

ФАКУЛТЕТ БЕЗБЕДНОСТИ
УНИВЕРЗИТЕТ У БЕОГРАДУ

**Планирање као фаза безбедносног менаџмента у приватним
организацијама**

— Дипломски рад —

Ментор:
проф. др Зоран Драгишић

Студент:
Младен Матић

Београд, 2021. године

Садржај:

<u>УВОД</u>	<u>1</u>
<u>1. ПОЈМОВНО ОДРЕЂЕЊЕ ПЛАНИРАЊА</u>	<u>3</u>
1.1. ФАЗЕ ПЛАНИРАЊА	5
1.2. СВРХА ПЛАНИРАЊА	7
1.3. ЗНАЧАЈ ПЛАНИРАЊА	9
<u>2. ФЕНОМЕНОЛОГИЈА БЕЗБЕДНОСНОГ МЕНАџМЕНТА.....</u>	<u>11</u>
2.1. ЗАДАЦИ БЕЗБЕДНОСНОГ МЕНАџМЕНТА	13
2.2. ФАЗЕ БЕЗБЕДНОСНОГ МЕНАџМЕНТА	14
2.3. УПРАВЉАЊЕ БЕЗБЕДНОСНИМ РИЗИЦИМА.....	16
<u>3. БЕЗБЕДНОСНО ПЛАНИРАЊЕ У ПРИВАТНИМ ОРГАНИЗАЦИЈАМА.....</u>	<u>18</u>
3.1. ИМПЛЕМЕНТАЦИЈА БЕЗБЕДНОСНЕ ПОЛИТИКЕ У ПРИВАТНИМ ОРГАНИЗАЦИЈАМА	23
<u>ЗАКЉУЧАК</u>	<u>27</u>
<u>ЛИТЕРАТУРА.....</u>	<u>29</u>

Увод

„Планови нису ништа, а планирање је све.“

– Двајт Ајзенхауер

Ово су речи чувеног Америчког војсковође и политичара, најпознатији по успешном командовању савезничким снагама у западној Европи током другог Светског рата који је знао да испланира своје потезе пре и током сваке борбе. Добро планирање је основа даљег рада организације и остварења обличних резултата, планирамо како не би наишли на проблеме током рада и како би били спремни на изазове који су испред нас. Као једна од функција унутар менаџмент процеса видимо да планирање представља темељ целокупног процеса, и видимо да ако је темељ лоше постављен онда ће и све што следи после њега да буде фалишно, и баш због овога је битно да се спроведе добро планирање сада битно, како не би дошло до проблема даље у другим процесима менаџмента. У циљу бољег разумевања планирања рад је подељен на три елемената који формирају кохерентну целину.

У првом делу бавимо се појмовном одређивању планирања где се прича о битности планирања као функције менаџмента безбедности и где се планирање дефинише, следећи део представљају фазе планирања у којима има више елемената који су међусобно повезани у једну целину, и на крају овог првог дела прича се о која је сврха планирања која је битна да се разуме јер помаже организацији смањити неизвесност и значај планирања који организацији пружа велике могућности и предности.

У другом делу се посвећујемо феноменологији безбедносног менаџмента у коме говоримо о појму безбедносног менаџмента и дефинишемо шта је безбедносни менаџмент после тога се сагледамо то који су задатци безбедносног менаџмента задатак безбедносног менаџмента јесте да сви задаци унутар организације теку на начин који не компромитује безбедност организације, следеће јесте који су конкретне фазе безбедносног менаџмента оне су нужно повезане и једна исходи из друге и на крају како се врши управљање безбедносним ризицима где се дефинише шта је то ризик па онда сагледамо различите ризике који могу да настану унутар организације.

Док би у трећем делу причали о суштини а то је безбедносном планирању у приватним организацијама где има елемената који су јако битни за планирање и које су од

великог значаја за организацију, на крају говоримо о имплементацији безбедносне политике у приватним организацијама где причамо о примени ових елемената унутар организације.

1. Појмовно одређење планирања

Једна од најбитнијих менаџерских функција јесте планирање. Као такво, оно потпада у оно што би Питер Дракер (*Peter Drucker*) окарактерисао као пет базичних менаџерских операција у које спадају: постављање задатака, организовање, мотивација и комуникација, мерење и развој људи (Drucker, 2006: 341). Оно би се могло сврстати у категорију постављања задатака и то као њен *sine qua non*.

Процес планирања се заснива на систематском и континуалном размишљању о будућности пре него што се донесу одлуке о деловању, уз покушај предвиђања последица које ће то садашње деловање имати у будућности (Драгишић и Радојевић, 2018: 51). Менаџер, поготово менаџер безбедности, планирањем гледа да у својој будућности елиминира што је већи број негативних фактора, а да максимизира позитивне факторе по организацију. Планирање је есенцијално за сваког менаџера, независно од његове позиције или нивоа на коме се налази.

Као менаџерска функција, планирање је њен темељ и везује се за доношење одлука путем којих се организација усмерава према будућности. Међу тим одлукама, најбитније су визија, мисија, циљеви, стратегије и планови (Лабовић, 2015: 78). На поменутом темељу се граде све функције организације. Говорећи у контексту циљева и њиховог остваривања, може се рећи да је резултат процеса планирања – планска одлука. Из тога проистиче да случају лошег планирања нужно долази до доношења лоших одлука. Међу главним планским одлукама налазе се циљеви, тј. доношење циљева. Из тога проистичу све остале одлуке које имају допунску функцију (Драгишић и Радојевић, 2018: 51). Иако се планирање често не започиње без задатог циља, само формулисање циљева јесте део планирања. Тачније, формулација циљева се може сматрати једним обликом претпланских активности. Касније, када се та активност оконча, а циљеви поставе могуће је прећи на даље фазе у менаџменту. Оне, последично морају пратити задати курс кретања и функционисати у склопу планских одлука.

С обзиром на значај планских одлука, било би неопходно кратко одређење значења тог појма. Планске одлуке представљају једну врсту шаблона, односно оријентира који ће користити у доношењу правовремених и квалитетних одлука. Као што је споменуто, оне се

односе на курс кретања организације, тачније речено, оне проистичу из задатих циљева и практично операционализују сваку менаџмент фазу.

