B., Modelling of safety management Systems, *Safety Science*, Vol. 26, No. 1/2, 1997, pp. 121-140.)

Ниво структуре система и менаџмента се бави свепрожимајућим принципима СБМ, како се поставља и одржава и како функционише. Овај ниво отеловљава оквир који је предложен у раду (I1) и широке принципе на основу којих

²¹⁷ Основна сврха мониторинга јесте да се прикупе подаци о насталој штети, затим подаци на основу којих се може утврдити ефикасност предузетих мера и вероватноћа настанка оштећења (детаљније: Backman, B. F., *Composite Structures, Safety Management*, 2nd ed., Elsevier Ltd., Oxford, 2008.).

се адаптира да би одговарао култури одређене организације (на пример, степен децентрализације и саморегулације, стручњаци на супрот културе линијских менаџера, унутрашњи на супрот уговореним задацима у различитим фазама животног циклуса). Овај ниво се активира (препознаје проблем) када организација сматра да постојећи ниво Р не постиже одређени квалитет или побољшања на извршном нивоу (I2) или да је потребна промена у смислу решавања проблема. То је мета ниво на којем се прати нормално функционисање СБМ (I3) и кроз који се стално побољшава и одржава (O2, O3) када долази до промена у спољашњем окружењу организације. Сигнали да се активира ниво структуре могу настати због појаве већих ванредних догађаја, неодговарајућем извештају контроле, неодговарајућој конкурентској предности (II) и сл.

Треба нагласити да ова три нивоа представљају апстракције у односу на различите типове повратне везе (исправка, учење/побољшања и реструктурирање). Они се не посматрају одвојено од хијерархијских нивоа менаџмента. Активности које су специфициране на сваком од апстрактних нивоа се могу алоцирати на много различитих начина: служба безбедности може имати задатак да напише процедуре, аутономне радне групе могу имати слободу да поставе и прате своје системе безбедносног менаџмента у одређеним границама, или се СБМ може специфицирати од стране највишег руководства, спољни консултанци или менаџери на вишим нивоима могу повремено вршити рутинске инспекције и бити укључени у истраживање ванредних догађаја, итд. „Избор начина на који се алоцирају задаци одражава културу и методе пословања појединих предузећа.“²¹⁸

Овај оквир даје нормативу о начину на који СБМ треба да буде структуриран и на који треба да функционише. То ради на релативно апстрактном нивоу. На пример, преписује да се одређени задаци решавања проблема обављају ради контроле опасности, али не одређује ко треба да их обавља. Наглашава токове информација и ресурса, што указује да морају постојати канали којима се преносе, али оставља довољно слободе организацији да одлучи какви су ти канали. Предлаже да се формулишу критеријуми за процену безбедности сваког корака у примарном процесу

²¹⁸ Hale, A. R, at al., исто.

и адекватности сваког корака у циклусу решавања проблема, као и да ти критеријуми треба да буду конзистентни између нивоа, али њихову спецификацију оставља свакој појединачној организацији. Разлике у начинима на који се прелази са апстрактног на конкретан ниво у организацијама које се баве истом делатношћу указују на њихову безбедносну културу. То значи да „различите организације имају различите ставове и безбедносне културе“²¹⁹. Тиме се уклањају неке нејасноће у постојећој литератури.

3.3.1. Интегрисано схватање појма безбедности

Истраживања о безбедности су открила да људски фактор утиче на фундаменталну улогу у успешности система безбедности који постоје у организацијама. Људски фактор се сматра основним узрочником ванредних догађаја у преко 80% случајева²²⁰, због високе поузданости електронских и механичких компоненти и нове улоге људи у сложеним системима. Безбедност се често дефинише као најмањи могући и прихватљиви ризик, док се ризик схвата као производ могућих оштећења и вероватноће њиховог настанка.²²¹ „Генерално гледано, управљање ризиком подразумева предвиђање одређених ситуација и процене вероватноће настанка ванредних догађаја“.²²²

Запослени су последња заштита од ризика, а њихово понашање је кључно за избегавање материјалних и људских губитака. Међутим, „небезбедно понашање запослених често представља последицу латентних неуспеха у организацији и управљању система“²²³. Ови поремећаји укључују: „недостатак упутстава или одговарајуће обуке, демотивацију, недостатак радних процедура, лоше осмишљене задатке, недостатак контроле, ниску посвећеност менаџмента безбедности и

²¹⁹ Genseric, R. L. L., *Multi-Plant Safety and Security Management in Chemical and Process Industries*, Wiley-VCH Verlag GmbH&Co., Weinheim, 2010., стр. 43.

²²⁰ Видети: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., Safety management system: Development and validation of a multidimensional scale, *Journal of Loss Prevention in the Process Industries*, Volume 20, Issue 1, January 2007, Pages 52-68.

²²¹ Видети: Grote, G., Understanding and assessing safety culture through the lens of organizational management of uncertainty, *Safety Science*, Volume 45, Issue 6, July 2007, Pages 637-652.

²²² Oxelheim, L., Wahlborg, C., *Corporate Decision-Making with Macroeconomic Uncertainty – Performance and Risk Management*, Oxford University Press, Inc., New York, 2008., стр. 17.

²²³ Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

неадекватне безбедносне мере и системе безбедносног менаџмента²²⁴. Овакви проблеми представљају унутрашње претње по организацију. Поред тога, постоје претње које долазе споља, а које се манифестују на различите начине, од крађа и провала, до штете која настаје услед елементарних непогода. Будући да су несигурност и ризик нешто што је саставни део живота, „неопходно је да се делује у правцу њиховог сузбијања“²²⁵. Научници признају да безбедносни менаџмент игра важну улогу у достизању и одржавању високог нивоа безбедности и у смањењу губитака, било да су они последица како унутрашњих тако и спољашњих проблема. Да би безбедносни менаџмент могао да оствари своју улогу, потребно је да се осмисли тако да штити организацију од свих поменутих опасности. Зато је потребно да се сам појам безбедности посматра интегрисано, односно холистички.

Овде треба напоменути да постоје две школе мишљења: они који сматрају да постоји јасна разлика између унутрашње и спољне безбедности и они који сматрају да је безбедност недељива²²⁶. У овом раду се усваја ово друго мишљење. Тако схваћена безбедност омогућава да се систем безбедносног менаџмента обликује у складу са претпостављеним претњама, ризицима и опасностима. Односно, безбедносни менаџмент прераста у интегрисани систем безбедносног менаџмента. Како тврде Ивандић Видовић и др. овај систем мора бити ефикасан и интегрисан систем заштите предузећа и његов најзначајнији одбрамбени механизам.²²⁷ Поред тога, овакав систем мора бити у потпуности усклађен и прилагођен датој организацији, односно, мора бити имплементиран у њене основне токове.

Систем безбедносног менаџмента, у овом раду, се односи на управљачке активности које регулишу два битна сегмента безбедности организације: систем безбедности и заштите на раду, систем самозаштите или физичко-техничког обезбеђења, али и систем управљања заштитом животне средине и систем

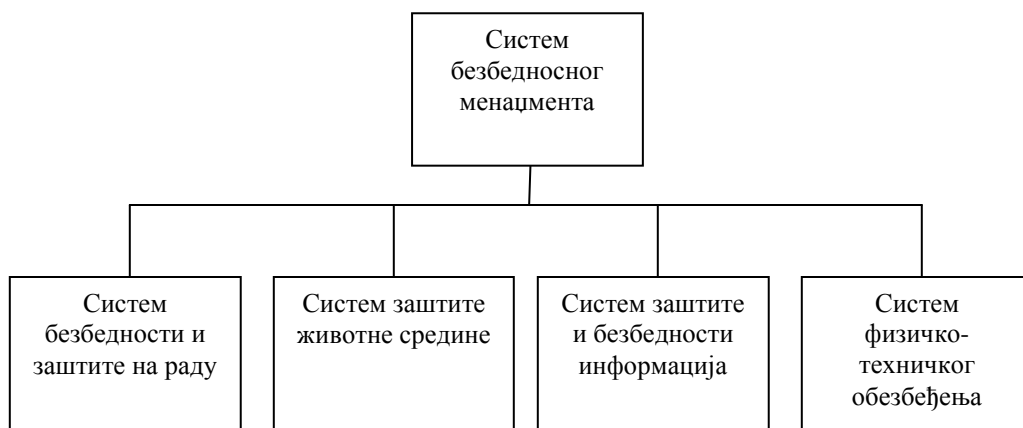
²²⁴ Исто.

²²⁵ Czarniawska, B., Fisher, R., *Organizing in the face of risk and threat*, CBI, London, 2009.

²²⁶ Видети: Van Brabant, K., *Mainstreaming the Organizational Management of Safety and Security. A review of aid agency practices and a guide for management*, Overseas Development Institute, HPG Report 9, London, 2001.

²²⁷ Видети: Ивандић Видовић, Д., Карловић, Л., Остојић, А., *Корпоративна сигурност*, ХУМС, Загреб, 2011., стр. 66.

безбедности и заштите информација. Овај систем се може представити као на слици 2. Сваки од подсистема представља самосталан и веома комплексан систем, али сви они заједно представљају једну заокружену целину чија је сврха постизање што је могуће већег нивоа безбедности неке организације. Тренутно су ови системи у организацијама углавном одвојени једни од других и мало је иницијативе да се интегришу у јединствен систем. Напомињемо да, с обзиром да се ради о системима управљања, сви ови подсистеми треба да буду организовани по истим принципима менаџмента и зато има смисла њима управљати из једног јединственог центра. Посебно је то битно за велике организације у којима је безбедност основни услов опстанка, а послови везани за основну делатност организације су сами по себи јако комплексни. У таквим организацијама безбедност представља додатну бригу, па сматрамо да овакав начин организовања система безбедности заправо представља олакшање топ менаџменту организације.



Слика 2. Интегрисани систем безбедносног менаџмента

3.3.2. Основне особине интегрисаног система безбедносног менаџмента

Систем безбедносног менаџмента одражава посвећеност организације безбедности и представља чинилац који утиче да запослени схвате безбедност као значајан фактор у организацији. „Овај систем обухвата све људе, све ресурсе,

процедуре, *hardware* и *software* који су ангажовани у циљу повећања безбедности²²⁸. То је скуп политика и процедура које имају за циљ да позитивно утичу на ставове запослених и њихова понашања у односу на ризике, а тиме смањују небезбедне активности. Циљ је да се повећа свест о безбедности, разумевање, мотивисаност и посвећеност свих радника²²⁹. Тако систем безбедносног менаџмента представља предуслов за постојање безбедносне климе, која представља „ставове запослених и њихова схватања о значају организационе привржености безбедности“²³⁰.

Дакле, систем безбедносног менаџмента се може схватити као скуп политика, стратегија, поступака, процедура, улога и функција повезаних са безбедношћу. Систем безбедносног менаџмента обухвата механизме који се интегришу у организацију и имају за циљ да контролишу опасности које могу утицати на здравље и безбедност запослених, али и на безбедност уже и шире околине, као и безбедност информација. Основни циљ система безбедносног менаџмента јесте да омогући достизање општих циљева организације, односно он повећава вредност пословања кроз смањење ризика²³¹. У исто време, овај систем омогућава да се организација лакше прилагоди законској регулативи. Да би систем био ефикасан и ефективан мора бити прихваћен и примењен од стране запослених. То значи да овај систем мора промовисати позитивну безбедносну климу. Због тога је потребно да га сви нивои менаџмента подржавају и промовишу. Фернандез-Муњис и група аутора²³², сматрају да ефикасан и ефективан систем безбедносног менаџмента треба да се састоји од:

1) Развоја *безбедносне политике*, која укључује посвећеност организације безбедности и формално изражава циљеве, принципе, стратегије и упутства која треба следити по питањима здравља и безбедности на раду. Исто тако, безбедносне политике одређују функције и одговорности сваког члана организације у тој области.

²²⁸ Maguire, R., *Safety Cases and Safety Reports – Meaning, Motivation and Management*, Ashgate Publishing Ltd., Aldershot, 2006., стр. 22.

²²⁹ „Да би се избегли губици у пословању, потребно је повећати свест запослених о безбедносним процедурама, као и да се обезбеди адекватна обука менаџера безбедности.“ - Canning, A., *The Need for a Community for a System and Functional Safety Professionals, Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 31.

²³⁰ Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

²³¹ О овоме шире: Merna, T., Al-Thani, F., *Corporate Risk Management*, 2nd Edition, John Wiley and Sons, Ltd., Chichester, 2008.

²³² Видети: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

Њихов циљ је да се створи повољна клима и осигура да појединци на свим нивоима учествују и дају свој допринос безбедности. Штавише, такве политике треба да буду засноване на непрестаним побољшањима и на учењу које је засновано на искуству, стога се не препоручује да се политике детаљно одреде док се бар једном не затвори циклус процеса безбедносног менаџмента²³³. Наравно, „повремено је потребно радити ревизије и према потреби уводити промене безбедносне политике“²³⁴.

2) *Подстицања партиципације запослених* у активностима које се тичу здравља и безбедности, у циљу промовисања безбедног понашања и укључивања запослених у процесе одлучивања, путем средстава казне и награђивања или путем консултовања о условима на радном месту. Њихов циљ је да покажу запосленима да се цени њихов допринос безбедности у организацији, па стога и да се обликују њихове идеје, вредности и поступци да би се постигло безбедно понашање.

3) *Обуке* и развој компетентности запослених. Обука о питањима безбедности има за циљ да оспособи запослене да исправно обављају своје задатке. Она их информисе о ризицима на радном месту и доступним процедурама за њихово спречавање, корекцију или минимизирање. Она такође има за циљ да промени ставове, тако да и руководиоци и запослени постану укључени и прихвате чињеницу да је безбедност основни чинилац добро обављеног посла. У исто време, организације треба да иницирају систем сталне реедукације и сталне обуке који запосленима дају најновија знања.

4) *Комуникације* и преноса информација о могућим ризицима на радном месту и како се најбоље борити са њима. Дobar систем комуникације у организацији треба да обухвати серије елемената, и то формалних и неформалних, који обезбеђују одговарајући ток информација, са врха на доле и са дна ка врху, као и побочно. Ово ће бити од користи за мотивацију и стимулисати партиципацију свих чланова организације.

²³³ Видети: Segal, S., *Corporate Value of Enterprise Risk Management, The Next Step in Business Management*, John Wiley & Sons Inc., New Jersey, 2011.

²³⁴ Norman, T. L., *Risk Analysis and Security Countermeasure Selection*, CRC Press, Boca Raton, 2010., стр. 237.

5) *Планирања*, где се прави разлика између превентивног планирања и планирања за ванредне ситуације. Превентивно планирање одређује могуће опасности у окружењу, анализира ризик од њиховог појављивања и предлаже систем мера за превенцију незгода и губитака. Да би се проценила безбедност могу се користити бројни методи за анализу ризика: квантитативна процена ризика, „Шта-ако“ анализа, и сл. Према листи приоритета која се прави на основу ових техника, могу се предузети превентивне и заштитне мере. С друге стране, план за ванредну ситуацију укључује организовање скупа људских и материјалних ресурса који су потребни да би се брзо и ефективно одговорило на ванредни догађај, где је циљ да се максимално ограниче потенцијалне последице. Ово, поред осталог, подразумева усвајање мера прве помоћи, гашења пожара, евакуације радника.

б) *Контроле* и ревизије активности које се спроводе унутар организације. Ово допушта стална побољшања. Могу се разликовати два типа контроле: унутрашња контрола и технике *benchmarking*-а. Унутрашња контрола се спроводи средствима анализе операција и радних услова – инспекција и провера и кроз идентификацију, истрагу и бележење догађаја – акцидента, инцидента и пропуста, који се дешавају у организацији. *Benchmarking* представља процес учења који се заснива на истраживању најбољих система менаџмента на тржишту, који ће служити као препорука за боље перформансе. *Benchmarking* дозвољава да организације пореде своје стопе ванредних догађаја са организацијама које користе сличне процесе, као и да пореде поступке и технике менаџмента (на пример, контролне процедуре, технике за истраживање ванредних догађаја, ергономске карактеристике послова, програме обука, и сл.) које примењују са другим организацијама из било ког другог сектора, где се могу идентификовати снаге и слабости.

Хипотезе које су поставили Фернандез-Муњис и аутори²³⁵ се односе на планирање (превентивно планирање и планирање за ванредне ситуације), контролу (унутрашња контрола и *benchmarking*) и на природу безбедносног менаџмента (то је мултидимензиони проблем који се дели на шест делова – политика, подстицај, обука, комуникација, планирање и контрола). Ови принципи се лако применити на

²³⁵ Видети: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

интегрисани систем безбедносног менаџмента, што значи да би се избегла понављања на појединачним нивоима. Односно, интегрисани систем управљања безбедношћу би аутоматски могао да кроз безбедносну политику, подстицај, обуку, комуникацију, планирање и контролу изгради безбедносну культуру, успостави повољну безбедносну климу и да једноставним промовисањем ових вредности истовремено повећа свест запослених о безбедности у свим системима који се односе на безбедност и заштиту, а који су без оваквог приступа битно фрагментисани.

Циљ безбедносне политике је да обликује ставове запослених у смислу да они постану позитивни у односу на безбедност. Ови ставови су у корелацији са статистички значајним нижим стопама ванредних догађаја, где је понашање основни посредник. Безбедна понашања су ојачана коришћењем подстицаја. У исто време, запослени ће имати довољно знања и информација да извршавају задатке на прави начин и правиће мање грешака, ако постоје сталне обуке. Организација прави планове операција и превентивних мера које треба имплементирати после одређивања и процене ризика различитих процеса. Менаџери такође треба да планирају активности које се предузимају у ванредним ситуацијама, а о начинима реаговања се обавештавају сви запослени. Коначно, постоји контрола и ревизија да би се осигурало да сви ови елементи правилно функционишу. Овакав модел укључује скуп поступака у циљу контроле ризика процеса и усвајања безбедног понашања. Резултат оваквог система је смањење вероватноће дешавања ванредних догађаја у организацији и опадање броја прекида и ометања пословних процеса. Такође, овај систем укључује запослене у процес доношења одлука. Због тога долази до побољшања мотивације и задовољства послом, што ојачава идентификацију и посвећеност запослених организацији. То, заузврат, доводи до повећања продуктивности. Ванредни догађаји подривају морал, изазивају демотивацију у случају да менаџмент није довољно заинтересован за превенцију, или чак конфликте на радном месту, што може довести до протеста против неодговарајућих радних услова. Када нема опасности, запослени сматрају да их руководиоци цене и подржавају, а то доводи до имплицитне обавезе запослених да се убудуће понашају тако да доприносе успеху организације. Ово доводи до повећаног задовољства

послом, већег интересовања и укључивања у посао. Коначно, систем смањује одсуство са посла и вероватноћу напуштања организације од стране запослених. Тиме се одржава потребна образовна структура запослених. Мора се имати у виду да организација има губитке у случају прекида посла, јер се знање и искуство запослених не могу лако заменити, будући да „сваки запослени има одређене карактеристике, знање и потенцијал који доприносе успеху организације“²³⁶.

Овде треба напоменути да култура представља моћан и често несвестан скуп сила које утичу на понашање појединаца и група, њихово схватање живота и вредности уопште. Организациона култура утиче на стратегију, циљеве и начин функционисања организације.²³⁷ Безбедносна култура, као део организационе културе, се сматра основним аспектом способности организације да управља елементима који су повезани са безбедношћу производних процеса. Како сматрају многи аутори, „лоша безбедносна култура је фактор који доприноси развоју многих акцидентата“²³⁸. Зато је развој безбедносне културе од великог значаја за успешан безбедносни менаџмент.

На основу свега наведеног, систем безбедносног менаџмента се може дефинисати и као скуп људи, ресурса, политика и процедура који су у међусобној интеракцији и који су организовани на начин који умањује штету и губитке који настају у пословном процесу и на радном месту. Да би овај систем био ефикасан и постигао смањење стопе ванредних догађаја, мора да се интегрише у свакодневни рад организације и да охрабрује безбедно понашање запослених и њихово укључивање, за шта је од кључне важности да има подршку највишег руководства. Овај систем мора бити свеобухватан, да узима у обзир интеракцију са другим управљачким системима, као што је управљање квалитетом, и мора да буде заснован на филозофији непрестаног побољшања и да води изврности пословања.

²³⁶ Исто.

²³⁷ Видети: Schein, E. H., *The Corporate Culture Survival Guide*, John Wiley & Sons, Inc., San Francisco, 2009.

²³⁸ Bain, A., *Do we truly understand Safety Culture?*, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 11.

3.4. Елементи система безбедносног менаџмента

Као што је већ речено, систем безбедносног менаџмента се може дефинисати као скуп људи, ресурса, политика и процедура који су у међусобној интеракцији и који су организовани на начин који умањује штету и губитке који настају у пословном процесу и на радном месту. Да би овај систем био ефективан и постигао смањење нежељених догађаја, мора да се интегрише у свакодневни рад организације и да охрабрује безбедно понашање запослених и њихово укључивање у систем, за шта је од кључне важности да има подршку највишег руководства. Систем безбедносног менаџмента мора бити свеобухватан, да узима у обзир интеракцију са другим управљачким системима, као што су управљање квалитетом и животном средином, мора да буде заснован на филозофији непрестаног побољшања и да води изврсној пословања. Успех безбедносног менаџмента зависи од интеграције безбедности у све аспекте функционисања организације. Ниво до кога је систем безбедносног менаџмента интегрисан у шире системе менаџмента и управљања ризиком у организацији, зависи од развијености безбедносне културе и система безбедности, али и од сложености саме организације.

Према томе, основни елементи система безбедносног менаџмента су:

- филозофија,
- политика,
- процедуре и
- поступци.

Безбедносни менаџмент започиње са менаџмент филозофијом, односно схватањем да ће увек постојати претње безбедности, постављањем организационих стандарда и потврђивањем да је безбедност одговорност свих запослених. Политика дефинише начин на који ће се постизати циљеви. Она подразумева јасно изражене одговорности и ауторитете, развој организационих процеса и структура да би се инкорпорирали безбедносни циљеви у сваки аспект деловања организације и развијање вештина и знања који су неопходни да би се посао обављао на најбољи могући начин. Процедуре се односе на оно што менаџмент жели да људи ураде да би спровели политику у дело. Процедуре морају да обухватају јасна упутства свим

запосленим, средства за планирање, организовање и контролу и средства за праћење и процену безбедносног статуса и процеса. Поступци се односе на стварна дешавања на радном месту. Добро осмишљени и примењени поступци подразумевају „прихватање и поштовање ефикасних процедура, избегавање својеволјног скраћивања и промене у њима“²³⁹, јер то може довести до угрожавања безбедности и предузимање одговарајућих активности када се уочи неки безбедносни проблем²⁴⁰.

Организационе структуре и активности које чине систем безбедносног менаџмента се могу наћи широм организације, а сваки запослени доприноси повећању безбедности. У већим организацијама, активности безбедносног менаџмента би требале да буду видљивије у неким одељењима него у другим, али се систем мора интегрисати у саму суштину деловања. Ово се може постићи „имплементацијом и непрестаном подршком безбедносној политици што доводи до добро осмишљених процедура“²⁴¹.

Имплементација система безбедносног менаџмента зависи од иницијативе највишег руководства. Иницијативе не морају увек бити успешне. Основни чиниоци који доприносе њиховом неуспеху су недостатак посвећености, разумевања и компетентности. Ови елементи утичу и на успех безбедносног менаџмента. Посвећеност значи да су руководиоци ти који морају да се залажу за ефикасну примену принципа безбедносног менаџмента. Разумевање се односи на то да руководиоци разумеју природу и принципе управљања безбедношћу, а компетентност на то да ли су политика и процедуре одговарајуће, схваћене, прихваћене и примењене на одговарајући начин на свим нивоима у организацији.²⁴²

²³⁹ <http://www.tc.gc.ca/civilaviation/SystemSafety>.

²⁴⁰ „Одређивање безбедносног проблема подразумева јасно дефинисање три фактора: - врсте претњи које утичу на оно шта се чува, - вероватноће да се те претње претворе у догађаје који доводе до губитка и - утицај на имовину или организацију уколико дође до губитка“ - Walsh, J., *Asset Protection and Security Management Handbook*, POA Publishing LLC, Boca Raton, 2002., стр. 19.

²⁴¹ <http://www.tc.gc.ca/civilaviation/SystemSafety>.

²⁴² Више на: <http://www.tc.gc.ca/civilaviation/SystemSafety>.

3.5. Стандарди који утичу на обликовање СБМ

Као што је поменуто, на обликовање Система безбедносног менаџмента у овом раду, поред Директиве „Seveso II“ утиче и велики број стандарда. Ту спадају стандарди који се односе на заштиту животне средине, заштиту здравља и безбедности на раду, заштиту од пожара, заштиту и безбедност информација²⁴³.

Заправо, претпоставка овог рада јесте да се сви ти системи могу објединити у један јединствен систем безбедносног менаџмента. Иако на први поглед то изгледа компликовано, треба узети у обзир чињеницу да се ови системи тренутно уводе или већ функционишу у већини организација у развијеним земљама, тако да би њихово интегрисање представљало мали додатни напор. Сматрамо да би предности које би се тиме постигле увелико превазишле тај напор. Односно, основна предност оваквог приступа би била да се свим овим пословима управља из једног центра, тако да би топ менаџмент могао да има интегрисан и сублимиран извештај о безбедности, чиме би био растерећен парцијалних извештаја о стању у свакој појединачној области. Тако би слика о безбедности организације била много јаснија, што би, заузврат, олакшало доношење одлука и предузимање појединих мера.

3.5.1. Стандард за заштиту од пожара

Стандард који се односи на заштиту од пожара BS 9999:2008²⁴⁴ је британски стандард који се односи на то како ће се обликовати зграде и постројења, како ће се користити и њима управљати. Стандард одређује начине на који се постиже сагласност са законима о заштити од пожара на флексибилан начин. BS 9999:2008 обезбеђује структуру засновану на процени ризика која узима у обзир велики број фактора, укључујући и излаз у случају нужде за људе са посебним потребама. Стандард се може користити у већ постојећим зградама, у фази планирања изградње нових постројења или доградње постојећих, а може се применити приликом измена у постојећим зградама. Он обезбеђује средство за процену да би се могло утврдити да ли постојећа стратегија безбедности и даље има исту примењивост.

²⁴³ Више о стандардима на: http://www.iso.org/iso/iso_catalogue/standards_in_action.htm

²⁴⁴ Видети: http://www.aosh.org.uk/presentations/dec2009_fsm.pdf

Стандард BS 9999:2008 обезбеђује најбоља упутства за противпожарну заштиту. Он одређује начине за тестирање противпожарне стратегије, укључујући лак прилаз излазима, да би се осигурала безбедност људи који су у згради или који су у њеној близини. Такође, он одређује начин за управљање заштитом од пожара у току читавог животног циклуса зграде – од самог нацрта или плана за реновирање, до процене система противпожарне заштите и одржавања система за детекцију пожара. Овај стандард такође садржи упутства за обуку запослених о противпожарној заштити, где се даје и начин организовања и спровођења евакуације и расподела одговорности. Овај стандард такође води рачуна и о свим запосленим на пословима одржавања зграде и ватрогасцима.

Увођењем стандарда BS 9999 може се постићи очекивани ниво противпожарне заштите којим се може проценити одрживост датог решења, а постоји фундаментална претпоставка да ће се зградом управљати током читавог њеног употребног века. Стандард предвиђа да ако је зграда осмишљена на прави начин, правилно управљање њом мора да омогући да ће она и даље функционисати како је прописано. Документ обезбеђује упутства о функционисању управљања противпожарном заштитом и критеријуме по којима се може проценити то функционисање.

Стандард прописује да корисник мора пре свега да уради Профил Ризика за одређену зграду или постројење. Ако већ постоји одређено знање о заштити од пожара, тај профил се може одредити на основу датих принципа. Пошто се утврди профил, потребно је обезбедити минимум противпожарних мера, као што су одређена удаљеност, ширине степеништа и излаза и ниво противпожарног алармног система. Минимални пакет мера се одређује у односу на перцепциране ризике. Уколико се те мере не могу постићи, потребно је предузети инжењерске мере из области противпожарне заштите.

Уколико је могуће постићи минимални пакет мера, онда се мере морају даље анализирати да би се утврдило да ли је могуће постићи његову флексибилност. То се постиже увођењем побољшања у противпожарну заштиту тако што се користе додатне мере. Први део профила ризика се односи на карактеристике запослених.

Ово је важно зато што кад они који раде у згради (или живе) нису упознати са зградом или постројењем, или уколико пожар настане у току ноћи, потребно је више времена да би се извршила евакуација. Према категоријама ризика прописаним у стандарду се одређује и примена стандарда. Постоје више ризичне категорије у којима је стандард неупотребљив. За њих се користе други оштрији прописи.

Други део профила ризика се односи на ширење пожара. Стандард даје табелу према којој је могуће проценити ширење пожара, али је могуће да стручњаци везани за ову област сами одреде очекивану стопу ширења пожара у зависности од ситуације. Категорије у табели се односе на споро, средње, брзо или веома брзо ширење пожара у зависности од запаљивости коришћеног материјала за израду зграде или постројења.

Флексибилност система противпожарне заштите се постиже додатним мерама, које су изван минималног прописаног стандарда. На пример, јасно је да ће побољшан систем за детекцију пожара обезбедити боље време за евакуацију. Такође, високе таванице омогућавају више времена за евакуацију, јер ће диму требати више времена да се спусти на руте за евакуацију. Аутоматске прскалице дају могућност да се смањи стопа ширења пожара. Када се смањи процењена стопа ширења пожара, могу се променити остали захтеви везани за заштиту од пожара. Побољшан систем детекције и упозорења омогућавају већи број опција, где се флексибилност може постићи продуженом рутом за удаљавање од зграде или мањим промером противпожарног излаза, степеништа и сл. Поред тога, овај стандард узима у обзир да одређени део топлоте излази кроз вентилационе отворе, чиме се смањује период отпорности пожара уколико ти вентилациони отвори могу да се прилагоде појединим прописима.

Упутство за употребу стандарда јасно прописује дозвољене опције и веома је једноставно за коришћење. Да би овај стандард био ефективан и ефикасан, потребно га је применити у целини.

3.5.2. Стандарди OHSAS 18000

OHSAS 18000 је међународни стандард за управљање системом здравља и безбедности на радном месту. Он се састоји од два дела. OHSAS 18001 и 18002 и обухвата већи број сличних публикација.

OHSAS 18001 (Occupation Health and Safety Assessment Series)²⁴⁵ је стандард који дефинише захтеве за систем управљања здрављем и безбедношћу на радном месту. Има за циљ да помогне организацијама да контролишу ризике везане за здравље и безбедност на радном месту. Развијен је као одговор на широко распрострањене захтеве за стандардом који би служио за процену и сертификацију овог система. Компатибилан је са стандардима ISO 9001 и ISO 14001.

Заштита здравља на раду је намењена организацијама које су свесне значаја безбедности здравља својих запослених и стално настоје да унапреде и одржавају ниво физичке, менталне и друштвене безбедности радника свих занимања као и спречавање њихових повређивања.

Имплементацијом овог стандарда, предузеће стиче поверење заинтересованих страна уверавајући их да је руководство опредељено да испуњава захтеве из политике заштите здравља и безбедности на раду, да је нагласак на превентиви, а не на корективним мерама, да је могуће пружити доказе о томе да се OHSAS односи на целу организацију, а не само на процесе за које постоје законски прописи или зоне великих ризика, и да концепција OHSAS укључује процес сталног побољшавања.

Основна подручја којима се овај стандард бави су:

- планирање ради идентификације опасности;
- процена и контрола ризика;
- менаџмент здравља и безбедности на радном месту (*Occupational Health and Safety* - OHS), развијање свесности о овом проблему и компетенција, обука, комуникација, припремљеност за ванредне ситуације и брзи одговор, мерење перформанси и увођење побољшања.

²⁴⁵ Видети: <http://www.eurostandard.rs/sistem-menadzmenta-zastitom-zdravlja-i-bezbednoscu-na-raduo-hsas-18001/>

Стандард OHSAS 18002 обезбеђује упутства за имплементацију OHSAS 18001. Он објашњава захтеве и начин на који се може постићи имплементација и регистрација овог стандарда.

Између осталих, следећи документи су коришћени за одређивање ових стандарда:

- BS8800:1996 – упутство за системе менаџмента здравља и безбедности на радном месту;
- DNV Стандард за Сертификацију Система Менаџмента Здравља и Безбедности на Радном месту (OHSMS):1997;
- Технички Извештај NPR 5001:1997 – Упутство за систем менаџмента здравља и безбедности на радном месту;
- Нацрт LRQA SMS 8800 - Критеријуми за процену система за менаџмент здравља и безбедности на радном месту;
- SGS & ISMOL ISA 2000:1997 – Захтеви за Систем менаџмента здравља и безбедности на радном месту;
- BVQI Безбедносни Сертификат: Стандард за Управљање Здрављем и Безбедношћу на Радном месту;
- Нацрт AS/NZ 4801 Систем управљања здрављем и безбедношћу на радном месту – Спецификација и упутство за употребу;
- Нацрт BSI PAS 088 – Системи за управљање здрављем и безбедношћу на радном месту;
- UNE 81900 серија пред-стандарда о Превенцији ризика на раду;
- Нацрт NSAI SR 320 – Препоруке за Систем Менаџмента Здравља и Безбедности на радном месту.

Предности имплементације OHSAS 18001:

- ризик од повреда на радном месту своди на минимум;
- пружа заштиту од могућих повреда, како запосленима, тако и посетиоцима;
- доприноси спремности компаније да правовремено отклони опасност;

- усклађује радне процесе компаније са законским прописима;
- смањује трошкове (јер смањује премије за осигурање и компензације/казне у случају кршења уговора);
- побољшава перформансе организације (јер се повећава оперативна ефикасност због смањења акцидента и смањења времена опоравка);
- побољшава општу слику компаније;
- привлачи стране улагаче;
- улива поверење корисницима/купцима да постоји одређеност управљања заштитом здравља и безбедношћу на раду која се може доказати;
- отвара нове тржишне могућности за сарадњу са великим иностраним предузећима чији је један од основних циљева безбедност и здравље на раду.

3.5.3. Стандарди ISO 14000

ISO 14001 „дефинише захтеве за управљање заштитом животне средине“²⁴⁶.

Испуњавање ових захтева је потребно документовати како би постојао доказ о поштовању стандарда и о ефикасном раду у складу са стандардом.

Систем управљања заштитом животне средине ISO 14001:2004 је управљачки алат који омогућава организацији било које величине да:

- идентификује и контролише утицај својих активности, производа и услуга на животну средину,
- побољша однос према животној средини,
- имплементира систематски приступ којим ће постизати циљеве који се односе на заштиту животне средине и обезбеди доказ да је постигла постављене циљеве.

Имплементација Система управљања заштитом животне средине може се односити на читаву компанију, један огранак или на само један радни процес, а избор углавном зависи од потребе компаније.

Основни разлози који доводе до изражене потребе за увођењем система заштите животне средине ISO 14001:2004 су:

²⁴⁶ <http://www.eurostandard.rs/sistemi-upravljanja-zastitom-zivotne-sredine-iso-14001/>

- непрестано загађивање животне средине,
- страх од потпуног исцрпљења природних ресурса,
- недостатак организованог и систематског праћења последица загађења,
- повећана заинтересованост јавног мњења за очувањем животне средине,
- законска решења,
- посебни услови рада у угроженим областима.

