д-р ОЛИВЕР БАКРЕСКИ
д-р ДРАГАН ТРИВАН
м-р САШО МИТЕВСКИ

КОРПОРАЦИСКИ БЕЗБЕДНОСЕН СИСТЕМ

ОЛИВЕР БАКРЕСКИ
ДРАГАН ТРИВАН
САШО МИТЕВСКИ

КОРПОРАЦИСКИ БЕЗБЕДНОСЕН СИСТЕМ

СКОПЈЕ, 2012

КОРПОРАЦИСКИ БЕЗБЕДНОСЕН СИСТЕМ

Рецензенти:

д-р Милан **МИЛОШЕВИЌ**,
Криминалистичко-полициска академија – Београд

д-р Трајан **ГОЦЕВСКИ**,
Филозофски факултет – Скопје

д-р Желимир **КЕШЕТОВИЌ**,
Факултет за безбедност – Београд

д-р Денис **ЧАЛЕТА,**
Институт за корпоративни безбедносни студии – Љубљана

Издавач	Комора на Република Македонија за обезбедување на лица и имот
Лектор	м-р Лилјана **ПАНДЕВА**
Дизајн на корица	Ресана **МИХАИЛОВА**
Графички уредник	Билјана **ИВАНОВА**
Печати:	СТЕДА ГРАФИКА – Скопје
Тираж:	1000

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

351.746.3:347.72
351.759.5:347.72

БАКРЕСКИ, Оливер
Корпорациски безбедносен систем / Оливер Бакрески, Драган Триван, Сашо Митевски. - Скопје : Комора на Република Македонија за обезбедување на лица и имот, 2012. - 273 стр. ; 24 см

Фусноти кон текстот. - Библиографија: стр. 257-273

ISBN 978-608-65505-0-9

а) Корпорациска безбедност

COBISS.MK-ID 92758282

СОДРЖИНА

ПРЕДГОВОР

Во теориското дискурс се смета дека прашањата за корпорациските безбедносни системи се едни од најтешките, затоа што се врзани за управувањето со сите безбедносни процеси во корпорацијата, но ова не значи дека создавањето ваков систем само по себе ќе значи и соодветен придонес за поефикасна заштита на корпорациите од загрозувања кои се насочени кон безбедноста на имотот и кон работењето на компаниите. Сепак, нема дилема дека заштитата на имотот на корпорациите мора да биде врвен приоритет за корпорациската безбедност на компанијата која мора да биде исклучително добро организирана, имајќи ги предвид мотивите на сопствениците на имотот и капиталот да го заштитат и да го сочуваат по секоја цена. Токму во оваа насока треба да биде и корпоративната безбедност, односно да оневозможи да дојде до суптилно „губење или топење" на имотот како последица на разните обиди за оттуѓување и узурпација на имотот, како и намалување на материјалните загуби од различно потекло, настанати како резултат на заканите и ризиците со кои се соочува безбедноста на самата компанија.

Без разлика на интердисциплинираноста, комплексноста и сложеноста на проблематиката, корпорациската безбедност во оваа книга може да се разгледува низ призмата на одредени примери, случаи и проблеми во работата на корпорациите, како и со истакнување на автентичноста на идеите на самите автори врзани за повеќето аспекти на корпорациската безбедност за да допре до самите потешкотии кои се врзуваат за опфатот и за содржината на корпорациската безбедност. Оттука, во книгата не е направено само синтетичкото изучување на прашањата врзани за определување на безбедноста во сите нејзини елементи, туку направен е и еден сублимат на анализи и синтеза на одговори на прашања коишто се однесуваат на корпорациската безбедност како една своевидна анализа за содржините и за опфатот на ова област. Со ваквиот пристап се изразува определбата на авторите корпорациската безбедност да се доближи до сите оние кои директно или индиректно се занимаваат со изучување на вакви прашања, со цел да стекнат претстава за целината на безбедносното

организирање во корпорациите и нивно функционирање во чувствителни ситуации, но книгата според опфатот на содржината ја прави привлечна и интересна не само за оние личности кои се вклучени во образовниот процес туку и за сите оние што се надвор од образовната сфера, како што се вработените во безбедносниот сектор, како и за другите области во општествениот живот.