У концепцији планирања, могуће је уочити различите организационе приступе. Тако, Хенри Минцберг (*Henry Mintzberg*) сумирајући различите приступе и дефиниције планирања пише о пет приступа планирању, познатијем као 5П приступу. Исти се дели на (Машић и Џелетовић, 2015: 99):

- **планирање као размишљање о будућности;**
- **планирање као контрола будућности;**
- **планирање као процес доношења одлуке;**
- **планирање као интегрални процес доношења одлуке и**
- **планирање као формализована процедура која резултира интегралним системом доношењем одлука.**

1.1.Фазе планирања

Из наведеног одређења се може констатовати да је планирање процес доношења планских одлука. Овде би требало одредити шта се подразумева под планским одлукама. Разни аутори пишу о различитим планским одлукама које су међусобно повезане и интегрисане. Недовољно је рећи да су планске одлуке само циљеви–стратегије–плани, већ ту спадају и визија и мисија. Дакле према томе фазе планирања су: визија, мисије, циљеви, стратегије и плани (Машећ и Џелетовић, 2015: 135–139).

Визија. Она је на врху пирамиде фаза планирања, за визију је могуће рећи да у пословном свету значи далекосежни поглед на будућност, као и нови методи за решавање проблема. Визија мора бити замислива, привлачна, могућа, фокусирана и погодна за комуникацију. У супротном, она се не може сматрати визијом и као таква не може бити на врху пирамиде планирања.

Мисија. Она дефинише и даље операционализује визију организације. Ово се поготово односи на различите аспекте пословних подручја у којима организација жели да конкурише. Иста се могу односити на циљна тржишта, географска подручја пословања, филозофске и производне услове.

Циљеви. Имају сврху појачавања дефинисане мисије, у њеним кључним областима управљања растом и развојем. Утврђивање развојних циљева подразумева детаљну анализу трендова унутар средине и ван ње, затим се односи на посматрање организације и њених циљева као целине, потом креирање хијерархије циљева и на крају одређивање листе индивидуалних развојних циљева. Значај циљева односи се највише на обављање многобројних менаџерских активности.

Стратегија. Једна од најчешће коришћених речи у менаџменту. Она подразумева општи план акција које имају за сврху остваривање, раније споменутих, циљева. Када се говори о пословној стратегији, онда се ради о налажењу начина и приступа којима ће се остварити, првенствено мисије, а затим и циљеви предузећа (или организације у ширем смислу). Најчешће се пословна стратегија односи на период од три до пет година, те као таква подразумева један вид дугорочног пословног планирања (CioIndex, 2018).

Плани. Представљају најнижи облик операционализације визије, мисије и циљева. Они су фактички појединачне идеје о томе како спровести стратешке концепте. У

себи садрже детаљне тачке које инкорпорирају стратегију и свакодневно пословање предузећа или организације.

Фазе планирања могу се сагледати и на другачији начин. Тада се оне посматрају кроз следеће етапе (Машић и Целетовић, 2015: 100):

- базично финансијско планирање;
- планирање засновано на предвиђању;
- екстерно оријентисано планирање и
- стратешки менаџмент.

За сврхе овог рада, тачка ослонца ће бити на првобитно наведеним фазама. Разлог томе, лежи у чињеници да оне на целисходнији начин обухватају саму тематику рада, тј. планирање у безбедносном менаџменту.

1.2.Сврха планирања

Уколико се осврт направи на сврху планирања у проактивном светлу, његова сврха јесте да умањи ризик тако што смањује неизвесност при условима пословања и уочава последице поступака који су везани за управљање. Сврха овакве акције доводи до повећања степена организационог успеха. Тиме се види да је фундаментални сврха планирања – помоћ (Management Inovations, 2008).

Највећу могућност да се оствари циљ даје стратегијско планирање. Џорџ Штајнер (*George Steiner*) даје многобројне делове који покривају стратегијско планирање (Машић и Целетовић, 2015: 103).

Први део се односи на одлуке у стратегијском планирању. Фокус је дакле, доношење одлука у садашњости како би се оне оствариле у будућности. То онда не значи израда будућних одлука. Оне могу само у садашњости да се донесу. Сврха формалног стратегијског планирања јесте препознавање шанси и прилика које могу да се десе у будућности. Комбиновање шансе и претње са другим релевантним информацијама предузећа представља темељ за боље одлуке у искоришћавању шанси и отклањање претњи (Машић и Целетовић, 2015: 103).

Даље, планирање јесте поступак којим започиње утемељивање организационих циљева. Ово се односи на вођење организације путем раније споменуте визије, мисије и развојних циљева. Спрам овога се дефинишу политике и стратегије за њихово остварење и развој прецизних планова уз помоћ којих се обезбеђује имплементација стратегије којом се остварују циљеви и мисије предузећа (Машић и Целетовић, 2015: 103).

Потом, трећи део се односи на начин живота и представља један од делова који долази у обзир. Преданост стратегијском планирању иде даље од пуког мисаоног процеса и интелектуалне вежбе. Он је више од сета процедура, структура или техника. Како би се максимизирао учинак менаџера и запослених у предузећу, исти треба да верују и да хоће да раде у складу с својим способностима (Машић и Целетовић, 2015: 103).

На крају, четврти део јесте спајање три главне врсте планова и представља битан систем у стратегијском планирању. Ту се укључују стратегијски план, средњорочни програм, краткорочни буџет и оперативни планови. Према томе, Штајнер дефинише стратегијско планирање као систематски и више или мање формализовани труд предузећа

на утемељивању основе сврхе циљева, политике и стратегије компаније, као и развој прецизних планова примењивање политике и стратегије као и остварење циљева и базичне сврхе компаније (Машић и Целетовић, 2015: 103).

1.3.Значај планирања

Планирање игра значајну улогу у менаџмент процесу, јер даје велики и разнолике предности организацији. Значај планирање јесте у томе што се њиме добијају следеће могућности: повећање ефикасност; смањење ризика; омогућавање правилне координације; помоћ у организовању; пружање правца организацији; одржавање добре контроле; помоћ организацији при остварењу циљева; мотивација људи; подизање нивоа креативности и иновације; помоћ у одлучивању (Akranі, 2012).

Повећање ефикасност организације. Планирањем се оптимизује коришћење ресурса и избегава непотребно дуплирање и траћење. Поред тога, добија се највећи могући профит уз најниже могуће трошкове. На крају, планирањем се подиже свеобухватна организациона ефикасност (Akranі, 2012).