Предности имплементације система заштите животне средине ISO 14001:

- Смањење негативних учинака на животну средину,
- Смањење ризика од еколошких катастрофа,
- Повећање способности брзе и ефикасне интервенције,
- Побољшани углед и стварање поверења код заједнице,
- Компетитивна предност,
- Правна сигурност због поштовања закона о заштити животне средине,
- Лакше добијање овлашћења и дозвола од локалних и државних власти,
- Побољшање вашег угледа и угледа вашег клијента,
- Боље коришћење енергије и заштита вода, пажљиво бирање сировина и контролисану рециклажу отпада, доприноси смањењу трошкова и подиже вашу конкурентност,
- Смањује се ваш финансијски терет због реактивних управљачких стратегија као што су поправке, чишћења, плаћање казни због кршења закона,
- Побољшава се квалитет радних места и морал запослених,
- Отварају се нове могућности запошљавања на тржиштима где је важна еколошка производња,
- Еколошки свесни клијенти пословаће са компанијама попут ваше, јер истиче своју обавезу према очувању животне средине.

3.5.4. Стандарди ISO 27000

ISO 27001 је међународни стандард који се односи на заштиту и безбедност информација.²⁴⁷ Стандард подлеже различитим подручјима примене као и за разликовање могућих процеса у организацији који су повезани са управљањем и контролом безбедности као што су: политика безбедности, безбедност организације, контрола и класификација извора, безбедност особља, безбедност материјалних добара и животне средине, оперативно управљање и комуникација, контрола приступа, развој и одржавање разних система и управљање континуитетом пословања.

Ова серија обухвата стандарде који: дефинишу захтеве за ISMS као и захтеве за тела која сертифицију ISMS; обезбеђују подршку, детаљна упутства и инструкције за целокупан процес планирај-уради-провери-делуј (*Plan-Do-Check-Act*); даје специфична секторска упутства за ISMS и оцењивање усаглашености за ISMS.

Стандард ISO 27001 је значајан стандард за организације које се баве услугама у областима које су на било који начин повезане са Информационим технологијама и потребом за очување поверљивости информација. Његова имплементација и примена омогућавају бољу сарадњу са сличним организацијама широм света које послују по овом моделу. Овим стандардом, организације демонстрирају својим корисницима и осталим заинтересованим странама да послују са пословним процесима на бази принципа безбедности и да је пословна политика усмерена на стална побољшања у систему менаџмента за безбедност информација и процесима пружања услуга повезаним са њим.

Имплементација система заштите и безбедности информација пружа уверење клијентима и пословним партнерима да се према информацијама поступа одговорно и да се оне користе и дистрибуирају професионално и сигурно.

Предности ISO 27001:

- конкурентска предност,
- смањење ризика од оштећења и губитка информација, а самим тим и трошкова,

²⁴⁷ Видети: <http://www.eurostandard.rs/sistem-zastite-i-bezbednosti-informacija-iso-27001/>

- усаглашеност са важећим законским прописима,
- веће поверење клијената, запослених, сарадника, институција и свих заинтересованих страна због знања да су њихови подаци безбедни,
- постојање одговорности за безбедност информација од стране свих и на свим нивоима у организацији.

4. МЕТОДЕ ЗА ПРОЦЕНУ АКТИВНОСТИ БЕЗБЕДНОСНОГ МЕНАѢМЕНТА

Као што је речено, управљање подразумева постављање циљева, а затим праћење радног процеса и упоређивање постигнутог резултата са тим циљевима. Да би се тај процес могао остварити, потребно је одредити систем мерења, при чему циљеви морају бити што је могуће јасније дефинисани и мерљиви. Тако дефинисано, мерење омогућава да се разумеју процеси у организацији и да се на основу тога могу предузети активности у циљу побољшања пословања, вршити упоређивања, проучавати трендови и утврдити каузални односи између ресурса и стања у организацији²⁴⁸. Традиционално безбедност се мери преко „небезбедности“, на пример преко изгубљеног времена, стопе повреда на раду и сл. Иако су таква мерила од великог значаја за истраге, чињеница је да се она односе на стање после неког инцидента. Зато је битно да се пронађу мерила која би омогућила да се предузму активности пре него што се деси неки нежељени догађај. Оваква мерила укључују:

1. процене – мерење аспеката система менаѢмента,
2. мерење стања – стање опреме,
3. мерење понашања.

Како тврде Фернандез-Муњис и група аутора²⁴⁹, мерење стања укључује бар две врсте мерила: мерила физичког стања и мерила ризика. Мерење физичког стања се врши путем визуелног посматрања елемената који су описани као кључни. Тако се добијају нумеричке вредности које указују на стање опреме. Мерење ризика се врши путем метода за рангирања ризика²⁵⁰. За сваки елемент опреме се рачуна ниво ризика

²⁴⁸ Видети: Moseley, J. L., Dessinger, J. C., *Handbook of Improving Performance in the Workplace: Measurement and Evaluation*, Vol. 3, International Society for Performance Improvement, San Francisco, 2010., стр. 44.

²⁴⁹ Видети: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., Safety management system: Development and validation of a multidimensional scale, *Journal of Loss Prevention in the Process Industries*, Volume 20, Issue 1, January 2007, Pages 52-68.

²⁵⁰ Напомена: Сам термин „ризик“ није дефинисан у законским актима, нити се једнозначно одређује у корпоративним правилницима. У професионалном смислу, овај термин се дефинише на различите начине. На националним нивоима постоје различите регулативе које се односе на извештавање о управљању ризицима. (О томе детаљније: Woods, M., at al., *International Risk Management*, Elsevier, Ltd., Oxford, 2008.)

и исказује као комбинација оштећења (последица) и вероватноће да до њега дође. Кумулативне вредности могу указивати на укупан ниво ризика којем је изложена организација или њен део. Стање опреме је последица многих активности у организацији који су део система менаџмента. Такве активности укључују: - анализу опасности, - просторно планирање и инсталације, - одржавање и преглед опреме, - управљање променама, - преглед закона, кодова и стандарда у индустрији, - обуку запослених, - руковођење и надзор, - набавку материјала и опреме.

„Мерење стања опреме је средство које помаже да се открију превиди и грешке у самој структури пословања, открију одступања од почетних спецификација у плановима који су требали да буду реализовани, као и да се установи сагласност са кодовима, стандардима и уобичајеним праксама у одређеној привредној грани.“²⁵¹ Овако схваћено, стање опреме указује на ефективност активности менаџмента.

Мерење стања опреме и ризика се фокусира и на утврђивање ефикасности активности система менаџмента. Будући да су ове активности усмерене на елиминисање и контролу опреме која није у складу са стандардима (да би се губици могли држати на жељеном нивоу) и са тим повезаним ризицима, мерила стања овакве опреме могу бити индикатор ефикасности система контроле. Још један циљ се може повезати са овим мерама, а то је „утврђивање опреме која не задовољава стандарде и могућности да се то поправи“²⁵².

Мерење понашања се односи у првом реду на две групе: људе који су на руководећим позицијама (менаџери, супервизори и одговарајуће особље) и људе који су на критичним радним местима. Под руководећим радним местом се подразумевају све позиције на којима је могуће да се утиче на понашање других. Запослени на тим позицијама својим примером, тиме шта раде или не раде, понашањем приликом доношење одлука, указују на то шта је заправо за њих битно. Зато је од кључне важности да се мери „менаџерско“ понашање, будући да су менаџери ти који утичу на понашање осталих запослених. Понашање запослених на производним радним местима се може поделити на две категорије: - посматрање општег понашања, које се

²⁵¹ Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

²⁵² Исто.

односи на начин како се људи генерално понашају, и - посматрање понашања приликом извршавања задатака, које је усмерено на перформансе запослених приликом рада на конкретном задатку који се сматра критичним за пословање. „Мерење понашања одражава ставове које организација и запослени имају. Индивидуални ставови неких људи, нарочито врховног менаџмента, служе као основа за организационо понашање, што опет утиче на понашање осталих запослених и тако даље. Индивидуално и организационо понашање су повезани и утичу једно на друго.“²⁵³

Када је реч о управљању безбедношћу, управо је понашање запослених од кључне важности. Све што људи раде је последица њихових ставова и уверења. Понашање је оно што се може посматрати и мерити и што указује на ставове који стоје иза њега. „Пожељно“ понашање није нешто што се дешава случајно. Понашањем се мора управљати да би се добили најбољи резултати. Увек треба имати на уму да се „пожељно“ понашање односи на стандард, било да је реч о писаном или неком другом облику стандарда. Зато свако мерење мора почети одређивањем шта је то „пожељно“ понашање. Управљање понашањем укључује следећа питања:

- одабир људи који показују жељено понашање или који су спремни и способни да га покажу. Овај одабир постаје још важнији у ери када се све више иде на културу „овлашћења“²⁵⁴;

- начин на који се правила, процедуре и сл. постављају у организацији. Таква правила и процедуре указују на жељено понашање, иако нису дати у писаној форми.

Поред тога, у циљу утврђивања ефикасности и ефикасности система безбедносног менаџмента, потребно је разрадити средства и инструменте за мерење његове успешности. Постоје различита средства која се могу користити, као што су канали размене информација, различити састанци менаџера и запослених на нижим нивоима, итд. Међутим, примена ових средстава зависи од безбедносне културе и не

²⁵³ Исто.

²⁵⁴ „Култура овлашћења“ је концепт менаџмента који се пре свега ослања на делегирање ауторитета и одговорности запосленима на нижим нивоима, чиме се утиче на мотивацију запослених.

постоје јасно дефинисани индикатори за ову процену. Оно што је јасно, јесте да постоје генерички критеријуми за процену шта је то лош СБМ. Неки од њих су:

а) недостају неки кораци у циклусу решавања проблема или задаци нису распоређени, на пример, нема евалуације ефективности безбедносних мера;

б) нису доступни ресурси одређеног квалитета или квантитета на одговарајућем месту или у одговарајуће време, на пример, недостатак обуке за планере;

в) задаци се не распоређују људима са одговарајућим ауторитетом и могућношћу одлучивања или постоје конфликти међу задацима, на пример, менаџери којима се већ судило због ванредних догађаја који треба да охрабрују извештавање о њима;

г) задаци нису прихваћени или спроведени на прави начин;

д) комуникација и координација између задатака (ток информација) се не обавља у одређеним временским интервалима, на пример, између одржавања и обављања послова око модификација;

ђ) улази и излази и активности нису подвргнути одговарајућим проверама безбедности, а критеријуми нису разрађени, на пример, приликом предавања планова фази конструкције;

е) значајна одступања се дешавају и то са неприхватљивом учесталошћу и не исправљају се већ се толеришу као неизбежна;

ж) информације о успеху или неуспеху се не износе отворено и добровољно, о њима се не расправља и на њима се не ради, на пример, када постоји култура бацања кривице.

Студија коју су спровели Фернандез-Муњис и група аутора (Fernández-Muñiz, B., Montes-Peón, J., M., Vázquez-Ordás, C., J. Safety management system: Development and validation of a multidimensional scale, *Journal of Loss Prevention in the Process Industries*, Volume 20, Issue 1, January 2007, Pages 52-68) током 2006. године, се фокусира на идентификацију основних елемената који дозвољавају да безбедносни менаџмент буде ефективан и на развијање скале да би се мериле разлике у филозофијама и поступцима безбедности које доводе до смањења ванредних

догађаја, предлажући инструмент за процену безбедносног менаџмента у организацијама. Предложени модел треба да буде интегративни оквир који служи за развијање превентивних акција, тако да се може применити на различите типове организација. Циљ је да се обезбеде упутства на основу којих се може предузети превентивна акција са циљем да се умање незгоде и људски и економски губици.²⁵⁵ Управљање ризицима на интегрисан начин са операцијама у организацији има велики значај. Треба напоменути да је од круцијалне важности одређивање стратегије за управљање ризиком, јер се преко ње може „утицати на узроке и фреквенцију појаве кризе“²⁵⁶. Врло је мало покушаја да се утврди начин на који се могу мерити имплементиране политике и поступци у систем безбедносног менаџмента организације. На основу истраживања, Фернандез-Муњис и група аутора²⁵⁷ су одредили скалу за оцену система безбедносног менаџмента, састављену од 29 питања, који су структурисани у осам фактора: политика, подстицај, обука, комуникација, превентивно планирање, планирање за ванредне ситуације, унутрашња контрола и *Benchmarking* технике.

4.1. Перформансе система безбедносног менаџмента

Рад у сложеном окружењу захтева велика средства и може утицати на профитабилност организације. Заштита финансијског стања и стабилности организације је једно од главних питања којима се бави менаџмент. Све то доводи до великих изазова за многе активности у оквиру организације, а нарочито за безбедносни менаџмент. Трошкови²⁵⁸ директно утичу на пословање организације, па стога им се посвећује и велика пажња. Одговорни финансијски менаџери покушавају да „смање сваки трошак и да направе директну везу између улагања и добитка“²⁵⁹. Безбедносни менаџмент не представља изузетак. Улагања за безбедност могу

²⁵⁵ Видети: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

²⁵⁶ Aba-Bulgu, M., Islam, S. M. N., Corporate Crisis and Risk Management: Modelling, Strategies and SME Application, Elsevier, Amsterdam, 2007., стр. 40.

²⁵⁷ Више о томе: Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., исто.

²⁵⁸ „Трошак представља коришћење капитала са циљем да се оствари повраћај који би оправдао то улагање.“ - Klein, P. J., *Getting Started in Security Analysis*, 2nd ed., John Wiley & Sons, Inc., Hoboken, 2010.

²⁵⁹ Tiller, J. S., исто.

утицати на профитабилност организације. Зато се често дешава да организације безбедност посматрају као нешто што у крајњој линији не доноси корист. Ипак, да би услуга била квалитетна, мора се улагати у подизање њеног квалитета.²⁶⁰ С обзиром на динамичност промена у савременом окружењу, јасно је да свака организација која жели да опстане мора дугорочно размишљати о томе на који начин улаже финансијска средства. Да би могла да прати ефикасност инвестиција, организација уводи процесе управљања перформансама²⁶¹ и контроле пословања, а за то морају постојати „јасно дефинисани индикатори“²⁶².

Перформансе се углавном прате преко шест основних мерила: ефикасности, ефикасности, квалитета, правовремености, продуктивности и безбедности. Међутим, „свака организација ове мере обликује према сопственим потребама“²⁶³. Зато смо се у мерењу перформанси система безбедносног менаџмента, одлучили за ефикасност и ефикасност као основне показатеље успешног рада овог система. Највећи проблем у том погледу представља недостатак прихваћеног скупа мерљивих индикатора који би указали на повраћај инвестиције²⁶⁴. Мало је тога што организација може учинити у овој области. Често се раде мерења у контексту избегавања инцидената или утицаја уоченог ризика (на пример, утицај би коштао мање од контроле, па стога обезбеђује позитивну стопу повраћаја²⁶⁵). Даље, поставља се питање које инвестиције у безбедност треба мерити: техничке контроле, софтвер за надгледање, обезбеђење или

²⁶⁰ Основни трошкови квалитета се могу сврстати као трошкови: превенције, процене и трошкови лошег квалитета. - Neely, A., *Measuring Performance: the operations management perspective*, *Business Performance Measurement: Unifying Theories and Integrating Practice*, 2nd ed., Cambridge University Press, New York, 2007., 64-81.

²⁶¹ „Процес „утврђивања перформанси“ (*performance attribution*) се односи на одређивање појединих фактора који су утицали на повећање повраћаја на инвестиције.“ - Christophers, J. A., Carino, D. R., Ferson, W. E., *Portfolio Performance Measurement and Benchmarking*, McGraw Hill Companies Inc., New York, 2009., стр. 5.

²⁶² Scheer, A.-W., Jost, W., *From Process Documentation to Corporate Performance Measurement*, *Corporate Performance Management: ARIS in Practice*, Springer-Verlag, Heidelberg, 2006., 1-6.

²⁶³ TRADE, *How to measure performance, A Handbook of Techniques and Tools*, US Dep. of Energy, 1995., 1-5.

²⁶⁴ „Повраћај инвестиције (Return On Investment - ROI) представља једну од најчешће коришћених мера за мерење перформанси организације.“ - Friedlob, G. T., et al., *Essentials of Corporate Performance Measurement*, John Wiley & Sons, Inc., New York, 2002., стр. 4.

²⁶⁵ Стопа повраћаја представља корист коју добијамо када улажемо у неке ресурсе, а изражава се у процентима. Повраћај представља однос величине добитка/губитка према количини средстава која су уложена. Видети: Feibel, B. J., *Investment Performance Measurement*, John Wiley & Sons, Inc., Hoboken, 2003.

менацере. Ова дилема још увек није решена, тако да „организације и даље безбедност сврставају у један од трошкова“²⁶⁶. Опција да се безбедност посматра као инвестиција може довести до повећања њене вредности и може се сврстати у неопипљиву имовину организације (у рачуноводству се неке способности организације, као што су репутација, пружање услуга купцима, способност да се прилагоди ризичном окружењу и сл., једним именом „*goodwill*“, сматрају вредностима које организације поседује).

Ако се безбедност буде посматрала на овај начин, може се десити да управо вредност организације зависи од њене способности да заштити кључну имовину и процесе и повећа своју еластичност. Истина, организација која може заштити своју имовину и процесе у случајевима када дође до ванредних догађаја (и да управо побољша способност прилагођавања будућим догађајима) може имати већу вредност од оне која то не може, ако ни због чега, а оно због предности у пословању коју ствара. „Док организације не промене свој начин посматрања безбедности као терета, способност безбедносног менаџмента да ефикасно и ефективно обавља посао на организационом нивоу ће бити угрожена“.²⁶⁷

Перформансе организације указују на успешност њеног пословања, па се из тог разлога и врши њихово мерење. „Мерење перформанси“²⁶⁸ дословно значи „процес квантификовања прошлих активности“²⁶⁹. Или, „скуп мерила која се користе за квантификовање ефикасности и ефективности активности“²⁷⁰. Организације достижу постављене циљеве тиме што задовољавају интересе свих укључених страна

²⁶⁶ Jacquith, A., исто.

²⁶⁷ Caralli, R. A., Wilson, W. R., исто.

²⁶⁸ Поред термина „мерење перформанси“ користи се и термин „управљање перформансама“. Процес управљања перформансама је шири и у његовој основи је мерење перформанси. О томе више: Sole, F., Schiuma, G., *How to Use Different Measures for Different Management Model for Public Organizations, Business Performance Measurement and Management: New Contexts, Themes and Challenges*, Springer-Verlag, Heidelberg, 2010., pp. 103-113.

²⁶⁹ Neely, A., Adams, C., Kennerley, M., *The Performance Prism: The Scorecard for Measuring and Managing Business Success*, Pearson Education Limited, London, 2002., стр. 12.

²⁷⁰ Neely, A., Gregory, M., Platts, K., *Performance measurement system design: a literature review and research agenda, Int J Oper Prod Manag 15 (4), 1995, pp. 80–116.*

и сопствене потребе ефективније и ефикасније од конкурената. Па се термини „ефективност“ и „ефикасност“ заправо и користе у овом контексту.²⁷¹

Ефективност је принцип или захтев који полази од унапред дефинисаних и утврђених циљева предузећа и расположивости неопходних компонената фактора, односно ресурса за њихово остваривање. Циљ ефективности је да се коришћењем расположивих ресурса, односно компонената остваре максимално могући резултати у складу са постављеним планским циљевима. Ефективност је оријентисана на избор потреба које ће предузеће задовољити у процесу пословања и обављања своје делатности. Најкраће речено, „ефективност предузећа означава степен успешности у остваривању његових циљева“²⁷².

Ефикасност је принцип или захтев за реализацијом постављених циљева предузећа уз најмање коришћење и трошење расположивих ресурса и компонената предузећа. Ефикасност изражава рационалност употребе расположивих компонената и изражава се односом остварених резултата према учињеним улагањима. У основи принципа ефикасности је успешност трансформације материјалних и људских компонената улагања у резултате пословања. Та трансформација се обавља у процесу рада и пословања. „Овај принцип се најопштије изражава односом резултата пословања предузећа (*output*) и улагања (*input*) учињених да се ти резултати остваре. Уколико се са мањим обимом улагања остваре пројектовани и жељени резултати, односно ако се са расположивим обимом улагања расположивих фактора предузећа остварују већи резултати, утолико је ефикасност предузећа већа и обратно.“²⁷³

Стандарди перформансе треба да се успоставе тако да се перформансе мере у односу на њих. „Мерење перформансе“, које укључује низ провера и надзорних активности, се односи на прикупљање информација о имплементацији и ефективности организационих планова и стандарда. Организације треба да процењују своје перформансе у односу на унапред одређене планове и стандарде. Ово може да им олакша увођење, функционисање и одржавање система који

²⁷¹ Више о томе у: Caralli, R. A., Wilson, W. R., исто.

²⁷² Исто.

²⁷³ Живковић, М., исто, стр. 229.

омогућавају да се њихове перформансе процене на објективан начин. Процес мерења перформанси укључује системе „активног“ надзора да би се проценио успех планова, а неуспех контролних активности се процењује преко „реактивног“ система надзора, који захтева системе истраге, извештавања и систем за одговор. „Процена“ укључује прикупљање независних информација о ефикасности, ефективности и поузданости целокупног система безбедносног менаџмента организације и развијање планова за корективну акцију. „Ревизија“ подразумева активности које организација може да користи да би донела суд о својим перформансама, донела одлуке о побољшању перформанси, као и да даље развија политике које се односе на безбедност и здравље. Неопходно је да се ревизије обављају редовно на основу података који се добијају из надзорних активности и активности процене. Наглашено је да је „ова функција основа саморегулације и посвећености непрестаном побољшању, што укључује политике развоја, приступе имплементацији и технике контроле ризика“²⁷⁴.

4.1.1. Приступи мерењу ефективности и ефикасности пословања

У теорији и пракси постоје разни приступи дефинисању, обради и мерењу ефективности и ефикасности пословања предузећа и других привредних субјеката. Класични или традиционални приступ ефективности и ефикасности карактерише парцијално мерење резултата пословања, односно пословног успеха предузећа. Полази се од тога да сваки циклус репродукције и делатности предузећа захтева одређена материјална улагања и људске ресурсе, технолошки условљен процес рада и делатности и на крају резултате. Овај приступ полази од циљева које је предузеће поставило и тежи да их у оквиру процеса своје репродукције оствари. Стога се суштина и садржина класичног приступа у предузећу своди на утврђивање и мерење степена успешности у остваривању задатих и постављених циљева. „Класичним приступом се такође мери и способност предузећа да прибави потребне ресурсе за своје пословање.“²⁷⁵

²⁷⁴ Santos-Reyes, J., Beard, N. A., исто.

²⁷⁵ Живковић, М., исто.

Ефективност и ефикасност, поред осталог, мере се и способношћу организације да прибави потребне и недостајуће ресурсе из окружења, односно потребне факторе пословања. Као критеријум ефикасности и ефективности узимају се и интерни пословни процеси и биланси стања и успеха у предузећу. Овај приступ се заснива на људским и другим ресурсима којима предузеће располаже. Фактори ове врсте ефикасности су корпоративна култура предузећа, међуљудски односи, мотивација, као и квантитативно изражени резултати пословања. Мерење ефикасности и ефективности класичним приступом заснива се на циљевима и резултатима пословања и њиховом односу. Када су јасно и прецизно утврђени и пројектовани циљеви, када их је могуће мерити и динамички пратити - овај метод се једноставно примењује у пракси пословања предузећа. Пошто се предузеће оснива ради остваривања одређених економских и других циљева, то су и сви поступци, активности и делатност предузећа и свих носилаца функција у процесу његовог пословања, циљно усмерени и оријентисани. Поступак изражавања и мерења ефикасности и ефективности претпоставља идентификовање и квантификовање циљева у облику планова, програма, одлука и сл., како би се на основу степена њиховог остваривања мерила успешност пословања предузећа. Циљеви се могу односити на разне аспекте и области пословања предузећа, факторе производње, тржиште, прибављање финансијских средстава, расподелу, запослене кадрове и др. У изражавању и мерењу ефикасности и ефективности, мора бити јасно постављен и одабран систем мерљивих и упоредивих циљева. На основу тако постављених и остварених резултата ће се изражавати и пратити како ефикасност тако и ефективност предузећа. Остваривање једног циља или групе циљева не мора аутоматски значити остваривање и осталих постављених циљева предузећа. Ако су циљеви квантификовани, односно мерљиви, тада је могуће утврдити критеријуме и стандарде за мерење и праћење ефективности пословања. Принцип ефикасности пословања је тешко квантитативно глобално исказати. У пракси се као најзначајнији парцијални показатељи и мерила ефикасности предузећа користе: продуктивност, економичност и рентабилност (профитабилност). „Циљ пословања сваког предузећа је усмеравање рада, начина пословања, понашања запослених и укупне активности у

правцу остваривања максимално могућих резултата ради подмирења потреба окружења, предузећа и запослених.²⁷⁶

Степен и квалитет ефикасности и ефективности може се мерити различитим показатељима у зависности од врсте предузећа, услова пословања, технологије и деловања окружења. Међу релевантним мерилима, са становишта предузећа, нарочито су наглашени:

- степен искоришћености сировина, енергије, репроматеријала, опреме, капацитета, радног времена запослених и др;
- брзина протока или обрта материјала, полупроизвода, готових производа, новчаних средстава и др., сходно постављеним процесима рада и пословања и
- величина и квалитет остварених резултата пословања и њихов однос према обиму и квалитету компонената улагања.

Када се говори о мерилима и утицајним факторима успеха, односно успешним и ефикасним предузећима, поред обима оствареног профита као израза финансијског резултата пословања треба нагласити три битна фактора:

- позиција на тржишту, која подразумева бригу о купцима, односно клијентима;
- организациону културу и климу, приврженост и оданост запослених предузећу;
- ефикасност одлучивања, односно менаџмента и руковођења.

У теорији и пракси разни аутори користе бројна мерила, односно елементе ефикасног пословања предузећа. Међу тим мерилима ефикасности су најзначајнији:

- људи (запослени), који у процесу рада квалитетно обављају послове и задатке;
- раст предузећа, који у временској динамици треба да буде видљив и постојан;
- предвиђање тржишних услова и захтева и задовољавање потреба купаца;
- планирање промена и управљање променама;
- задовољство запослених.

Мерила ефикасности пословања предузећа могу бити квалитативно и квантитативно изражена. Њиховим упоређивањем и праћењем у односу на временско раздобље и у односу на конкурентска и слична предузећа, може се сагледати глобална оцена ефикасности пословања.

²⁷⁶ Исто, стр. 230.

Треба напоменути да предузеће као економска организација стално тежи повећању сопствене ефикасности и ефективности. При томе је ефикасност пословања већа и повољнија:

- ако се при истим резултатима смањује обим улагања,
- ако се са истим улагањима повећају резултати,
- ако се резултати и улагања повећавају тако да стопа пораста резултата расте брже од стопе пораста улагања и
- ако се и резултати и улагања смањују, према одређеним правилима и условима, али се при томе улагања смањују брже од смањења резултата.

Повећање или смањење ефикасности је резултат бројних фактора, услова и околности пословања предузећа. Релевантни фактори повећања и смањења ефикасности су тржиште и тржишни услови, технолошки параметри пословања, позитивно или негативно деловање мера државе, као и учинак запослене радне снаге, односно људског фактора.

Савремени приступ ефективности и ефикасности заснива се на комплексном обухватању и проучавању бројних активности, одлука и ресурса предузећа. Савремени приступ ефективности и ефикасности комбинује већи број показатеља успешности пословања у једну компаративну целину. Полази се од тога да савремено предузеће реализује већи број циљева и при томе обавља бројне активности. Овај приступ уважава и факторе окружења и интерне факторе и напушта парцијално мерење ефикасности и ефективности. Различити субјекти предузећа као што су: власници, запослени, потрошачи, кредитори, добављачи, влада и др., имају различите критеријуме и показатеље ефикасности и ефективности. За власнике је то превасходно профит, за запослене висина зараде и радни услови, за потрошаче квалитет производа и услуга, за владу поштовање прописа и закона, плаћање пореза и сл. Различите релативне вредности ових показатеља отварају проблем њиховог релативног значаја у укупној оцени ефикасности и ефективности предузећа. Савремени приступ користи више критеријума ефикасности и ефективности, узимајући у обзир све фазе процеса пословања и све дејствујуће утицајне факторе и чиниоце. При томе не постоје универзални критеријуми ефикасности и ефективности

који се могу применити у сваком предузећу. Међу утицајним факторима посебан значај имају утицај менаџера и руководиоца, мерљивост циљева предузећа и услови окружења. „Обједињавањем ефективности и ефикасности у јединствени израз укупне економске ефикасности предузећа је у функцији мерења укупних ефеката и успешности његовог пословања. Кроз сагледавање укупног, збирног ефекта омогућава се и ефикасније управљање економијом и пословањем предузећа.“²⁷⁷

4.1.2. Фактори који утичу на мерење ефективности и ефикасности

Фактори који утичу на организациону ефективност и ефикасност су²⁷⁸: 1) величина и сложеност организације, 2) сврха организовања, 3) технолошки тип производње, 4) рутине у процесима, 5) степен бирократизације, 6) фаза у животном циклусу предузећа, 7) стратегије наступа на тржишту, 8) конкурентност окружења и могућност предвиђања његовог понашања и сл.

Ефикасност и ефективност различитих организација је могуће упоређивати по следећим критеријумима²⁷⁹:

- 1) тренутни и прошли ниво ефективности и ефикасности (временско упоређивање);
- 2) ефективност и ефикасност различитих целина исте организације;
- 3) ефективност и ефикасност једне организације са ефективношћу и ефикасношћу друге из исте индустријске гране;
- 4) тренутно стање ефективности и ефикасности у односу на минимални стандард и сл.

Сваки модел мерења ефикасности и ефективности представља одређен скуп вредности и има свој антипод супротних вредности. Операционализација поступка захтева да се одреде чиниоци пословања који су критични за опстанак организације, израчунају оцене важности коју сваки чинилац пословања додељује сваком од

²⁷⁷ Исто, стр. 231.-233.

²⁷⁸ Видети: Durbin, T., Measuring Safety: Challenging and Besting Traditional Methods at PPG, *Safety management*, Aug2000, Issue 449, pp. 1-2.

²⁷⁹ Исто.

скупова вредности, представљање кумулативних резултата будући да оцењивање врши појединац у оквиру групе, могућност упоређивања два или више предузећа на истом дијаграму. Резултати показују области у којима се главни чиниоци пословања слажу, тј. не слажу, види се које критеријуме треба побољшати, фокус руководиоца према одређеном моделу. „Критеријуме треба одабрати у односу на то ко су главни клијенти, односно шта је жељено стање организације и који критеријуми одржавају достизање тог стања, затим у односу на друга стања или услове који промовишу опште циљеве или су прикладни као критеријуми ефективности.“²⁸⁰ „Ради утврђивања ефективности система, потребно је одредити релативну вредност у следећим областима: интегритет, поузданост, реакција на случајне грешке и реакција на системске грешке“²⁸¹. Осим тога, потребно је одредити како се прихватају „додатни приоритети“²⁸².

Иако се модели за мерење перформанси непрестано развијају²⁸³, пет главних елемената остају „кључни за успех организације:

1. активно руковођење на свим нивоима менаџмента,
2. партиципација запослених у организационој клими која охрабрује отворену дискусију о безбедносним праксама и идејама за њихово побољшање,
3. ефективна обука свих запослених о опасностима и ризицима и начинима за њихово избегавање,
4. просторни планови који у себе укључују безбедносне стандарде,
5. стратегије за процену понашања запослених са аспекта безбедности.“²⁸⁴

Ових пет основних елемената олакшавају прикупљање података. Двосмерна комуникација је кључ успеха, и то како са запосленима на производним радним местима, тако и са супервизорима. Такође, јако је битно да се нагласи значај

²⁸⁰ Durbin, T., исто.

²⁸¹ Hampton, P., Survey of Safety Architectural Patterns, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 139.

²⁸² Durbin, T., исто.

²⁸³ Видети: Manzoni, A., Islam, S. M. N., *Performance Measurement in Corporate Governance*, Physica-Verlag, Heidelberg, 2009.

²⁸⁴ Durbin, T., исто.

безбедности у читавој организацији, што се може учинити путем разних летака, штампаног материјала од стране највишег руководства или, ако је изводљиво, путем интерне телевизијске мреже.

Да би се могле мерити перформансе система безбедносног менаџмента, потребно је одредити критеријуме, односно мерила на основу којих морамо прикупљати податке. Неки од тих критеријума су: 1. активно руковођење, 2. стандарди хигијене (колико је дозвољено да запослени буду изложени штетним супстанцама) који морају задовољавати OSHA стандарде, 3. ергономска решења (тим стручњака који прати постојеће радне активности и усвојене праксе), 4. мерење понашања, 5. анкетање запослених о њиховим ставовима, 6. осигурање запослених (трошкови по запосленом), 7. укупна стопа повреда на раду, 8. укупни временски губици који настају због повреда. Да би ова мерила била приступачнија, могу се графички представити са осам графикана који показују текуће и претходно стање ових критеријума.²⁸⁵ Тако менаџмент има увид у дате податке и може да одреди чему треба посветити више пажње.

4.1.3. Ефективност као перформанса безбедносног менаџмента

Дефинисање организационе ефективности захтева примену више критеријума, при чему „различите организационе функције се оцењују коришћењем различитих карактеристика, а потребно је да се анализирају и процеси и резултати“²⁸⁶. Процес који је од значаја у процени ефективности је процес организационог развоја који се односи на развој интерних капацитета организације и омогућава реализацију мисије и опстанак организације у дугорочном периоду. Према дефиницији коју је дао Бекхард²⁸⁷ организациони развој је планирани напор који обухвата сваки сегмент организације, а који има за циљ да повећа организациону ефективност и „здравље“

²⁸⁵ Детаљније о овоме: Durbin, T., *Measuring Safety: Challenging and Besting Traditional Methods at PPG, Safety management, Aug2000, Issue 449, pp. 1-2.*

²⁸⁶ Tiller, J. S., исто.

²⁸⁷ Видети: Beckhard R., *Organization development strategies and models*, Addison-Wesley, Boston, 1969., стр. 9.

организације, путем планираних интервенција у организационим процесима, користећи знање о понашању људи.

Као што је напоменуто, ефективност означава степен до којег организације остварују своје циљеве. Ефективност је пре свега усмерена на „што боље остварење постојећих потенцијала у једној организацији“²⁸⁸. Дакле, да би се ефективност постигла, потребно је деловати у складу са постизањем циљева. То значи да је, да би се утврдила ефективност безбедносног менаџмента, потребно да циљеви безбедносног менаџмента буду што јасније и прецизније одређени. „Циљеви могу бити одређени као норме или као одређени радни задаци. Колико је значајно добро формулисати и поставити циљ, исто толико је битно тај циљ саопштити и пренети запосленом на разумљив начин.“²⁸⁹ Поред тога, циљеви безбедносног треба да буду специфични, мерљиви, достижни, релевантни и правовремени, а да се при том постигне посвећеност запослених за остваривање циљева.

Ако се за циљеве постављају одређени стандарди, јасно је зашто се у свим стандардима пре свега пажња поклања обуци запослених да би они на што бољи начин постигли постављене циљеве. Ни безбедносни менаџмент није изузетак. Специфичност безбедносног менаџмента је у томе што он покрива све аспекте организације, тако да су, у крајњој линији, сви запослени потенцијалне жртве, али и потенцијални изазов за безбедност. Тиме се спектар послова, а самим тим и циљева, безбедносног менаџмента у великој мери усложњава. Због тога је битно да се у читавој организацији, а у оквиру развоја организационе културе, развија и позитивна безбедносна култура.