Нашата голема благодарност им ја должиме на почитуваните рецензенти, проф. д-р Милан Милошевиќ, проф. д-р Трајан Гоцевски, проф. д-р Желимир Кешетовиќ и проф. д-р Денис Чалета за искажаните позитивни оцени за книгата и за препораките за нејзино објавување, на сите оние кои со своите стручни анализи и сугестии помогнаа да се доближиме до вкупните состојби во оваа област. Изразуваме голема благодарност на нашите семејства за разбирањето и поддршката во долгиот процес на создавање на оваа книга. Исто така, изразуваме благодарност и на „Бортас" ДОО – Скопје, „Пивара Скопје АД", „НЃ-Инжинеринг", „Дени Интернационал" – Скопје, „Ројал Трејд" – Куманово, „Промес" – Скопје, „Кватро" – Куманово, „Урбан Десинг" – Скопје, ресторан – „Имес", ресторан „Џино" кои финансиски го помогнаа публикувањето на книгата. Особено му се заблагодаруваме на издавачот „Комора на Република Македонија за обезбедување лица и имот" што овозможи да ја споделиме корпорациската безбедност со читателите.

Скопје, декември 2012 година

Авторите

ВОВЕД

Познато е дека технолошката револуција, урбанизацијата и индустријализацијата редовно ги следи пораст на организираниот и на класичниот криминалитет, како и на други асоцијални појави. Во овој контекст на загрозувањето на безбедноста на луѓето, на имотот и на работењето на компаниите секако дека влијание има и зголемениот број т.н. „опасни или „валкани" технологии, така што со право може да се говори за нови облици на криминалитет: нуклеарен, еколошки и други. Во сферата на стопанското работење постојано е присутна и опасноста од акциденти, бидејќи јонизирачките зрачења, отровните и експлозивните испарувања и другите продукти на модерната технологија константно се следени од деструктивни појави коишто може да предизвикаат многу штетни последици.

Овие опасности неминовно ја наметнуваат потребата на современото општество на сите нивоа сеопфатно и енергично да се спротивставува на сето она што ги загрозува животите и здравјето на луѓето, на имотот и на работењето на компаниите. Тоа спротивставување мора да биде стручно, професионално и перманентно, но и да опфаќа широк спектар на мерки и постапки, како на планот на превенција, така и во поглед на санирањето на штетните последици. Поради тоа организираните деловни субјекти, а особено големите техничко-технолошки системи, се принудени да применуваат адекватни превентивни мерки да посветуваат и максимално внимание на прашањата врзани за безбедност и за заштитата. Во таа смисла, корпорациската безбедност е составен дел од организацијата на работата и на работниот процес во компаниите кои се состојат од повеќе меѓусебно комплементирани потсистеми. Организациската единица задолжена за безбедност на компанијата, односно на фирмата мора перманентно да биде вклучена во механизмите на корпоративното управување за да го штити и да го обезбеди нормално одвивање на деловните процеси, како и да ги отстранува акутните безбедносни проблеми, но и да создава услови за работа и за производство.

Оттука, корпорациската безбедност ги обезбедува клучните претпоставки за сестран развој, но истовремено ја намалува

веројатноста од појава на ризици во работењето во компанијата со што ѝ се доверува улогата да биде гарант во осигурувањето на континуираното работење и решавање на проблемите од комплексен карактер. Корпорациската безбедност, меѓу другото, придонесува и за зголемена енергетска безбедност на државата, која подразбира дивергентни правци за снабдување, стабилност на испораката и производството на енергенси, како и создавање неопходна автономност и јакнење на регионалната позиција во снабдувањето со енергенси и производи. Во овој контекст, една од целите на корпорациската безбедност е да обезбеди корпорациите, во согласност со можностите, да ги поддржат безбедносните и одбранбените подготовки на национално ниво и во случај на загрозување на безбедноста на државата да помогнат во обезбедувањето на потребите на населението, како и да обезбедат логистичка поддршка на клучните структури во системот на националната безбедност. За навремено преземање на овие мерки, особено е важно да постои усогласување на постојните и донесување нови прописи кои би придонеле за поголема оперативност во реагирањето на компаниите и на државите во различни ситуации.

Проучувањето на корпорациската безбедност во оваа книга главно ја темелиме на пет основи.

Првиот пристап се базира на определување на безбедноста и на проучување на безбедносните концепти. Безбедноста придонесува во голема мера за осигурување на мирот и стабилноста на државите, со најмалку неколку елементи, и тоа: прво, преку она што се нарекува справување со безбедносни ризици и закани кои ја загрозуваат стабилноста на државите или одредени подрачја. Суштинска карактеристика на тие ризици и закани е тоа што тие сè повеќе стануваат непредвидливи, асиметрични и имаат транснационален карактер; второ, безбедноста во насока на решавање социјални немири кои се закануваат да ја нарушат внатрешната стабилност на државата, и трето, преку она што таа прави – со промовирање на глобална безбедност преку соработка.