Смањење ризика који је укључен у модерно пословање. Као што је већ јасно, постоје многи ризици у савременом свету пословања. Оно што је значај планирања, у таквим околностима, јесте његово покушавање да предвиди те ризике и начини идејну скицу њиховог превазилажења. Та скица је један општи оквир за израду оперативних планова избегавања ризика и одговора на будуће потенцијалне проблеме (Akranі, 2012).

Омогућавање правилне координацију унутар организације. Планирање је есенцијално за унутрашњу координацију. Иако су интерни елементи веома често међусобно добро координисани, додатно планирање не може да шкоди. Оваква ситуација важи за комплетну хијерархијску структуру организације. Дакле, од нивоа највишег менаџмента, па до индивидуалног нивоа радника, планирање доводи до боље и правилније координације индивидуалних карика у систему (Akranі, 2012).

Помоћ у организовању. Организовање, у овом контексту, се односи на могућност окупљања свих расположивих ресурса. Потпуно је очигледно да је овај процес немогућ без адекватног планирања. У том случају, планирање говори колику количину ресурса треба употребити и где да је искористити (Akranі, 2012).

Пружање правца организацији. Усмеравање организације у одређеном правцу је круцијално за њен опстанак. У том смислу, прецизне информације, инструкције и упутства могу бити велика предност уколико се пруже запосленима. У том смислу, планирање представља основицу која намеће шта треба да се уради и како (Akranі, 2012).

Одржавање добре контроле. Из аспекта контроле, учинак запослених се не може измерити уколико не постоји одређена референтна тачка. Та референтна тачка се поставља управо плановима. Дакле, учинак је могуће мерити на основу планова и последично кориговати недостатке или наградити добре резултате (Akrani, 2012).

Помоћ организацији при остварењу циљева. Раније је било много речи о циљевима и њиховом односу са планирањем. Овде треба напоменути да је рекапитулација тог односа осликана у чињеници да планирања помаже организацији да оствари своје циљеве. Такође, адекватан процес планирања доводи до смањења могућности да се ураде или одвију неке насумичне радње суманутог или сувишног карактера (Akrani, 2012).

Мотивација људи. С обзиром на раније споменути значај планирања у погледу напретка и опстанка организације, намеће се закључак да је финансијски просперитет и процват директно зависан од целисходности процеса планирања. У том смислу, већа финансијска стабилност, омогућава постизање материјалне мотивације људи. Такође, с обзиром да није све у материјалној мотивацији, те да нематеријални облици мотивације имају велики значај у расту и развоју организације (Бодин, 2019: 136–171), финансијска средства омогућавају управо те нематеријалне облике мотивисања.

Подизање нивоа креативности и иновације. Када се планови израђују, неопходан је релативно несвакидашњи приступ и одређена доза креативности у циљу што бољег одређивања курса кретања организације. Управо је тај приступ и креативност оно што се развија кроз укљученост у процес планирања (Akrani, 2012).

Помоћ у одлучивању. Једна од најстреснијих улога које менаџер носи јесте доношење одлука и формирање алтернативних праваца. Како би се то амортизовало, планови представљају ослонац менаџера у доношењу тих одлука. С обзиром на њихову холистичну природу, они предвиђају велики број могућих ситуација. Стога менаџер не мора да трпи притисак да ће својом одлуком угрозити организацију. Дакле доношење одлуке је олакшано планирањем (Akrani, 2012).

2. Феноменологија безбедносног менаџмента

Ако посматрамо менаџмент из историјског концепта он је настао у далекој прошлости и има везе са способношћу да са што мање улагање добије много више и оствари бољи резултати. Оно што данас знамо о менаџменту може се наћи још у старим цивилизацијама. Правовремене одлуке и добар план су били од кључног значаја за преживљавање и развој једне цивилизације. Иако менаџмент досеже далеко у прошлост, зачетци његове распрострањеније примене у модерном добу, налази се у индустријском раздобљу, где се тај процес одвијао што рационалније у сврху повећања профита (Драгишић и Радојевић, 2018: 10).

Изрази и облици менаџмента се различито гледају у јавној и приватној сфери која је настала као подела у капиталистичком друштву. Али менаџмент се користио као термин за делатности управљањем предузећа, док се управљање државним организацијама поготову војском и полицијом чешће користе изрази као што су руковођење и командовање као специфичне функције менаџмента (Драгишић и Радојевић, 2018: 11).

Појединачни аутори безбедносни менаџер представљају као субјекат који организује и руководи системом обезбеђења лица и имовине, тј. професионално управљање (физичка компонента), опремом (техничка компонента) и безбедносним процедурама у ширем смислу. Безбедносни менаџмент смишља читав систем обезбеђивања, усклађује рад особља, операционализује и координира планиране активности с другим субјектима безбедности, врши контролу рада и сноси одговорност за реализацију планских активности (Лабовић, 2015: 76).

Посматрано из ширег гледишта безбедносни менаџмент подразумева се као доношењем одлука о безбедносним циљевима организационог система о начинима и средствима помоћ у којих ћемо избегавати негативне утицаје које долазе ван организације или унутар ње, као и да смањи њихов штетни ефекат. Менаџмент у свакој организацији придаје велику пажњу безбедности као једном од главних услова који су потребни остварити како би се стекли услови за раст и напредак организације. Свака организација има своје посебне изазове, ризике и претње с којима се суочава. Различити изазови, ризици и претње којима су изложене предузећа и организације као и као и одговорност које те

организације имају према окружењу по питању безбедности, значајно утичу на безбедносни менаџмент тј. како ће бити донете одлуке о безбедности (Драгишић и Радојевић, 2018: 11).

2.1.Задаци безбедносног менаџмента

Ако се пође од претпоставке да је задаци менаџмента у општем смислу, обухватају планирање, буџетирање, организовање, прикупљање људства, контролисање и решавање проблема (Kotter, 1996: 25), онда би се могло рећи да је главни задатак безбедносног менаџмента да сви ови задаци теку на начин који не компромитује безбедност организације и њених чланова.

Међутим, неопходно је нешто конкретније дефинисати задатке безбедносног менаџмента. Разлог за то јесте чињеница да ефективност безбедносног менаџмента зависи од нивоа конкретизације саме делатности менаџера безбедности.