4.1.4. Ефикасност као перформанса безбедносног менаџмента

Као што је речено, ефикасност организације изражава делотворност организације у обављању основних процеса. Она се изражава односом резултата функционисања организације и улагања која су неопходна да се ти резултати остваре. Односно, ефикасност подразумева постизање резултата уз што мање трошкова.

²⁸⁸ Стевановић, З., Лојић, Р., Управљање радном ефективношћу запослених, *Војно дело, Јесен/2011*, стр. 380-396.

²⁸⁹ Исто.

Када је реч о ефикасности система безбедносног менаџмента, она се огледа у што мањој штети насталој у организацији приликом њеног функционисања. Да би се утврдио утицај безбедносног менаџмента у овој области, потребно је пратити све могуће застоје у раду организације, квалитативно и квантитативно одредити њихове узроке и последице и проценити у којој мери су они могли бити под утицајем безбедносног менаџмента.

Проблем ефикасности безбедносног менаџмента се заправо своди на то да ли су улагања у систем безбедности заправо оправдана. Уколико је штета настала у организацији већа од неке прихватљиве вредности, онда је то поуздан знак да систем безбедносног менаџмента не оправдава улагања у њега.

Одређивање ефикасности безбедносног менаџмента је ипак много комплекснији проблем него што изгледа на први поглед. Прво, поставља се питање утврђивања износа улагања у безбедносни менаџмент. Ту обично спадају надокнаде за рад запослених, улагања у опрему, одржавање опреме и сл. Затим, потребно је одредити узроке због којих је дошло до догађаја који је изазвао или могао изазвати штету организацији. Без познавања узрока, тешко да можемо утврдити одговорност за такве догађаје, а самим тим и могућност система безбедности да правовремено реагује и догађај спречи.

Треба напоменути и опцију када није било штете у организацији. То представља ситуацију у којој нисмо сигурни да ли је то што штете није било последица рада безбедносног менаџмента или последица случајности.

Наравно, све ово подразумева да је систем безбедносног менаџмента потпуно уведен, организован и да функционише без већих проблема.

4.2. Модели за процену перформанси система безбедносног менаџмента

Организација мора да на мерење перформанси гледа као на континуиран процес који је састављен од низа кључних активности. Прво, потребно је осмислити јасан пословни модел који ће омогућити свим запосленим да увиде шта је то што повећава вредност пословања. Затим је потребно да се тај модел интегрише у организационе процесе, чиме се омогућава прављење извештаја и остварење

безбедносних циљева. На крају је потребно јасно повезати предности које се добијају побољшањем перформанси са системом награђивања.²⁹⁰

За развијање модела за процену перформанси система безбедносног менаџмента може да послужи „приступ Модела вредности мултиатрибута са три нивоа (*multi-attribute value model* - МАВТ)“²⁹¹. Тај модел су предложили Тео и Линг 2006. године.²⁹² Користећи овај модел, може да се одреди Безбедносни индекс (БИ) постројења на основу независне процене ревизора.

Прво је потребно развити модел за бодовање, у којем се сваком атрибуту приписује тежински фактор који одређује његов значај. „Тежински фактор се множи проценом ранга, а онда се за свако производно одељење ови производи сабирају.“²⁹³ Инпути у моделу су атрибути које треба проценити и њима доделити тежинске факторе у складу са значајношћу сваког атрибута. „Атрибути се затим деле у три нивоа.“²⁹⁴ Први ниво представља атрибуте који су главне компоненте или фактори који су од есенцијалног значаја за систем безбедносног менаџмента у општем случају. „За одабир ових атрибута, може се користити принцип циклуса: Планирање, Спровођење, Контрола, Акција (*Plan, Do, Control, Act* - PDCA).“²⁹⁵ Ови фактори су есенцијални елементи у многим системима безбедносног менаџмента који укључују стандарде OHSAS 18001 и ILO-OSH-2001²⁹⁶, тако да је модел могуће применити на постројења која су успоставила системе у складу са тим стандардима.

Планирање у овом моделу се односи на политику и планове, а на другом нивоу ту спадају атрибути као: посвећеност менаџера на високом нивоу, организација и одговорности, закони и регулативе, процена ризика. Спровођење се

²⁹⁰ Видети: Fahy, M., Roche, J., Weiner, A., *Beyond Governance: Creating Corporate Value through Performance, Conformance and Responsibility*, John Wiley & Sons Ltd., Chichester, 2005., стр. 26, 27.

²⁹¹ Chang, J. I., Liang, C.-L., Performance evaluation of process safety management systems of paint manufacturing facilities, *Journal of Loss Prevention in the Process Industries*, Volume 22, Issue 4, July 2009, Pages 398–402.

²⁹² Видети: Тео, А. Л. Е., Ling, Y. Y. F., Developing a model to measure the effectiveness of safety management systems of construction sites, *Building and Environment*, Volume 41, Issue 11, November 2006, Pages 1584–1592.

²⁹³ Исто.

²⁹⁴ Chang, J. I., Liang, C.-L., исто.

²⁹⁵ Исто.

²⁹⁶ Препорука за менаџмент система заштите безбедности и здравља на раду Међународне Организације Рада (International Labour Organisation).

односи на имплементацију и функционисање планова. У оквиру овог атрибута се могу развити атрибути другог нивоа, попут: образовање и обука, одговор на ванредне ситуације, само-надзор, дозвола за рад, управљање опремом за безбедност, управљање опасним материјама, заштита на раду, комуницирање. Контрола се односи на проверу и корективне мере, а ту спадају атрибути другог нивоа: мониторинг радног окружења, здравствени прегледи, истраге акцидената, ревизија безбедности. Акција се односи на менаџмент ревизију. „Атрибути другог нивоа су: ревизија планова, извршења и саме контроле.“²⁹⁷

Сваки од атрибута другог нивоа се дели у неколико мерљивих подкатегија који су заправо мерљиви атрибути трећег нивоа. Коначна листа се састоји од листе атрибута који сачињавају листу Безбедносних Индекса. Да би им се доделили тежински фактори могу се користити Аналитички Хијерархијски Процес (АХП) и факторска анализа. Када се доделе тежински фактори, прави се упитник који треба да попуне стручњаци из области безбедности. Коришћењем различитих техника или рачунарског програма, могуће је анализирати одговоре да би се добили тежински фактори и мера конзистенције. Како препоручује Сати²⁹⁸ вредност од 0.1 за мере конзистенције као што је Индекс Конзистенције или Рацио Конзистенције. Када је вредност овог индекса мања или једнака 0.1, сматра се да је постигнута сагласност у погледу судова. Када су једном добијени тежински коефицијенти атрибута, може се развити средство за процену перформанси. Ово средство треба да садржи атрибуте поређане на основу тежинских коефицијената. Пример за рангирање атрибута трећег нивоа може бити: 0/1 (0 или 1), 0-1 (интервал између 0 и 1), 0/1/НП (0, 1 или није применљиво) или 0-1/НП (интервал између 0 и 1 или није применљиво).

Када се рангирају атрибути трећег нивоа, њихов допринос укупном резултату се рачуна коришћењем следеће једначине (1):

$$B_i(\text{безб. резултат}) = T_i(\text{тежински коефицијент}) \times R_i(\text{ранг}) \quad (1),$$

где су:

- B_i безб. резултат за i -ти атрибут,

²⁹⁷ Chang, J. I., Liang, C.-L., исто.

²⁹⁸ Видети: Saaty, T. L., *Fundamentals of decision making and priority theory with the AHP*, Raws Publications, Pittsburgh, 1994.

- T_i фактор значајности за i -ти атрибут, а
- R_i процена i -тог атрибута од стране ревизора за одређено постројење или организацију.

Укупан безбедносни резултат (BI) организације се рачуна сабирањем производа тежинског коефицијента и ранга за све атрибуте, по једначини (2):

$$BI = \sum T_i R_i \quad (2).$$

Ограничење овог модела је то што су тежински коефицијенти и атрибути под јаким утицајем локалне безбедносне културе и праксе. Па је за примену овог модела у различитим земљама, потребно радити додатна истраживања. Друго ограничење је то што не постоје објективни критеријуми за ревизоре за рангирање атрибута трећег нивоа. Када не постоји скуп критеријума или стандарда за процену перформансе, ревизор мора да се ослони на сопствено искуство. Овај модел је могуће прилагодити организацијама у различитим областима индустрије, што је његова предност. Међутим, преко њега није могуће мерити ефективност мера система безбедносног менаџмента. Тако да се у нашем случају овај модел не може користити.

Истраживачи су годинама покушавали да утврде „квантитативне и квалитативне индикаторе за процену ефективности безбедносног процеса“²⁹⁹. Како тврде Кардер и Раган³⁰⁰ добра безбедносна култура и клима могу да утичу на ниску стопу повреда са веома високим нивоом статистичке значајности, али њихово истраживање није довољно да се процени ефективност система безбедносног менаџмента јер је постојао мали проценат акцидентата са малом вероватноћом дешавања а великим последицама. Према статистичкој анализи података о овим акцидентима³⁰¹ на основу информација добијених из Програма за управљање

²⁹⁹ Luo, H., The effectiveness of U.S. OSHA process safety management inspection – A preliminary quantitative evaluation, *Journal of Loss Prevention in the Process Industries*, Volume 23, Issue 3, May 2010, Pages 455–461.

³⁰⁰ Видети: Carder, B., Ragan, P., A survey-based system for safety measurement and improvement, *Journal of Safety Research*, 34 (2003), pp. 157–165.

³⁰¹ Акциденти са малом вероватноћом дешавања, а великим последицама се означавају ознаком LP-HC (*Low Probability – High Consequences*), а представљају догађаје који се ретко дешавају, али када се десе њихов утицај је екстреман. Будући да о оваквим акцидентима постоји врло мало података и веома мало искуства, за појединачну организацију је јако тешко да ублажи ризике који су везани за њих. Јан Тредголд предлаже да се ови догађаји третирају на нивоу целе индустрије, а не у оквиру појединачног предузећа. Више о томе: Threadgold, I. M., Reducing the Risk of Low-Probability High-Consequence

ризиком из периода од 1996. до 2000. године, „није пронађена значајна веза између стопе повреда на раду и катастрофалних губитака који су настали због акцидента у производњи“³⁰². Како су предвидели Тули и Апостолакис³⁰³, укључивање организационих фактора у традиционалне анализе узрока акцидента би довело до побољшања способности за превенцију акцидента уколико би се резултати анализе узрока применили на прави начин. Блер³⁰⁴ је спровео једноставно истраживање у току 2004. године у којем је укључио податке о истрази 21 хемијског акцидента. Анализирао је рангирање категорија у оквиру недостатака и неуспеха у систему управљања - што се показало као најчешћи директан или посредан узрок акцидента или инцидента. Пет главних категорија су „процедуре одржавања“, „анализа опасности“, „инжењерски нацрти и ревизије“, „управљање променама“ и „оперативне процедуре“, које су у складу са прописима везаним за Управљање безбедношћу и здрављем на раду. Ова студија је показала да без обзира на величину постројења и сложеност процеса, побољшање система управљања представља основ за превенцију акцидента.³⁰⁵

На основу претходних истраживања, Луо³⁰⁶ је обавио истраживање са циљем да се процени ефективност инспекцијског надзора система безбедносног менаџмента тако што се испитује статистичка корелација између података добијених из надзора и налаза истраге акцидента. Претпоставка је да ефективан инспекцијски надзор стандарда заштите и безбедности на раду треба да открије главне узроке акцидента. Луово истраживање је спроведено са аспекта перформанси, а подаци су коришћени из информационих система везаних за систем безбедности и заштите на раду и података које су обезбедиле државне агенције у вези истраге акцидента. Луо је

Events, *Society of Petroleum Engineers Americas E&P Health, Safety, Security and Environmental Conference*, Houston, Texas, USA, 21–23 March 2011.

³⁰² Elliott, M., Kleindorfer, P., Dubois, J., Wang, Y., Rosenthal, I., Linking OII and RMP info data: does everyday safety prevent catastrophic loss?, *International Journal of Risk Assessment and Management*, 10 (1/2) (2008), pp. 130–146.

³⁰³ Видети: Tuli, R., Apostolakis, G., Incorporating organizational issues into root-cause analysis, *Trans IchemE*, 74 (B) (1996), pp. 3–15.

³⁰⁴ Видети: Blair, A., Management system failures identified in incidents investigated by the U.S. Chemical Safety and Hazard Investigation Board, *Process Safety Progress*, 23 (4) (2004), pp. 232–236.

³⁰⁵ Више о томе у: Луо, Н., исто.

³⁰⁶ Исто.

претпоставио да су ти подаци објективнији од података које прикупљају саме организације приликом евиденције повреда на раду и анализе ризика. Његова основна претпоставка је била да су се у инспекцијском надзору приликом прегледа Система за управљање безбедношћу и здрављем на раду могли видети проблеми који су касније повезани са настанком акцидентата. Статистичка значајност и јака корелација између података добијених на основу надзора и истрага акцидента требало је да потврди ову хипотезу.³⁰⁷

Према подацима о инспекцијском надзору система за управљање безбедношћу и здрављем на раду, највећи ранг су имали прекршаји који се односе на механички интегритет, оперативне процедуре и анализу опасности у процесу. Како је Луо закључио, слични подаци су добијени и на основу истрага акцидентата. Статистичка корелација је показала да су, у општем случају, инспекцијски надзори заиста указали на основне узроке који су касније довели до појаве акцидентата. Временом се ефективност ових надзора повећала. Међутим, индустријске организације имају слободу да уводе стандарде према сопственим потребама, што представља основни изазов за индустрије и инспекцијске органе. Адекватан број инспекцијских надзора, а нарочито програмираних инспекцијских надзора, треба да утиче на прихватање стандарда и прошири њихову примену на све индустријске процесе.³⁰⁸

Луово истраживање се односило на процену ефективности инспекцијског надзора стандарда везаног за безбедност индустријског процеса. Овакав приступ је заиста користан за проблем истраживања у овом раду. Иако је Луова студија ограничена на инспекцијски надзор, аналогија са нашим проблемом је прилично јасна. Односно, његов приступ може користити као основни принцип у процени ефективности безбедносног менаџмента.

³⁰⁷ Исто.

³⁰⁸ Исто.

4.3. Утврђивање индикатора за процену ефективности и ефикасности система безбедносног менаџмента

Индикатори за процену безбедносног менаџмента представљају моћно средство за евалуацију и могу да укажу на то где су слабе тачке у систему³⁰⁹, утичу на више руководство да стекне поверење у безбедносни менаџмент и олакшавају постављање безбедносних циљева. Јасно постављени циљеви позитивно утичу на запослене и омогућавају подршку свих нивоа менаџмента безбедносним циљевима. Индикатори за процену система безбедносног менаџмента омогућују успостављање равнотеже између посвећености политици безбедности на различитим нивоима у организацији, али и олакшавају утврђивање користи које организација има од система безбедносног менаџмента. „Многи процеси за процену активности безбедносног менаџмента могу да се имплементирају на основу постојећих контролних механизма, а резултати мерења индикатора се добијају у прилично кратком року.“³¹⁰

Само мерење се односи на утврђивање чињеница о систему који се мери и односа који постоји између мерења и менаџерских одговорности. „Сазнавање ових чињеница подразумева одговор на следећа питања:

1. ко је укључен у ту област, које су улоге, одговорности, циљеви и вредности, које доводе до потреба организације? На ова питања се одговара на основу процењених потреба за ресурсима, информацијама итд. у организацији;

2. који је циљни систем, имовина, услуга или функција која је подређена менаџменту? Које су то безбедносне особине које треба чувати и одржавати? Какво је развојно и оперативно окружење система? На ова питања се одговара развијањем модела циљног система. Ово је корисно јер постоје значајне разлике у појединим системима;

3. које су безбедносне активности од значаја? Како се манифестује активност безбедносног менаџмента? Како се потреба за овом активношћу повезује са осталим атрибутима интегрисаног система или услуге? На ова питања се одговара путем

³⁰⁹ Видети: Vellani, K. H., *Strategic Security Management*, Elsevier Inc., Burlington, 2007.

³¹⁰ Jacquith, A., исто.

модела концепта безбедности. Циљ је да се обезбеди веза између менаџера на свим нивоима и сектора безбедности. Овај модел омогућава да се потребе за ресурсима декомпонују до мерљивог нивоа методом „*top-down*“;

4. како се постиже жељена особина одређеним функцијама? Који послови и производи треба да буду укључени? На ова питања се одговара развијањем репрезентативног модела, који се заснива на најбољим решењима и стандардима у одређеној области;

5. коначно, развија се мерљиви модел одређеног ентитета. Идентификују се радни процеси и производи који су повезани са процесима менаџмента, а који имају мерљиве атрибуте. Овај модел обезбеђује основу за синтезу потенцијалних мерила методом „*bottom-up*“.³¹¹

Ових пет питања омогућавају да се развију смислени индикатори, односно мерила, која су корисна у безбедносном менаџменту. „Један од начина да се утврде индикатори ефективности примењених безбедносних мера јесте процена рањивости појединих ресурса.“³¹²

Утврђивање индикатора за процену ефективности и ефикасности система безбедносног менаџмента се може вршити у „неколико корака: - одређивање циљева који се постижу преко индикатора, - развијање индикатора, - одређивање начина за извештавање о индикаторима, - примена индикатора, - одређивање пожељног нивоа односно вредности за индикаторе и - формално одређивање временског циклуса у коме треба вршити ревизију индикатора, како би се обезбедило њихово прилагођавање тренутном стању у организацији“³¹³.

Индикатори треба да буду повезани са упутствима за мерење и начинима на који их треба прилагодити специфичним технологијама и организацијама.³¹⁴ Очигледне користи од примене ових принципа у области безбедности су: 1. успостављање заједничких принципа мерења у различитим гранама, технологијама и

³¹¹ Murdoch, J., Security Measurement, *White Paper 2 v2.0* 12-Jul-05, http://www.psmc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf

³¹² Wheeler, E., *Security Risk Management*, Elseiver Inc., Waltham, 2011.

³¹³ Nichols, E. A., Sudbury, A., Implementing Security Metrics Initiatives, *Information Systems Security*, November 2006., Pages 30-38.

³¹⁴ Видети: Jacquith, A., исто.

специфичним окружењима, 2. интеграција индикатора безбедности са другим мерним системима, 3. одређивање индикатора за обавештавање о питањима која се тичу менаџмента на разним нивоима, што доводи до премошћивања јаза између одговорности менаџера и техничких служби. Потребно је да индикатори буду што је могуће више једноставни, али довољно детаљни. Ови мерљиви концепти треба да се провере у пракси, за шта је потребно да се укључе специјалисти из различитих области.

Увођење индикатора за евалуацију безбедносног менаџмента се може вршити у пет фаза³¹⁵:

- идентификација, дефиниција и развој индикатора,
- сакупљање података о индикаторима и анализа података,
- идентификација активности за увођење побољшања,
- процена потребних ресурса,
- техничке, административне и оперативне активности.

Развијање мерљивих индикатора мора да узме у обзир техничке потребе пословног система, потребе за извештавањем, стратешке потребе и све друге захтеве који се постављају пред организацију. Оно што је значајно јесте да сваки од индикатора осветљава стање безбедности у одређеној области пословања. Индикатори за евалуацију безбедносног менаџмента могу да утичу на запослене да посвете већу пажњу питањима безбедности и да своје активности ускладе са безбедносном политиком.³¹⁶

На основу датог модела система безбедносног менаџмента, могу се одредити следећи индикатори преко којих се може пратити безбедносни менаџмент:

- у оквиру стратегије и политике: правила и прописи у области безбедности и њихова усклађеност са међународним стандардима;
- у оквиру имплементације: учесталост сервисирања и трошкови одржавања, иновација, информациона технологија и сл.;

³¹⁵ На основу фаза које је предложио Jacquith (видети: *The Security of Applications: Not All Are Created Equal*, 2002.).

³¹⁶ Видети: Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007.

- у оквиру људских фактора: број и структура запослених на пословима безбедности, број и садржина програма едукације и тренинга и сл.;
- у оквиру мониторинга и повратне везе: врста нежељеног догађаја, број криминалних радњи, „места где се чешће појављују нежељени догађаји“³¹⁷, узроци и број несрећа, број жртава, материјална штета, трошкови враћања у првобитно стање, укупан промет новца, информација, робе и сл.

Када се дефинишу индикатори за процену система безбедносног менаџмента, онда је могуће континуирано пратити њихове вредности и на основу добијених података вршити корекције у самом систему. Постоји више техника и препорука на основу којих је могуће стално вршити побољшања перформанси.³¹⁸

Користи које организација има од процене система безбедносног менаџмента могу се свести на следеће:

- више руководство добија јасна мерила ефикасности и ефикасности безбедносног менаџмента. При томе је потребно развити начин извештавања и приказивања индикатора безбедности и ризика. Мерљиви индикатори безбедности указују на то где су основне слабости у систему;
- индикатори су моћно средство које даје подршку одлучивању;
- омогућава се упоређивање безбедносног менаџмента једне организације са системима који се примењују у другим, сличним организацијама;
- откривају се слабости и пропусти у систему, па се тиме доприноси побољшању самог безбедносног менаџмента и смањењу ризика;
- омогућава се тачно утврђивање користи која се стиче улагањем у безбедносни менаџмент.

³¹⁷ Collier, P., *Measuring Police Performance, Business Performance Measurement: Unifying Theories and Integrating Practice*, 2nd ed., Cambridge University Press, New York, 2007., 363-382.

³¹⁸ О томе више: Paladino, B., *Five Key Principles of Corporate Performance Management*, John Wiley & Sons, Inc., Hoboken, 2007.

4.4. Балансирана листа мерила безбедности

Балансирана листа мерила је систем који се користи у стратешком планирању и менаџменту који се користи у пословним, индустријским, владиним и непрофитним организацијама широм света да би се активности ускладили са визијом и стратегијом организације, побољшања интерне и екстерне комуникације и пратиле перформансе организације у односу на постављене стратешке циљеве. Настао је као оквир за мерење перформансе од стране Роберта Каплана и Дејвида Нортон³¹⁹. Иако је фраза „балансирана листа мерила“ настала током 1990-тих година, корени овог приступа сежу даље у прошлост и потичу још из извештаја *General Electric*-а током 50-тих година прошлог века и француских инжењера који су осмислили *Tableau de Bord* – буквално „инструмент табла“ за мерила перформансе, почетком XX века.

Балансирана листа мерила је временом прерасла у менаџмент систем за стратешко планирање. Балансирана листа мерила трансформише стратешки план из пасивног документа у конкретне задатке који се свакодневно постављају пред организацију. Она не само да обезбеђује увид у мерила перформансе, већ помаже планерима да идентификују шта треба да буде урађено и измерено. Омогућава да се стратегије заиста и у потпуности испуне.

Овај нови приступ стратешком менаџменту омогућава јасну перцепцију тога шта треба да се мери да би избалансирани финансијску перспективу. Значи, он омогућава организацијама да стратегију пресликају у конкретан план дневних активности. Осим тога, обезбеђује повратне информације о пословним процесима и постигнутим ефектима да би се континуирано побољшавале перформансе и резултати. Када се у потпуности користи, балансирана листа мерила трансформише теорију у саму срж предузећа.³²⁰

³¹⁹ Више у: Kaplan, R. S., Norton, D. P., “Using the Balanced Scorecard as a Strategic Management System”, *Harvard Business Review*, Jan/Feb96, Vol. 74 Issue 1, p75-85.

³²⁰ Мада истраживања у пракси показују да се углавном користе *ad hoc* мерила, односно да се ретко користи избалансирани приступ. Видети: Barnes, D., Hinton, M., *The Benefits of e-Business Performance Measurement Systems*, Elsevier Ltd., Burlington, 2008.

Иако су финансијски индикатори³²¹ саставни део балансиране листе мерила, треба нагласити да су они индикатор прошлих догађаја. Ова мерила нису у стању да прате компаније новог доба које „морају да обрађају пажњу на кориснике, снабдеваче, запослене, процесе и технологије и иновације, да би опстале“³²². „Будући да истраживачи у последње време покушавају да процене до које је мере организација у могућности да испуни захтеве свих заинтересованих страна, основни аспект мерења перформансе може постати баш задовољство заинтересованих страна.“³²³

Перспективе у Балансираној листи мерила се односе на гледишта са којих се посматра организација:

1) Перспектива „Учења и раста“ укључује обуку запослених и ставове организационе културе који се односе на индивидуално и организационо напредовање. С обзиром на брзину којом се мења технологија, постаје неопходно да се запослени стално образују и обучавају. Мерила у овом домену се могу успоставити у циљу усмеравања алокације ресурса за обуке тамо где је обука најпотребнија. Каплан и Нортон³²⁴ упозоравају да „учење“ представља много више од „обуке“. Поред обуке, оно укључује менторства унутар организације, као и олакшавање комуникације између запослених што им омогућава да пронађу помоћ кад год им је потребна.

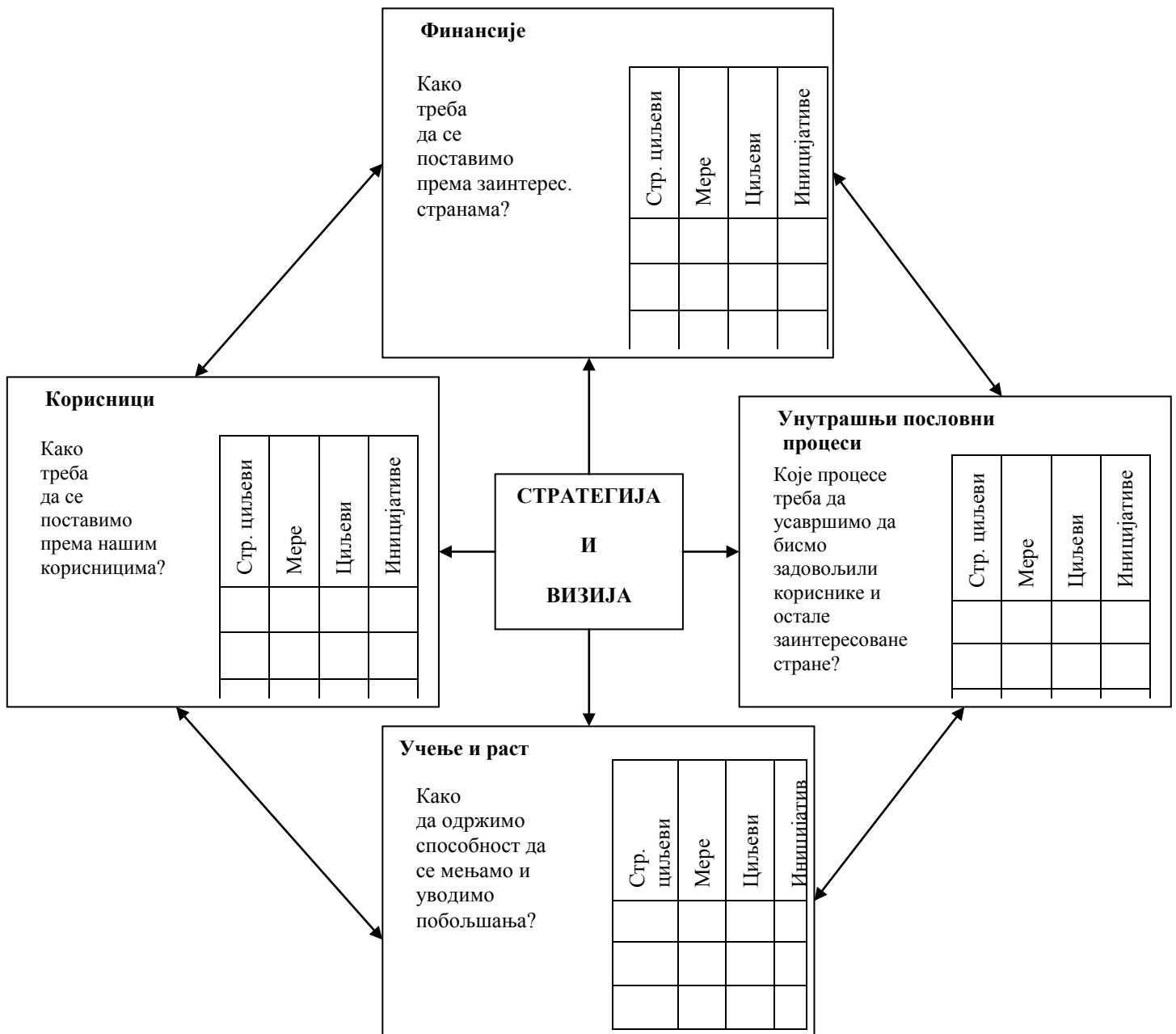
2) Перспектива „Пословних процеса“ се односи на унутрашње пословне процесе. Мерила која се примењују из ове перспективе треба да омогуће менаџерима да упознају процес пословања и да увиде да ли се производи и услуге прилагођавају захтевима корисника (мисија). Ова мерила треба да се пажљиво осмисле и да буду у складу са мисијом конкретне организације.

³²¹ Треба напоменути да постоје субјективна и објективна мерила перформансе. Видети: Andrews, R., Boyne, G. A., Walker, R. M., Subjective and objective measures of organizational performance: An empirical exploration, *Public Service Performance: Perspectives on Measurement and Management*, Cambridge University Press, New York, 2006., стр. 16.

³²² Kaplan, R. S., Norton, D. P., исто.

³²³ Orlitzky, M., Swanson, D. L., *Toward Integrative Corporate Citizenship: Research Advances in Corporate Social Performance*, Palgrave Macmillan, Basingstoke, 2008., стр. 195.

³²⁴ Видети: Kaplan, R. S., Norton, D. P., исто.



Слика 3. Балансирана листа мерила

(Kaplan, R. S., Norton, D. P., "Using the Balanced Scorecard as a Strategic Management System," *Harvard Business Review*, Jan/Feb96, Vol. 74 Issue 1, p75-85.)

3) Перспектива „Корисника“ се односи на задовољство корисника производима и/или услугама. Уколико корисници нису задовољни, одустаће од сарадње са датом организацијом и пронаћи неке конкурентске понуде. Уколико су перформансе лоше из ове перспективе, то може указати на будућу пропаст организације, чак и ако су тренутни финансијски показатељи позитивни. Да би се развила мерила у овом домену, потребно је да се спроводе истраживања и анализе захтева корисника и процеса који би омогућили производњу производа и/или услуга који задовољавају потребе корисника.

4) Иако су финансијски показатељи традиционални и не показују реалну слику ситуације у којој се налазе организације у савременом пословању, њих не треба занемарити. Чињеница је да је у традиционалном приступу овим показатељима придавано превише пажње. Балансирана листа мерила заправо даје само одмеренији значај овим показатељима. У овој перспективи, није на одмет укључити додатне податке, као што су процена ризика, подаци *cost-benefit* анализе и сл.

Још један од корисних менаџмент алата су стратешке мапе. Стратешке мапе су дијаграми који се користе за приказивање начина на који се ствара вредност у организацији. Оне показују логичку везу између стратешких циљева (представљају се у овалним облицима на дијаграму) и узрочно-последичног ланца који доводи до њиховог испуњења. Принципи који стоје иза стратешке мапе су следећи: 1. стратегија треба да уједначи супротне интересе, 2. стратегија се заснива на диференцираним предлозима за повећање вредности крајњим корисницима, 3. вредност се ствара у унутрашњим пословним процесима, 4. стратегија се састоји од симултаних, комплементарних делова, 5. вредност неопипљиве имовине се одређује преко усаглашавања стратегије.³²⁵

У последње време менаџери безбедности се све више окрећу листама мерила перформанси, у нади да ће се изградити пословни системи за одређивање трошкова и проширење одговорности изван пословних јединица. Највећи проблем у овој представља чињеница да је мерење пословних процеса у младим организацијама веома тешко. Потребно је уложити много труда да би се направиле ефикасне листе

³²⁵ Видети: Kaplan, R. S., Norton, D. P., исто.

мерила безбедности, а пре свега за „дефинисање индикатора, прикупљање података, осмишљавање и израду извештаја и комуникацију“³²⁶. Поред тога, потребно је осмислити и систем за контролу перформанси.³²⁷ У последње време се користи и систем Стандарда за Презентацију Перформанси (*Performance Presentation Standards* - PPS) који се првенствено заснива на мерењу перформанси, а затим на даљим анализама.³²⁸

Упркос наведеним проблемима, „користи које балансиране листе могу донети су вишеструке и то:

- омогућавају лако проналажење ризичних тачака унутар организације,
- прецизно указују на могуће мере за опоравак,
- мере унутрашњу сагласност са политиком организације,
- откривају непотпуне унутрашње процесе,
- имају предност у односу на неповратне трошкове који су повезани са безбедношћу.³²⁹

Приликом развијања листе безбедносних мерила, важно је да се има на уму да постоје два типа мерила. Прво, мерила која се односе на ефективност основних безбедносних активности организације у сузбијању опасности и ризика. Ова мерила утврђују разлику између тренутних ризика и оних који су пожељни. Она помажу да се одговори на питање „да ли организација ради оно што би требала да ради?“. Постоје и мерила која се односе на безбедносне активности пословних јединица. Ова мерила указују на одговорност за ризике и одговарају на питање „да ли се заиста ради оно што се тврди да се ради?“³³⁰. Она такође треба да се ослањају на политику организације.

³²⁶ Kaplan, R. S., Norton, D. P., исто.

³²⁷ То је процес праћења перформансе, упоређивање са стандардима или унапред дефинисаним вредностима и увођење неких промена уколико резултати нису одговарајући - видети: Kenis, P., *Performance control and public organizations, Public Service Performance: Perspectives on Measurement and Management*, Cambridge University Press, New York, 2006., стр. 113.

³²⁸ Видети: Loistl, O., Petrag, R., *Asset Management Standards: Corporate Governance for Asset Management*, Palgrave Macmillan, New York, 2003., стр. 136.

³²⁹ Kaplan, R. S., Norton, D. P., исто.

³³⁰ Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007.

За развијање листе безбедносних индикатора постоје два различита приступа. Један је одозго на доле (*top-down*), а други одоздо на горе (*bottom-up*). Иако оба приступа дају сличне податке, компаније треба да се одлуче за приступ који одговара тренутној ситуацији, односно расположивим средствима и потребама за које се израђују листе индикатора. Приступ одозго-на-доле је формалнији и свеобухватан и омогућава да се дефинишу потребе и циљеви. Други приступ је мање формалан, али омогућује организацијама које немају много искуства са безбедносним проблемима да убрзају развој листе индикатора.

Менаџери и стручњаци за безбедност применом првог приступа могу да дефинишу кључне индикаторе безбедности пре него што се прикупе подаци. Оно што је од великог значаја јесте да се укључе све заинтересоване стране³³¹, будући да пословни циљеви пре свега зависе од власника организације. Одговорности власника и других заинтересованих страна укључују:

- вође у сектору безбедности – дефинисање циљева безбедносних мерила и области мерења,
- стручњаке за поједине области безбедности – превођење циљева и мерних области у мерила и потребе за подацима,
- кориснике услуга – потврда циљева и потреба за подацима у односу на постојеће мере контроле и инсталирање потребне опреме.

Одређивање индикатора полази од дефинисања апстрактних концепата, који се затим операционализују у мерљиве и конкретне показатеље.³³²

Индикатори који су погодни за пословне јединице треба да:

- садрже потребне податке за подршку везе између пословних јединица,
- понашање пословних јединица у великој мери утиче на њих, то нису индиректна мерила безбедносних активности,
- све пословне јединице доприносе прикупљању података,

³³¹ „Заинтересоване стране” (*stakeholders*) су појединци или група људи који имају утицај или су под утицајем организационих циљева. - Schreck, P., *The Business Case for Corporate Social Responsibility: Understanding and Measuring Economic Impacts of Corporate Social Performance*, Physica-Verlag, Heidelberg, 2009., стр. 15.