Вториот пристап се фокусира на прашањата врзани за корпорациската безбедност. Тука, корпорациската безбедност се сведува на тоа дека таа е системски организирана дејност, која е насочена кон осигурување на безбедноста на компанијата и кон конкретна заштита на одредени лица, простор, објекти, бизниси итн. Обезбедувањето на посакуваната состојба на безбедносно работење на корпорацијата зависи од голем број фактори кои придонесуваат за појава на позитивни или на негативни безбедносни

појави. Секоја корпорација може да се соочи со голем број ризици, при што за менаџментот од клучно значење е соодветно да ги идентификува, но и да направи соодветна процена на веројатноста за појавување определен ризик, како и да ја предвиди големината на штетата која може да настане за корпорацијата во такви услови.

Третиот пристап го објаснува влијанието на корпорациската безбедност врз националната од аспект на економијата. Тука се истакнува дека корпорацијата е пример на сложена организација во која напорите за создавање екокономска стабилност на државата се гледаат во контекст на националните политики за развој на корпорациите. Оттука, напорите треба да бидат насочени кон поголема заинтересираност на државата за корпорациите во делот на овозможување подобри услови за работа, оневозможување на нелојалната конкуренција на пазарот, подобрување на правната уреденост во делот на работењето, постоење адекватен систем за контрола и евиденција врз чија основа би можело да се направи увид во тој сектор, елиминирање политички влијанија и манипулации, спречување криминализација во делот на преземање и давање услуги за обезбедување итн.

Четвртиот пристап го објаснува влијанието на корпорациската безбедност врз националната во доменот на организираниот криминал. Движечка сила на сите активности на организираниот криминал на национално и на транснационално ниво е профитот што се остварува од нелегалната трговија (често заснована на монопол), криумчарење, трговија со дрога и оружје, економски криминал итн. Значаен дел од тие пари циркулира низ легалните финансиски системи или се вклучени во легалните финансиски институции или во вложувања во недвижности, а еден дел се држат, односно се чуваат како готовина, додека трети се составен дел на финансиски операции на трансферот преку интернет. Со овие, како и со други форми, секогаш се настојува да се прикрие или да се маскира правната природа на сопственоста на средствата стекнати со незаконско работење.

Петтиот пристап се однесува на влијанието на корпорациската врз националната безбедност од аспект на информациската безбедност. Во современи услови остварувањето на целите на корпорациите е незамисливо без ефикасно спроведување на информациската безбедност. Во тој контекст, информациската безбедност подразбира заштита на националните информациски ресурси и потенцијали од физичко загрозување, во отсуство на опасности кои можат да ја загрозат информационата стабилност и самостојност.

I глава

КОНЦЕПОТ БЕЗБЕДНОСТ

1. ОПРЕДЕЛУВАЊЕ НА БЕЗБЕДНОСТА

Безбедноста влегува во доменот на оние термини што при инфлација на сопствената употреба, придружена со голем број дефиниции, на крајот доживуваат ефект обратен од посакуваниот. Наместо разјаснување, настанува замаглување. Наместо откривање на суштината, доаѓа до нејзино (не)намерно затскривање. Ваквите заклучоци може да звучат необично, ако се има предвид дека глобалните и националните актери манифестираат желба за поместување на фокусот на интересот на безбедносните студии од државата кон низа општествени прашања, кои во минатото беа целосно занемарени и ретко споменувани во овој контекст. Така, навидум, безбедносната дебата доби поттик и на научен и на политички план, особено со вклучувањето на новите референтни објекти на безбедноста („она што треба да се заштити“), како што се општествените групи (социетална безбедност), човечкото суштество (хумана безбедност) или животната средина (еколошка безбедност). Светот е денес побогат за бројни теориско-безбедносни иновации низ кои се настојува да се објаснат современите случувања. Истовремено, тие исти концепти не ретко служат за маскирање на воените, на политичките и на другите неуспеси, особено во контекст на толку посакуваната превенција.[1]

Поимот безбедност има повеќе значења и за да може да се разбере треба да се разгледува од повеќе аспекти (теориски, политички, правни, социолошки и др.,) за да може да го утврдиме значењето на безбедноста за државата. Инаку, појавата на безбедноста, односно нејзините корени датираат уште пред постоењето на државата што значи дека безбедноста постоела многу порано, дури и пред настанувањето на државата. За безбедноста се говори дека настанала уште кога се појавил човекот и неговите напори како да се преживее. Дури подоцна безбедноста се проширува на сета заедница, односно на државата.