Добро дефинисана организациона структура омогућава искоришћавање шанси и заобилажење претњи, као и претварање тадашњих проблема у предности. Менаџмент безбедности треба да обезбеди контролу над факторима који могу да угрозе организацију коју он штити. Контролом и праћењем фактора угрожавања остварују се две ствари. Прво фактор угрожавања се може елиминисати пре него што се испољи, или уколико је могуће неутралисати односно елиминисати штетне последице фактора угрожавања. Друго ако је фактор ризика такав да се не може избећи нити неутралисати последице које он оставља, топ менаџмент треба да предвиди штетне последице које носе за собом фактори ризика ,и то представља битно полазиште за доношење стратешких одлука које су везане за штетне последице. (Драгишић и Радојевић, 2018: 14-15).

Основа за безбедносни менаџмент било које организације јесте циљеви, које та организација поставила. Нормално је да се ти циљеви повремено преиспитивају. Циљ безбедносног менаџмента јесте заштита виталних вредности организације, као и унапређење и напредак организације и остварење њених циљева. Доношење стратешких одлука не доноси безбедносни менаџмент, али може да утиче на њихово доношење, преко информација који обезбеђује топ-менаџменту и процена који утичу на дефинисање стратешких циљева и доношење оперативне одлуке , у којој на крају зависи опстанак и даљи развој предузећа. (Драгишић и Радојевић, 2018: 15).

2.2. Фазе безбедносног менаџмента

Посматрајући планирање као процес, намеће се закључак да постоје одређене фазе у том процесу. Те фазе нужно су повезане и једна исходи из друге. Оне се не могу и не смеју посматрати као самосталне целине јер на тај начин немају никакву сврху. Фазе планирања обухватају следеће функције: дефинисање циљева; безбедносна процена; доношење одлука и израда планова.

Дефинисање циљева. Одређивање циљева јесте веома битан део планирања. Свако планирање креће од донете одлуке. Та одлука се односи на оно што се жели остварити унутар или ван организације. Може се приметити да постоје разлике у постављању циљева између приватног и јавног сектора. У приватном сектору, тј. у приватним организацијама менаџери безбедности добијају готове циљеве које је поставио топ-менаџмент, а од њих се даље очекује да омогуће безбедно спровођење истих. Са друге стране, у јавном сектору (у који спадају и војска и полиција), циљеви који се постављају руководиоцима свих нивоа, представљају део државне политике. У том смислу, наведени руководиоци не би смели утицати на те одлуке, ни у ком случају (Драгишић и Радојевић, 2018: 51).

Безбедносна процена. Битан аспект у планирању безбедносних мера и стварању организационе структуре јесте безбедносна процена, она треба да реализује прописане безбедносне мере и процедуре. Зависно од квалитета безбедносне процене, зависи нам учинковитост целокупног система уједно представља главни показатељ за стварање организације и за све остале кораке које ће се применити. (Драгишић и Радојевић, 2018: 52-53).

Одлучивање. У процесу планирања одлучивање је значајан део процеса планирања, али не само планирања већ и менаџмента. Спровођење одлука представља рутински посао менаџера и од тих одлука зависи какви планови могу бити донети и који ће исходи бити постигнути. Квалитетно донете одлуке, као и брзина којом је одлука доноси и на који начин се спроводе донете одлуке, значајно утичу на то какав ће успех имати организација. (Драгишић и Радојевић, 2018: 79).

Израда планова. Фаза израде планова је техничко административног карактера путем којим се формулишу планске одлуке и њена репрезентација кроз један или више планских докумената. Током израде плана уносе се сви делови одлуке, ти делови су

циљеви, задаци, снаге, средства, рокови, мере безбедности и слично. Због непредвидивости у коме ће се предузеће наћи флексибилности у планирању манифестује се кроз израду мулти варијантних планова, то представља основни механизам којима се менаџер осигурава у будућности.

2.3.Управљање безбедносним ризицима

У циљу управљања безбедносним ризицима, неопходно је превасходно знати шта је безбедносни ризик и каква је његова природа. Да би се у томе успело, потребно је направити анализу, тј. процену ризика коју Закон о приватном обезбеђењу („Сл. Гласник РС“, бр. 104/2013, 42/2015 и 87/2018) дефинише као анализу и оцену ризика у заштити лица, имовине и пословања. Међутим, ова дефиниција је недовољно прецизна, те је као таква не превише корисна за разумевање концепта управљања ризицима. Кековић и сарадници дају далеко комплетнију дефиницију управљања ризицима, те наводе да је то значајан аспект управљања квалитетом који има улогу подржавања у остварењу захтеваног квалитета који је поставио систем. Примарни циљ управљања квалитетом јесте уградња стратешког плана управљања који осигурава све прохтеве система квалитета, док је циљ управљања ризиком да чак и у случају ризичних догађаја задржи квалитет система. Управљањем ризиком треба осигурати опстанак система (Кековић и сар., 2011: 51).

У својој књизи „Живот у канцеларији“, Бартман даје једно занимљиво запажање. Наиме, он каже: „На чудан начин смо постали владари који не владају али имају утицај кроз управљање. Управљамо собом, нама повереним сарадницима, нашим процесима и нашим инструментима“ (Bartmann, 2012: 133).

Такође се на ризике гледа кроз аспекте перцепције и информисања о ризицима, процену ризика и управљање ризика, под ризиком подразумевамо и потенцијалне директне или индиректне губитке по друштвене субјекте или систем. Ризик се може видети и као вероватноћа да ће одређени ниво губитка бити подржан датим серијама елемената као резултат датог нивоа утицаја опасности. Једна од најједноставнијих и најзаступљенијих дефиниција везано ризике, према којој ризици представљају вероватноћу последица одређених катастрофа. Људи доживљавају ризике веома различито и томе придоноси перцепција ризика која утиче на доношење одлука на индивидуалном, организационом, општинском нивоу. Управљање ризиком јесте функција која се састоји од неколико под функција, које заједно раде у циљу информативног одлучивања на свим нивоима организације и заједнице. Према међународној стратегији за смањење ризика од катастрофа управљање ризицима представља систематичан приступ и праксу управљањем неизвесностима, како би се смањили губитци и потенцијална штета. Управљањем ризиком

од катастрофа може да се дефинише и као системски процес коришћења административних одлука, оперативних вештина и капацитета за имплементацију података, стратегија и капацитета друштва и заједнице да се изборе и смање ефекти природне катастрофе (Цветковић, 2017: 35–40). Врсте ризика је уопштено могуће поделити на следеће: правне ризике, информационе ризике, кризне ситуације и ризици који обухватају управљање људским ресурсима.