³³² Видети: Kuchinka, P., *Levels of Corporate Globalization: Developing Measurement Scale for Global Customer Management*, Palgrave Macmillan, Basingstoke, 2004., стр. 66.

- мере понашање за које су пословне јединице одговорне.

Добри индикатори су блиско повезани са пословним циљевима, зрелошћу организације и њеним окружењем. Мерење се може вршити у следећим областима:

- утицање на подизање свести о безбедности,
- изузеци у политикама високог ризика,
- безбедност информационе мреже (лиценце за софтвер, вируси, црви, *spyware*, *adware* и сл.),
- системи за управљање, као што је СБМ,
- украдена или изгубљена опрема,
- потенцијални партнери који су у процесу провере,
- политике, процедуре и контроле које су у процесу анализе ризика.

Потребно је обратити пажњу да то што индикатори говоре о понашању пословних јединица. Индикатори могу да буду у складу са величином организационих јединица, уколико је потребно. Уколико и кад је год могуће, треба се послужити постојећим безбедносним стандардима.

Када се ради о прикупљању података, прво треба проучити постојеће изворе, као што су документа и безбедносни извештаји.

Приступ одоздо-на-горе у развоју индикатора се односи на техничку процену доступних података са аспекта безбедности и одабир индикатора безбедносних активности. Овај приступ даје брже резултате, али се може десити да се неки битни индикатори занемаре. Потребно је радити са руководиоцима на нижим нивоима да би се стекла представа о безбедносним циљевима организације. Ови циљеви морају да се упореде са стратегијом израде мерила. У том случају се заказују састанци са корисницима безбедносних услуга и објашњавају циљеви израде листе мерила.

Прикупљени подаци би требало да задовољавају следеће критеријуме:

- садрже потребне информације које подржавају корелацију са одређеном пословном јединицом,
- понашање пословне јединице утиче на њих,
- све пословне јединице морају бити заступљене у подацима,
- мере активности за које су одговорне пословне јединице.

Основни проблем када је реч о процени података је да се често прикупљају само тактички подаци. Ово се често дешава са контролним мерама физичко-техничког обезбеђења, основне заштите рачунара и сл.

Прикупљене податке треба пажљиво размотрити да би се међу њима пронашли кандидати за мерила, а основни критеријум треба да буде начин на који они директно или посредно указују на утицај који организациона јединица има на ризик. Примери директних индикатора су, нпр. инциденти са рачунарским мрежама (вируси, црви, *spyware*), приступ осетљивим и заштићеним подацима, заобилажење контролних мера приступа и сл. Примери посредних индикатора су понашање које је одобрено као изузетак од политике организације, свест запослених о безбедносној политици, учествовање запослених у неким безбедносним процесима и сл.³³³

По одабиру кључних индикатора, мерила се морају прилагодити величини пословне јединице и сл. индикаторима. Добро мерило има добре основе, односно што је већи узорак и мерило је поузданије.

Потом је потребно да се одабрана мерила упореде са свим пословним јединицама. Од критичне је важности да су мерила конзистентна у свим организационим јединицама. За свако мерило треба одабрати један циљ, где се врши балансирање између смањења ризика и прихватања листе од стране пословне јединице.

³³³ О томе више у: Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007.

5. МЕТОДЕ ЗА ПРОЦЕНУ ЕФИКАСНОСТИ И ЕФЕКТИВНОСТИ БЕЗБЕДНОСНОГ МЕНАЏМЕНТА У ОРГАНИЗАЦИЈАМА У РЕПУБЛИЦИ СРБИЈИ

Почеци бригае о безбедности на раду датирају из 1970. године, када је у САД донета Уредба о безбедности и здрављу на раду (*The Occupational Safety and Health Act* - OSHA) у циљу развијања стандарда за безбедност и здравље на раду.³³⁴ Ова Уредба је установила обавезне процедуре и потребну документацију за развој и регулисање питања безбедности и заштите здравља на радном месту, спровођење истраживања и инспекцијског надзора да би се утврдила сагласност са стандардима и прописима и предложили казне у случају да се ти стандарди и прописи не поштују. Многи менаџери безбедности заправо имају задужења да проверавају сагласност са овим стандардима и да их уводе уколико су они недовољно примењени.³³⁵

Касније су у САД донети и други закони који се односе на повећање безбедносних мера. Међу овима је од већег значаја Закон о безбедности банака (*Bank Security Act*), који је донет 1968. године. Овај закон је донет зато што је број злочина у банкама био у сталном порасту током 60-тих година двадесетог века. Повећан број пљачки, провала и изнуда је утицао на Конгрес САД да затражи од федералних банкарских институција да спроведу одређене безбедносне мере за смањивање ризика од криминалних дела. Међутим, саме мере нису смањиле насиље и злочине против финансијских институција које обухвата закон. Заправо, број ових дела је и даље био у порасту током наредних година. Касније су уследиле промене овог закона због прилагођавања са променама које су настале током индустријског развоја. На пример, закон из 1968. године је прописивао минимум безбедносне опреме и процедура које су се односиле на специфичну технологију против крађа, што је постало мање битно када су се изумели нови типови камера и опреме за надзор. До почетка 90-тих година прошлог века, банкарски су имали већи избор за осмишљавање

³³⁴ Детаљније: Friend, M. A., Kohn, J. P., *Fundamentals of Occupational Safety and Health*, 4th ed., Government Institutes, Lanham, 2007.

³³⁵ Видети: Gustin, J. F., *Safety Management: A Guide for Facility Managers*, 2nd ed., The Fairmont Press, Inc., Lilburn, 2008.

безбедносних система који је више одговарао њиховим потребама. Иако Закон о безбедности банака није директно повезан са повећаним бројем криминалних дела у банкама, било је јасно да те институције морају имплементирати одговарајуће мере за заштиту запослених и јавности. Можда би се број злочина повећао још више да Закон није донет. Овај закон је један од примера када влада доноси мере које представљају директан одговор на угрожавање безбедности и утицао је на развој безбедносног менаџмента у одређеном домену, у овом случају у финансијској сфери.

Други, чак успешнији, пример како законске иницијативе утичу на обликовање стратегије безбедности односи се на отмице авиона комерцијалних авио-компанија. Овај тип злочина је дошао у фокус 24. новембра 1971. године, када је Дан Купер усмерио лет из Портланда у Сијетл. Путници су пуштени у Сијетлу новац од откупнине и падобрани су однети авионом. Купер је наредио да авион слети у Рено. После тога је нестао са новцем и падобранима. У наредних шест месеци десило се шест сличних покушаја. Већина је била неуспешна, али је ризик од овог злочина запретио саобраћају у целини. Треба напоменути, да случај са Купером није био први злочин ове врсте³³⁶, већ је забележен значајан пораст у периоду од 1968. до 1971. Међутим, када су приватни и јавни сектор одлучили да се супротставе број злочина је почео да пада³³⁷. Предузете мере су дале резултате у смањењу ризика од злочина у ваздухопловству и повратила поверење у авио компаније. То је позитиван пример како координисана безбедносна политика може да умањи интернационални проблем. Међутим, многе друге привредне гране су развијале безбедносне програме независно од законске регулативе. На пример, не постоји закон који прописује безбедносне мере у трговини. Али, значајни и мерљиви губици у овој грани су довели до стварања менаџера који су задужени за процену губитака и проналажење начина за њихово умањивање. Исто се дешава и са другим комерцијалним гранама – приватним, јавним и непрофитним организацијама. Саобраћај, шпедиција, рударство, процесна

³³⁶ Први забележен случај отмице авиона се десио 1930. године у Перуу. Од 1930.-1967. десило се свега девет покушаја овог злочина. Током 1968. број се повећао на 17, а од тога је 13 било успешних. Током следеће године било је 40 случајева и то 33 успешна (McCrie, R. D., исто, стр. 42.).

³³⁷ У периоду 1973.-1979. број забележених случајева је пао на 31, од чега су свега три била успешна (McCrie, R. D., исто).

индустрија и велики број услужних делатности су побољшали своје безбедносне политике и системе. Ови фактори су убрзали развој безбедносних програма. То је довело до развоја савремене безбедносне индустрије, која се проширила на задовољавање безбедносних потреба. У међувремену, многе организације су делимично или потпуно прошириле своје безбедносне активности на спољне услуге.

5.1. Нормативно-правни оквир и стандарди безбедности

У Србији је 1991. године донет Закон о заштити на раду, који је више пута мењан („Службени гласник РС“ бр. 42/91, 53/93, 67/93, 48/94 и 42/98), а 2005. године, тај закон је значајно промењен и преименован у Закон о безбедности и здрављу на раду („Службени гласник РС“ бр. 101/05). На основу овог Закона, априла 2009. године је усвојена Стратегија безбедности и здравља на раду за период од 2009. до 2012. године. Стратегија своје упориште налази у Закону о безбедности и здрављу на раду („Службени гласник РС”, број 101/05), конвенцијама МОП-а, директивама ЕУ и кроз поштовање кључних принципа промовисаних тим документима, а на којима се данас заснива систем безбедности и здравља на раду.

Поред тога, сва правна лица, на основу Закона о заштити од пожара („Сл. гласник РС“, бр. 37/88, 53/93, 67/93, 48/94, 101/ 05) дужна су да имају:

1. Правилник о заштити од пожара Чл. 8,
2. Програм обуке радника из области заштите од пожара Чл. 24,
3. Извршену обуку радника из области заштите од пожара Чл. 24,
4. Уређаје, опрему и средства за гашење пожара Чл. 21,
5. Ангажовано лице за вођење послова заштите од пожара (месечни реферат) Чл. 7.

На основу новог Закона о заштити од пожара („Сл. гласник РС“, бр. 111/2009 од 29.12.2009.), који је почео да се примењује од 05. 09. 2010. године, сва правна лица и предузетници су дужни да имају:

- План заштите од пожара уколико решењем МУП-а буду разврстани у 1. или 2. категорију угрожености - члан 27.
- Санациони план за отклањање последица пожара – члан 16.

- Правила за заштиту од пожара (за 3. категорију) са Планом евакуације и Упутством за поступање у случају пожара – члан 28.
- Уређаје, опрему и средства за гашење пожара - члан 42 и 43.
- Програм за основну обуку и проверу знања запослених на који се мора обезбедити сагласност МУП-а – члан 53.
- Да изврше обуку запослених и проверу знања најмање једном у три године – члан 53.
- Да за те послове ангажују Правно лице или Предузетника са овлашћењем МУП-а за обављање тих послова – члан 24 и 25. Међутим, занемарује се чињеница да безбедност захтева адекватан свеобухватан менаџмент који значи много више од плана безбедности.

Закон о изменама и допунама Закона о заштити животне средине, усвојен у Скупштини Републике Србије маја 2009. године, у себи садржи препоруке „Seveso“ II директиве. Дефинисано је „Seveso“ постројење, као постројење у којем се обављају активности у којима је присутна и може бити присутна опасна материја у једнаким или већим количинама од прописаних. Такође, дефинисане су обавезе оператера Севесо постројења, који мора да достави обавештење, односно да изради *Политику превенције удеса* или *Извештај о безбедности* и *План заштите од удеса*. Министарство животне средине и просторног планирања Републике Србије је идентификовало постројења која подлежу обавезама Seveso II директиве и објавило Прелиминарни списак постројења. Тренутно се у изради налазе и три подзаконска акта, што ће омогућити комплетну примену ове директиве која омогућава превенцију, припремљеност и брзи одговор на хемијски удес.³³⁸

5.1.1. Систем безбедности и здравља на раду

Систем безбедности и здравља на раду у Републици Србији уређен је Законом о безбедности и здрављу на раду. Међутим, систем безбедности и здравља на раду има подршку и у Закону о раду („Службени гласник РС”, бр. 24/05 и 61/05), Закону о здравственој заштити („Службени гласник РС”, бр. 107/05), Закону о здравственом

³³⁸ Више на: http://www.kombeg.org.rs/aktivnosti/c_tehno/Detailnije.aspx?veza=498

осигурању („Службени гласник РС”, бр. 107/05 и 109/05), Закону о пензијском и инвалидском осигурању („Службени гласник РС”, бр. 34/03, 64/04, 84/04, 85/05, 101/05 и 63/06), Закону о општој безбедности производа (предлог закона у скупштинској процедури) и многим другим законима, техничким прописима и стандардима којима се остварују безбедни и здрави радни услови.

У циљу примене и извршавања Закона о безбедности и здрављу на раду донети су следећи подзаконски прописи:

- Правилник о програму, начину и висини трошкова полагања стручног испита за обављање послова безбедности и здравља на раду и послова одговорног лица („Службени гласник РС”, бр. 29/06 и 62/07);
- Правилник о условима и висини трошкова за издавање лиценци за обављање послова у области безбедности и здравља на раду („Службени гласник РС”, бр. 29/06, 72/06 и 62/07);
- Правилник о висини трошкова поступка утврђивања испуњености прописаних услова у области безбедности и здравља на раду („Службени гласник РС”, број 60/06);
- Правилник о поступку утврђивања испуњености прописаних услова у области безбедности и здравља на раду („Службени гласник РС”, број 60/06);
- Правилник о начину и поступку процене ризика на радном месту и у радној околини („Службени гласник РС”, бр. 72/06 и 84/06-исправка);
- Правилник о садржају и начину издавања обрасца извештаја о повреди на раду, професионалном обољењу и обољењу у вези са радом („Службени гласник РС”, бр. 72/06 и 84/06-исправка);
- Правилник о поступку прегледа и испитивања опреме за рад и испитивања услова радне околине („Службени гласник РС”, бр. 94/06 и 108/06-исправка).
- Правилник о евиденцијама у области безбедности и здравља на раду („Службени гласник РС”, број 62/07);
- Правилник о претходним и периодичним лекарским прегледима запослених на радним местима са повећаним ризиком („Службени гласник РС”, бр. 120/07 и 93/08);

- Правилник о превентивним мерама за безбедан и здрав рад при коришћењу средстава и опреме за личну заштиту на раду („Службени гласник РС”, број 92/08).

Поред Закона о безбедности и здрављу на раду и наведених подзаконских прописа, донета је и Стратегија безбедности и здравља на раду у Републици Србији за период од 2009. до 2012. године. У систему безбедности и здравља на раду примењују се и посебне мере као правна правила и опште признате мере којима се обезбеђује безбедност и здравље запослених на раду. Међутим, права, обавезе и одговорности послодаваца и запослених у овој области уређују се општим актом послодаваца, односно колективним уговором и уговором о раду.

У законодавном систему безбедности и здравља на раду примењују се тридесет и два подзаконска прописа који садрже опште и посебне мере, а које се примењују као правна правила у разним врстама делатности и у различитим технолошким процесима. Наведени прописи су застарели и превазиђени те је потребно усмерити активности на доношењу нових прописа усаглашених са директивама ЕУ, а постојеће ставити ван снаге. Један од најважнијих услова за успешно остваривање циљева Стратегије безбедности и здравља на раду, је пуна укљученост свих институција и социјалних партнера повезаних са њеном применом, на националном нивоу. Власништво над Стратегијом не треба да има само Влада, Министарство рада и социјалне политике, Управа за безбедност и здравље на раду и Инспекторат за рад, већ и социјални партнери, невладине организације и други актери у овој области. Министарство рада и социјалне политике предлаже, извршава, развија, примењује и координира политику Владе у области безбедности и здравља на раду; директно организује и координира активности у изради Акционог плана безбедности и здравља на раду и по усвајању Стратегије припрема и предлаже Акциони план за њену реализацију и у сарадњи са другим институцијама прати остваривање циљева и извршавање оперативних задатака утврђених у Стратегији и Акционом плану, што укључује посебне активности Управе за безбедност и здравље на раду и Инспектората за рад.

Законом о безбедности и здрављу на раду прописано је да Управа обавља следеће послове:

- 1) припрема прописе у области безбедности и здравља на раду, као и мишљења за њихову примену;
- 2) припрема стручне основе за израду националног програма развоја безбедности и здравља на раду и прати његово остваривање;
- 3) прати и оцењује стање безбедности и здравља на раду и припрема ставове за јединствено уређивање мера безбедности и здравља на раду које су предмет овог закона и других прописа;
- 4) истражује и подстиче развој у области хуманизације рада;
- 5) пружа стручну помоћ у области безбедности и здравља запослених;
- 6) припрема методологије за обављање послова прегледа и испитивања у области безбедности и здравља на раду;
- 7) проучава узроке и појаве који за последицу имају повреду на раду, професионалне болести и болести у вези са радом;
- 8) организује полагање стручних испита, о чему води евиденцију;
- 9) врши надзор над законитошћу рада правних лица и предузетника као и одговорних лица са лиценцом и припрема предлоге решења за издавање и одузимање лиценци, о чему води евиденцију;
- 10) прикупља и анализира податке о повредама на раду, професионалним обољењима, болестима у вези са радом и појавама које утичу на здравље запослених;
- 11) обавља информационо-документациону делатност у области безбедности и здравља запослених;
- 12) организује саветовања, врши едукацију запослених, послодаваца, лица за безбедност и здравље на раду, инспектора и др., објављује различите материјале и информише јавност о стању у области безбедности и здравља на раду;
- 13) стара се о примени међународних аката у области безбедности и здравља на раду;
- 14) подстиче образовање и развијање културе рада у области безбедности и здравља на раду;
- 15) обавља друге послове одређене законом.

Законом о министарствима („Службени гласник РС”, број 65/07) који је ступио на снагу 15. 05. 2007. године, уследила је организациона измена Сектора инспекције рада формирањем Инспектората за рад, као органа у саставу Министарства рада и социјалне политике, а који има већу самосталност од оне коју је имао Сектор инспекције рада.

Инспекторат за рад у свом саставу има 28 подручних јединица – одељења и одсека, који су смештени у управним окрузима и граду Београду (3 одељења), као и 2 одељења у седишту Инспектората за рад. У Инспекторату за рад послове инспекцијског надзора обавља укупно 308 инспектора рада различитих профила и то 172 дипломирана правника, 135 дипломираних инжењера и 1 лекар, који врше надзор над применом прописа у овој области. Инспекторат за рад преко инспектора рада обавља инспекцијске послове и са њима повезане стручне послове у области безбедности и здравља на раду и радних односа, који се односе на редовни и контролни надзор, увиђаје повреда на раду, утврђивање испуњености прописаних услова у области безбедности и здравља на раду пре почетка обављања делатности послодавца, као и друге послове одређене законом.

У складу са Законом о безбедности и здрављу на раду у поступку инспекцијског надзора, инспектор рада има право и дужност да предузима радње којима се контролишу безбедност и здравље на раду, а нарочито хигијена и услови рада, производња, стављање у промет, коришћење и одржавање средстава за рад, средстава и опреме за личну заштиту, опасне материје и др. као и да послодавцима запосленима, њиховим представницима и синдикату даје обавештења и савете у области безбедности и здравља на раду, као и о мерама чијом применом се обезбеђује извршавање овог закона на најефикаснији начин.

Увођење новог система у области безбедности и здравља на раду, заснованог на директивама ЕУ увођењем одговорности послодавца за примену мера, захтева промене традиционалног приступа рада инспектора рада у поступцима вршења надзора односно напуштање старих и увођење нових метода рада.

Да би се постигла већа ефикасност рада инспектора рада, краће трајање инспекцијских надзора, као и уједначеност у поступању инспектора рада у истим

правним ситуацијама, суштински се мора променити начин планирања, организовања, спровођења и праћења, као и свеобухватни ниво обављања посла из делокруга рада Инспектората за рад, како у квантитативном тако и у квалитативном смислу. У складу са наведеним, основни циљ Инспектората за рад је увођење интегрисаног метода рада инспектора, који подразумева да ће један инспектор на одговарајући, квалитетан, обједињен и стручан начин, вршити надзор по свим основним питањима из области радних односа и безбедности и здравља на раду приликом једне инспекцијске посете. Министарство здравља има водећу улогу у стварању услова за подизање нивоа здравља запослених кроз активну улогу службе медицине рада.

Законом о безбедности и здрављу на раду дата је значајна улога служби медицине рада у примени мера којима се осигурава здравље запослених на радним местима, а нарочито да учествује у идентификацији процене ризика, упознаје запослене са ризицима по здравље који су повезани са њиховим радом и обавља послове оспособљавања запослених за пружање прве помоћи, утврђује и испитује узроке настанка професионалних болести и болести у вези са радом, оцењује и утврђује посебне здравствене способности које морају да испуњавају запослени за обављање одређених послова на радном месту са повећаним ризиком или за употребу, односно руковање одређеном опремом за рад, врши претходне и периодичне лекарске прегледе запослених на радним местима са повећаним ризиком и издаје извештаје о лекарским прегледима у складу са прописима о безбедности и здрављу на раду, учествује у организовању прве помоћи, спасавању и евакуацији у случају повређивања запослених или хаварија, даје савете послодавцу при избору другог одговарајућег посла према здравственој способности запосленог, саветује послодавца у избору и тестирању нових средстава за рад, опасних материја и средстава и опреме за личну заштиту на раду, учествује у анализи повреда на раду, професионалних болести и болести у вези са радом и непосредно сарађује са лицем за безбедност и здравље на раду.

Законом о здравственој заштити утврђено је оснивање Завода за медицину рада за територију Републике Србије који ће обављати делатност из области

медицине рада, односно заштите здравља запослених на раду, са основним задатком да прати и проучава услове рада, организовања и спровођења информационог система прикупљања података о повредама на раду, професионалним болестима и болестима у вези са радом. Тим законом прописано је оснивање здравствених установа за заштиту здравља запослених и на нижим нивоима организовања.

Министарство просвете има важну улогу у стварању услова на пројекцији образовних потреба и подизању нивоа образовања и стручности радне снаге (усавршавање и иновирање модела образовних програма, увођење нових програма различитих организационих модела и облика, начина и сарадње професионалне праксе у предузећима/привредним друштвима, а на основу уговора о партнерству и сарадњи између школа и социјално-економских партнера, увођење специјалистичких и сличних студија – блок наставе и др.). Министарство просвете има значајну улогу у примени превентивних мера у области безбедности и здравља на раду.

Министарство економије и регионалног развоја са другим ресорним министарствима и Агенцијом за развој малих и средњих предузећа одговорно је за Стратегију привредног развоја и спровођење економске политике усмерене ка подстицању развоја малих и средњих предузећа. Министарство економије и регионалног развоја предлаже доношење закона из области стандардизације, техничких прописа (Закона о техничким захтевима за производе и оцењивању усаглашености), акредитације, мера (метрологије) и драгоцених метала. Ово министарство, припрема и доноси техничке прописе, из свог делокруга, којима се, између осталог, прописују технички, безбедносни и други захтеви који утичу и на обезбеђивање безбедности и здравља на раду. Институт за стандардизацију Србије доноси српске стандарде. Примена тих стандарда је добровољна. Подржава се примена закона и техничких прописа које предлаже ово министарство, као и доношење стандарда од стране Института за стандардизацију Србије, а посебно када је у питању њихов утицај на безбедност и здравље на раду, пре свега запослених, дакле оних који користе и употребљавају производе за које се прописују технички и безбедносни захтеви.

Министарство животне средине и просторног планирања, Министарство рударства и енергетике, Министарство унутрашњих послова, Министарство пољопривреде, шумарства и водопривреде и Министарство одбране у оквиру својих надлежности доносе прописе који непосредно имају утицаја на јачање и развој колективних мера безбедности и здравља на раду запослених, што намеће потребу укључивања тих министарстава у спровођењу ове стратегије.

Друга министарства у домену своје надлежности такође у значајној мери учествују у примени поменуте Стратегије.

Фонд здравственог осигурања и Републички фонд за пензијско и инвалидско осигурање, као надлежне организације сарађују и учествују у доношењу заједничких ставова о питањима унапређивања безбедности и здравља на раду и старају се о развоју и унапређивању опште културе безбедности и здравља на раду.

Републички завод за статистику и друге организације у чијој надлежности је вођење евиденција у значајној мери учествују као подршка спровођењу ове стратегије.

Улога судства у систему безбедности и здравља на раду огледа се у кажњавању за прекршај и учињена кривична дела због непридржавања прописа о безбедности и здрављу на раду.

Социјално-економски савет (на свим нивоима на којима се оснива) има улогу успостављања и развијања социјалног дијалога по свих питањима од значаја за безбедност и здравље на раду. У свом раду стара се о остваривању права запослених, њиховог материјалног и социјалног положаја као и о условима њиховог живота и рада. Улога Социјално-економског савета је и да разматра нацрте закона и предлоге других прописа из области безбедности и здравља на раду, да о њима даје мишљења, а од изузетног значаја је што је у оквиру Социјално-економског савета формирано радно тело за питања безбедности и здравља на раду са задатком разматрања и предлагања ставова из области безбедности и здравља на раду.

У Србији је први пут Одлуком Владе („Службени гласник РС”, број 42/2001) образован Савет за заштиту на раду, који је Одлуком Владе („Службени гласник РС”, број 40/05) ревидиран и образован као Савет за безбедност и здравље на раду, а у

којем су били заступљени представници репрезентативних синдиката, Уније послодаваца Србије, Министарства рада и социјалне политике, Министарства рударства и енергетике, високошколских установа, невладиних организација и др. Одлуком о измени Одлуке о образовању Савета за безбедност и здравље на раду („Службени гласник РС”, број 71/07) потврђено је образовање Савета за безбедност и здравље на раду.

Задаци Савета јесу да: даје иницијативе за доношење прописа у области безбедности и здравља на раду, даје иницијативу за израду националног програма развоја безбедности и здравља на раду, својим деловањем доприноси приближавању различитих ставова учесника у социјалном дијалогу у овој области, иницира превентивну политику по свим питањима која се односе на безбедност и здравље на раду. Овом групом су обухваћене следеће институције: Организације послодаваца и запослених (удружења и уније послодаваца, синдикати и одбор запослених).

У Републици Србији постоје, једно репрезентативно удружење послодаваца и то Унија послодаваца Србије и два репрезентативна синдиката – Савез самосталних синдиката Србије и УГС „Независност”.

Унија послодаваца Србије учествује у креирању политике безбедности и здравља на раду на макро плану, а њене организације на микро плану имају велику улогу у пружању помоћи послодавцима у примени прописа путем организовања разних едукација и саветовања. Синдикати, одбори за безбедност и здравље на раду и представници запослених имају веома значајну улогу у спровођењу Стратегије путем утицаја који остварују кроз систем колективних уговора у афирмацији безбедности и здравља на раду и непосредној примени мера безбедности и здравља на раду код послодавца. Стручне асоцијације и невладине организације, као и други субјекти, треба да имају важну улогу у провери кључних смерница Стратегије и праћењу њиховог спровођења.

Министарство рада и социјалне политике, односно Управа за безбедност и здравље на раду издаје лиценце за обављање послова безбедности и здравља на раду, као и послова прегледа и испитивања опреме за рад и испитивања услова радне околине. Правна лица и предузетници који су стекли лиценцу имају посебну улогу у

обезбеђивању и повременом контролисању (прегледима и испитивањима) мера за безбедност и здравље на раду. Квалитет обављених послова прегледа и испитивања опреме за рад и услова радне околине односно, веродостојност података утврђених у току прегледа и испитивања представљају најважније чињенице (елементе) за оцењивање стања безбедности и здравља на раду, процењивање професионалних ризика и предузимање превентивних мера код послодавца. Уколико се прихвати и реализује иницијатива, референтна лабораторија треба да преузме улогу арбитра између послодавца и правног лица са лиценцом у циљу утврђивања веродостојности података у стручним налазима.

Да би се обезбедила општа сагласност и спречили отпори спровођењу Стратегије, нужно је обезбедити довољно информација за доношење одлука, а такође и постављене циљеве представити јавности. У првом реду, редовно извештавање је потребно у периоду оцене могућих ефеката, узимајући у обзир ставове разних интересних група. У циљу постизања ефикасности, Стратегија мора да буде сачињена на бази принципа отворености, транспарентности, интегритета и међусобног уважавања. Сви они који су укључени у консултације треба да су у стању да утичу на сакупљање информација, дефинисање инструмената, периода, начина и рокова спровођења ове стратегије.

Биће предузете активности усмерене ка обезбеђењу пуне информисаности јавности о свим чињеницама у вези са безбедношћу и здрављем на раду, користећи свако погодно и ефикасно средство информисања. Ово подизање свести јавности треба да омогући спровођење свеобухватних, доступних и ефикасних програма који се, најчешће, односе на:

- 1) професионалне ризике, као и предлог мера за контролу и управљање ризицима;
- 2) добробит од спровођења процедуре процене ризика;
- 3) саопштавање битних информација о активностима на спречавању повреда на раду, професионалних болести и болести у вези са радом и постигнутим резултатима;

4) упозоравања на здравствене и економске последице на нивоу послодавца, као и на последице по друштво услед непримењивања мера безбедности и здравља на раду.

Обезбеђивање функционисања система безбедности и здравља на раду у складу са захтевима који проистичу из Закона о безбедности и здравља на раду, докумената ЕУ и Међународне организације рада (МОП) остварује се³³⁹:

1) увођењем начела превенције применом превентивних мера које се обезбеђују у складу са савременим прописима о безбедности и здрављу на раду, техничким, правним, здравственим, образовним, организационим и другим мерама, као и обезбеђивањем средстава за отклањање ризика од повређивања и оштећења здравља запослених и свођења ризика на најмању могућу меру;

2) увођењем осигурања од повреда на раду, професионалних болести и болести у вези са радом ради обезбеђивања накнаде штете;

3) едукацијом и образовањем из области безбедности и здравља на раду запослених и послодаваца;

4) давањем услуга у области безбедности и здравља на раду у складу са прописима (специјализоване техничке, медицинске и научне институције, истраживачки институти, лабораторије и др.);

5) укључивањем људских ресурса активних у области безбедности и здравља на раду (инспектори, специјалисти медицине рада, правници, инжењери различитих профила, итд.);

6) истраживањем у области безбедности и здравља на раду;

7) увођење механизма за евидентирање и анализу података о повредама на раду, професионалним болестима и болестима у вези са радом, као и размену статистичких података између послодаваца, запослених и власти;

8) подршком на свим нивоима за прогресивно побољшање безбедности и здравља на раду, а нарочито у микро, малим и средњим предузећима;

³³⁹ Видети: Стратегија безбедности и здравља на раду у Републици Србији за период од 2009. до 2012. године.

9) сарадњом послодаваца, синдиката, државних органа и других чинилаца у систему безбедности и здравља на раду у доношењу заједничких ставова о питањима безбедности и здравља на раду;

10) промовисањем и афирмисањем безбедности и здравља на раду ангажовањем медија, организовањем кампања итд.

Стање безбедности и здравља на раду у Републици Србији, приказано у овој стратегији³⁴⁰ засновано је на Извештајима о раду Управе за безбедност и здравље на раду и Инспектората за рад за 2007. годину. По доношењу Закона о безбедности и здрављу на раду, ради обезбеђења његове примене, у периоду 2006-2007. године донети су подзаконски прописи наведени у тачки 5.2. Стратегије.

Упућен је Народној скупштини Предлог закона о потврђивању Конвенције Међународне организације рада број 167. о безбедности и здрављу у грађевинарству и Предлог закона о потврђивању Конвенције Међународне организације рада број 187. о промотивном оквиру безбедности и здравља на раду.

Управа је извршила едукацију о примени Закона и подзаконских прописа који обезбеђују функционисање система, а посебно Правилника о начину и поступку процене ризика на радном месту и у радној околини у 2006. и 2007. години око 12.000 запослених, послодаваца и инспектора рада. Едукација је извршена у сарадњи са социјалним партнерима, а на захтев менаџмента едукација је извршена и у великим пословним системима. На основу првих показатеља, у току спровођења едукација у вези са подизањем свести и културе рада у области безбедности и здравља на раду, уочено је да је потребно осавременити начин едукације свих учесника у систему образовањем јединственог Центра за едукацију у овој области.

У складу са Акционим планом за спровођење поменуте Стратегије безбедности и здравља на раду у Републици Србији, у циљу реализације активности „Израда анализе примене закона и подзаконских аката“, у оквиру појединачног циља „Успостављање, одржавање и прогресивно развијање и периодично ревидирање система безбедности и здравља на раду у консултацији са репрезентативним

³⁴⁰ Видети: Стратегија безбедности и здравља на раду у Републици Србији за период од 2009. до 2012. године.

организацијама послодаваца и запослених“, формирана је Радна група за израду анализе примене закона и подзаконских прописа из ове области. У циљу реализације поменутих активности, Радна група има конкретан задатак да изради анализу и предлоге за измену одређених подзаконских аката.

5.1.2. Систем физичко-техничког обезбеђења

Државни органи и институције, изградњом јединственог система безбедности и развијањем капацитета друштва за управљање кризама треба да омогуће наставак привредних и пословних активности друштвене заједнице и у кризним условима (ванредне ситуације, елементарне непогоде, ратно стање и др.). Унапређењем техничких, људских, организационих и функционалних веза међу свим заинтересованим странама, у које спада и област приватног обезбеђења, држава чува свој јавни интерес – заштиту живота, здравља и имовине грађана.

Приватно обезбеђење, као интегрални део система националне безбедности Србије усклађено са новим схватањима појма безбедности, има своје посебно место и значај. Пре свега, то је индустријска грана која производи услуге намењене обезбеђењу лица, имовине и пословања за која не постоји законом прописана обавеза организовања система обезбеђења од стране војске или полиције. Приватни сектор обезбеђења или алтернативна безбедност није конкуренција држави и њеним службама безбедности, већ је израз потребе друштва, капитала и грађана да, у сарадњи са институцијама државе, повећа личну и имовинску безбедност свих грађана. Иако ова област није законски регулисана, „потражња за услугама приватног обезбеђења бележи стални раст“³⁴¹. Основни задаци који су стављени пред организације из ове индустријске гране су: анализа, откривање и спречавање потенцијалних опасности и противправних радњи које нарушавају достојанство и угрожавају пословање, живот и физички интегритет лица, угрожавајуштићени простор или умањују вредност имовине³⁴² која је предмет приватног обезбеђења.

³⁴¹ Kinsey, C., *Corporate Soldiers and International Security*, Routledge, New York, 2006., стр. 151.

³⁴² При томе, имовина обухвата опипљива и неопипљива добра, односно интелектуална својина, а у коју, између осталих, спадају: посећеност на Интернету, односи са клијентима, ауторска права,

Појавни облици ове делатности су заштитна делатност, самозаштитна делатност и детективска делатност.

Правилно разумевање, позиционирање приватног обезбеђења и безбедности уопште почев од стратешких докумената до законских и подзаконских аката, први је корак ка реалној потреби да своју улогу остварује у пуној координацији са јавном безбедношћу, јер су им циљеви исти, а задаци слични. Традиционално схватање да је само полиција одговорна за безбедност, у свету је одавно напуштено. Нема сумње да приватно обезбеђење доприноси ефикаснијој заштити виталних вредности друштва и да ће процес преношења неких послова безбедности са државе на приватни сектор имати узлазни тренд, нарочито због неминовности смањења јавне потрошње. Опште је познато да је у приватном сектору обезбеђења концентрисано истраживање, развој и примена најсавременијих технологија из области безбедности и заштите (GPS, примена електро-хемијске заштите готовине, алармни системи, видео обезбеђење итд.)³⁴³ – чији значај је истакнут и у Стратегији националне безбедности.