[1] Пошироко види: Ванковска Б., *Меѓународна безбедност*, Филозофски факултет, Скопје, 2011, стр. 11.

Значи, во почетокот со цел да се обезбеди потребното ниво на безбедност, луѓето почнале да се здружуваат во мали заедници. Многу брзо овие мали заедници со својата структура и едноставен систем на општествена контрола почнале да се менуваат, односно да еволуираат во големи групирања. Со тоа се јавила потребата за нови форми на регулација и заштитата во безбедносна смисла. Тој еволутивен пат на развој, како и распаѓањето на одделни заедници, како и сите антагонизми кои се резултат на раздвоеноста на поединците во развојниот процес на малите заедници, се основна причина за новиот термин безбедносен механизам. Во таа смисла, заедницата од најрани времиња, а подоцна сè повеќе во ликот на своите институции и системи, се појавува како главен носител на регулација на системското легитимно влијание на однесувањето на луѓето кон однапред, во рамките на таа иста заедница, поставени критериуми. Тој процес го следи развојот на безбедноста низ историјата, кој имал различни форми на дејствување во разни историски ситуации.[2]

Терминот безбедност е многу комплексен и изразито сложен општествен феномен. Во текот на историјата под поимот безбедност се подразбирале различни содржини. Етимолошки гледано, изразот безбедност е во врска со латинскиот збор securutas – atas, што значи безбедност, отсуство на опасности, извесност, самодоверба, заштитеност (securus лат. – сигурен, безбеден, доверба, уверен, постојан, цврст, вистински итн.). Овој терминолошки израз послужил како основа за употреба во теоретското изучување на проблемот на безбедноста во многу држави. Така, во англискиот јазик се користат два израза: security и safety. Терминот security се користи во смисла на национална безбедност (secure – сигурен, да се осигура) – national security, што имплицира остварување и заштита на државните национални интереси, додека терминот safety означува способност за дејствување, за да не дојде до непосакувани безбедносни ситуации, или такви околности кои можат да предизвикаат безбедносни импликации. Во францускиот јазик постои и се користи изразот securite и surete, додека во рускиот јазик се користи терминот безопасност и значи отсуство на материјална беда, а во италијанскиот јазик се користи изразот sigureza (sicyramente – сигурно), додека во Германија тој израз е sicherheit.[3] Сличен е коренот и во македонскиот јазик

[2] Masleša R., *Teorije i sistemi sigurnosti,* „Magistrat" Sarajevo, 2001, str. 3.

[3] Стајић Љ. и Гаћиновић Р., *Увод у студије безбедности*, Стучна књига, Београд, 2007., стр, 24.

безбедност – „без“ „беда“ (без загроза). Сепак, базично е прашањето за тоа *што* или *кој* е оставен без грижа и колку евентуалната грижа е реална (објективна безбедност) или имагинарна (субјективна безбедност).[4]

Во основа, треба да се разбере дека безбедноста сама по себе не создава ништо, но од друга страна таа го овозможува опстанокот и развојот на општеството и во однос на државата и во однос на поединецот, таа е и биолошки и рационално фундирана за да го обезбеди потребното ниво на безбедност за државата, за нацијата, за граѓаните итн.

Во однос на државата, безбедноста ги синтетизира државните функции врз основа на искажани потреби на граѓаните. Значи, во процесот на гарантирање оптимален степен на безбедност, државата остварува одредени функции. На неа се гледа како на комплексен процес кој бара учество на бројни институции. Државата ги изведува следните работи за да гарантира висок степен на национална безбедност: прво, внатрешни политички гаранции за националната безбедност. Државата, со помош на националната дипломатија, се стреми да постигне внатрешна средина во која националната безбедност е гарантирана. Второ, безбедност. Безбедноста значи гарантирање и давање поддршка на мирот и стабилноста, заштита на националните интереси и вредности, поддршка на економијата итн. и трето, менаџмент и контрола на процесот на гарантирање на висок степен на национална безбедност. Ефикасно постигнување на националната безбедност е невозможно без управувачка и контролна функција.[5]