3. Безбедносно планирање у приватним организацијама

Безбедносно планирање у приватним организацијама има разне аспекте које мора да сагледа један од тих аспекта јесте и нормативно правни део односно правни ризици. Тешко је наћи дефиницију правног ризика у литератури, међутим у међународним стандардима и другим документима изостаје појам правни ризик, термин се помиње ,или је описан или као подврсту других класификација ризика. Према Базелском комитету за надзор банака који је 1988. године усвојио сет од три препоруке – то су Базел 1, Базел 2 као и Базел 3 – они се односе на оперативне и финансијске ризике које могу да се десе у банкарству. Базел 2, је оригинално усвојен 2004. године, ту се директно помињу правни ризици, али их не дефинише, него се сврстају у категорију оперативних ризика. Међународна адвокатска асоцијација је 2005, године у списима на тему менаџменту ризиком које су рађене за потребе адвокатских канцеларија и приватних друштава, где је постављена дефиниција правног ризика који гласи последица дефектне трансакције, правног захтева друге стране, неиспуњавања прописа или законских. У литератури је истакнуто поред тога што изостаје експлицитна помињање правних ризика у законодавству Европске уније, тај концепт у Европи се спроводи кроз разне принципе права ЕУ. У Европском законодавству правни ризици се спроводе кроз: стварање нове обавезе у европском праву; измена у законодавству; недовољно дефинисане норме и правила законодавства европске уније; непоштовањем облигације које су биле постављене у европском законодавству и добијање правних захтева према лицу на бази европског законодавства. Битна ствар у безбедносном планирању јесте и дефинисање ризика ту постоји подела на шире и уже опције у погледу дефинисању ризика. У ширем аспекту правни ризици су сви пословни ризици који остављају велике правне последице промена. Ужи приступ дефинише правне ризике као ризике које могу да настану из правног делања или правне неизвесности, и тиме оставља последице на пословне активности. Заступљена је и намера да се правни ризици не везују експлицитно правне последице које могу да настану него и штете по углед, ако и последице на организациону културу унутар организације. Такође код ширег приступа правни ризик се одређује као вероватноћа настанка негативног правног резултата смерну тежином потенцијалне правне штете. Правни ризик би онда био вероватноћа наступања нежељеног правног догађаја (као нпр. Губитак спора) и тежине правне последице (једна од последица је између осталог и

накнада штете).Притом други приступ би узео на разматрање да су ови ризици квалитативног карактера. По овоме правни ризик би био утицај правне неизвесности (нпр. Промена законодавства) на остварење циљева (пословних и репутационих) при томе да будући догађаји могу имати и позитивну страну (Милошевић и Младеновић, 2018: 42–44).

Следећи елемент који игра круцијалну улогу у безбедносном планирању јесте информациони ресурси, јер свако добро планирање захтева добре информације. Корпоративни ресурси су добра која служе да побољшају способности корпорације и да ради односно послује у том правцу који ће фирми донети профит. Најбитнија корпоративна добра која компанија може да поседује јесте људство, имовина и подаци тј. информације. Анализом и обрадом тренутних података/сазнања и употребом истих, податак као такав добија већу квалитативну вредност и постаје информација. Процес обраде података од стране онога ко га поседује јесте поступак којим податак постаје информација. Таквим процесом податак добија квалитативну основу, и може се користити у процесу планирања као и у процесу доношења одлука. У тренутку коришћења информација, податак постаје информација. Вредност податка тј. колико је он употребљив као пословна информација зависи од неколико елемената: актуелност, поузданост, тачност, трајност, расположивост као и колико задовољава потребе организације. Битан део протока информација и где се информације чувају јесу рачунари и рачунарске мреже. Рачунари и рачунарске мреже су под великим ризиком и претњама. Процес према коме се идентификују претње јесте веома сложен ,почевши од физичких па све до виртуелних (вируси) у сајбер простору. Амбијенталне околности такође могу да буду део претњи, између осталог и елементарне непогоде, технички кварови, грешке у пројектовању и коришћењу рачунара, али и намерне штете коју су појединци изазвали у физичком или у сајбер простору. Рачунарски системи нису само циљ или мета напада, већ могу бити употребљени и у чињењу кривичних дела, из тога проистиче и факат да су они битан доказ у процесу доказивања кривичног дела. Кривична дела у сајбер напада је веома тешко доказати и идентификовати нападача и повезати га са средством извршења напада (Путник ,2018: 55–59).

Битна елемент који треба сагледати јесте кризне ситуације, према речима Бенцамина Френклина који се често цитиран у литератури за кризни менаџмент, која гласи само су две ствари у животу неизбежне порез и смрт. Без обзира на делатност организације ово се односи на све организације. На кризе нису имуни ни организације попут клубови цркви и

музеја. У данашњем времену глобализације и динамичном друштву, у профитном сектору постоје разне врсте кризних ситуација константа, мада на немилосрдном тржишту нису сви подједнако угрожени тј. подложне кризама. Што је околина у којој фирма послује динамичнија, то је већа могућност да дође до кризе. Кризе које имају утицај на здравље и безбедност, посебно утичу на људе као што је рецимо криза око безбедност хране и/или лекова које могу да оставе дуготрајне последице по репутације прехранбене и фармацеутске организације. Белике и угледне компаније нису имућне на кризе, и код њих може да се деси криза. У свету који је међусобно повезан различите кризе и епизоде које се догађају долази и до радних места. Проблеми који су се често јављали изван пословне сфере, сад су нашле њихов пут до фабрика, постројења и канцеларија. Тако су корпоративни проблеми полако прелазе у друштвену сферу, а тиме још доприносе и медији који имају кључну улогу социјалном конструисању света. Најјаче и најперспективније корпорације могу да буду тешко оштећене кризним ситуацијама, што је кључно *differentia specifica* у односу на кризе у државама и јавним институцијама који не могу да нестану (Кешетовић, 2018: 119–121).