Пошто није Законом уређено ко испуњава услове за рад на пословима физичко-техничког обезбеђења и како се добија лиценца, формално-правно гледано, свако може да обавља те послове. Агенције за физичко-техничко обезбеђење, после полиције, важе за најбројнију оружану формацију у Србији. Њихово оснивање и рад још увек нису законом регулисани, па је непознаница и колико тачно има фирми које се баве овим пословима, број људи које оне запошљавају, као и колико се комада разног оружја налази у њиховим рукама. Према неким незваничним подацима, у Србији постоји више од 3000 агенција које пружају услуге физичке и техничке заштите лица и имовине, док број запослених у овом сектору обухвата између 40000 и 50000 људи, док је процењено да у овом сектору има око 47000 комада лаког и малокалибарског оружја и око 15000 различитих видова заштитне опреме.³⁴⁴

различите врсте уговора и сл. Видети: Zyla, M. L., *Fair Value Measurements: Practical Guidance and Implementation*, John Wiley & Sons, Inc., Hoboken, 2010.

³⁴³ Видети: Johnson, K., *Asset Protection and Security Management Handbook*, POA Publishing LLC, Boca Raton, 2003.

³⁴⁴ Савић, А., *Приватна безбедност у систему националне безбедности, Приватна безбедност – стање и перспективе*, Факултет за правне и пословне студије, Нови Сад, 2008., стр. 15-23.

Заштитна и самозаштитна делатност у обезбеђивању лица, имовине и пословања пружа услуге физичке заштите, техничке заштите, менаџмент вредностима и менаџмент из контролног центра. Разлика између заштитне и самозаштитне делатности је само у власништву над предметом заштите. Код заштитне делатности обезбеђују се лица, имовина и пословање у власништву друге стране – корисника услуге. Самозаштитна делатност се, ангажовањем својих запослених у организацијама, обавља за сопствене потребе, односно за заштиту сопствене имовине, лица и пословања и/или путем „аутсорсинг“ услуга приватног обезбеђења.³⁴⁵ До скоро је држава фирме за приватно обезбеђење третирали исто као и друга привредна друштва, не узимајући у обзир битну специфичност – да су привредна друштва из области приватног обезбеђења – наоружана, а која су због недостатка закона о делатности легално и легитимно ангажована на задацима унутрашње безбедности – како у јавним институцијама и предузећима од посебног значаја за Републику Србију, тако и у осталим великим индустријским системима, објектима од јавног значаја, привредним, пословним и резиденцијалним објектима широм Србије. Међутим, временом је то постала значајна привредна делатност која остварује профит, запошљава велики број радника и одговара за безбедност скоро 80% државне имовине. У том смислу МУП РС је предложио нацрт Закона о приватном обезбеђењу. Поред тога, Удружење за приватно обезбеђење и Центар за квалитет ПКС покренули су иницијативу да се донесе српски стандард за услуге приватног обезбеђења.

Нацртом Закона о приватном обезбеђењу је уведено лиценцирање фирми које се баве физичко-техничким обезбеђењем и њихових запослених. Предвиђено је да лиценце, на предлог МУП-а, издаје Агенција за послове приватног обезбеђења. Дефинисани су и начини обављања послова приватног обезбеђења, као и овлашћења радника обезбеђења. Наведени разлози упућују да се област приватног обезбеђења, као интегралног дела система безбедности – нормативно уреди, и то не само законом о приватном обезбеђењу, него и сродним законима као што је Закон о ванредним

³⁴⁵ Видети: Kovacich, G. L., Halibozek, E. P., *Security Metrics Management*, Butterworth Heinemann, Boston, 2006.

ситуацијама и сл., који отвара могућност превођења већ постојећих организационих делова (служба физичке заштите, мобилни интервентни тимови, контролни центри, сервисне техничке службе и сл.) у активну резерву, опште и специјализоване јединице цивилне заштите – што би се могло регулисати уговором између фирми за приватно обезбеђење и надлежних републичких и органа локалне самоуправе (кризни штабови) – чиме би се постигло јачање функционалних веза свих субјеката на целој територији РС. То је у интересу државе, јер би се на тај начин појачала одговорност свих припадника приватног обезбеђења (од оснивача до извршилаца) и створили услови за оптималну употребу „готових снага“ у случају потребе, а нарочито је у интересу великих привредних система (првенствено оних који су од посебног значаја за државу), а који скоро 80% потреба за обезбеђењем решавају уговором са фирмама за приватно обезбеђење – чији запослени, ако се не нађе системско решење у проглашењу ванредног или ратног стања – у правилу подлежу обавези одзива у ратне јединице (активна резерва Војске и Полиције). На тај начин поменуте организације од посебног значаја за државу неминовно постају рањиве на претње и ризике. При томе, остаје и правни проблем статуса закључених уговора о обезбеђењу у делу који се односи на накнаду евентуалне штете настале због напуштања објеката због мобилизације службеника обезбеђења.

Институт за стандардизацију Републике Србије, крајем 2008. године је донео национални стандард услуга приватног обезбеђења (SRPS A.L2.000:2008, *Друштвена безбедност – Услуге приватног обезбеђења*) – који у значајној мери може допринети ефикасној тржишној контроли квалитета услуга обезбеђења на тржишту. То је први национални стандард донет у последњих 50 година на иницијативу домаће привреде, а да није настао преношењем европског или светског стандарда. На семинару о „Стандардима и квалитету услуга приватног обезбеђења“ који је одржан од 1. до 4. октобра 2009. године у Врњачкој Бањи, промовисан је сертификат квалитета тих врста услуга, које издаје Центар за квалитет Привредне коморе Србије. Сврха сертификата је подизање нивоа узајамног поверења између понуђача и корисника ових услуга на домаћем тржишту, посебно осигуравајућих друштава која имају интерес да сертификат уграде у захтеве за одређивање вредности полисе осигурања.

Сертификат се издаје са роком важења од годину дана и он потврђује да је услуга приватног обезбеђења испунила захтеве наведеног стандарда до задовољавајућег нивоа квалитета.

5.2. Постојећи индикатори ефикасности и ефективности система безбедносног менаџмента

У Републици Србији, у већини организација су уведени, или су у фази увођења, систем управљања заштитом животне средине (нарочито преко увођења стандарда ISO 14000), систем безбедности и заштите здравља на раду, систем заштите од пожара и сл. Ови системи су у суштини потпуно одвојени једни од других и између њих има врло мало контакта, размене информација и сарадње.

Индикатори рада појединих служби задужених за послове безбедности су, у складу са организацијом послова, такође фрагментисани. У областима у којима су добро развијени и уведени стандарди, ревизија, надзор и контрола се односе на праћење стања и извештавања о одступањима од постављених стандарда. Проблем настаје у областима које нису законски регулисане и којима руководство не поклања нарочиту пажњу. Иако су саме обавезе људима који су задужени за те послове прилично јасне, чињеница је да немају повратну информацију о томе у којој су мери послови које обављају важни за организацију.

Показатељи таквих послова се свде на прикупљање података и слање извештаја о инцидентима који су се десили или су избегнути и евентуалне штете која је настала услед њих. Извештаји се, углавном, шаљу вишем руководству, а сами запослени немају повратних информација о томе шта се на вишим инстанцама одлучује. Особе задужене за управљање службама из области безбедности и заштите (најчешће је то позиција шефа – нпр. шеф обезбеђења) нису у великој мери упознате са стратегијом и политиком безбедности, већ се њихове управљачке активности свде на краткорочно планирање у циљу спровођења свакодневних обавеза.

Најчешћи индикатори се односе на број и учесталост појављивања безбедносних проблема и износ штете који је настао услед њихове појаве, независно

од тога о којим се конкретно пословима ради. Нпр. за службу заштите од пожара, јасно је да је индикатор број детектованих пожара, број пожара који су на време откривени, штета настала услед пожара и сл. Ови подаци се најчешће путем редовних извештаја шаљу вишем руководству, а највећа пажња се поклања томе да ли је било озбиљних повреда здравља на раду и могућностима наплате штете од осигуравајућих кућа.

Све то указује да прави показатељи ефективности и ефикасности рада ових служби нису развијени и/или се не примењују.

5.3. Могућности процене ефективности и ефикасности система безбедносног менаџмента у предузећима у Републици Србији

У циљу непрестаног побољшања, мерење перформанси има значајну улогу у:

- утврђивању и праћењу успеха у односу на постављене дугорочне циљеве,
- утврђивању прилика за увођење побољшања и
- упоређивању перформансе са унутрашњим и спољашњим стандардима.

Када се утврђује правац стратешких активности потребно је проценити перформансе организације да би се одредило које су то снаге и слабости, као и да би се могао подићи квалитет и продуктивност активности које организација проводи.

Као што је речено, утврђивање перформанси система безбедносног менаџмента се пре свега односи на одређивање његове ефективности и ефикасности. То подразумева и одређивање трошкова који настају приликом функционисања овог система. Ови трошкови морају бити право мерило средстава и рада који се улажу у безбедносне активности. Осим тога, трошкови указују на то колико је безбедност битна руководиоцима, односно утичу на подизање свести о значају безбедности за организацију у целини.

Трошкови улагања у безбедност се, пре свега, могу класификовати као:

- трошкови превенције,
- трошкови процене и
- трошкови услед неког инцидента.

Превентивни трошкови се односе на осмишљавање, имплементацију и одржавање система безбедносног менаџмента. Они су планирани унапред и настају пре него што систем почне да функционише. Под овим трошковима се могу подразумевати:

- одређивање захтева и специфичности производа и/или услуга са аспекта безбедности,
- планирање, односно одређивање планова безбедности, поузданости, надзора и сл.,
- осмишљавање и одржавање система безбедносног менаџмента,
- обука – развијање, припрема и одржавање програма.

Трошкови процене се односе на одређивање угрожености организације. Разматрају се изазови, ризици и претње који долазе како из саме организације, тако и на оне који долазе из њеног ужег и ширег окружења. Овде се могу сврстати трошкови верификације, односно провере усаглашености организационих активности са стандардима безбедности, безбедносне провере потенцијалних клијената и пословних сарадника и сл.

Трошкови који настају услед инцидента се могу поделити на оне који настају услед кварова и инцидената који настају због грешака унутар организације и оне који настају због спољашњих узрока и елементарних непогода. Ови трошкови се односе на улагања у поправку опреме, отклањање штете, опоравак повређених радника и сл.

Улагања у превентивне активности треба да дају одређени поврат, који се може мерити преко:

- смањења трошкова који настају услед инцидента,
- смањења трошкова процене,
- повећања продуктивности запослених,
- повећања поверења од стране клијената,
- повећања удела на тржишту и сл.

Овим путем безбедност директно утиче на повећање профита организације.

Још један модел за утврђивање трошкова безбедносног менаџмента је модел процесних трошкова, који трошкове безбедности дели на:

- трошкове пружања услуга безбедности и прилагођавања тих услуга стандардима и на
- трошкове који настају као последица штете настале услед неког инцидента.

Да би се утврдила, разумела и исплатила улагања у безбедност, потребно је да се испуне следећи услови:

- највише руководство треба да буде заинтересовано за утврђивање стварних трошкова и улагања у безбедност,
- потребно је осмислити систем и менаџерски тим за утврђивање трошкова безбедности који ће анализирати и обавештавати о свим трошковима који су повезани са безбедношћу,
- увести обуку о трошковима који настају због угрожавања безбедности, да би сви запослени постали свесни колико је финансијски неопходно да се уведу побољшања у овој области и
- укључивање свих запослених у безбедносне процесе.

Када се једном uvede систем безбедносног менаџмента, он треба да постане динамичан и да има позитиван утицај на остваривање мисије, дугорочних и краткорочних циљева организације.

Ради мерења перформанси система безбедносног менаџмента, потребно је да мерила буду³⁴⁶:

- сврсисходна, недвосмислена и лако разумљива,
- доступна одређеним тимовима у организацији,
- заснована на поузданим подацима,
- таква да је прикупљање података усклађено са нормалним активностима,
- способна да подстичу побољшања,
- повезана са критичним циљевима и основним покретачима организације.

³⁴⁶ Видети: Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007.

Постоје „четири основна корака за успостављање система мерења перформанси (слика 4.):

- безбедносни циљеви организације се конвертују у жељене стандарде,
- развијају се мерила која омогућавају упоређивање жељених безбедносних стандарда са постигнутим стањем безбедности,
- утврђују се одступања,
- предузимају се корективне акције.“³⁴⁷

Да би се циљеви дефинисали, може се користити Балансирана листа мерила, као што је већ поменуто. Битно је да циљеви буду специфични, мерљиви, достижни, релевантни и правовремени.



Слика 4. *Кораци у мерењу перформанси*
(<http://www.dti.gov.uk/quality/Performance.pdf>)

Када се дефинишу циљеви, потребно је одредити мерење резултата, односно шта је то што се треба мерити да би се утврдило да ли су циљеви испуњени. Уколико је тешко утврдити мерила за циљеве, онда је могуће да су они погрешно постављени или да нису критични за успех система безбедносног менаџмента.

За свако мерило резултата треба поставити питање „који мерљиви чиниоци утичу на овај резултат?“. Када се начини листа, потребно је одабрати мерила која имају највећи утицај на безбедносни менаџмент и рангирати их у складу са тим.

³⁴⁷ <http://www.dti.gov.uk/quality/pdfs/sections/Performance.pdf>

Свака организација треба да развије за њу специфичан скуп мерила, али када је реч о безбедносном менаџменту, они не би требали да се много разликују од једне до друге организације. „Мерила морају обухватати три главне области:

1. ефикасност = (стварни резултати/очекивани резултати)*100 - мерила ефикасности треба да укажу на то да ли су испуњени жељени циљеви. На пример, да ли је било инцидената за које су предвиђене превентивне мере или успостављен систем заштите, број таквих инцидената и сл.,

2. ефикасност = (коришћени ресурси/планирани ресурси)*100 - ово мерило се односи на ресурсе, нпр. раднике, опрему и сл., и указује на менаџмент систем.

3. продуктивност = излаз/улаз, што се може односити на:

а) очекивану продуктивност = очекивани резултати/планирани ресурси и

б) стварну продуктивност = стварни резултати/стварно утрошени ресурси.³⁴⁸

Обично се користе једноставни показатељи, као што је нпр. број успешних интервенција на дан или по запосленом раднику обезбеђења.

Затим, потребно је осмислити процес прикупљања података/извештавања коришћењем следећих корака³⁴⁹:

- успоставити систем за прикупљање података и извештавање,
- осмислити јасне дефиниције,
- успоставити метод за утврђивање тренутног нивоа перформансе,
- направити списак потребних ресурса,
- усагласити системе за форматирање и класификацију података ради агрегације и консолидације,
- утврдити могуће изворе за упоређивање података са системима безбедносног менаџмента у другим организацијама,
- утврдити календар извештавања,
- успоставити улоге и одговорности,
- направити захтеве за обуком,
- усагласити све са заинтересованим странама.

³⁴⁸ <http://www.dti.gov.uk/quality/performance>

³⁴⁹ Више на: <http://www.dti.gov.uk/quality/pdfs/sections/Performance.pdf>

Потом је потребно измерити одступања од жељених нивоа перформанси. Нека мерила и подаци већ постоје, па је препоручљиво да се прво прикупе ти подаци.

Када се прикупе сви потребни подаци, потребно је одредити циљне нивое перформанси и то у краткорочном и дугорочном периоду. Нивои перформансе морају бити достижни и треба да буде могуће да се рашчлане на краће временске интервале, на пример за следећи квартал, месец и сл.

Да би се увео оквир за мерење перформансе система безбедносног менаџмента, потребно је осмислити план са тачно одређеним роковима и додељеним одговорностима³⁵⁰. Када се имплементира овај план и прикупе подаци, могуће је извршити упоређивање са стандардима, поставити нове циљеве и стандарде.

Мерила, циљеви и корективне акције се морају делегирати широм организације, а у процес мерења треба укључити запослене на свим нивоима и обезбедити тимски рад у осмишљавању нових мерила, алата за прикупљање података и корективних активности.

Корективне активности се могу применити приликом упоређивања стандарда и остварених резултата на сваком нивоу менаџмента. Као минимум, овај процес треба да буде скуп достижних и спроводљивих мера, планова, делегираних одговорности и власника.

Критични елементи добрих мерила су слични као код процеса за успостављање система безбедносног менаџмента:

- вођство и посвећеност највишег руководства,
- добро планирање и стратегија имплементације,
- укључивање запослених,
- једноставне мере и процене и
- побољшање контроле.

³⁵⁰ Као што се и мерење перформансе радника врши на основу детаљног описа радног места. О томе више: Sennewald, C. A., *Effective Security Management*, 4th edition, Butterworth-Heinemann, Burlington, 2003.

6. АНАЛИЗА БЕЗБЕДНОСНОГ МЕНАЦМЕНТА У ПРЕДУЗЕЋИМА У РЕПУБЛИЦИ СРБИЈИ - РЕЗУЛТАТИ ИСТРАЖИВАЊА

Приказаним теоријским оквиром истраживања, анализом литературе и нормативно-правне регулативе, постављени су основи за истраживачки део којим се настоји утврдити да ли законски дефинисани оквири и инструменти који су на располагању корпорацијама у Републици Србији функционишу и да ли у њима постоје развијени механизми за мерење учинка безбедносног менаџмента на стање безбедности.

У истраживачком делу смо настојали да утврдимо колико је заправо развијен систем безбедносног менаџмента у пракси, као и да одредимо да ли постоје могућности за увођење новог модела интегралног безбедносног менаџмента и могућности мерења његове ефективности и ефикасности. Заправо, основни циљ истраживачког дела рада јесте да потврдимо основну хипотезу да садашњи ниво организованости и функционисања система за процену ефективности и ефикасности безбедносног менаџмента у организацијама у Републици Србији није адекватан потребама, односно не даје реалне резултате о утицају безбедносног менаџмента на превенцију и ублажавање последица угрожавања безбедности и заштиту организација, свих субјеката, животне средине и културних добара.

Истраживачки инструмент који је примењен у истраживању је *анкетни упитник*, док је квалитативном сегменту истраживања примењен и други истраживачки инструмент – *експертски интервју*. Истраживање је спроведено у периоду од јуна до септембра 2011. године.

У истраживању је примењен једноставан случајни узорак, на основу података Агенције за привредне регистре Републике Србије. Будући да је систем безбедносног менаџмента комплексан, истраживање је рађено на великим привредним друштвима, којих је према регистру Агенције у 2010. години имало 831³⁵¹. Администрација упитника спроведена је као само-администрација, односно, упитник је достављен

³⁵¹ Видети: Агенција за привредне регистре, *Саопштење о пословању привреде у републици Србији у 2010 години*, Београд, 2011, стр. 43.

испитаницима, путем електронске поште, а они су самостално одговарали на питања. Узорком је обухваћено 277, што представља 30% од укупног броја великих привредних друштава. На крају, реализовани узорак је обухватио 75 привредних субјеката, што представља 9% укупне популације или 27% првобитног узорка.

Други значајан инструмент у овом делу био је структурирани интервју. Интервју је, када је то било могуће, обављен са професионално ангажованим и одговорним лицима који се баве наведеном проблематиком, чиме је омогућено да се оствари увид у структуру њихових ставова о различитим димензијама истраживаног феномена. Интервју је обављен са менаџерима безбедности и лицима задуженим за заштиту на раду и заштиту животне средине.

Поред упитника и интервјуа, у овом делу примењен је и метод анализе садржаја, који се односио на анализу годишњих и месечних извештаја о безбедности, заштити на раду и заштити животне средине.

Подаци добијени истраживањем су обрађени стандардним статистичким методама.

6.1. Презентација резултата добијених анализом упитника

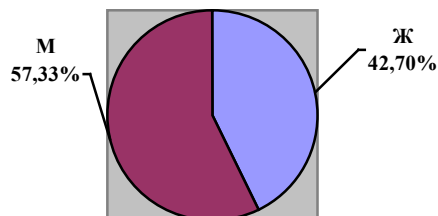
Упитник који је примењен у истраживању структурисан из три дела. Први део јесте идентификациони и састављен је од социо-демографских питања: пол, старост и стручна спрема. Други део односи се на постављена питања у виду скале ставова са утврђеном категоријом, док је трећи део отвореног типа, односно, испитаницима је понуђена могућност да наведу препоруке за унапређење безбедносног менаџмента и корпоративне безбедности.

Одговори на ставке у упитнику су понуђени у два формата: скала процена (Ликертова скала) и дихотомна скала. Већина ставки третирана је Ликертовом скалом са пет утврђених категорија, док је на неколико питања одговор понуђен у форми дихотомне скале (у форми ДА и НЕ).

6.1.1. Социо-демографски подаци

У оквиру питања о социо-демографским подацима утврђени су и систематизовани следећи идентификациони подаци о испитаницима: пол, старост и стручна спрема.

Дистрибуција одговора на питање о полу приказана је на графикону 1.

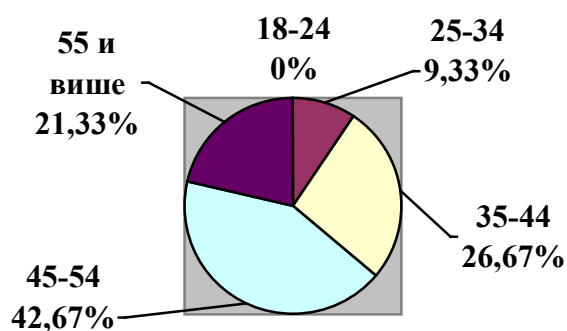


Графикон 1. Заступљеност испитаника по полу

Табела 1. Заступљеност испитаника по полу

Пол	Број испитаника	Заступљеност
Мушки	43	57,33%,
Женски	32	42,70%,
Укупно	75	100%

Реализовани узорак је обухватио 75 испитаника, од којих су 43 или 57,3% испитаника мушког пола, док је 32 или 42,7% испитаница женског пола. Резултати показују полно равномерну структуру испитаника, будући да је близу 50% испитаника мушког и женског пола.



Графикон 2. Заступљеност испитаника по годинама старости

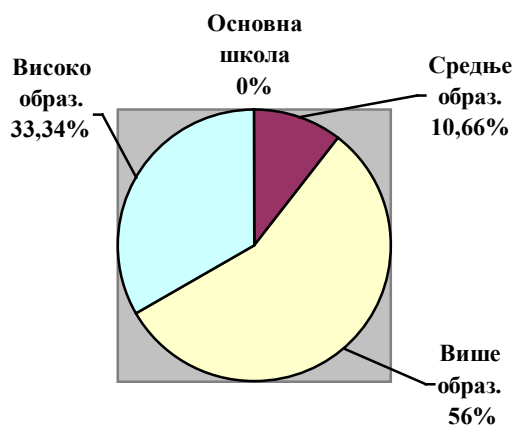
Табела 2. Заступљеност испитаника по годинама старости

Узрасна група	Број испитаника	Заступљеност/процент
18 – 24	-	-
25 – 34	7	9,33%
35 – 44	20	26,67%
45 – 54	32	42,67%
55 и више	16	21,33%
Укупно	75	100%

Мање од 10% испитаника који су попунили упитник припада узрасту од 25 - 34 године, 26,67% испитаника узрасту од 35 - 44 године, 42,67% испитаника узрасту од 45 - 55 година, док 21,33% анкетираних испитаника припада узрасној групи од 55 и више година.

Резултати показују старосно неравномерну структуру испитаника, односно највише је испитаника узраста од 45 - 54 године. То указује на тенденцију да се за људе који воде бригу о безбедности постављају људи са већим искуством. Нарочито, ако се узме у обзир да кумулативно две најстарије узрасне групе (од 45 - 55 и више година) чине 64% од укупног броја испитаника.

Одговор на питање о степену образовања је добијен у свих 75 реализованих упитника. Дистрибуција одговора на питање о степену образовања приказана је на графикаону 3.



Графикон 3. Заступљеност испитаника по степену образовања

Табела 3. Заступљеност испитаника по степену образовања

Степен образовања	Број испитаника	Заступљеност
Основна школа	-	-
Средње образовање	8	10,66%
Више образовање	42	56%
Високо образовање	25	33,34%
Укупно	75	100%

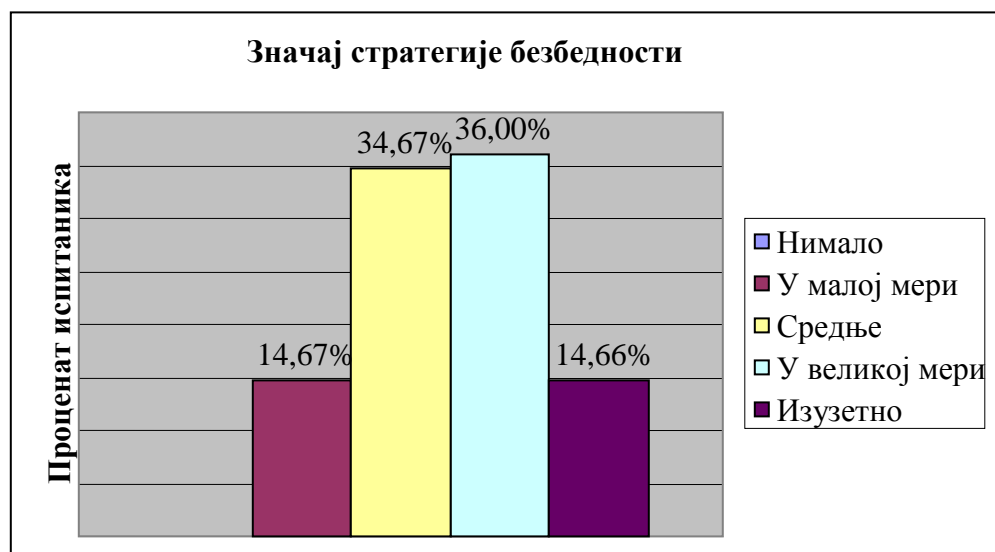
Са графикаона се види да је структура испитаника по образовању различита, почевши од средњег до високог образовања. Највећи број испитаника има више образовање (56%), док високо образовање има 33,34% испитаника. Најмање испитаника (10,66%) има средње образовање. Овакав резултат може бити последица тога што је у прошлости у Републици Србији био мали број факултета који су давали диплому високог образовања из области безбедности и заштите на раду. Ипак, на

основу добијених података (укупно више и високо образовање испитаника чини 89,34%) може се закључити да послодавци сматрају да је образовање битан показатељ оспособљености кадрова који се баве безбедношћу.

6.1.2. Оцена значајности појединих елемената система безбедносног менаџмента

Како се међу најзначајнијим елементима система безбедносног менаџмента наводе јасно одређена стратегија и политика безбедности, безбедносне процедуре и стандарди и безбедносна култура, у упитнику су постављена питања која се односе на оцену значаја ових елемената.

Оцена значаја стратегије безбедности за успешан безбедносни менаџмент је дата у графикону 4.



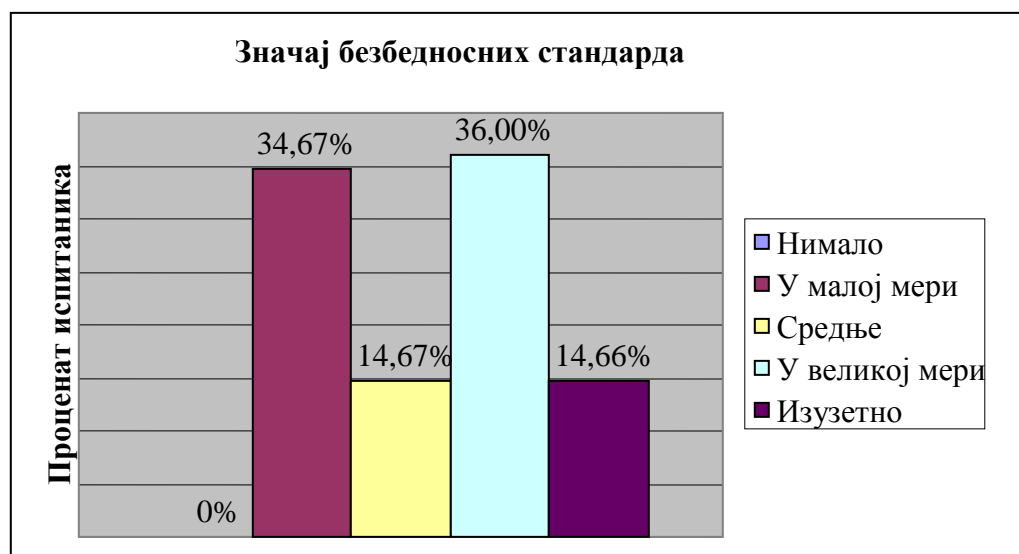
Графикон 4. Значај јасно одређене стратегије безбедности за ефикасност безбедносног менаџмента

На питање о оцени значаја јасно одређене стратегије безбедности за ефикасан и ефективан безбедносни менаџмент одговорили су сви испитаници (75). Изузетно значајним овај елемент сматра свега 14,66% испитаника, док 36% испитаника

сматра стратегију безбедности значајном у великој мери. Од укупног броја испитаника 34,66% испитаника оценило је овај елемент као средње значајан, а 14,66% испитаника сматра да је јасно одређена стратегија безбедности значајна у малој мери. Као што се могло и очекивати, није било испитаника који стратегију безбедности сматрају безначајном.

Будући да је највећи број испитаника оценио стратегију безбедности као средње и у великој мери значајну за успешан безбедносни менаџмент, може се закључити да лица која су запослена на пословима безбедности сматрају безбедносну стратегију као значајну за успешан рад система безбедности. Овакви одговори иду у прилог тези да без стратегије нема ни успешног менаџмента.

Оцена значаја стандарда безбедности је дата у графикаону 5.

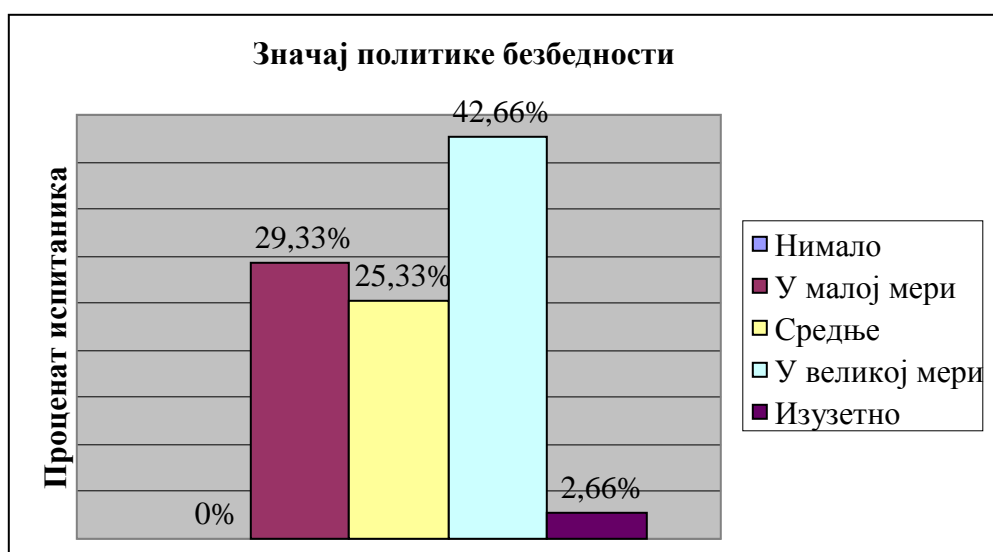


Графикон 5. Значај безбедносних стандарда

Када је у питању значај безбедносних стандарда за успешан рад безбедносног менаџмента, од укупног броја анкетираних који су исказали свој став, 34,67% сматра овај чинилац значајним у малој мери, 14,67% средње значајним, 36% верује да су стандарди безбедности битни у великој мери, док 14,66% сматра да су изузетно битни.

Овакав резултат се може тумачити чињеницом да су стандарди безбедности релативно нова област код нас и да су тек од скоро почели да се примењују. Биће потребно време да се стандарди устале у нашој свакодневној безбедносној пракси, тако да се очекује би у неком наредном испитивању однос ових одговора био знатно већи у корист значаја безбедносних стандарда. Ипак, позитивно је то што међу испитаницима нема оних који сматрају да стандарди нису нимало битни. То указује на чињеницу да ће се безбедносни стандарди примењивати.

Дистрибуција одговора везаних за значај безбедносне политике за успешан рад безбедносног менаџмента је дата у графикону 6.

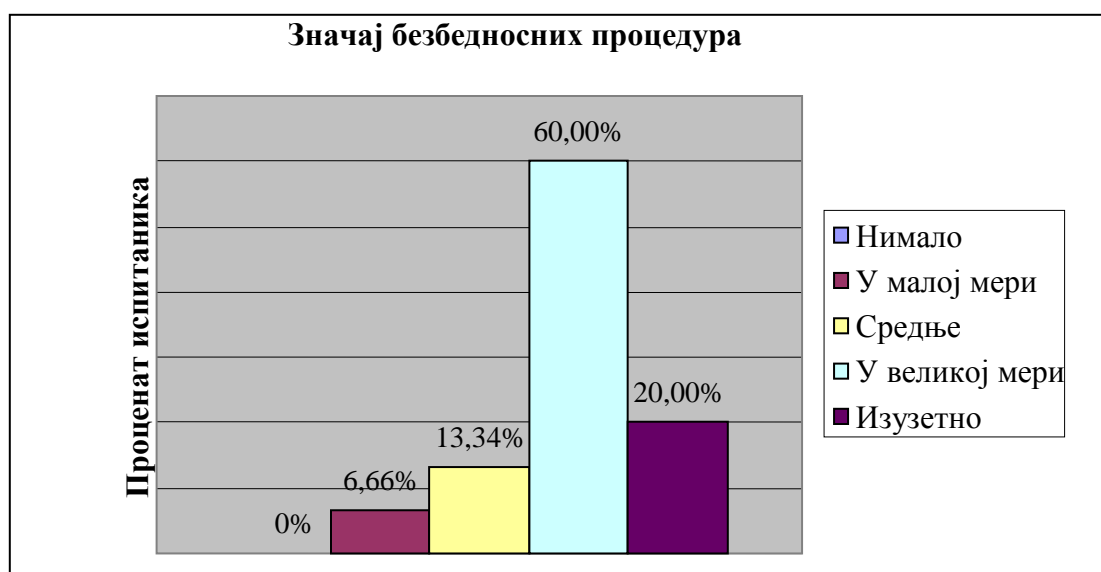


Графикон 6. *Значај политике безбедности за ефикасност безбедносног менаџмента*

На питање о значају политике безбедности за ефикасан и ефективан безбедносни менаџмент одговоре је дало свих 75 испитаника. Највећи број њих (42,66%) сматра да је безбедносна политика битна у великој мери. 29,33% сматра да је она битна у малој мери, а сличан број, односно 25,33% сматра да је средње битна. Свега 2,66% испитаника сматра да је политика безбедности изузетно значајна, док 0% испитаника сматра да није значајна за безбедносни менаџмент.

У сваком случају, одговори на питање о значају политике безбедности за ефикасан безбедносни менаџмент заслужују пажњу јер представљају својеврсно упозорење, будући да 29,33% испитаника сматра да овај инструмент има мали значај за рад безбедносног менаџмента. Додатни проблем у овом погледу представља чињеница да су у интервјуима многи испитаници показали да не схватају сврху безбедносне политике. Треба напоменути да „безбедносна политика представља основне циљеве организације у погледу безбедности, представља основ за успостављање безбедносних стандарда, а при томе утиче на повећање свести запослених у организацији о значају безбедности“³⁵².

Оцена значаја безбедносних процедура за успешан безбедносни менаџмент дата је у графикону 7.