Значи, постигнување чувство за безбедност е фундаментална задача на државата во новата безбедносна средина во која државните институции треба да одговорат адекватно на променетата природа на внатрешните и на надворешните закани, ризици и предизвици. Така, во контекстот на намалена веројатност за воен конфликт помеѓу државите, општествата сè повеќе ги согледуваат организираниот криминал, трговијата со дрога, тргувањето со луѓе, перењето пари и економскиот криминал како главни закани по нивната безбедност. Друг голем предизвик во безбедносната

[4] Види: Ванковска Б., *Меѓународна безбедност*, Филозофски факултет, Скопје, 2011, стр. 16.

[5] *Management of Defence*, Democratic and Civilian Control, Including Integration of Security Sector, pp. 2-3.

средина претставува и процесот на глобализација. Глобализацијата е феномен карактеризиран од неколку процеси и услови, вклучувајќи доминација на капитализмот и слободната трговија, интеграција на економските и на политичките системи, технолошки прогрес, глобални комуникации и отсуство на бариери за протокот на информации, ресурси, идеи и вредности. Глобализацијата го зголемува просперитетот на учесниците во процесот, но во исто време наметнува ризици и закани за државите.[6]

Колку поимот безбедност е интересен, значаен и сложен, најдобро говори податокот дека тој заинтересирал повеќе истражувачи. Приодот кон безбедноста најдобро го изразил угледниот истражувач Арнолд Волферс (Arnold Wolfers), чии истражувања за безбедноста, а особено националната безбедност, се едни од поистакнатите во оваа област.[7] Предупредувајќи на повеќедимензионалноста и сложеноста на проблемот на безбедноста, Волферс, безбедноста ја одредил како „неодреден симбол" кој може, но и не мора да има некое значење. Поради тоа, за да се разбере безбедносниот феномен, потребно е да се изучуваат темелните категории на поимот безбедност, видовите на безбедност, механизмите за неговото остварување, видовите на загрозување итн.

Во литературата постојат голем број дефиниции за тоа што е безбедност. За потребите на овој труд ние ќе издвоиме само неколку од широката лепеза дефиниции без притоа понатаму пошироко да ги разгледуваме и да ги анализираме сите поединечно. Така, безбедноста е повеќезначна и во теоријата и во практиката и таа се користи за да се означат разновидните елементи и односи.

Според дефиницијата за безбедност изработена во рамките на ООН во 1986 година, „безбедноста е состојба во која државите сметаат дека нема опасност од воен напад, од политички принуди или од економски присили, така што можат слободно да се развиваат и да напредуваат".[8]

Во тој контекст, се и размислувањата на Фискер кој идентично како и во претходното елаборирање смета дека „безбедноста е состојба во која државите сметаат дека нема опасност од загрозувања, па така тие можат слободно да се развиваат. Исто

[6] Ibid., p. 1.

[7] Wolfers A., *National Security as an Ambiguous Symbol, Discord and Collaboration*, John Hopkins University Press, Baltimore, 1962.

[8] *Conception de la sécurité*, Série d`études 14, Publication des Nations Unise, 1986, A/40/533

така, во понатамошната елаборација тој наведува дека безбедноста на индивидуите и на заедниците од кои се состојат државите е осигурана со гаранции за ефикасно почитување на индивидуалните слободи, политички, социјални и економски права, како и со заштита или обнова на поволната животна средина за сегашните и за идните генерации. Безбедноста, исто така, имплицира дека основните човекови потреби, пред сè, во делот на исхраната, образованието, домаќинството и јавното здравство, се осигурани на трајна основа, и дека е потребно да се одржува адекватна заштита од евентуални опасности за безбедноста. Начините и средствата за добивање ваков вид безбедност се дефинирани во национални, во меѓувладини, во невладини и во глобални услови".[9]

Според Јан Лодер и Нил Вокер, безбедноста е драгоцено јавно добро, односно нужен елемент на секое „добро општество", и дека нужна и доблесна задача на демократската држава е да го создаде и да го одржува ова јавно добро.[10]

Во аргументацијата на Манголд стои дека безбедноста е изразена преку високиот степен на неприкосновеното право за опстанок и за одбрана на виталните интереси на државата. Со тоа безбедноста тежнее кон осигурување на стабилноста на државата преку насочување на своите потенцијали за справување со заканите.[11]