Планирање у људским ресурсима је изузетно битан посао јер се тиме зацртава мапа којом организација иде, што се тиче људских ресурса, тиме она усаглашава своје тренутне и будуће потребе које се тичу људских ресурса. Планирање у области људских ресурса је систематична и системски процес откривања и предвиђања шта ће се од запослених тражити како би се направила резерва запослених и волонтера са битним вештинама и знањем када се укаже прилика. Планирање људским ресурсима треба да докаже како квалитетно управљање људским ресурсима унапређује ефикасност организације и њен даљи развој. Оно што организације треба да ураде приликом управљања људским ресурсима је да дефинишу и позиционирају као стратешки део организације. Организација је израдила следеће битне ставке: Стављање процедура за сталну процену потреба запослених; резервне планове за сваког кључног запосленог у случају одсуства или губитка; преглед критичних радних позиција за функционисање организације и стављања планова занављања и наслеђивања. Како би сето остварило потребни су стручњаци из разних области права, менаџмента, психологије, безбедности и информационих технологија. Када говоримо о регрутацији и селекцији који зовемо „максимална величина опасности“ утврђује да: Није утврђена ни одобрена анализа радних позиција /места и задатак за позицију организације;

систем за регрутовање није сталан процес који се заснива на циљевима; нису утврдили нити документовали критеријум којим се селекује кандидат за радно место и кандидати не потписују документа с којима се упознаје са ситуацијом која је везана за посао који ће радити (Спасић, 2018: 169). Исти критеријуми за „минималну величину опасности“ утврђује да је: урађена и одобрена анализа радних позиција/места и задатак за све позиције у организацији; систем регрутовања успостављен као стални/континуални процес засниван на циљевима; утврђени су и документовани критеријуми за селекцију кандидата за радне позиције; сви кандидати за посао у компанији отписују документа којима се упознавају са свим релевантним информацијама о свом радном месту, као и обавезама и правима између фирме и појединца. (Спасић, 2018: 167–169).

Битна ставка у безбедносном планирању јесте информација која се добија путем пословног обавештајства – БИ (*Business Intelligence – BI*). Значење пословног обавештајства није увек једнозначно у свету се користи дуже од четврт век, а праксу на коју се односи користе готово све компаније у свету. Појам БИ се погрешно изједначава са нелегалним или тајним пословима тј. шпијунажом као и са појмом конкурентско обавештајство који се појавио у САД крајем 50–их година 20. века. Израз пословно обавештајство потиче од Хауарда Дреснера, експерт и компаније *Gather Group* (САД), који је ај појам сковао 1989. године, с намером да изврши категоризацију методолошких концепата и техника које могу бити од велике користи топ менаџменту компанија у процесу одлучивања. Постоји неусаглашеност ван енглеског говорног подручја око превођења појма „*Business Intelligence*“ због чега се он користи у његовом оригиналном облику. У домаћој литератури, медијима, огласима, фирми које нуде те врсте услуга и стручној јавности, све чешће се чује термин „пословна интелигенција“, „пословно обавештајно деловање“, „пословно истраживање“, „управљање пословним информацијама“ и слични појмови. Пословно обавештајство одликују три кључне одлике: процес легалног и етичког прикупљања података који после обраде постају информација; процес је усмерен на податке и информације који се могу искористити да проценимо будућу ситуацију и кризе; у питању је инструмент који има важну улогу процесу доношења одлука на нивоу организације. (Триван, 2018: 179–180). Циљ пословног обавештајства јесте прикупљање повољних информација пре конкуренције тј. рано откривање пословних претњи који прете из

окружења, како би се менаџери припремили за евентуалне кризне ситуације (Триван, 2018: 179–180).

3.1.Имплементација безбедносне политике у приватним организацијама

Један од најегзотичнијих примера када је у питању значај имплементације безбедносне политике у приватним организацијама јесте спречавање обавештајног рада усмереног на конкурентност. Као такав, он представља процес који умногоме наличи на класичан обавештајни процес, карактеристичан за националну безбедност (Кековић и сар., 2018: 205).

Информационо–комуникациони ресурси играју кључну улогу у имплементацији безбедносне политике у приватним организацијама. У информативно–комуникационих система (ИКС) организација у коме се складишти огроман број информација, и притом неки од тих података могу бити од велике вредности или се могу сматрати тајним податком или као личну, пословну или професионалну тајну. Бас из тих разлога било какав напад на информационо–комуникационих система може да доведе до тешке и непоправљиве штете по организацију. Заштита информационих система и инфраструктуре има двојаку функцију: да спречи злоупотребу ИКС–а као и да када дође до злоупотребе да се изврши увиђај и брзо открије ко је одговоран за напад на ИКС. Организације се редовно сусрећу са великим опсегом безбедносних претњи који се фокусирају на информационо–комуникационе системе и њихове кориснике – мрежним нападима и упадима у систем у стварном свету коришћење социјалног инжењеринга, саботажама, вандализмом, кампањама које руше углед, електронско насиље и много више. Напади који долазе са свих страна из дана у дан постају све опаснији и комплекснији, као и учесталост тих напада је у порасту. Како би се такве претње спречиле потребно је да менаџер створи планове везане за политику безбедности информационо–комуникационих ресурса, и њихових корисника. Менаџери који планирају безбедносну политику ИКС треба да приђу са холистичне стране проблему и да сагледавају различите аспекте заштите информационо–комуникационих ресурса и њихових корисника и њихових корисника. На основу досадашњој пракси тј. добром искуству погодно би било применити моделе вишеслојне заштите. Он је по својој природи проактиван и има неколико елемената (Путник, 2018: 71):

- Логично–технички (употреба логичких и техничких средстава заштите);
- Физички (средства за контролни приступ);
- Кадровски (планирање и избор кадрова);

- Организациони (организациона структура, смернице и стандарди итд.) и
- Нормативни (закони, упутства, планови и други прописи).

Елементи који имају логичне, техничке и физичке спадају у технички аспект заштите, док организациона, кадровска и нормативна спада у друштвени аспект заштите. Оба аспекта су од великог значаја и само се њиховим комбиновањем и кооперацијом између два дела може достићи задовољавајући ниво заштите информационо–техничких система и података. Сви аспекти заштите треба да буду присутни у политици информационо–комуникационих ресурса и њихових корисника. Један од кључних елемената који треба да се нагласе у безбедносној политици јесте и сегмент заштите приватности корисника информационо комуникационих технологија, као и борба против електронског насиља. Наиме, постављање безбедносне политике у области заштите ИКТ систем не треба посматрати као изолован процес, независно од осталих система безбедносне заштите организације. Холистички приступ којим се прилази организационој безбедности организације представља мултикаузално сагледавање међуповезаним ризицима где заштита ИКТ система представља елемент јединственог и динамичног система безбедносног менаџмента. Сходно томе стварање смерница за градњу безбедносне политике треба да почне да препознаје опасности и сам процени ризик јер се стратегије заштите заснива баш на тим елементима (Путник, 2018: 70–72).