Графикон 7. *Значај безбедносних процедура за ефикасност безбедносног менаџмента*

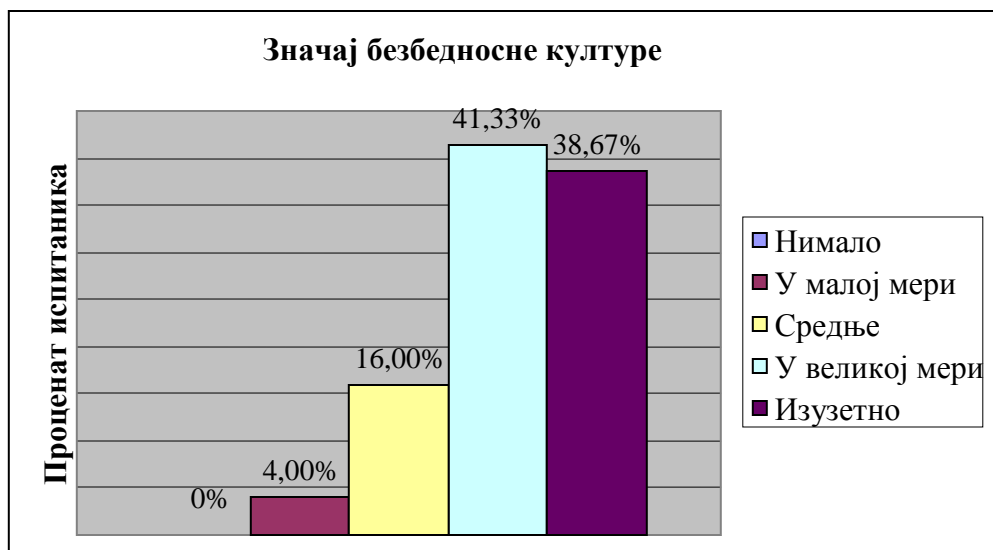
Оцену о значају безбедносних процедура за ефикасност и ефективност безбедносног менаџмента дало је свих 75 испитаника. Као што показује графикон,

³⁵² <http://www.sans.org/security-resources/policies/>

највећи број испитаника (60%) сматра да је овај фактор веома битан. Изузетно битним овај фактор сматра 20% испитаника.

Иако у овом случају доминирају позитивне оцене, приметно је да чак 20% испитаника изнело другачији став. То није добро, с обзиром на значај безбедносних процедура за ефикасност и ефективност безбедносног менаџмента. Треба имати на уму да су безбедносне процедуре сама суштина функционисања система безбедности уопште и да без квалитетних процедура нема ни квалитетног безбедносног менаџмента.

На графикону 8. је дата расподела одговора везаних за значај безбедносне културе за успешан рад безбедносног менаџмента.

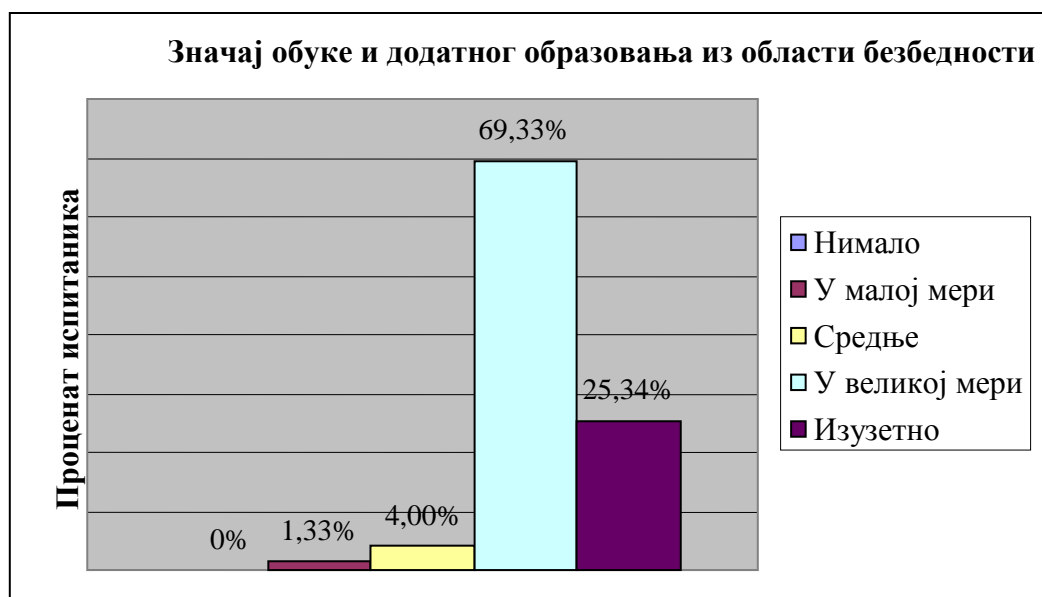


Графикон 8. Значај безбедносне културе за ефикасност безбедносног менаџмента

На питање о оцени значаја безбедносне културе одговор је дало свих 75 испитаника. Изузетно значајном безбедносну културу сматра 38,67% испитаника, док је 41,33% испитаника оценило значајном у великој мери. Свега 4% испитаника сматра да је безбедносна култура у малој мери битна, а 16% је сматра средње значајном. Позитивно је то што није било испитаника који је сматрају небитном.

Овакви одговори указују да веома велики број стручњака који се баве безбедношћу у привредним организацијама у Републици Србији има високо развијену свест о безбедности. Сам став да безбедносна култура игра важну улогу у безбедносном менаџменту је доказ да постоји воља да се она даље развија и шири међу запосленима. Међутим, интервјуи који су спроведени са лицима запосленим на пословима безбедности показују мало другачији резултат. Односно, иако сматрају да је култура битна, врло мало тога се ради у конкретним ситуацијама да би се она развијала и неговала.

Оцене значаја тренинга и образовања из области безбедности за успешан безбедносни менаџмент су дате у графикону 9.



Графикон 9. Значај обуке и додатног образовања за успешан безбедносни менаџмент

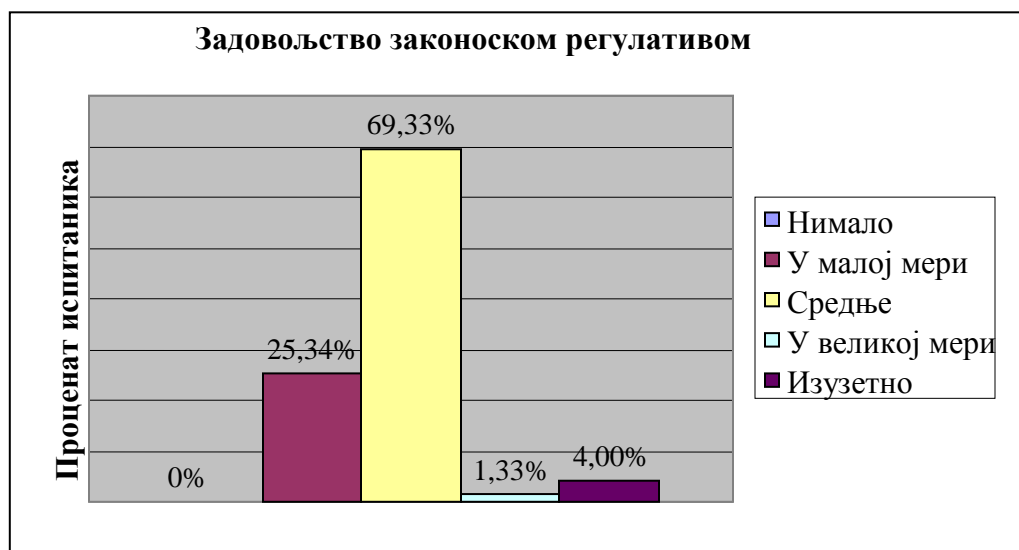
Као што се из графикана може видети, највећи број испитаника (69,33%) сматра да су обуке и образовање у великој мери битни за рад безбедносног менаџмента. Ако се узме у обзир да 0% сматра да додатно образовање и обука нису битни, 1,33% да су битни у малој мери и 4% да су средње битни, јасно је да је свест стручњака из области безбедности о овом фактору на високом нивоу. Иако свега око

једне четвртине испитаника (тачније 25,34%) сматра овај елеменат изузетно битним, сматрамо да је овакав резултат позитиван.

6.1.3. Оцена задовољства елементима система безбедносног менаџмента

Један број питања у упитнику се односио на то колико су запослени на пословима безбедности задовољни тренутним стањем система безбедности у њиховој организацији. На следећим графиконима су приказани њихови одговори.

Што се тиче задовољства законском регулативом која уређује систем безбедности и заштите на раду, оцене су дате у графикону 10.

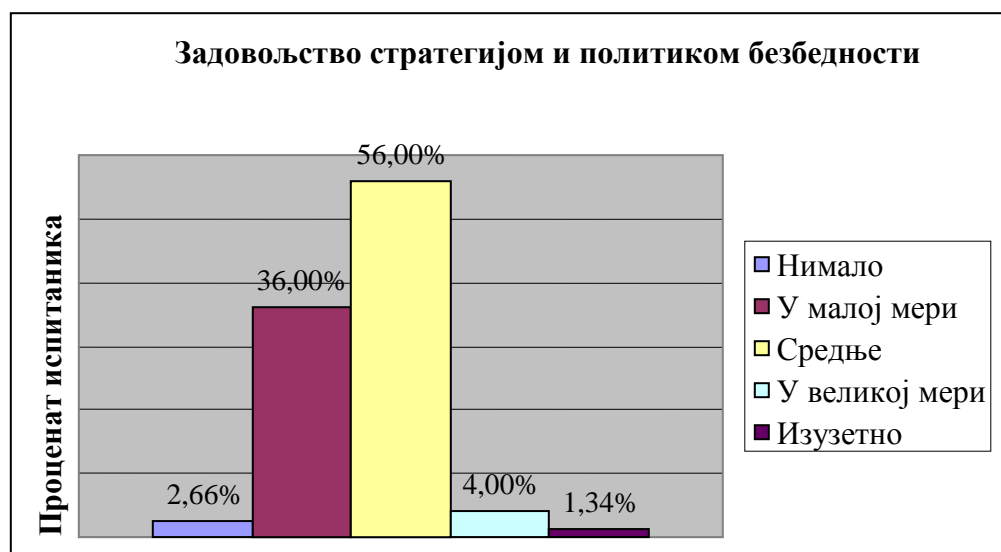


Графикон 10. *Задовољство законском регулативом из области безбедности и заштите на раду*

Највећи број анкетираних особа сматра да је постојећа законска регулатива из области безбедности и заштите на раду средње развијена (69,33%), док је око четвртине њих у малој мери задовољно (25,34%). Занемарљив је број оних који су у великој мери задовољни постојећом регулативом (1,33%), нема оних који нису уопште задовољни, а 4% оних који су изузетно задовољни.

Треба напоменути да је законска регулатива из области безбедности и заштите на раду код нас у великој мери усклађена са законима у развијеним земљама и Европској унији, само што постоји проблем њеног спровођења. Као и код безбедносних стандарда, то је још увек релативно нова област, па би се у неком наредном периоду могли очекивати другачији резултати.

Задовољство постојећом стратегијом и политиком безбедности у организацији је дато у графикону 11.

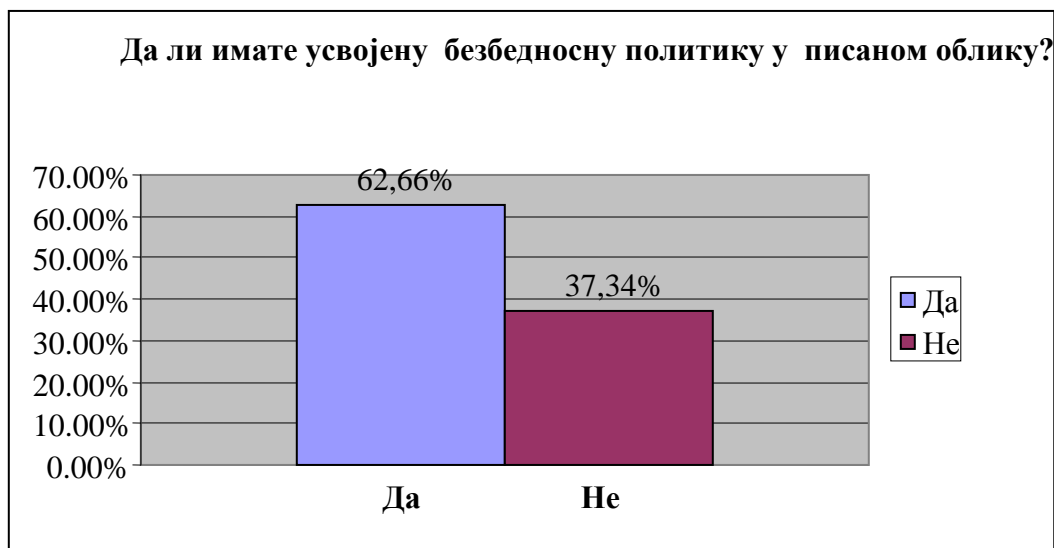


Графикон 11. *Задовољство стратегијом и политиком безбедности*

Највећи број испитаника је у средњој (56%) и у малој (36%) мери задовољно постојећим стратегијама и политикама безбедности. Уколико се узме у обзир значај који се придаје овим елементима, можемо рећи да су мање-више оцене конзистентне. Односно, стратегија и политика безбедности су развијене у организацијама отприлике у истој мери у којој се сматрају значајним.

Ипак, забрињава то да је само 1,34% испитаника у потпуности задовољно овим елементима, а да ипак 2,66% није нимало задовољно њима. Свега 4% сматра да су у њиховој организацији стратегија и политика безбедности развијене у великој мери.

Одговори о постојању безбедносне политике у писаном облику у испитаним организацијама су дати у графикону 12. Као што се види, 62,66% испитаника је дало потврдан одговор на ово питање, а 37,34% негативан.

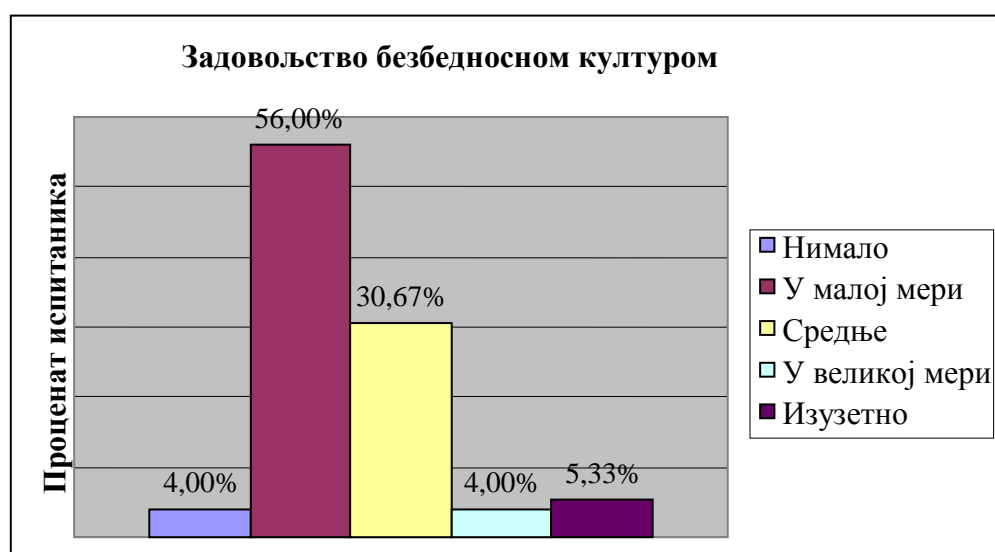


Графикон 12. Процент организација које имају безбедносну политику у писаном облику

Графикон показује да већина од испитаних организација ипак схвата значај безбедносне политике, јер када је она дата експлицитно у писаној форми много јасније указује на посвећеност организације безбедности. Интервју са стручњацима из области безбедности је указао да постоји тенденција да се у организацијама у којима већ не постоји уводи политика у писаном облику, али је било и оних који уопште нису разумели питање. Односно, показало се да један број организација о томе уопште не размишља. Морамо напоменути да је ово забрињавајуће, с обзиром на оцене значаја безбедносне политике (чак 42,66% испитаних сматра да је политика у великој мери значајна).

Дистрибуција одговора везаних за оцене задовољства постојећом безбедносном културом у организацији су дате у графикону 13. Као што се може видети, чак је 56% испитаника у малој мери задовољно ставовима и нормама

понашања у вези са безбедношћу, а који владају у њиховој организацији. Око трећине испитаника, односно 30,67% је оценило постојећу безбедносну културу у организацији као средње развијену, 5,33% сматра да је изузетно развијена, а по 4% да није нимало или да је развијена у великој мери.



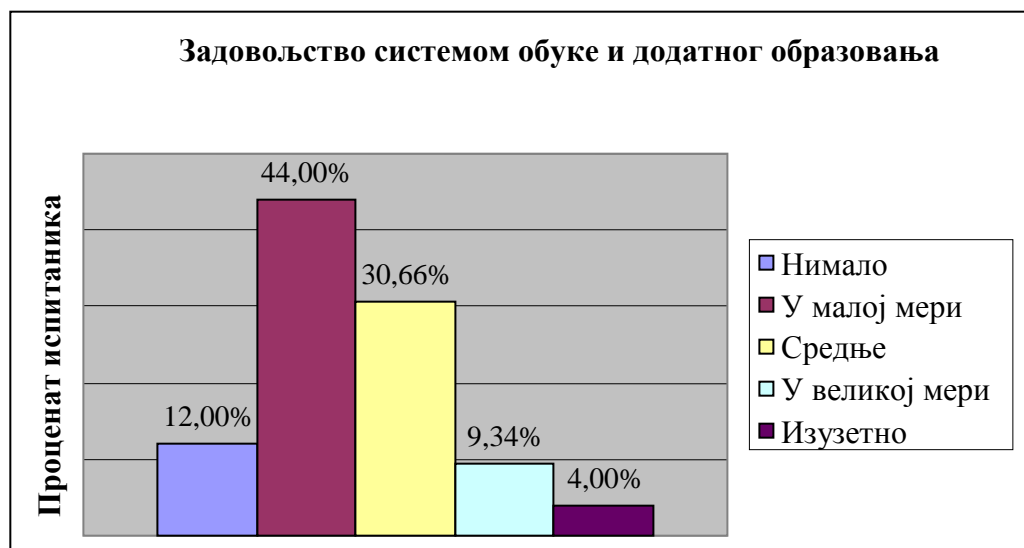
Графикон 13. *Задовољство безбедносном културом*

Овакви подаци су забрињавајући, с обзиром на то да највећи број испитаника безбедносну културу сматра у великој мери или изузетно важном за успешан безбедносни менаџмент. Приликом интервјуа са појединим стручњацима за безбедност, дошло се до закључка да чак ни овако лоша слика стања није реална. Наиме, дешавало се да одговори указују на то да у појединим организацијама уопште не постоји свест о организационој, а камо ли о безбедносној култури.

Сматрамо да је то последица релативно застарелог начина размишљања који је, на жалост, у великој мери присутан у привредној сфери Србије. Дакле, код нас постоје кадрови који још увек нису упознати са значајем културе за само пословање организације, људи који нису имали обуку из менаџмента и нису компетентни да одговоре савременим пословним изазовима. Самим тим, да се закључити да они још увек немају развијену свест о томе да се и безбедност може посматрати системски и

да је безбедносни менаџмент у великој мери неопходан и саставни део стратешког, али и оперативног менаџмента.

Слика ставова о томе какав је постојећи систем обуке и професионалног усавршавања у испитаним организацијама је дата у графикону 14.



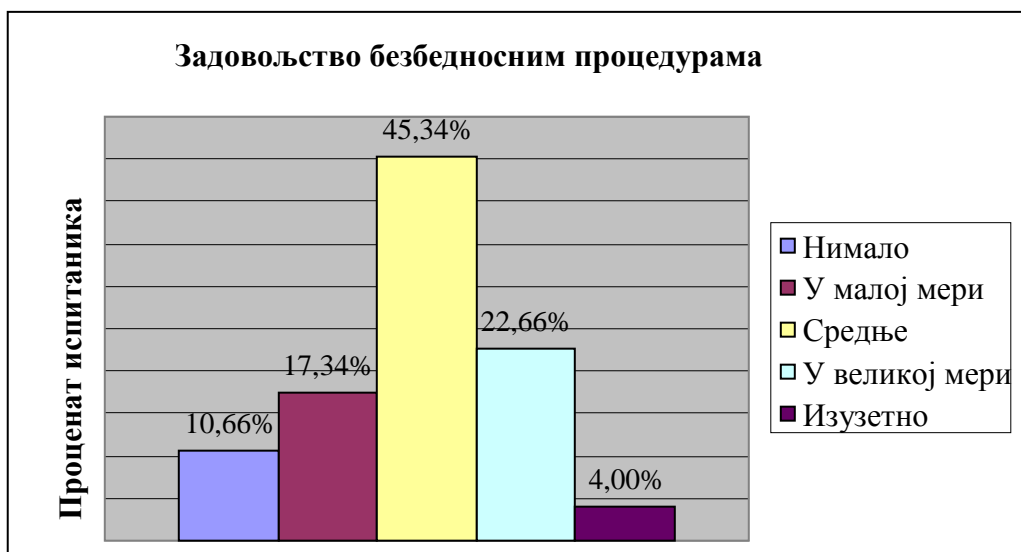
Графикон 14. *Задовољство системом за обуке и додатно образовање из области безбедности*

С графикана се може видети да највећи број испитаника (44%) је у малој мери задовољно постојећим системом обуке и професионалног усавршавања из области безбедности у њиховој организацији. Ако се узме у обзир да 12% испитаника сматра да је тај систем скоро потпуно запостављен (кумулативно два најслабија одговора дају 56% испитаника), долазимо до закључка да је обука релативно занемарен део безбедносног менаџмента у привреди Србије. Ипак, 30,66% испитаника је средње задовољно, 9,34% у великој мери, а свега 4% изузетно овим системом, па то указује да се полако поклања пажња овој области.

Интервју са појединим лицима задуженим за безбедност у испитаним организацијама је указао на тенденцију да се из године у годину повећава број

обавезних семинара и тренинга из области безбедности. То ублажава слику добијену анкетом. Тако да би могли, ако би се анкетирање поновило у неком наредном периоду, очекивати позитивније одговоре испитаника. Нарочито ако се узму у обзир одговори везани за значај обуке и тренинга за безбедносни менаџмент.

Расподела одговора везаних за задовољство испитаника постојећим безбедносним процедурама у организацији је дата у графикону 15.



Графикон 15. *Задовољство безбедносним процедурама*

Од свих анкетираних, највећи број или 45,34% сматра да су безбедносне процедуре у њиховим организацијама у средњој мери развијене. Иако је 22,66% оних који су у великој мери задовољни и 4% оних који су изузетно задовољни постојећим безбедносним процедурама, забрињавајуће је што 10,66% није нимало задовољно и што је 17,34% у малој мери задовољно њима.

Наиме, безбедносне процедуре представљају начин на који се безбедност спроводи и реализује у пракси. Оне су нарочито битне у кризним ситуацијама и јако је важно да буду у потпуности разумљиве свим запосленим. Сматрамо да када су у питању безбедност живота и здравља запослених и животне средине, као и имовине предузећа, толеранција мора бити нула. То значи да се и безбедносне процедуре

морају много више разрадити и њихов смисао и значај морају бити потпуно јасни свим људима који раде у било којој организацији.

6.1.4. Оцена финансијских показатеља рада система безбедносног менаџмента

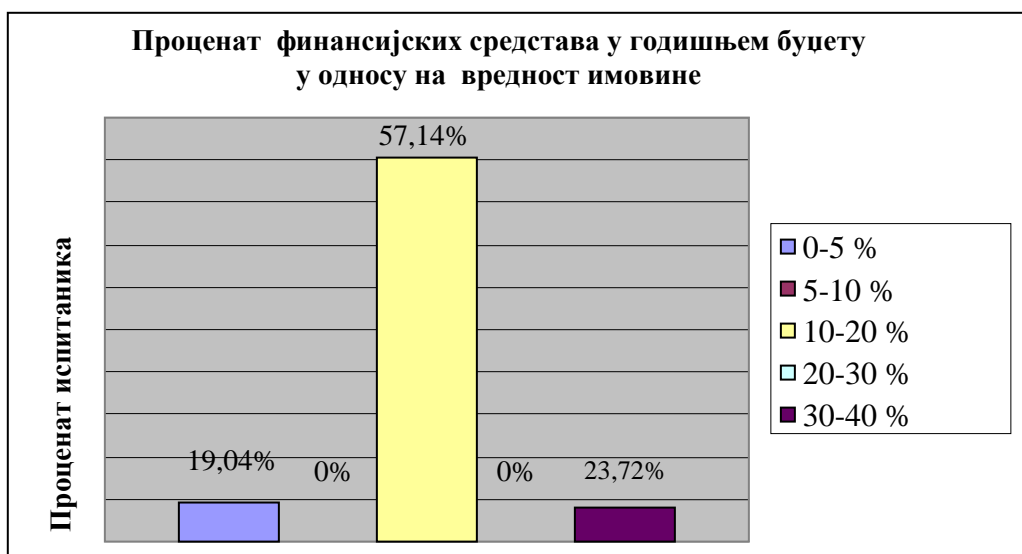
Што се тиче истраживања финансијских показатеља рада безбедносног менаџмента, добијени резултати се не могу сматрати репрезентативним.

Наиме, веома мали број испитаника (21 од 75) је дао одговор на ова питања. Основни аргумент за овакав став је био то да су: финансијска улагања у систем безбедности, вредност опреме која постоји и која треба да се набави, као и издвајања за плате стручњака и особља које се бави питањима безбедности заправо поверљиви подаци. Поред тога, велики број испитаних једноставно не располаже датим подацима. Са становишта овог рада, то се сматра једним великим недостатком, зато што људи који се баве безбедносним менаџментом не могу проценити сопствени утицај у целокупном предузећу ако не знају колика је укупна вредност имовине коју штите.

Додатни проблем у овом погледу представља и то што систем безбедности, како је дефинисан у овом раду, у испитаним предузећима не постоји. Односно, службе и послови безбедности су подељене на различите делове, тако да се ни из финансијских извештаја не може јасно одредити тачна сума средстава која се за њих издваја.

Међутим, на основу оно мало добијених одговора и анализе доступних финансијских извештаја, дошли смо до следећих закључака, који се могу видети у графиконима 16., 17. и 18.

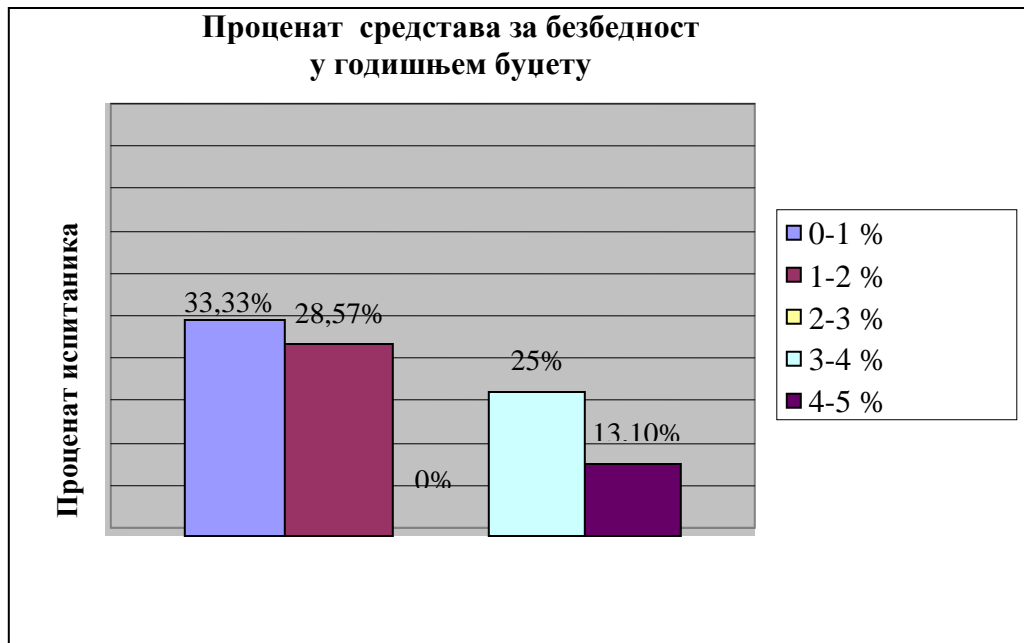
Процент финансијских средстава у годишњем буџету у односу на вредност имовине предузећа је приказан у графикону 16.



Графикон 16. *Однос средстава у буџету и укупне
вредности имовине (у процентима)*

Као што се може видети, највећи број испитаних предузећа издваја средства за годишњи буџет у вредности између 10 и 20% од укупне вредности имовине. Овај показатељ, сам по себи, нема неки посебан значај за анализу безбедносног менаџмента. Али је од значаја када се узме у обзир проценат средстава издвојених за безбедност у годишњем буџету.

Процент средстава издвојених за безбедност на годишњем нивоу у односу на средства из буџета је дат у графикону 17.



Графикон 17. Процент средстава за безбедност у
годишњем буџету (у процентима)

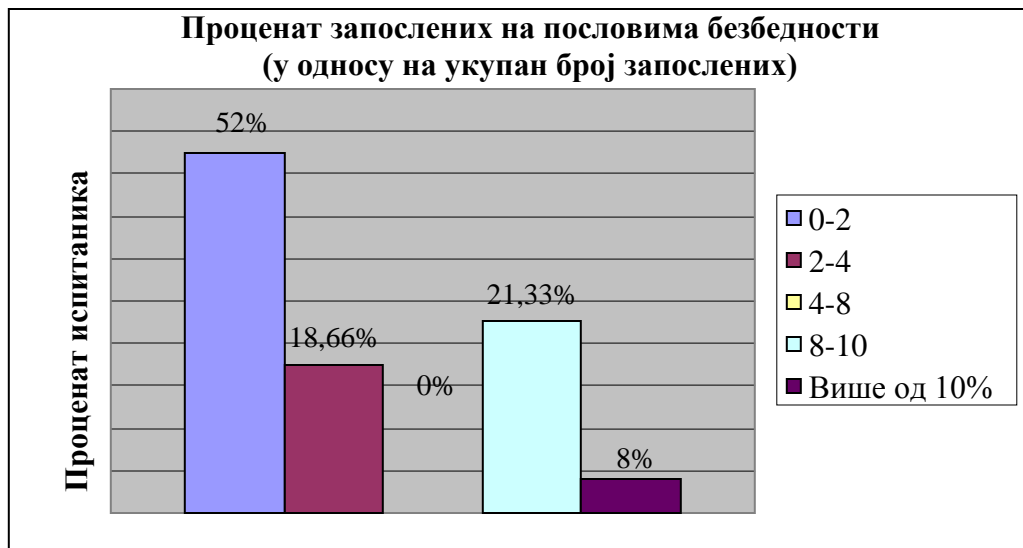
Као што се види у графикону, око трећине испитаника (33,33%) улаже мање од 1% средстава из годишњег буџета у безбедност. Једна четвртина испитаника (25%) улаже између 3 и 4 процента средстава из буџета за безбедност, 13,10% улаже од 4-5%, а 28,57% улаже од 1 до 2 процента ових средстава. Из графикона се може закључити да највећи број испитаника издваја минимална средства за безбедност и заштиту.

Даљом анализом упитника, дошли смо до закључка да она предузећа која издвајају већа средства за буџет и која имају већу имовину издвајају и већа средства за безбедност и заштиту. То се могло очекивати, с обзиром да већа вредност имовине тражи и већа улагања за превенцију могуће штете.

Упитник је садржао и питања која се односе на износ штете (у динарима) која је настала у предузећима у претходних годину дана. Морамо напоменути да је веома мали број испитаника дао одговор на ово питање. Делимично, разлог за то је што су испитаници сматрали да је и то поверљив податак, а делимично што једноставно

нису желели да дају одговор. Претпостављамо да је у питању жеља да се о организацији и свом послу да лепша слика. Међутим, оно мало одговора које смо добили, указује да штете ипак има. Према тим подацима, штета је углавном минимална, а највећа штета настаје у пожарима. Тако смо добили податак да је у једном предузећу укупна штета настала у једном пожару износила 100% свих годишњих средстава која се за безбедност издвајају из буџета. Наравно, то је био усамљен случај и добили смо информацију да се такви инциденти дешавају веома ретко. Највећи број предузећа има одличан систем противпожарне заштите са сензорима и алармима, тако да се велики број пожара открије на време, пре него што направи неку већу штету. Поред тога, из добијених одговора се могло закључити да је највише инцидената на које је систем безбедности успешно реаговао везано за физичку заштиту објеката. Из интервјуа се могло закључити да постоји прилично добра сарадња са представницима МУП-а, тако да је највећи број провалника уредно изведен пред лице правде. Самим тим, из године у годину је и мањи број провалних крађа.

Сматрамо да је за ову анализу индикативан и податак о томе колико је људи запослено на пословима безбедности, будући да и средства која се издвајају за зараде запослених на тим пословима представљају улагање у безбедност. Процент запослених на пословима безбедности у односу на укупан број запослених је дат у графикону 18. Овде треба напоменути да постоје организације које за послове безбедности ангажују специјализована предузећа за област безбедности и заштите, а у својој организацији немају уопште лица која се тиме баве. Оваква улагања се у буџету сврставају у остале трошкове. Код њих је одговор о броју запослених на пословима безбедности био 0. То, дакле, не значи да оне не воде рачуна о заштити, већ да послове безбедности обављају путем уговорних активности („аутсорс“ активности).



Графикон 18. *Процент запослених на пословима безбедности*
(у односу на укупан број запослених)

Као што се види у графикону, највећи број испитаних предузећа (52%) има минималан број запослених на пословима безбедности. Морамо напоменути, да у та предузећа спадају и она која уговорним односом ангажују друге организације за обављање тих послова. Ипак, 21,33% испитаних предузећа има између 8 и 10% запослених на пословима безбедности. Свега 8% има више од 10% запослених који се баве безбедношћу, а 18,66% има од 2 до 4% запослених на тим пословима.

Ако се узме у обзир графикон улагања у безбедност на годишњем нивоу, морамо рећи да је овај резултат прилично у сагласности са њим. Односно, можемо закључити да улагања у безбедност из годишњег буџета у највећој мери иду за зараде запослених, док се у саму опрему улаже мање.

6.2. Дискусија резултата добијених истраживањем

На основу резултата добијених анализом упитника и одговора које смо добили приликом интервјуа, дошли смо до неких битних закључака. Иако су поједини безбедносни послови у потпуности обухваћени обавезујућим законским прописима, у Републици Србији је свест о корпоративној безбедности и безбедносном менаџменту још увек на незавидном нивоу.

Генерално гледано, послови у оквиру правних лица у Републици Србији, а који се односе на безбедност и заштиту се могу поделити на:

- послове физичког обезбеђења,
- послове техничког обезбеђења,
- послове заштите здравља на раду,
- послове противпожарне заштите,
- послове заштите животне средине и
- послове заштите информационих система.