Милетиќ безбедноста ја дефинирал како „правно уредување и обезбедување на општествените односи и унапредување на состојбата во државата, што овозможува ефективна заштитеност на државата и на граѓаните кои во неа живеат од сите (надворешни и внатрешни) противправни акти (активности) со кои се загрозува уставниот поредок, суверенитетот, независноста и територијалниот интегритет на државата, работата на државните органи, извршување на стопанските и општествените дејности и остварување на слободата, правата и должностите на човекот и граѓанинот."[12]

Според Маслеша, безбедноста претставува најосновната општествена цел без која нема опстанок на општеството и овој поим

[9] Fischer, D., *Nonmilitary Aspects of Security: A Systems Approach*, Aldershot: United Nations Institute for Disarmament Research, 1993, p. 10.

[10] Ian Loader and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press, 2007., преземено од Ванковска Б., Меѓународна безбедност оп. цит.

[11] Mangold P., *National Security and International Relations*, Rotledge, London and New York, 1990.

[12] Милетиќ С., *Полицијско право*, Полицијска академија, Београд, 1997.

се употребува речиси во сите области на животот и работата и оттука сите настојувања одат во правец на воспоставување соодветна рамнотежа помеѓу човекот и безбедноста.[13]

Синиша Таталовиќ смета дека безбедноста е структурен елемент на опстојувањето и на дејствувањето на поединците, општествата, државите и меѓународната заедница и таа е една од основните животни функции.[14]

Митко Котовчевски смета дека безбедноста можеме да ја третираме како состојба во која е осигуран урамнотежениот физички, духовен, душевен и материјален опстанок на поединецот и на општествената заедница во однос на другите поединци, општествени заедници и природата или безбедноста во суштина претставува иманентен структурен дел на општеството што во себе вклучува определена состојба, односно определени особини на состојбата, а исто така и дејност, односно систем.[15]

Поаѓајќи од политиката што ја гради Република Македонија во сферата на безбедноста, под безбедност се подразбира: (1) одредена (достигната или проектирана) состојба на безбедност, (2) функционално подрачје на дејствување различни безбедносни институции, заедно со вкупните општествени настојувања на полето на постигнување на безбедносните цели и (3) безбедносните институции, поврзани во одреден систем на односи.

Од изнесеното може да се заклучи дека без соодветно ниво на безбедност, нема ниту индивидуални слободи на граѓаните. Во таа смисла, слободно можеме да кажеме дека безбедноста има функција на служење. Меѓутоа, во ниту едно општество не може да се оствари максимална безбедност, ниту апсолутна слобода. Се работи за потреба од обезбедување рамнотежа помеѓу безбедноста и заштита на основните права и слободи на граѓаните и интересите на државната заедница. Во таа смисла, слободата и безбедноста сеопфатно треба да се сфатат како варијабилни величини, со оглед на дивергентните, конфликтните и непомирливите интереси на поединците и на групите во секое општество. Истражувањето на феноменот безбедност и безбедносните системи и нивното

[13] Masleša R., *Teorije i sistemi sigurnosti,* Magistrat, Sarajevo, 2001, str. 7.

[14] Tatalović S., *Nacionalna i međunarodna sigurnost*, Politička kultura, Zagreb, 2006, str. 11.

[15] Котовчевски М., *Национална безбедност на Република Македонија*, прв дел, Македонска цивилизација, Скопје, 2000, стр. 21.

непосредно научно објаснување имплицира посебен акцент на анализа и разбирање на политичко-историските процеси и на политичките системи.[16]

2. ТЕРМИНОЛОШКИ ДИВЕРГЕНЦИИ ОКОЛУ ПОИМОТ И УПОТРЕБАТА НА ТЕРМИНОТ БЕЗБЕДНОСТ

Безбедноста е еден од феномените на човековото општество, и тоа во сите фази од неговиот развој. Без разлика дали станува збор за безбедност на поединецот, на државата, на повеќе држави или на меѓународната заедница секогаш се работи за настојување да се осигураат вредностите и состојбите за кои се смета дека се од витално значење. Заради тоа, неопходно е да се разбере овој поим, особено како однос во одреден период и во конкретен регион поаѓајќи од неговите специфичности.[17]

Ако се направи одредена етимолошка анализа со дивергентното сфаќање на терминот безбедност, таа ќе нè упати кон сета сложеност на овој поим. Јазичниот развој има свој придонес во сложеноста на овој поим, почнувајќи од тоа како овој поим се развивал и се доживувал во различни историски периоди и како се приспособувале безбедносните институции да одговорат на сета сложеност на предизвиците во современиот свет. Исто така, во самата комплексност и потешкотија околу дефинирањето и употребата на поимот безбедност нè упатуваат и самите терминолошки нејаснотии кои се јавуваат како резултат на различниот пристап што го имаат некои теоретичари околу елементите кои се составен дел на безбедноста, што секако ги отежнува одговорите на прашањата околу опфатот и содржината на безбедноста и доведува до дефиниции конфузии, а понекогаш и до неаргументирана елаборација на поимот и на употребата на терминот безбедност.