Супротно пословном обавештајству и његовом деловању, јесте офанзивно обавештајство (*Business Counterintelligence* – CI). Офанзивно обавештајство се састоји од прикупљању података, такође постоји и друга дефанзивна димензија пословног обавештајства која се састоји од противобавештајног деловања. Ова димензија пословног обавештајства јесте усмерена на остваривање безбедности и постављање механизма за његову заштиту од пословног обавештајства деловања супарничке организације као и заштиту виталних пословних података од шпијунаже и осталих противзаконских деловања. Темељни циљ пословног обавештајства јесте задржавање тренутне пословне позиције организације у пословном окружењу, процена могућих опасности и претњи по организацију као и заштита од нелегалних активности других субјеката против организације. За обе наведене димензије пословног обавештајства, одговоран је стратешки менаџмент који је на крају и корисник резултата таквих активности. Офанзивно обавештајство је састоји од неколико фаза прва фаза се састоји од планирања тј. постављањем задатака. У овој фази се

утврђују разлози због које би организација могла бити мета угрожавања, анализа пословних планова као и сагледавање односа организације са субјектима који могу да угрозе организацију. Друга фаза се састоји од тога да се детектују извори угрожавања и претње, тј. утврђују се потенцијалне конкурентске организације који могу да нанесу штету организацији. Због тога се мора сазнати шта конкуренцију интересује и које податке тражи, и тиме сазнати које ће методе конкуренција користи у циљу прикупљања података од интереса. Додатно треба направити анализу властитих способности и тражити потенцијалне рупе унутар организације тј. слабе тачке које могу да буду експлоатисане од стране конкуренције. Трећа фаза јесте дефинисање и развој одговарајућих противмера, а затим и одговарајући механизам заштите против напада конкуренције. После свих ових фаза следи задња фаза, анализа постигнутих резултата. Циљ офанзивног обавештајства јесте заштита информација који су од виталног значаја за функционисање организације, као и спречити потенцијалне претње и подићи сигурност организације. То се може постићи једино ако су подаци тотално заштићени тј. ако се примењују све сигурносне мере у свим релевантним деловима који су битни с аспекта пословања. С обзиром на то да се важне информације за даљи ток функционисања организације налазе у разним медијима, пре свега потребно је предузети одговарајуће мере који за циљ имају за задатак заштиту тајности и интегритета информатичких и других комуникационих средстава унутар организације. Информацијама најчешће баратају запослени и њима треба усадити квалитетне и правилне навике у руковању информацијама. Потребно је поставити и то које информације се сматрају тајним и поверљивим као и мере које се предузимају како би информације остале скривене. Такође треба преузети одговарајуће техничке мере како би спречило недозвољени улаз у организацију и тиме спречи крађа и други видови угрожавања. И коначно битно је поставити одговарајуће безбедносне механизме приликом селекције и регрутације, као и приступ битним пословним информацијама како би се ризик од злоупотребе смањено на минимум (Караловић, Ивановић Видовић, Остојић, 2011: 238–239).

Битна ставке како би се имплементирала безбедносна политика јесте и безбедносна култура у кризном управљању. Безбедносна култура је битна за стварање индивидуалних и групних вредности, ставова, перцепција, компетенција и образаца понашања који одређују посвећеност здрављу и доброти организације и менаџмента безбедности. Организације у којима је безбедносна култура има карактеристике комуникација засноване на међусобном

поверењу , и тиме се међусобно деле схватања о значају безбедности ,ако и уверење у деловање проактивних мера. Дешавања током акутне фазе кризе, организација тада реагује тј. примењује мере које су предвиђене у кризном плану и тиме прелази из нормалног режима рада у кризни режим рада максимално настојећи оствари своје основне функције. Треба нагласити да је кризни менаџмент не представља егзактну науку већ праксу која је руковођена теоријом, такође ни кризни план није решење за све и не садржи сва решења које треба механички следити да би се проблем реши, веш је то скуп принципа и процедура које су флуидне и креативно их применити у кризи када дође до ње. Кад је притисак ја к ситуациони лидери су много значајнији од формалних лидера. Када стварамо план морамо се фокусирати на сигурност људи у организацији, као и комуникацију и смањење штете у организацији. Када је план направљен он се мора повремено ажурирати и прилагођавати. Битни функционални делови који се активирају како би се захватиле све потенцијалне опасности на које се криза може усредсредити и унапред успоставила подручија одговорност и ланац командовања јесу: операције, кадрови, логистика, техничка подршка, и комуникације. Овај приступ ради у великим организацијама, а суштина је да се добијају рани инпути из различитих функционалних елемената (Кешетовић, 2018: 129–130).

Закључак

Планирање има велико место у фазама безбедносног менаџмента приватних организација. У првом делу овог рада говорило се о појмовном одређењу планирања у коме се прво дефинисало шта је планирање и како је од великог значаја за менаџмент и наравно гледање других аутора на појам менаџмента и колико је битно знати прво шта је планирање пре него што се било шта уради. Такође се говорило и о фазама у којима се види како планирање тече, и како су те фазе међусобно повезане и интегрисане једна с другом и тиме помажу даљем разумевању планирања у безбедносном менаџменту. Сврха планирања је следећи део у коме се говори колико предности има у томе када се планирање спроведе и каже се да планирање доводи до побољшања у организацији, као и то да имплементацијом стратегије и политике организација како би остварила сврху и базични циљ организације. На крају првог дела битан део разумевања планирања јести и његов значај који даје велики број предности као што су повећава ефикасност; смањење ризика; омогућавање правилне координације; помоћ у организовању; пружање правца организацији; одржавање добре контроле; помоћ организацији при остварењу циљева; мотивација људи; подизање нивоа креативности и иновације; помоћ у одлучивању због ових елемената је планирање од круцијалног значаја.