Начин на који су груписани ови послови зависи од многих фактора, као што су природа делатности, величина предузећа, законски прописи, локација у којој се организација налази и сл. Поједини од ових послова су у потпуности регулисани законима и усвојеним стандардима. То се нарочито односи на заштиту здравља и безбедности на раду и противпожарну заштиту. Остали послови су више-мање препуштени самим организацијама и оне их конципирају у складу са сопственим потребама. У највећој мери као додирна тачка између њих представља систем ФТО, који се углавном своди на физичко обезбеђење (односно, присуство људи који врше контролу и надзор проласка). Физичко обезбеђење је у већим организацијама добро технички опремљено – сигурносним камерама, механичком заштитом и сл.³⁵³, тако да се може рећи да је интеграција самог ФТО прилично добра. У великој мери је то последица тога што је у последње време опрема лако доступна и релативно

³⁵³ Видети: Gouin, B., *Security Design Consulting*, Elsevier Inc., Burlington, 2007.

јефтина³⁵⁴, као и тога што је усвојен стандард услуга приватног обезбеђења. Међутим, овај стандард је још увек у фази увођења и не може се рећи да је заступљен у већини организација у Републици Србији. То значи да велики утицај на начин организовања послова безбедности има највише руководство.

Чињеница је да је руководство у већини организација у Републици Србији усмерено на само пословање и постизање резултата, а послови безбедности су прилично занемарени³⁵⁵. Руководству се једном месечно или једном у 6 месеци шаљу безбедносни извештаји, или се шаљу извештаји у случају неког инцидента. То је заправо једина веза менаџера безбедности са топ менаџментом. Повратне информације ретко да има.

Безбедносни менаџмент, у смислу како је овде дефинисан, скоро да и не постоји. Увођење система интегрисаног безбедносног менаџмента би се могло спровести и он би представљао управљачки центар који обухвата све наведене безбедносне послове. Тиме би се пословима безбедности поклонила дужна пажња, а стандарди и регулативе које се односе на поједине области би тиме постали у великој мери разумљиви и примењени на послове који нису покривени обавезним прописима (већ је поменут метод *Benchmarking*, који би могао послужити за „пресликавање“ појединих принципа са једних на друге послове безбедности).

Сваки од ових послова је заступљен у већини организација, па се сходно томе и врши њихова контрола, надзор и ревизија. У ту сврху се уводе поједини индикатори, односно показатељи успешности обављања појединих послова. Врло често се послови заштите од пожара групишу са ФТО, будући да техничко обезбеђење углавном обухвата и противпожарне сензоре и аларме³⁵⁶. Међутим, у неким организацијама је посао заштите од пожара груписан са пословима заштите животне средине. Што се тиче заштите животне средине, послови су углавном

³⁵⁴ Нарочито су значајни интегрисани видео системи за надгледање. О томе више: Bragdon, C., *Transportation Security*, Butterworth-Heinemann, Boston, 2008.

³⁵⁵ Немаран став према безбедности, заштити на раду и заштити животне средине није само пракса у Србији. О томе више: Taylor, B., *Effective Environmental Health and Safety Management Using the Team Approach*, John Wiley & Sons, Inc., Hoboken, 2005.

³⁵⁶ Више о противпожарној заштити видети: Coleman, R. J., *Opportunities in Fire Protection Services Careers*, McGraw-Hill, New York, 2003.

повезани са заштитом безбедности и здравља на раду. Као што је већ речено, то у највећој мери зависи од природе делатности. Организације које се баве производњом запаљивих и отровних супстанци, више пажње поклањају противпожарној заштити и заштити безбедности и здравља на раду, као и заштити животне средине. Организације које у свом опсегу деловања имају више заступљено електронско пословање, већу пажњу поклањају заштити информационих система, док организације чији је основни домен пружање услуга, поклањају већу пажњу физичкој заштити, због имиџа и стварања поверења код клијената. У Републици Србији постоји и велики број организација које су у иностраном власништву или су оријентисане ка западном тржишту, тако да није редак случај да се у њима примењују стандарди и прописи који су важећи у државама из којих потиче власник или су неопходан услов за извоз у те земље. Треба још напоменути и то да постоје организације које немају сопствене службе безбедности, већ ангажују правна лица која су регистрована за пружање датих услуга – „аутсорсинг“. Најчешће су то послови физичког обезбеђења, али и послови противпожарне заштите и заштите безбедности и здравља на раду. У великој мери је заступљена сарадња са јединицама МУП-а, нарочито у случају противпожарне заштите и приликом транспорта вредности.

7. МОДЕЛ МОГУЋЕГ СИСТЕМА ЗА ПРОЦЕНУ ЕФИКАСНОСТИ И ЕФЕКТИВНОСТИ БЕЗБЕДНОСНОГ МЕНАѢМЕНТА

Сврха постојања неке организације је изражена у њеној мисији, преко које се препознаје основна делатност, а у њој су садржани и сви захтеви свих заинтересованих страна. Мисија се преводи у циљеве, након чега се дефинишу и процеси и активности који су неопходни за њихово постизање.³⁵⁷ Степен до кога су испуњени циљеви, а тиме и сама мисија, утврђује се мерењем и упоређивањем са постављеним циљем. Поређење остварених и утврђених вредности перформанси неког процеса или саме организације са жељеном вредношћу може довести и до измене саме мисије организације.

Термин перформанса се преводи, између осталог, као учинак или успех. Дакле, перформанса процеса се може превести као учинак или успех процеса, а он се мора изразити неком величином. Мерење представља скуп радњи с циљем утврђивања вредности неке величине. Мерење перформанси процеса, сходно томе, може да се односи на утврђивање вредности или учинка тог процеса. Највећи број мера перформанси се може изразити преко следећих шест група: ефикасност, ефективност, квалитет, рокови, продуктивност и безбедност. Са аспекта овог рада, прихватамо дефиницију коју су дали Гунасекаран и Кобу, 2007.: „мерење перформанси се може дефинисати као процес квантификовања ефикасности и ефективности акције“³⁵⁸. У литератури постоје многи други термини, који се свде на синониме термина мерила перформанси, а то су индикатори успешности процеса, индекси перформанси, параметри и др. Перформансе се дефинишу на различитим нивоима у организацији и то на организационом, нивоу процеса и индивидуалном

³⁵⁷ Видети: Coda, V., *Entrepreneurial Values and Strategic Management*, Palgrave Macmillan, Chippenham, 2010.

³⁵⁸ Gunasekaran, A. and Kobu, B., Performance Measure and Metrics in Logistics and Supply Chain Management: A Review of Recent Literature (1995-2004) for Research and Applications, *International Journal of Production Research*, 45(12), 2007. p. 2821.

нивоу. Битно је да индикатори успешности процеса буду прецизно дефинисани и међусобно усклађени у циљу добијања реалне слике стања у организацији³⁵⁹.

7.1. Успостављање система за мерење перформанси

Први корак у успостављању система мерења перформанси, јесте утврђивање заинтересованих страна и њихових захтева.³⁶⁰ Последње деценије прошлог века, многи аутори су покушали да примене избалансирани приступ за утврђивање успешности процеса. Такав приступ подразумева да се пажња, поред задовољства корисника, усмери на све заинтересоване стране, односно власнике, запослене, испоручиоце итд. Најпознатији модел који је настао у то време је Балансирана листа мерила (*Balanced Scorecard*). Када је реч о безбедносном менаџменту, заинтересоване стране су у најопштијем случају, пре свега власници и сви запослени, али и корисници услуга, уколико је реч о услужним предузећима. Јасно је да су заинтересоване стране различите од организације до организације, али у табели 4. је дат списак могућих заинтересованих страна, који би могао важити у општем случају. Један од највећих изазова у одређивању успешности организације или процеса, јесте одлука о томе шта треба мерити, на који начин и колико често. Чињеница са којом се сви слажу, јесте да треба мерити процесе који су кључни или базни. Уколико процес дефинишемо као скуп међусобно повезаних активности који улазне елементе претварају у излазне, онда су излазни елементи кључних процеса извештаји и процене безбедности, а улазни планови, циљеви, уложена средства и сл.³⁶¹

³⁵⁹ Видети: Conrow, E. H., *Effective Risk Management: Some Keys to Success*, 2nd ed., American Institute of Aeronautics and Astronautics, Inc., Reston, 2003.

³⁶⁰ Видети: Радовић, М., Голубовић, Д., *Поступак мерења перформанси процеса*, *SymOrg 2010*, ISSU, Београд.

³⁶¹ Видети: исто.

Табела 4. Пример заинтересованих страна у СБМ

Р.б.	Заинтересоване стране	Захтеви
1.	Власници	Избећи губитке, смањити штету, повећати ефикасност
2.	Запослени (менаџери безбедности, руководиоци, радници обезбеђења, производни и услужни радници, администрација)	Избећи повреде, безбедносне инциденте
3.	Корисници (производа и услуга)	Безбедност производа и услуга
4.	Држава (Влада, министарства, агенције, локална самоуправа)	Безбедност животне средине
5.	Остале заинтересоване стране (пословни партнери, снабдевачи и сл.)	Захтеви осталих заинтересованих страна

Вредност, односно мера перформансе, састоји се од броја и мерне јединице. Свака мерна јединица мора бити одређена дефиницијским једначинама и факторима пропорције за дату величину. Односно, мера перформансе је вредност величине којом се изражава учинак или успешност организације, процеса, ресурса или запосленог. При томе, мерна јединица представља вредност неке величине за коју је договором утврђено да има вредност један³⁶². Број показује величину нечега (профита, прихода, расхода, производа итд.) и представља одговор на питање „колико“, а мерна јединица даје значење броју, односно даје одговор на питање „шта“ „чега“ (динара, комада, итд.). Мера перформансе је увек у вези са циљем, који представља жељено стање, односно жељену вредност перформансе. Вредност перформансе се може изразити кроз једнодимензиону мерну јединицу (час, долар, број извештаја, број грешака и сл.) које уобичајено представљају основна мерила

³⁶² Видети: Пешалјевић, М., *Инжењерске комуникације и логистика*, Факултет техничких наука, Нови Сад, 1995.

неког процеса. Чешће се употребљавају вишедимензионе јединице мере. Оне се изражавају као рацио две или више основних јединица.

Мера перформансе је показатељ степена испуњености циља. Циљ перформансе, или стандард, представља жељено стање или жељену вредност или жељену меру перформансе и изражен је истим мерним јединицама. Јасно је да је циљ свих активности безбедносног менаџмента да се деси што мање појава угрожавања безбедности (ради једноставности, једним именом ће се називати безбедносни инциденти), а штета од таквих појава треба да се избегне или у најгорем случају, треба да буде минимална. У табели 5. је дат пример циљева система безбедносног менаџмента у општем случају. Наравно, овај списак би могао да се прошири и прилагоди конкретној организацији, или делу организације.

Табела 5: *Пример циљева система безбедносног менаџмента*

Р.б.	Ознака и назив мерила перформанси СБМ	Мерна јединица	Циљ	Начин рачунања	Динамика мерења
1.	33.02.01 Укупан број безбедносних инцидентата месечно	(1)	0	Сума броја инцидентата	Месечно
2.	33.02.02 Процент инц. на које је успешно одговорено	(%)	100%	Број инцидентата на које је успешно одговорено/Ук. број	Месечно

				безбедносних инцидената	
3.	ЗВ.01.01 Укупна штета настала због безбедносних инцидената	(%)	0 (%)	Штета настала због безбедносних инцидената/ Укупна вредност имовине организације	Месечно
4.	33.02.03 Број пожара месечно	(1)	0	Сума броја пожара	Месечно
5.	33.02.04 Број провалних крађа месечно	(1)	0	Сума броја крађа	Месечно
6.	33.02.05 Просечно време одговора на инцидент	(час)	<8	Просек (време реакције на инцидент-време појаве инцидента)	Сваки инцидент
7.	ЗВ.01.02 Штета настала због пожара	(%)	0 (%)	Штета настала од пожара/Укупна вредност имовине организације	Месечно

Након дефинисања заинтересованих страна, њихових захтева, перформанси и циљева, потребно је установити критичне и кључне процесе које треба мерити. Овај корак је од кључне важности за успех мерења перформанси. Једно од решења је да се

идентификује листа приоритетних, кључних и критичних процеса. Уобичајено је да се мере они процеси који су најзначајнији за кориснике, како интерне, тако и екстерне, како би се испунили њихови захтеви. Приоритетни процеси су они који из одређених разлога (закони или стандарди) уживају хитно разматрање. Критични процеси су они који при свом одвијању изазивају проблеме у погледу квалитета, трошкова или рокова, а кључни они од којих у највећој мери зависи испуњење циљева организације.³⁶³

Након одређивања који процеси ће бити мерени, потребно је идентификовати активности у којима ће се вршити мерење, да бисмо могли управљати њима. Активности процеса у којима се врши мерење називају се контролне тачке. Потребно је дефинисати активности, резултате и носиоце активности, одговорне извршиоце и потребне податке. Најважније питање у успостављању било ког система мерења је „шта желим да знам о процесу“, а затим „како прикупити потребне податке“³⁶⁴.

С обзиром да се овде ради о мерењу безбедносне перформансе, онда је оправдано да се читав процес безбедносног менаџмента посматра као јединствен будући да је тешко, са аспекта ефикасности и ефикасности СБМ, априори одредити која безбедносна активност представља приоритет. Односно, усвајамо становиште да је основни циљ система безбедносног менаџмента да се избегну губици или да се, уколико је то немогуће, штета смањи на најмању могућу меру, невезано од тога који је инцидент ту штету изазвао. Имајући у виду да се неки безбедносни инциденти не могу предвидети, нити се на њих може у већој мери утицати, безбедносни процес нећемо посматрати кроз поједине активности (нпр. превентивне и репресивне). Дакле, безбедносни менаџмент посматрамо интегрално, као процес који има за циљ да штити организацију од свих могућих појава угрожавања, па се и овим моделом тај процес процењује у целини. Потпуно нови проблем у овом погледу представља утврђивање који од елемената система безбедносног менаџмента даје најбоље резултате, односно да ли је неки од њих вреднији у смислу остваривања циљева. Решење тог проблема захтева свеобухватно истраживање у појединим гранама

³⁶³ Видети: Радовић, М., Голубовић, Д., исто.

³⁶⁴ Видети: исто.

индустрије, тако да превазилази потребе и могућности овог рада. Ипак, има смисла раздвојити послове безбедности на две основне активности безбедносног менаџмента – планирање и реализацију, из простог разлога што се мере заштите уводе у складу са безбедносним проценама. Односно, подразумева се да фаза планирања у безбедносном менаџменту представља кључни процес. С тим у вези, треба напоменути да је контрола у интегрисаном систему безбедносног менаџмента, између осталог задужена и за утврђивање степена до ког је безбедносни план реализован. Дакле, основни проблеми са којима се безбедносни менаџмент сусреће се односе на следећа питања: да ли предузете мере заштите одговарају реалној ситуацији? (то је могуће утврдити анализом ефикасности), да ли су предузете мере ефикасне?, али и да ли су предузете мере у складу са планираним? (на то питање треба да одговори контрола). Последње питање се тиче процеса безбедносног менаџмента конкретне организације, а у овом раду се подразумева да је реализација усклађена са плановима.

Успостављање система мерења перформанси подразумева реализацију низа активности: превођење перформансе организације у перформансе процеса, идентификовање сирових података уз чију помоћ се израчунавају вредности перформансе, утврђивање места настанка сирових података, дефинисање мерног инструмента и обима и учесталости мерења.³⁶⁵

„Превођење захтева и циљева заинтересованих страна у перформансе организације, а затим у перформансе процеса, представља превођење питања „шта желим да знам о процесу“ у мерила перформанси“.³⁶⁶ У овом случају, ради се о безбедности организације и безбедносном процесу који постоји да би организација правилно функционисала. Безбедносни циљеви организације постају директно циљеви система безбедносног менаџмента, али и обрнуто – специфични циљеви безбедносног менаџмента су имплицитно садржани у основним циљевима организације. На пример, ако је циљ власника да има што већи профит, јасно је да то подразумева што мање губитке, а самим тим и мањи број безбедносних инцидената.

³⁶⁵ Исто.

³⁶⁶ <http://konsultuj.me/2011/postupak-merenja-performansi-procesa/>

Вредности перформансе и подаци неопходни за њихово израчунавање морају дати одговор на постављено питање. Уколико је одговор изражен бројевима, утолико боље. Утврђивање мера перформансе је лакше уколико су успостављени и квантификовани циљеви. У том случају, мерила перформанси су изражена у истим или сличним мерним јединицама као и циљ. Када се дефинишу перформансе активности процеса, потребно је идентификовати потребне податке које треба мерити. За сваки податак је потребно дефинисати тип и вредности које може имати. Затим, треба повезати активности, резултате и податке, чиме се утврђује место настанка података. Мерни инструмент је средство или особа која је у стању да детектује присуство или недостатак неког феномена, односно неке величине, квантитативно израженог интензитета и јединице мере. Мерни инструмент је неко или нешто ко спроводи мерење и класификацију података. За техничке производе и процесе постоје мерни инструменти који мере дужину, температуру и сл. За остале производе и процесе то су базе података, временске картице, „чеклисте“, итд. Постоје случајеви у којима сензори врше мерење, а човек бележи податке, као и они у којима је једини могући сензор човек. Многе контролне активности могу бити спроведене искључиво од стране човека. Постоје системи аутоматске обраде и класификације података који не захтевају учешће човека, осим у активностима калибрације и одржавања. Са аспекта безбедносног менаџмента, мерни инструмент су запослени стручњаци безбедности, који прикупљају податке о свим могућим безбедносним инцидентима и праве безбедносне извештаје. Некад су то запослени на нивоу менаџера, некада самостални стручњаци за безбедност, некада ангажовано приватно физичко-техничко обезбеђење. Посебно је значајна сарадња са стручњацима за информационе технологије, будући да важан део безбедносног менаџмента представља безбедност информација. Подаци о таквим инцидентима се, готово редовно, примају директно од запослених у тим одељењима. У већим организацијама, поготово онима којима је електронско пословање велики део активности, постоје посебно обучени менаџери за безбедност информационих технологија. Овде се подразумева да је и безбедност информација саставни део

система безбедносног менаџмента, било да је организована као посебна јединица или је у саставу сектора за безбедност.

Поред тога, потребно је дефинисати учесталост мерења и обим утврђивања сирових података, јер ће се у неким случајевима оно дешавати сваки пут када се појава дешава (нпр. безбедносни инцидент), а неки пут на крају утврђеног временског периода (нпр. годишњи извештај). Након утврђивања учесталости мерења, потребно је утврдити обим мерења, који може бити 100% или селективно, на основу узорка. Начин узорка зависи од тога да ли се ради о утврђивању нумеричких вредности или атрибутивних величина.

Дефинисање одговорних страна подразумева утврђивање извршилаца који ће реализовати активности мерења перформанси, као и одговорног руководиоца, који ће бити одговоран за измерену вредност перформанси. Важно је именовати особу или особе које ће бити задужене за активности прикупљања и класификације података и обучити их за ову активност. Овде се подразумева да су то стручњаци за безбедност и/или менаџери безбедности. Један од начина контроле је самоконтрола, која представља збир активности контролисања, које обавља извршилац у процесу рада и то чини заједно са основним активностима при обављању посла. За процесе већег обима и значаја, могуће је увести посебно тело које ће вршити ову контролу.

Након успостављања система за мерење перформанси процеса, потребно је приступити прикупљању и класификацији података у складу са дефинисаним елементима система од стране одговорних особа. Подаци се на крају анализирају и праве се извештаји о оствареним вредностима перформанси. Резултати анализе и извештавања морају да буду такви да буду употребљиви за поређење остварених вредности са циљем. Резултати морају бити закључци о оствареним вредностима перформанси.

Поређење остварених вредности перформанси са циљем је претпоследња фаза у поступку мерења перформанси процеса. Одговорни менаџер (менаџер безбедности) врши поређење добијених података са унапред постављеним циљем и презентује закључке. Менаџер безбедности може да донесе закључке у вези са процесом којим управља, да постави питање узрока и да у наредном кораку предузме одговарајуће

мере да би се убудуће остваривали постављени циљеви, или у крајњој мери, преиспитали сами циљеви.

Последњи корак у предложеном моделу јесте да се донесе одлука у вези са оствареним перформансама процеса и организације³⁶⁷. На располагању су две најважније одлуке: одржавање или побољшање. Одржавање се односи на активности које се тичу одржавања постојећих безбедносних, менаџерских и оперативних стандарда (циљева). Побољшање се односи на унапређивање постојећих стандарда (циљева). Сваки менаџер има три основне опције³⁶⁸:

- 1) да не предузима мере – у случају када су уочене вредности у складу са циљем,
- 2) предузимање корективних мера – у случају када су остварене вредности испод жељених и када је утврђено да је узрок неусаглашености у начину одвијања процеса и
- 3) измена циља – у случају када су остварене вредности испод жељених и када је утврђено да је узрок неусаглашености у погрешно постављеном циљу.

Поступак мерења перформанси безбедности никако не сме бити замишљен као просто прикупљање података, већ се мора посматрати искључиво као свеукупан систем менаџмента који је усмерен на испуњавање захтева свих заинтересованих страна и стално унапређење. Овако замишљен, овај модел треба да сваком менаџеру, а посебно менаџерима безбедности, пружи ону врсту информација које су неопходне за доношење квалитетних и правовремених одлука. Поред тога, овај модел треба да буде систем који организацији треба да омогући да акумулира знања о својим корисницима, процесима и ресурсима и да спроводи стална унапређења у домену безбедности, чиме се осигуравају опстанак, раст и развој организације.

³⁶⁷ Видети: Радовић, М., Голубовић, Д., исто.

³⁶⁸ Видети: TRADE, *How to measure performance, A Handbook of Techniques and Tools*, US Dep. of Energy, 1995.

7.2. Алгоритам за одређивање ефикасности мера заштите у системима безбедносног менаџмента

На основу датог модела и модела који су поставили проф. Л. Петровић и З. Петровић, можемо представити алгоритам који указује на ефикасност мера заштите у системима безбедносног менаџмента. Према моделу који су дали проф. Л. Петровић и З. Петровић, „стање организационог система може да се представи матрицом стања $[S_{rs}]$, стање на улазу у систем се може представити матрицом улазних $[X_{ij}]$, а на излазу, матрицом излазних стања $[Y_{pq}]$. На организациони систем се делује активностима угрожавања које се могу представити матрицом угрожавања $[U_{mn}]$. Елементи ове матрице представљају испољене ефекте угрожавања m који делују на n елемената организационог система. Након испољених ефеката угрожавања, у систему се примењују одређене мере заштите, које су приказане помоћу матрице заштите $[Z_{kn}]$. Елементи ове матрице представљају број мера заштите (k) примењених на n елемената организационог система.“³⁶⁹

У нашем моделу, сматрамо да је стање система најбоље представити на следећи начин:

1) Скуп елемената организационог система се састоји од одређеног броја организационих делова, броја радних места и коначног броја крајњих учесника, тј.

$$[S] = [s_{od}, s_{rm}, s_{ku}] \quad (1),$$

где је:

S – скуп елемената организационог система,

s_{od} – укупан број организационих делова,

s_{rm} – укупан број радних места и

s_{ku} – коначан број крајњих учесника.

2) На организациони систем делује окружење са m различитих облика угрожавања. Скуп испољених ефеката угрожавања је представљен матрицом угрожавања $[U_{ij}]$. Елементи скупа испољених ефеката угрожавања су:

³⁶⁹ Петровић, Л., Петровић, З., Алгоритам за одређивање ефикасности мера заштите у функционалним телекомуникационим системима, *Telfor*, 2002., 2-6.

$$[U] = [FU, U_{\text{žs}}, P, UI] \quad (2),$$

где је:

U – скуп испољених ефеката угрожавања,

FU – физичко угрожавање организационог система,

U_{žs} – угрожавање животне средине,

P – пожари

UI – угрожавање информационог система у организационом систему.

Матрица испољених ефеката угрожавања [U_{mn}] се може написати у облику:

$$[U_{mn}] = \begin{pmatrix} u_{11} & u_{12} & - & - & - & u_{1n} \\ u_{21} & u_{22} & \cdot & \cdot & \cdot & u_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ u_{m1} & u_{m2} & \cdot & \cdot & \cdot & u_{mn} \end{pmatrix} \quad (3).$$

Елементи матрице u_{ij} су једнаки нули уколико на j -том елементу система није испољен i -ти ефекат угрожавања, а у супротном је једнак јединици.

3) У организационом систему примењене су мере заштите које се могу исказати матрицом примењених мера заштите [Z_{kn}], која се може написати у облику:

$$[Z_{kn}] = \begin{pmatrix} z_{11} & z_{12} & - & - & - & z_{1n} \\ z_{21} & z_{22} & \cdot & \cdot & \cdot & z_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ z_{k1} & z_{k2} & \cdot & \cdot & \cdot & z_{kn} \end{pmatrix} \quad (4).$$

Елемент матрице примењених мера заштите z_{ij} је једнак нули уколико на j -том елементу система није примењена i -та мера заштите, а у супротном је једнак јединици.

4) Стање система на излазу из система $[Y]$ одређено је параметрима који улазе у систем $[X]$ и тренутним стањем система $[S]$. Тренутно стање зависи од угрожавања $[U]$ и предузетих мера заштите које су дефинисане матрицом заштите $[Z]$.

5) Матрица стања система $[S]$ се може одредити као производ матрице угрожавања и матрице заштите (4):

$$[S_{mk}] = [U_{mn}] \times [Z_{kn}] \quad (5), \text{ односно:}$$

$$[S_{mk}] = \begin{pmatrix} s_{11} & s_{12} & \cdot & \cdot & \cdot & s_{1k} \\ s_{21} & s_{22} & \cdot & \cdot & \cdot & s_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{m1} & s_{m2} & \cdot & \cdot & \cdot & s_{mk} \end{pmatrix} \quad (6).$$

При томе је $s_{ij} < \bar{S}$, уколико i -ти ефекат угрожавања није неутрализован j -том мером заштите и $s_{ij} > \bar{S}$ у супротном. \bar{S} је средња вредност елемената добијене матрице стања система.

Ако је износ елемената матрице стања мањи од средње вредности елемената добијене матрице стања система, то значи да ефекат угрожавања, који је испољен на било ком елементу организационог система, није неутрализован применом мере заштите на датом елементу организационог система.

Ако је износ елемената матрице стања већи од средње вредности елемената добијене матрице стања система, то значи да је испољени ефекат угрожавања на било

ком елементу организационог система неутралисан применом мере заштите на датом елементу организационог система.

У реалној ситуацији, корисник може да формира матрицу угрожавања на основу добијених података из безбедносне процене, као и матрицу заштите на основу познавања система безбедности и могућности примене мера заштите. Помоћу овог алгоритма могуће је брзо доћи до података да ли примењена мера заштите може парирати испољеном ефекту угрожавања или не. Уколико је одговор не, врло се лако може одредити које су то мере заштите које се успешно супротстављају испољеном ефекту угрожавања. Поред тога, могуће је посматрати појединачни и кумулативни утицај мера заштите на функционисање самог организационог система. Уколико се ефикасност организационог система умањи испод 15%, онда је то прихватљива граница³⁷⁰, а уколико примењене мере заштите умањују ефикасност организационог система изнад ове границе, онда те мере немају смисла.

³⁷⁰ Видети: Ricci, F. J., *U. S. Military Communications: AC*3I Force Multiplayer*, Computer Science Press, 1999.

ЗАКЉУЧНА РАЗМАТРАЊА

Безбедност остаје једна од најнерегулисанијих и несхваћених области корпоративног живота. Два основна разлога су узрок овоме. Прво, много тога што се описује као „корпоративна безбедност“ је често сакривено тајношћу. Корпоративна безбедност указује на одговорност за ризике и акциденте невезано за девијантно или криминално понашање. Свака организација има функције које се односе на ризик и безбедност, иако је начин на који су оне разлучене једна од друге скоро у потпуности јединствен за сваки организациони контекст. Друго, већина послова који се тичу корпоративне безбедности се категоризује као нека друга област. Безбедност представља индустрију која је у великој експанзији, а задаци који су јој поверени су разноврсни. Од превенције криминала до високо елаборисаних корпоративних планова за управљање кризама и катастрофама, интерних и екстерних контрола, функција које се тичу здравља и безбедности на раду, осигурања, куповине и безбедности на интернету.

У добро организованом предузећу особље које се бави питањима безбедности има шест одређених функција, а свака од њих има важну улогу за успех организације. Без обзира на број запослених, функције су константне. Свака функција је јединствена, критична за целину. То су:

1. управљање/надгледање рада,
2. секретарски послови,
3. послови пријема,
4. чиновнички послови,
5. чување података и
6. пошта.

Ако неки од тих послова није одрађен на адекватан начин, значи да ни безбедност није на одговарајућем нивоу. Поред тога, ако се неки од безбедносних инцидената дешава чешће или су његове последице велике, било са становишта материјалне штете или повреда, значи да систем безбедности не функционише на

прави начин. Међутим, уколико нема проблема на пољу безбедности поставља се неминовно питање: да ли је то последица добро организованог система или случајност? Тиме се враћамо проблему истраживања, односно могућности утврђивања ефективности и ефикасности система безбедносног менаџмента.

Полазна хипотеза тврди да постојећи ниво функционисања система за процену учинка безбедносног менаџмента у организацијама у Републици Србији не даје реалне резултате о утицају на превенцију и ублажавање последица угрожавања безбедности и заштиту организација, свих субјеката и животне средине. Можемо рећи да је тај систем код нас прилично запостављен и да се своди на прављење извештаја о стању безбедности, при чему менаџери безбедности углавном немају повратну информацију о томе како топ менаџмент цени њихов рад.

Треба напоменути да стандарди безбедности и заштите на раду у Републици Србији постоје, усклађени су са важећим стандардима у земљама Европске Уније и још увек су у фази увођења, тако да не можемо са сигурношћу тврдити да нису добро дефинисани. Међутим, треба да прође изван период њихове примене да би се могли утврдити њихови ефекти на стварно стање безбедности у организацијама.

Када је реч о индикаторима безбедности, може се рећи да они заиста нису довољно јасно и прецизно дефинисани. Ови индикатори се свде на податке о инцидентима који су се десили, а свест о њиховом развијању није довољно заступљена.

Модел за процену ефективности безбедносних активности у организацијама у Републици Србији нису развијени, а једини показатељ који руководиоци користе јесте цена коштања услуга безбедности. Односно, топ менаџмент у већини организација одлучује о начину организовања система безбедности на основу трошкова који настају приликом његовог организовања и функционисања. Врло ретко се у обзир узимају трошкови који би настали у случају да дође до неког инцидента. Дакле, и трећа хипотеза је потврђена.

Када је реч о процени ефикасности, можемо рећи да се систему безбедносног менаџмента у организацијама у Републици Србији поклања врло мало пажње, док је одговорност на њима велика. Иако се послови обезбеђења и заштите проводе, у

већини ових организација ретко се дешава да се успешност тих послова доведе у везу са ниском стопом безбедносних инцидената. Односно, о ефикасности система безбедносног менаџмента се врло мало размишља.

Коначно, ово истраживање има за циљ да укаже на проблеме у овој области и да отвори врата ка развијању свести о важности система безбедносног менаџмента. С обзиром на то да се о безбедности у предузећима у Републици Србији размишља само у случају када се деси неки инцидент, јасно је да овај систем не добија заслужену пажњу.

Када би се на правилан начин осмислили показатељи рада овог система, топ менаџмент би добио праву слику о послу који овај систем обавља, као и о користима које произилазе из његовог функционисања. Дакле, потребно је одредити начин за утврђивање ефикасности и ефикасности система безбедносног менаџмента да би се на јасан и концизан начин могло указати на суштину његовог постојања, а то је заправо његов основни циљ, односно опстанак, несметано функционисање, раст и развој саме организације.