Во научната безбедносна теорија има голем број различни пристапи со повеќезначни контроверзни и тешкоприфатливи одредувања. Овие разлики остваат простор и можност за дивергентно сфаќање и на самата суштина и улога на безбедноста во едно општество и пошироко, што секако може негативно да се одрази

[16] Masleša R., *Teorije i sistemi sigurnosti,* Magistrat, Sarajevo, 2001, str. 4.

[17] Славески С., *Безбедносен систем*, Европски универзитет, Скопје, 2009, стр. 4-17.

како на индивидуалната, така и на националната безбедност, односно на безбедноста во меѓународни рамки. Без разлика на широкиот опфат на дефиниции, останува фактот дека безбедноста е цел кон која се стреми секој поединец, држава и општествена заедница, што претставува фундаментален предуслов за обезбедување и дефинирање на формата на општествено однесување, која се темели на едно системско, легитимно и хуманистичко влијание кон претходно поставени отворени демократски и безбедносни критериуми.[18]

3. ОСНОВНИ КАТЕГОРИЈАЛНИ КОНЦЕПТИ НА БЕЗБЕДНОСТ

На почетокот на втората деценија на новиот милениум и две децении од крајот на Студената војна, дискурсот за концептот на безбедноста не само што не губи од актуелноста, туку сè повеќе се „збогатува". Самото проширување и продлабочување на меѓународната агенда не доведе до поголема ефикасност и успешност во справувањето со акутните и со хроничните безбедносни проблеми. Не помогна ниту богатата и разновидна планета на референтни објекти на безбедноста, бидејќи сè уште доминираат старо-новите методи за разрешување на безбедносните предизвици.[19] Значи, сведоци сме на суштинско продлабочување и проширување на концептот за безбедност, па во тој контекст денес различните димензии на безбедноста ја нагласуваат потребата од поголема заштита на човекот, заштита на енергенсите, суровините и критичната инфраструктура, заштита на посебноста на културата и на идентитетот, заштита на имотот, заштита на корпорациите итн. Ова доведе на безбедносната агенда да бидат прифатени нови безбедносни концепти како „хумана безбедност", „енергетска безбедност", „социетална безбедност"[20], „приватна безбедност", „корпоративна безбедност". Овие концепти јасно ја изразуваат

[18] Masleša R., *Teorije i sistemi sigurnosti,* Magistrat, Sarajevo, 2001, str. 7.

[19] Ванковска Б., *Меѓународна безбедност*, Филозофски факултет, Скопје, 2011, стр. 11.

[20] Социеталната безбедност е дефинирана како „способност да се обезбедат соодветни услови за развојот на посебноста на јазикот, културата, религиозниот и национален идентитет и обичаите." (Waver Ole, *Societal Security: The Concept*, 1993, p. 23).

и ја отсликуваат промената која се случи во сфаќањето на традиционалните концепти за безбедност, наспроти растечката важност на новите безбедносни концепти.

Нема дилема дека безбедноста е феномен кој е изразен со многу меѓусебни односи, но и феномен, за кој и покрај тоа што се има впечаток дека е лесен за прецизно одредување, сепак искуството говори дека станува збор за исклучително тешко детерминирање на неговото значење. Оттука, овој есенцијално значаен феномен мора да биде израз на целосното сфаќање на основните концепти на безбедност за да се разбере самата суштина на самиот поим безбедност. Во тој контекст ќе бидат аргументирани неколкуте клучни концепти значајни за безбедноста на државите во современи услови, и тоа: концептот на индивидуална безбедност, концептот на национална безбедност и концептот на меѓународна безбедност.