У другом делу рада се бавимо феноменологијом безбедносног менаџмента у којима говоримо шта је менаџмент безбедности кад је настао и колике предности он пружа организацијама као га имплементира, поред тога менаџмент безбедности је битан и код одлука које доноси јер те одлуке су од кључног значаја за организацију јер елиминише губитке. Фазе менаџмента безбедности су итекако битне за његово разумевање јер те фазе нам говоре како менаџмент безбедности функционише и како он тече, те фазе су међусобно повезане и исходе једна из друге како би оствариле задатке које су им задати. Задатци које безбедносни менаџмент постави пред собом су од великог значаја како би организација остварила своје циљеве, то успевамо тако што склапамо елементе као не би компромитовали један другог и тако дођу до циља. Следећа ствар која је битна за разумети јесте безбедносни ризици који имају значајан аспект управљања квалитетом који има улогу помагања у достизању зацртаног квалитета који је поставио систем и да ако се то спроведе успешно да је шанса да дође до ризика значајно смањена.

Трећи део јесте суштина рада у коме се бавимо планирањем у приватним организацијама и имплементацијом безбедносне политике. Овај део се састоји од елемената који нам помажу у разумевању теме, ти елементи су из правне безбедности у коме се правни ризици јављају као претња и који морају да буду обухваћени планирањем да би то на крају довело до позитивног исхода и како би избегли штету не само финансијску већ и губитак репутације организације. Информационо–комуникациони део се бави информацијама од значаја како се податак претвара у информацију значај чувања података и које врсте података се чувају, као и колика штета може да настане ако се подаци открију или се систем злоупотреби, Значајно је крине ситуације које могу да настану, оне су неизбежне и могу се десити свим организацијама зато се гледа да се они елиминишу као не би дошло до већих проблема тако што се ставља акценат на безбедносну културу унутар организације. Укључивање људских ресурса је исто битно, јер ћемо планирањем зацртати пут људским ресурсима. Планирање у оквирима људских ресурса је јако битно јер так сагледавамо аспекте као што су анализа радног места, критеријуми везани за регрутацију и селекцију као и прича о правима и задацима запосленог. Задњи део је пословно обавештајство које је од великог значаја за добијање информација и у исто време одбрана својих информација од конкуренције и злоупотребе, јер се квалитетно планирање заснива на dobrим информацијама.

На основу овога може да се закључи да је планирање неизбежан део када се ради о безбедносном менаџменту у приватним организацијама, јер планирањем ми гледамо како да у време динамичне околине и непредвидивог тржишта смањимо и по могућности елиминишемо све ризике које су везане за пословање, и организацији обезбедимо сигурније пословање у будућности и профите. Јер како је говорио Бенџамин Френклин, чувени амерички научник, политичар и један од твораца америчког устава „Ако не планирате, ви планирате неуспех.“

Литература

1. Akrani, G. (2012). *Importance of Planning - Why Planning is Important?*. Kalyan City Life. Преузето 15. априла 2021. године са shorturl.at/mVY59
2. Bartmann, C. (2012). *Leben im büro – Die schöne neue Welt der Angestellten*. München: Carl Hanser Verlag.
3. CioIndex. (2018). *Business Strategy*. cio-wiki.org. Преузето 04. априла 2021. године са https://cio-wiki.org/wiki/Business_Strategy
4. Drucker, P. F. (2006). *The practice of management*. New York: Harper Collins.
5. Kotter, J. P. (1996). *Leading change*. Boston: Harvard Business Review Press.
6. Management Inovations. (2008). *Planning Characteristics*. Преузето 09. априла 2021. године са <https://managementinnovations.wordpress.com/tag/purpose-of-planning/>
7. Бодин, М. (2019). *Менаџмент људских и друштвених ресурса*. Београд: Факултет безбедности.
8. Димитријевић, И. и Кучековић, З. (2018). Пословно-обавештајни рад усмерен на конкурентност. У: Кековић, З., Димитријевић, И. и Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 195–208). Београд: Факултет безбедности.
9. Драгишић, З. и Радојевић, К. (2014). *Безбедносни менаџмент*. Београд: Факултет безбедности.
10. Ђорђевић, И. (2013). *Људска безбедност*. Београд: Институт за упоредно право и Досије студио.
11. Закон о приватном обезбеђењу („Сл. Гласник РС“, бр. 104/2013, 42/2015 и 87/2018)
12. Караловић, Л., Ивановић Видовић, Д. и Остојић, А. (2011). *Корпоративна сигурност*. Загреб: Удруга Хрватских менаџера сигурности.
13. Кековић, З., Димитријевић, И. и Шекарић, Н. (2018). *Корпоративна безбедност – Хрестоматија*. Београд: Факултет безбедности.
14. Кековић, З., Савић, С., Комазец, Н., Милошевић, М. и Јовановић, Д. (2011). *Процена ризика и заштита лица, имовине и пословања*. Београд: Центар за анализу ризика и управљање кризама.
15. Кешетовић, Ж. (2018). Функционисање корпорација у кризним условима (кризне ситуације, кризно комуницирање и медији). У: Кековић, З., Димитријевић, И. и

- Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 119–144). Београд: Факултет безбедности.
16. Лабовић, Д. (2015). *Приватна безбедност у Републици Србији – правни аспекти и компаративна искуства*. Докторска дисертација. Крагујевац: Правни факултет.
17. Машић, Б. и Целетовић, М. (2015). *Увод у менаџмент*. Београд: Иновациони центар Факултета безбедности Универзитета у Београду и Академска књига.
18. Милошевић, М. и Младеновић, М. (2018). Управљање правним ризицима као елемент корпоративне безбедности. У: Кековић, З., Димитријевић, И. и Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 39–52). Београд: Факултет безбедности.
19. Пешић, Ј. (2020). *Лидерство у приватном безбедносном менаџменту*. Дипломски рад. Београд: Факултет безбедности.
20. Путник, Н. (2018). Систем корпоративне безбедности: информациони аспекти. У: Кековић, З., Димитријевић, И. и Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 53–74). Београд: Факултет безбедности.
21. Спасић, С. (2018). Критеријуми ризика у управљању људским ресурсима према националном стандарду СРПС А.Л2.003 Безбедност и отпорност – процена ризика. У: Кековић, З., Димитријевић, И. и Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 157–176). Београд: Факултет безбедности.
22. Стратегија националне безбедности Републике Србије („Сл. Гласник РС“, бр. 94/2019-13)
23. Триван, Д. (2018). Значај пословно-обавештајног деловања за корпоративну и националну безбедност. У: Кековић, З., Димитријевић, И. и Шекарић, Н. (ур.). *Корпоративна безбедност – Хрестоматија*. (стр. 177–194). Београд: Факултет безбедности.