СПИСАК ЛИТЕРАТУРЕ

Монографије, уџбеници и текстови у часописима

1. Aba-Bulgu, M., Islam, S. M. N., *Corporate Crisis and Risk Management: Modelling, Strategies and SME Application*, Elsevier, Amsterdam, 2007.;
2. Abdel-Maksoud, A. B., Abdel-Kader, M. G., *Non-Financial Performance Measurement and Management Practices in Manufacturing Firms: A Comparative International Analysis*, Elsevier Ltd., Oxford, 2007.;
3. Andrews, R., Boyne, G. A., Walker, R. M., Subjective and objective measures of organizational performance: An empirical exploration, *Public Service Performance: Perspectives on Measurement and Management*, Cambridge University Press, New York, 2006., стр. 14-34.;
4. Бабић, М., Ставрић, Б., *Менаџмент*, КИЗ Центар, Београд, 1999.;
5. Bain, A., Do we truly understand Safety Culture?, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 11-24.;
6. Barnes, D., Hinton, M., *The Benefits of e-Business Performance Measurement Systems*, Elsevier Ltd., Burlington, 2008.;
7. Backman, B. F., *Composite Structures, Safety Management*, 2nd ed., Elsevier Ltd., Oxford, 2008.;
8. Beckhard R., *Organization development strategies and models*, Addison-Wesley, Boston, 1969.;
9. Bentley, P. D., Sockley, J. D., Hazard management and safety management systems: a structured approach, *Offshore Technology Conference (OTC) Proceedings*, May 1992, pp. 471–476.;
10. Bentley, P. D., Mundhennk, D.L., Jones, M.G., Geert de Jong, Visser, J. P., Development and implementation of an HSE management system in E&P companies, *Journal of Petroleum Technology (JPT)*, 1, 1995, pp. 54–60.;
11. Biazzo, S., Garengo, P., *Performance Measurement with the Balanced Scorecard: A Practical Approach to Implementation within SMEs*, Springer-Verlag, Heidelberg, 2012.;

12. Blair, A., Management system failures identified in incidents investigated by the U.S. Chemical Safety and Hazard Investigation Board, *Process Safety Progress*, 23 (4) (2004), pp. 232–236.;
13. Blyth, M., *Risk and Security Management: Protecting People and Sites Worldwide*, John Wiley & Sons Inc., Hoboken, 2008.;
14. Booz, A. H., *Convergence of Enterprise Security Organizations*, AESMR, 2005.;
15. Borodzicz, E. P., *Risk, Crisis and Security Management*, John Wiley & Sons Ltd., Chichester, 2005.;
16. Boumans, M., *Measurement in Economics: A Handbook*, Elsevier Inc., Burlington, 2007.;
17. Bragdon, C., *Transportation Security*, Butterworth-Heinemann, Boston, 2008.;
18. Briggs, R., Edwards, C., *The Business of Resilience*, DEMOS, London, 2006.;
19. Broder, J. F., *Risk Analysis and the Security Survey*, 3rd ed., Butterworth-Heinemann, Burlington, 2006.;
20. Wade, D., Recardo, R., *Corporate Performance Management: how to build a better organization through measurement-driven strategic alignment*, Butterworth-Heinemann, Woburn, 2001.;
21. Walsh, J., *Asset Protection and Security Management Handbook*, POA Publishing LLC, Boca Raton, 2002.;
22. Van Brabant, K., *Mainstreaming the Organizational Management of Safety and Security. A review of aid agency practices and a guide for management*, Overseas Development Institute, HPG Report 9, London, 2001.;
23. Vellani, K. H., *Strategic Security Management*, Elsevier Inc., Burlington, 2007.;
24. Willis, A., Watson, B., Biggs, H. C., Comparing safety climate factors as predictors of work-related driving behavior, *Journal of Safety Research*, Volume 37, Issue 4, 2006, Pages 375-383.;
25. Vishwanath, S. R., Krishnamurti, C., *Investment Management*, Springer – Verlag, Heidelberg, 2009.;

26. Whittingham, B., Holloywell, P., Ensuring you take credit for an effective safety management system, *Incorporating the Human Factors into Offshore Safety Cases Conference*, Aberdeen, 1 March 1994.;
27. Woods, M., at al., *International Risk Management*, Elsevier, Ltd., Oxford, 2008.;
28. Wheeler, E., *Security Risk Management*, Elseiver Inc., Waltham, 2011.;
29. Garratt, B., *Thin on Top: Why Corporate Governance Matters and How to Measure and Improve Board Performance*, Nicholas Braely Publishing, London, 2003.;
30. Genserik, R. L. L., *Multi-Plant Safety and Security Management in Chemical and Process Industries*, Wiley-VCH Verlag GmbH&Co., Wetnhetm, 2010.;
31. Gerencser, M., Aguirre, D., "Security Concerns Prominent on CEO Agenda," *strategy + business*, 12 Feb., 2002.;
32. Gouin, B., *Security Design Consulting*, Elsevier Inc., Burlington, 2007.;
33. Graham, B., Dodd, D. L., *Security Analysis*, 6th ed., McGraw Hill Inc., New York, 2009.;
34. Grote, G., Understanding and assessing safety culture through the lens of organizational management of uncertainty, *Safety Science, Volume 45, Issue 6, July 2007, Pages 637-652.*;
35. Gunasekaran, A. and Kobu, B., Performance Measure and Metrics in Logistics and Supply Chain Management: A Review of Recent Literature (1995-2004) for Research and Applications, *International Journal of Production Research, 45(12), 2007., pp. 2819-2840.*;
36. Gupta, P., *Six Sigma Business Scorecard*, McGraw-Hill, New York, 2004.;
37. Gustin, J. F., *Safety Management: A Guide for Facility Managers*, 2nd ed., The Fairmont Press, Inc., Lilburn, 2008.;
38. Dalton, D. R., *Rethinking Corporate Security in the post 9/11 Era*, Elsevier Butterworth-Heinemann, Burlington, 2003.;
39. Davies, S. J., Hertig, C. A., *Security Supervision and Management*, 3rd edition, Elsevier, Burlington, 2008.;

40. Degani, A., Wiener, E.L., Procedures in complex systems: the airline cockpit, *IEEE Trans. on Systems, Man and Cybernetics—Part A: Systems and Humans*, 27 (3), 1997, pp. 302–312.;
41. Dessler, G., *Management, Leading Organizations in the 21st Century*, FIU, New Jersey, 2004.;
42. Donaldson, T., Dunfee, T. W., *Ties that bind: A social contracts approach to business ethics*, Harvard Business School Press, Boston, 1999.;
43. Драгишић З., *Безбедносни менаџмент*, Службени Гласник РС, Београд, 2007.;
44. Durbin, T., Measuring Safety: Challenging and Besting Traditional Methods at PPG, *Safety management, Aug2000, Issue 449, pp. 1-2.*;
45. Elliott, M., Kleindorfer, P., Dubois, J., Wang, Y., Rosenthal, I., Linking OII and RMP info data: does everyday safety prevent catastrophic loss?, *International Journal of Risk Assessment and Management*, 10 (1/2), 2008, pp. 130–146.;
46. Epstein, M. J., The Challenges of Simultaneously Improving Social and Financial Performances: New Research Results, *Performance Measurement and Management Control: Inovative Concepts and Practices*, Emerald Group Publishing Ltd., Bingley, 2010., pp. 9-18.;
47. Ericsson, K. A., *Development of Professional Expertise: Towards Measurement of Expert Performance and Design of Optimal Learning Environments*, Cambridge University Press, New York, 2009.;
48. Esque, T. J., *Making an impact: Building a top-performing organization from the bottom up*, CEP Press, Atlanta, 2001.;
49. Живковић, М., *Економика пословања*, 6. издање, Мегатренд универзитет, Београд, 2006.;
50. Zyla, M. L., *Fair Value Measurements: Practical Guidance and Implementation*, John Wiley & Sons, Inc., Hoboken, 2010.;
51. Ивандић Видовић, Д., Карловић, Л., Остојић, А., *Корпоративна сигурност*, ХУМС, Загреб, 2011.;
52. Jacquith, A., *Security metrics – replacing fear, insecurity and doubt*, Addison&Wesley, 2007.;

53. Јовановић, Б., *Руковођење ОНО и ДСЗ*, Привредапублик, Београд, 1988.;
54. Johnson, K., *Asset Protection and Security Management Handbook*, POA Publishing LLC, Boca Raton, 2003.;
55. Young, C. S., *Metrics and Methods for Security Risk Management*, Elsevier Inc., Burlington, 2010.;
56. Јурина, М., *Елементи организације полиције*, МУП Републике Хрватске, Загреб, 1995.;
57. Yücesan, E., *Competitive Supply Chains: A Value-Based Management Perspective*, Palgrave Macmillan, Chippenham, 2007.;
58. Kandola, B. S., Risk based approach to fire safety engineering, *Fire Engineers Journal*, 1997, Pages 21–26.;
59. Kaplan, R., Norton, D., The Balanced Scorecard - Measures that drive performance, *Harvard Business Review*, Jan/Feb92, Vol. 70 Issue 1, p71-79;
60. Kenis, P., Performance control and public organizations, *Public Service Performance: Perspectives on Measurement and Management*, Cambridge University Press, New York, 2006., стр. 113-129.;
61. Kinsey, C., *Corporate Soldiers and International Security*, Routledge, New York, 2006.;
62. Kirchsteiger, C., Review Of International Industrial Safety Management Frameworks, *Trans IChemE*, Vol 80, Part B, September 2002, pp. 235-244.;
63. Klein, P. J., *Getting Started in Security Analysis*, 2nd ed., John Wiley & Sons, Inc., Hoboken, 2010.;
64. Kovacich, G. L., Halibozek, E. P., *The Managers Handbook for Corporate Security*, Butterworth-Heinemann, Boston, 2003.;
65. Kovacich, G. L., Halibozek, E. P., *Security Metrics Management*, Butterworth-Heinemann, Boston, 2006.;
66. Kuchinka, P., *Levels of Corporate Globalization: Developing Measurement Scale for Global Customer Management*, Palgrave Macmillan, Basingstoke, 2004.;
67. Liou, J. J. H., et al., Building an effective safety management system for airlines, *Journal of Air Transport Management* 14, 2008, Pages 20-26;

68. Loistl, O., Petrag, R., *Asset Management Standards: Corporate Governance for Asset Management*, Palgrave Macmillan, New York, 2003.;
69. Maguire, R., *Safety Cases and Safety Reports – Meaning, Motivation and Management*, Ashgate Publishing Ltd., Aldershot, 2006.;
70. Manzoni, A., Islam, S. M. N., *Performance Measurement in Corporate Governance*, Physica-Verlag, Heidelberg, 2009.;
71. Meyer, M. W., *Rethinking Performance Measurement: Beyond Balanced Scorecard*, Cambridge University Press, New York, 2003.;
72. Merna, T., Al-Thani, F., *Corporate Risk Management*, 2nd Edition, John Wiley and Sons, Ltd., Chichester, 2008.;
73. Ming, K. T., Application of a quality management system approach to health, safety and environment, *Offshore South East Asia, Proceedings of the 10th Conference and Exhibition World Trade Centre*, Singapore, 6–9 December 1994, pp. 739–745.;
74. Mitchison, N., Papadakis, G. A., Safety management systems under Seveso II: implementation and assessment, *Journal of Loss Prevention the Process Industries*, 12 (1999), pp. 43–51.;
75. Mitchison, N., Porter, S., *Guidelines on a major accident prevention policy and safety management system, as required by Council Directive 96/82/EC, SEVESO II*, EUR 18123 EN, European Commission, DG JRC, Ispra, 1988.;
76. Moseley, J. L., Dessinger, J. C., *Handbook of Improving Performance in the Workplace: Measurement and Evaluation*, Vol. 3, International Society for Performance Improvement, San Francisco, 2010.;
77. McDermid, J., Rae, A., Goal-Based Safety Standards: Promises and Pitfalls, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 257-270.;
78. McCrie, R. D., *Security Operations Management*, Butterworth-Heinemann, Boston, 2001.;
79. Neely, A., Measuring Performance: the operations management perspective, *Business Performance Measurement: Unifying Theories and Integrating Practice*, 2nd ed., Cambridge University Press, New York, 2007., 64-81.;

80. Neely, A., Adams, C., Kennerley, M., *The Performance Prism: The Scorecard for Measuring and Managing Business Success*, Pearson Education Limited, London, 2002.;
81. Neely, A., Gregory, M., Platts, K., Performance measurement system design: a literature review and research agenda, *Int J Oper Prod Manag* 15 (4), 1995, pp. 80–116.;
82. Nichols, E. A., Sudbury, A., Implementing Security Metrics Initiatives, *Information Systems Security*, November 2006., Pages 30-38.;
83. Norman, T. L., *Risk Analysis and Security Countermeasure Selection*, CRC Press, Boca Raton, 2010.;
84. Orlitzky, M., Swanson, D. L., *Toward Integrative Corporate Citizenship: Research Advances in Corporate Social Performance*, Palgrave Macmillan, Basingstoke, 2008.;
85. Османагић Беденик, Н., Ивезић, В., Бенчмаркинг као инструмент савременог контролинга, *Зборник економског факултета у Загребу*, година 4, Загреб, 2006., стр. 331-346.;
86. Oxelheim, L., Wihlborg, C., *Corporate Decision-Making with Macroeconomic Uncertainty – Performance and Risk Management*, Oxford University Press, Inc., New York, 2008.;
87. Paladino, B., *Innovative Corporate Performance Management*, John Wiley & Sons, Inc., Hoboken, 2011.;
88. Paladino, B., *Five Key Principles of Corporate Performance Management*, John Wiley & Sons, Inc., Hoboken, 2007.;
89. Papadakis, G. A., Amendola, A., *Guidance on the Preparation of a Safety Report to meet the Requirements of Council Directive 96/82/EC*, Joint Research Center, European Commission, 1997;
90. Pey, A., Lerena, P., Suter, G., Campos, J., Main differences on European regulations in the frame of the Seveso Directive, *Process Safety and Environmental Protection*, Volume 87, Issue 1, January 2009, Pages 53–58.;
91. Петровић, Л., Петровић, З., Алгоритам за одређивање ефикасности мера заштите у функционалним телекомуникационим системима, *Telfor*, 2002., 2-6.;

92. Пешалјевић, М., *Инжењерске комуникације и логистика*, Факултет техничких наука, Нови Сад, 1995.;
93. Радовић, М., Голубовић, Д., Поступак мерења перформанси процеса, *SymOrg 2010*, ISSU, Београд;
94. Радовић, М., Карапанџић, С., *Инжењеринг процеса*, ФОН, Београд, 2005.;
95. Ramanathan, R., *An Introduction to Data Envelopment Analysis: A Tool for Performance Measurement*, Sage Publications India Pvt Ltd., New Delhi, 2003.;
96. Reason, J., *Managing the risks of organisational accidents*, Ashgate, Aldershot, 1997.;
97. Reichheld, F., *The Loyalty Effect*, Harvard Business School Press, Boston, 2001.;
98. Ricci, F. J., *U. S. Military Communications: AC*3I Force Multiplayer*, Computer Science Press, 1999.;
99. Rodricks, B., A system for managing fire safety on passenger vessels, *Fire Prevention*, 260, 1993, pp. 24–28.;
100. Rowlinson, S., An Overview of Safety Management Systems, *Construction Safety Management Systems*, Spon Press, London, 2004., pp. 82-88.;
101. Rossiter, J. R., *Measurement for the Social Sciences: the C-OAR-SE Method and Why It Must Replace Pshychometrics*, Springer Science+Business Media, New York, 2011.;
102. Rothwell, W. J., Lindholm, J. E., Wallick, W. G., *What CEOs Expect from Corporate Training*, AMACOM, New York, 2003.;
103. Saaty, T. L., *Fundamentals of decision making and priority theory with the AHP*, Raws Publications, Pittsburgh, 1994.;
104. Савић, А., Приватна безбедност у систему националне безбедности, *Приватна безбедност – стање и перспективе*, Факултет за правне и пословне студије, Нови Сад, 2008., стр. 15-23.;
105. Santana, G., Tourism: Toward a Model for Crisis Management, *Turizam*, Vol. 47, No. 1, 1999.;
106. Santos-Reyes, J., Beard, A. N., Assessing safety management systems, *Journal of Loss Prevention in Process Industries*, Vol. 15, Issue 2, March 2002, Pages 77-95.;

107. Segal, S., *Corporate Value of Enterprise Risk Management, The Next Step in Business Management*, John Wiley & Sons Inc., New Jersey, 2011.;
108. Sennewald, C. A., *Effective Security Management*, 4th edition, Butterworth-Heinemann, Burlington, 2003.;
109. Sole, F., Schiuma, G., How to Use Different Measures for Different Management Model for Public Organizations, *Business Performance Measurement and Management: New Contexts, Themes and Challenges*, Springer-Verlag, Heidelberg, 2010., pp. 103-113.;
110. Spitzer, D. R., *Transforming Performance Measurement: Rethinking the Way We Measure and Drive Organizational Success*, AMACOM, New York, 2007.;
111. Стајић, др Љ., *Основи система безбедности*, Правни Факултет, Нови Сад, 2010.;
112. Стевановић, З., Лојић, Р., Управљање радном ефикасношћу запослених, *Војно дело, Јесен/2011, стр. 380-396.*;
113. Стевановић, О., *Руковођење у полицији*, ПА, Београд, 2002.;
114. Schein, E. H., *The Corporate Culture Survival Guide*, John Wiley & Sons, Inc., San Francisco, 2009.;
115. Scheer, A.-W., Jost, W., From Process Documentation to Corporate Performance Measurement, *Corporate Performance Management: ARIS in Practice*, Springer-Verlag, Heidelberg, 2006., 1-6.;
116. Schreck, P., *The Business Case for Corporate Social Responsibility: Understanding and Measuring Economic Impacts of Corporate Social Performance*, Physica-Verlag, Heidelberg, 2009.;
117. Taylor, B., *Effective Environmental Health and Safety Management Using the Team Approach*, John Wiley & Sons, Inc., Hoboken, 2005.;
118. Teo, A. L. E., Ling, Y. Y. F., Developing a model to measure the effectiveness of safety management systems of construction sites, *Building and Environment, Volume 41, Issue 11, November 2006, Pages 1584–1592.*;
119. Tiller, J. S., *Adaptive Security Management Architecture*, Taylor & Francis Group, Boca Raton, 2011.;

120. Tyson, D., *Security Convergence – Managing Enterprise Security Risk*, Elsevier Inc., Burlington, 2007.;
121. Тодоровић, Ј., Ђуричин, Д., Јаношевић, С.: *Стратегијски менаџмент*, Економски факултет, Београд, 2003.;
122. Trivan, D., Corporate safety in the Republic of Serbia: overview and prospects, *Corporate security in dynamic global environment – challenges and risks*, Institute for Corporative Security Studies, Ljubljana, 2012., pp. 227-236.
123. Tuli, R., Apostolakis, G., Incorporating organizational issues into root-cause analysis, *Trans IchemE*, 74 (B), 1996, pp. 3–15.;
124. Fay, J. J., *Contemporary Security Management* (Second Edition), Elsevier Butterworth-Heinemann, Burlington, 2006.;
125. Fahy, M., Roche, J., Weiner, A., *Beyond Governance: Creating Corporate Value through Performance, Conformance and Responsibility*, John Wiley & Sons Ltd., Chichester, 2005.;
126. Feibel, B. J., *Investment Performance Measurement*, John Wiley & Sons, Inc., Hoboken, 2003.;
127. Fennelly, L. J., *Effective Physical Security*, 3rd ed., Elsevier Inc., Burlington, 2004.;
128. Fernández-Muñiz, B., Montes-Peón, J. M., Vázquez-Ordás, C. J., Safety management system: Development and validation of a multidimensional scale, *Journal of Loss Prevention in the Process Industries*, Volume 20, Issue 1, January 2007, Pages 52-68.;
129. Fowler, D., Pierce, R., Safety Engineering - a Perspective on Systems Engineering, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 115-136.;
130. Friedlob, G. T., et al., *Essentials of Corporate Performance Measurement*, John Wiley & Sons, Inc., New York, 2002.;
131. Haddow, G. D., Bullock, J. A., Coppola, D. P., *Introduction to Emergency Management*, 3rd ed., Elsevier, Burlington, 2008.;
132. Hale, A. R., et al., Modelling of safety management Systems, *Safety Science*, Vol. 26, No. 1/2, 1997, pp. 121-140.;

133. Hampton, P., Survey of Safety Architectural Patterns, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 137-158.;
134. Harrington, H. J., Harrington, J. S., *High Performance Benchmarking: 20 steps to success*, McGraw-Hill, New York, 1996.;
135. Harrison, F. E., *The Managerial Decision-Making Process*, 5th ed., Houghton Mifflin, Boston, 1999.;
136. Callahan, K., *Elements of Effective Governance: Measurement, Accountability and Participation*, Taylor & Francis Group, LLC., Boca Raton, 2007.;
137. Canning, A., The Need for a Community for a System and Functional Safety Professionals, *Achieving Systems Safety*, Springer-Verlag, London, 2012., стр. 25-34.;
138. Caralli, R. A., Wilson, W. R., *The Challenges of Security Management*, Networked Systems Survivability Program, Software Engineering Institute, www.cert.org/archive/pdf/ESMchallenges;
139. Carder, B., Ragan, P., A survey-based system for safety measurement and improvement, *Journal of Safety Research*, 34, 2003, pp. 157–165.;
140. Coda, V., *Entrepreneurial Values and Strategic Management*, Palgrave Macmillan, Chippenham, 2010.;
141. Coleman, R. J., *Opportunities in Fire Protection Services Careers*, McGraw-Hill, New York, 2003.;
142. Collier, P., Measuring Police Performance, *Business Performance Measurement: Unifying Theories and Integrating Practice*, 2nd ed., Cambridge University Press, New York, 2007., 363-382.;
143. Conrow, E. H., *Effective Risk Management: Some Keys to Success*, 2nd ed., American Institute of Aeronautics and Astronautics, Inc., Reston, 2003.;
144. Contos, B. T., et al., *Physical and Logical Security Convergence: Powered by Enterprise Security Management*, Elsevier Inc., Burlington, 2007.;
145. Czarniawska, B., Fisher, R., *Organizing in the face of risk and threat*, CBI, London, 2009.;

146. Chang, J. I., Liang, C.-L., Performance evaluation of process safety management systems of paint manufacturing facilities, *Journal of Loss Prevention in the Process Industries*, Volume 22, Issue 4, July 2009, Pages 398–402.;
147. Chermes, M., *The social, organizational and Cultural context effective leadership*, Harvard business review, 1984.;
148. Christophers, J. A., Carino, D. R., Ferson, W. E., *Portfolio Performance Measurement and Benchmarking*, McGraw Hill Companies Inc., New York, 2009.;
149. Xiao, X., Marchant, E., Griffit, A., Assuring the quality of fire safety systems in buildings, *Fire Prevention*, 261, 1993, pp. 27–31.

Извештаји, студије и нормативна регулатива

1. Агенција за привредне регистре, Саопштење о пословању привреде у републици Србији у 2010 години, Београд, 2011;
2. Guideline for Safe Automation of Chemical Processes, AIChE, New York, 1993.;
3. Закон о безбедности и здрављу на раду „Службени гласник РС“ бр. 101/05;
4. Закон о заштити од пожара, „Сл. гласник РС“, бр. 111/2009;
5. Закон о здравственој заштити, „Службени гласник РС“, бр. 107/05;
6. Закон о здравственом осигурању, „Службени гласник РС“, бр. 107/05 и 109/05;
7. Закон о министарствима, „Службени гласник РС“, број 65/07;
8. Закон о општој безбедности производа (предлог закона у скупштинској процедури);
9. Закон о пензијском и инвалидском осигурању, „Службени гласник РС“, бр. 34/03, 64/04, 84/04, 85/05, 101/05 и 63/06;
10. Закон о раду, „Службени гласник РС“, бр. 24/05 и 61/05;
11. Одлука о измени Одлуке о образовању Савета за безбедност и здравље на раду „Службени гласник РС“, број 71/07;
12. Стратегија безбедности и здравља на раду у Републици Србији за период од 2009. до 2012. године;
13. Стандард SRPS A.L2.000:2008, *Друштвена безбедност – Услуге приватног обезбеђења*, Институт за стандардизацију Републике Србије;

14. TRADE, *How to measure performance, A Handbook of Techniques and Tools*, US Dep. of Energy, 1995.;
15. The Occupational Safety and Health Act (OSHA) of 1970, Public Law 91-596 84 STAT. 1590, 91st Congress, S.2193;
16. Threadgold, I. M., Reducing the Risk of Low-Probability High-Consequence Events, *Society of Petroleum Engineers Americas E&P Health, Safety, Security and Environmental Conference*, Houston, Texas, USA, 21–23 March 2011.;
17. Canadian Aviation Regulations (CARs), Part I, Amendment 2007-2;
18. Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, Official Journal L 010, 14/01/1997 P. 0013 - 0033.

Интернет извори

1. <http://www.adizes.co.rs/>
2. <http://www.aosh.org.uk/>
3. <http://www.dti.gov.uk/>
4. <http://www.eurostandard.rs/>
5. <http://ec.europa.eu/>
6. <http://www.iso.org/>
7. <http://www.jha.ac/>
8. <http://www.kombeg.org.rs/>
9. <http://konsultuj.me/>
10. <http://www.psmc.com/>
11. <http://www.sans.org/security-resources/>
12. <http://www.smartinsights.com/>
13. <http://www.strategy-business.com/>
14. <http://www.tc.gc.ca/>
15. <http://www.hse.gov.uk/>
16. <http://www.cert.org/>

Прилог бр. 1

Упитник за стручњаке безбедности

Упитник ФБ-СБМ

пол: **М** **Ж** степен стручне спреме: **1. ОШ** **2. СШ** **3. ВСС**
 узраст: а. 18–24 б. 25–34 в. 35–44 г. 45–54 д. 55 и више

Упутство

Овај упитник је део истраживања које врши асистент Факултета безбедности у оквиру докторског истраживања које се бави проблематиком ефективности и ефикасности система безбедносног менаџмента.

Упитник се састоји од низа исказа поређаних по сличности. Молимо вас да прочитате сваку реченицу пажљиво и заокружите одговор који најбоље изражава ваше искуство и знање о датој теми. Истраживање је анонимно. Молимо вас да одговорите на свако питање.

Одговори на следеће исказе означавају следеће:

1	2	3	4	5
нимало	у малој мери	средње	у великој мери	изузетно

Оцените значај следећих елемената система безбедносног менаџмента:

1. јасно одређена безбедносна политика	1	2	3	4	5
2. дефинисана стратегија безбедности	1	2	3	4	5
3. стандарди безбедности	1	2	3	4	5
4. безбедносне процедуре	1	2	3	4	5
5. безбедносна култура	1	2	3	4	5
6. систем обуке и додатног усавршавања	1	2	3	4	5
7. посвећеност највишег руководства	1	2	3	4	5

Оцените задовољство елементима система безбедносног менаџмента у вашој организацији:

1. јасно одређена безбедносна политика	1	2	3	4	5
2. дефинисана стратегија безбедности	1	2	3	4	5
3. стандарди безбедности	1	2	3	4	5
4. безбедносне процедуре	1	2	3	4	5
5. безбедносна култура	1	2	3	4	5
6. систем обуке и додатног усавршавања	1	2	3	4	5
7. посвећеност највишег руководства	1	2	3	4	5

1. Да ли у вашој организацији постоји усвојена политика безбедности у писаном облику (заокружите одговор)?

1. да 2. не

2. Како су у вашој организацији организовани послови Физичко-техничког обезбеђења (заокружити на шта се односи)?

- 1 - сопствена служба безбедности
- 2 - појединац из редова сопствених запослених
- 3 - приватно обезбеђење

3. Физичка заштита се користи за (заокружити на шта се односи):

- 1 - физичку заштиту објеката,
- 2 - физичку заштиту лица

4. Техничка заштита се користи за (заокружити све на шта се односи):

- 1 - противпровалну заштиту,
- 2 - противпожарну заштиту,
- 3 - видео обезбеђење,
- 4 - контролу приступа и проласка,
- 5 - сателитско праћење возила,
- 6 - механичку заштиту,
- 7 - транспорт вредности,
- 8 - руковање банкоматима.

5. Колико је у вашој организацији било инцидената у последњих годину дана везаних за физичко-техничку заштиту и колика је штета настала у динарима (у односу на наведене врсте заштите)?

- | | |
|---------------------------------|--|
| - физичка заштита објеката: | бр. инцидената: _____, штета (у дин.) _____, |
| - физичка заштита лица: | бр. инцидената: _____, штета (у дин.) _____, |
| - противпровална заштита: | бр. инцидената: _____, штета (у дин.) _____, |
| - противпожарна заштита: | бр. инцидената: _____, штета (у дин.) _____, |
| - видео обезбеђење: | бр. инцидената: _____, штета (у дин.) _____, |
| - контрола приступа и проласка: | бр. инцидената: _____, штета (у дин.) _____, |
| - сателитско праћење возила: | бр. инцидената: _____, штета (у дин.) _____, |
| - механичка заштита: | бр. инцидената: _____, штета (у дин.) _____, |
| - транспорт вредности: | бр. инцидената: _____, штета (у дин.) _____, |
| - руковање банкоматима: | бр. инцидената: _____, штета (у дин.) _____. |

6. Колика је штета (у процентима у односу на вредност укупне имовине организације) настала због безбедносних инцидената у протеклих годину дана (Штета у динарима/вредност укупне имовине организације*100)?

7. *Колико (у процентима у односу на укупан буџет) издвајате годишње средстава из буџета за послове безбедности (заокружити број поред одговора)?*

1 - < 10%

2 - < 30%

3 - < 50%

8. *Колико (у процентима, у односу на укупан број запослених) имате запослених који се баве пословима безбедности?*

9. *Колико сте имали извршених/покушаја напада у претходном периоду (12 месеци)?*

10. *Колико сте имали успешних интервенција службе обезбеђења у претходних годину дана?*

11. *Ваше напомене, препоруке и предлози:*

Списак интервјуисаних лица

1. Иван Јовановић, служба за безбедност и заштиту на раду, „Delta Maxi“ Д.О.О.;
2. Јосип Ујчић, Сектор за саобраћајне послове и безбедност саобраћаја, ЈП „Железнице Србије“ А.Д.;
3. Жељко Бркић, служба за безбедност и заштиту на раду и заштиту животне средине, „Zorka Color“ А.Д.;
4. Марко Андрић, служба за безбедност, ЈП ПТТ саобраћаја „Србија“;
5. Саша Јовановић, служба за ФТО, безбедност и заштиту од пожара, „Хемофарм“ А.Д.;
6. Мр Александар Димитрић, Сектор за фармацеутску производњу и контролу квалитета, Ветеринарски завод „Суботица“ А.Д.;
7. Мирко Димитрић, Сектор за производњу, „Rauch Serbia“ Д.О.О.

Питања постављена приликом интервјуа

1. Да ли је у Вашој организацији написмено постављена посебна особа да координира програм безбедности?
2. Постоје ли писани стандарди за деловање управе у програму безбедности?
3. Да ли су стандарди програма безбедности дати свим нивоима управе?
4. Да ли се у Вашој организацији и колико често врше инспекције од стране линијске управе како би се проверило подвргавање безбедносним стандардима?
5. Да ли је у ревизије менаџера укључено и деловање по питањима безбедносних стандарда?
6. Да ли су циљеви годишњег програма безбедности постављени за организацију у којој радите?
7. Да ли у Вашој организацији постоји програм који захтева од менаџера да присуствују безбедносним тренинзима?
8. Колики је проценат менаџера имао тренинг у вези безбедносног програма?
9. Колики је проценат радника добио званичан тренинг о томе како вршити безбедносне дужности?
10. Да ли у Вашој организацији постоји централна база података са извештајима истрага безбедносних инцидената и колико Вам користи у раду и колико се дуго чувају ти извештаји?
11. Да ли и које технике за контролу система безбедности користите у Вашој организацији (техника само процене, техника ревизије и контроле и сл.)?
12. Према Вашем мишљењу, који су најзначајнији инструменти контроле службе безбедности и заштите на раду које примењује Ваша организација?
13. Колики је проценат потреба одређен контролом испуњен?

14. Да ли постоји писана процедура која обезбеђује предузимање одговарајућих корективних мера?
15. Према Вашем мишљењу, колики је значај буџета за рад службе и остваривање контроле њеног рада?
16. Да ли топ менаџмент посвећује пажњу и расправља о буџету за службу безбедности и заштиту на раду?
17. Да ли осећате неповерење од стране надлежних за буџет и финансије по питању одређивања средстава за безбедност и заштиту на раду?
18. Да ли се и колико често раде обрачуни и пописи како би се идентификовали безбедносни губици?
19. Да ли се врши ревизија извештаја о безбедносним губицима?
20. Према Вашем мишљењу, да ли је законска регулатива адекватна потребама за безбедношћу у Вашој организацији?
21. Да ли сматрате да је Ваша организација у потпуности усагласила систем безбедности и заштите на раду са законским обавезама?
22. Према Вашем мишљењу, колики значај имају стандарди безбедности и заштите на раду за безбедност у Вашој организацији?
23. Да ли се подношење безбедносног извештаја топ менаџменту врши у писаној форми?
24. Да ли остварујете контакте са надлежним службама за безбедност и заштиту на раду у локалној управи и шире (комунална полиција, МУП, инспекцијске службе)?
25. Да ли сте задовољни безбедносним стањем у Вашој организацији и, уколико нисте, шта мислите да би требало да се промени?

СКРАЋЕНИЦЕ

ASIS - The American Society for Industrial Security (Америчко Удружење за Индустијску Безбедност)

АХП - Аналитички Хијерархијски Процес

БИ - безбедносни индекс

БМ - Безбедносни менаџмент

GPS - The Global Positioning System (Систем за глобално позиционирање)

EMS - Environmental Management System (Систем за управљање животном средином)

EPSC - European Process Safety Centre (Европски Центар за Безбедност Процеса)

ЕУ - Европска Унија

ILO - The International Labour Organization (Међународна Организација Рада)

ИМО - The International Maritime Organisation (Међународна Поморска Организација)

ISMS - Information Security Management System (Систем за управљање безбедношћу информација)

ISO - International Organization for Standardization (Међународна организација за стандардизацију)

LPC - Least Preferred Co-worker (најмање прихваћени колега)

MAVT - Multi-Attribute Value Model (Модел вредности мултиатрибута)

MAPP - Major Accident Prevention Policy (Политике за Спречавање Акцидентата великих размера)

MARS - Major Accident Reporting System (Информациони систем који садржи податке о акцидентима већих размера)

МОП - Међународна Организација Рада

МУП РС - Министарство унутрашњих послова Републике Србије

ОН&S - Occupational Health and Safety (Здравље и безбедност на радном месту)

OSHA - The Occupational Safety and Health Act (Уредба о безбедности и здрављу на раду)

OHSAS 18000 - Occupation Health and Safety Assessment Series (Серија стандарда за управљање системом здравља и безбедности на радном месту)

ПА - Полицијска академија

ПКС - Привредна комора Србије

PPS - Performance Presentation Standards (Стандард за Презентацију Перформанси)

SADT - Structured Analysis and Design Technique (Техника структурне анализе и дизајнирања)

СБМ - Систем безбедносног менаџмента

SMS - Safety Management System

SEVESO I - Council Directive 82/501/EEC on the major-accident hazards of certain industrial activities (Директива Савета 82/501/ЕЕЦ о опасностима од великих катастрофа појединих индустријских активности)

SEVESO II - Council Directive 96/82/EC on the control of major-accident hazards (Директива Савета 96/82/ЕЦ о контроли опасности од катастрофалних акцидента)

УГС - Уједињени грански синдикати

ФТО - Физичко-техничко обезбеђење

HMA - Hazard Management Analysis (Анализа управљања опасностима)

HSE - The Health and Safety Executive (Директива за Здравље и Безбедност)

CEN - Comité Européen de Normalisation (Европски комитет за стандардизацију)

БИОГРАФИЈА

Кристина Радојевић је рођена 06. 02. 1977. године у Бијелом Пољу, Република Црна Гора. Дипломирала је на Факултету организационих наука у Београду 2001. године и стекла звање Дипломирани инжењер организационих наука – одсек за менаџмент. Магистрала је 2008. године на Факултету безбедности у Београду, одбранивши магистарску тезу под називом *„Модел безбедносног менаџмента у саобраћајним системима – студија случаја ЈП „Железнице Србије““*.

Одредила је приправнички стаж у Општини Бијело Поље, Република Црна Гора у периоду од маја 2002. до јуна 2003. године на радном месту комуналног инспектора. У јулу 2003. године је положила стручни испит за рад у државним органима у Подгорици.

Радни однос на Факултету безбедности засновала је 2004. године, у звању асистент-приправник, а 2009. године на Факултету безбедности бирана је у звање асистента за наставни предмет Безбедносни менаџмент.

Учесница је многих семинара и научно-стручних конференција из области безбедности и менаџмента.

Прилог 1.

Изјава о ауторству

Потписани-а _____ Кристина З. Радојевић _____

број уписа _____ 130 _____

Изјављујем

да је докторска дисертација под насловом

«Модел за процену ефективности и ефикасности система безбедносног
менаџмента» _____

- резултат сопственог истраживачког рада,
- да предложена дисертација у целини ни у деловима није била предложена за добијање било које дипломе према студијским програмима других високошколских установа,
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио интелектуалну својину других лица.

Потпис докторанда

У Београду, 26. 10. 2012.

Кристина Радојевић

Прилог 2.

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора Кристина Радојевић

Број уписа 130

Студијски програм Наука безбедности

Наслов рада “Модел за процену ефективности и ефикасности система безбедносног менаџмента“

Ментор проф. др Зоран Драгишић

Потписани Кристина З. Радојевић

изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла за објављивање на порталу **Дигиталног репозиторијума Универзитета у Београду**.

Дозвољавам да се објаве моји лични подаци везани за добијање академског звања доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

Потпис докторанда

У Београду, 26. 10. 2012.

Кристина Радојевић

Прилог 3.

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

„Модел за процену ефективности и ефикасности система безбедносног менаџмента“

која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигитални репозиторијум Универзитета у Београду могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство
2. Ауторство - некомерцијално
3. Ауторство – некомерцијално – без прераде
4. Ауторство – некомерцијално – делити под истим условима
5. Ауторство – без прераде
6. Ауторство – делити под истим условима

(Молимо да заокружите само једну од шест понуђених лиценци, кратак опис лиценци дат је на полеђини листа).

Потпис докторанда

У Београду, 26. 10. 2012.

Др. Милица Радојевић

1. Ауторство - Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце, чак и у комерцијалне сврхе. Ово је најслободнија од свих лиценци.

2. Ауторство – некомерцијално. Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела.

3. Ауторство - некомерцијално – без прераде. Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца не дозвољава комерцијалну употребу дела. У односу на све остале лиценце, овом лиценцом се ограничава највећи обим права коришћења дела.

4. Ауторство - некомерцијално – делити под истим условима. Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца не дозвољава комерцијалну употребу дела и прерада.

5. Ауторство – без прераде. Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, без промена, преобликовања или употребе дела у свом делу, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце. Ова лиценца дозвољава комерцијалну употребу дела.

6. Ауторство - делити под истим условима. Дозвољаваате умножавање, дистрибуцију и јавно саопштавање дела, и прераде, ако се наведе име аутора на начин одређен од стране аутора или даваоца лиценце и ако се прерада дистрибуира под истом или сличном лиценцом. Ова лиценца дозвољава комерцијалну употребу дела и прерада. Слична је софтверским лиценцама, односно лиценцама отвореног кода.