На прво место е **концептот на индивидуална безбедност**. За да се оствари таа, потребно е да постои заокружена демократска рамка со владеењето на правото и со сите општоприфатени граѓански и други слободи кои се услов за изградба на цивилното општество. Во таков демократски амбиент со многукратни форми на општествени мрежи доаѓа до меѓусубјективна комуникација помеѓу поединецот и групата, навистина со различни барања и интереси, кои понекогаш имаат непомирлив карактер, што поприма извесен степен на несигурност, бидејќи индивидуалната безбедност се однесува на секој поединец. Токму поради многубројните фактори кои влијаат на безбедноста на поединецот, индивидуалната безбедност е многу тешко да се дефинира. Таа во голема мера има детерминирачко значење за задоволување на нејзините севкупни потреби (личен интегритет, слобода на избор, економски статус, вработување, признавање на неотуѓиви права, образование итн.). Сите овие фактори се во непосредна корелација со функционирањето на демократската и правната држава. Значи, научната елаборација на индивидуалната безбедност треба да се набљудува во контекст на нејзината поврзаност со националната безбедност на државата, која во тој однос има двојна улога. Таа од една страна е одговорна за поволната состојба на безбедноста на поединецот, а од друга страна е извор на закани кои произлегуваат „од домашните пишани закони и употреба на сила, од директна политичка акција на државата против поединци и групи, закани произлезени од потребата за преземање контрола над државната

машинерија и тие кои произлегуваат од надворешно-безбедносната политика".[21]

Во последната декада на минатиот век наместо за индивидуалната безбедност сè повеќе се говореше за концептот на „*хумана или човекова безбедност*". Централно прашање околу идејата за човековата/хуманата безбедност е колку се безбедни и слободни индивидуите.[22] Посериозната артикулација за перспективите на концептот за хуманата безбедност се појави во 1990 година како концептуален одговор на две димензии: глобализацијата и крајот на Студената војна. Дискурсот на релацијата политички и економски трансформации рапидно го зголемија ризикот од внатрешни конфликти. Оваа, пак, го смени фокусот од небезбедност на нацијата -држава до небезбедност на поединецот и заедницата. Генерално земено, таа промена доведе до сознание дека за да се заштити и да се промовира човечкиот развој во иднина, мора да се третира прашањето на хуманата безбедност.[23]

Хуманата безбедност го менува фокусот на интерес од традиционалната безбедност кон безбедноста на личноста, односно, кон безбедноста на поединецот во општеството. Хуманата безбедност препознава дека личната заштита на поединецот и на зачувување на неговиот интегритет не доаѓа првенствено од штитењето на државата како политичка единка, туку од пристапот кон личната благосостојба и квалитетот на животот. Хуманата безбедност не ги вклучува единствено проблемите на индивидуалната добивка, како на пример образованието, здравствената грижа, заштита од криминалот и сл. Ако хуманата безбедност се сфати како зачувување и заштита на животот и дигнитетот на индивидуалното човечко суштество, тогаш може да се зборува за потесна или поширока дефиниција. Хуманата безбедност, дефинирана пошироко, вклучува неколку клучни елементи, и тоа: Првиот есенцијален елемент се однесува на можноста сите граѓани да живеат во мир и безбедност во државата. Тоа претпоставува

[21] Buzan B., *People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era*, Second Edition, Lynne Riener Publishrs, Boulder, Colorado, 1991, p. 25.

[22] Георгиева Л., *Менаџирање на ризици*, Филозофски факултет, Скопје, 2006, стр. 32-33.

[23] Митревска М., Концептот за хумана безбедност, во *Современа македонска одбрана*, вол.IV, бр. 10, декември 2004, стр.12-14.

можност и капацитет државите и граѓаните да превенираат и да ги решаваат конфликтите преку мирни и ненасилни средства, и откако конфликтот ќе заврши, и да имаат способност ефикасно да се справат со напорите за помирување. Вториот елемент е дека луѓето без дискриминација би требало да ги уживаат сите права и обврски, вклучувајќи ги човековите, политичките, социјалните, економските и културните права. Третиот елемент има социјална содржина или еднаков пристап кон политичките, социјалните и други процеси кои ја прават економската политика. Четвртиот елемент е воспоставување на владеење на законот и на независното судство. Секоја индивидуа во општеството би требало да ги има истите права и обврски и да биде предмет на исти правила. Само во тој случај хуманата безбедност значи многу повеќе од заштита од неструктурното-директното физичко насилство.[24]

На второ место се наоѓа **концептот на национална безбедност**. Историски гледано, современиот концепт на националната безбедност е Доктрина за неповредливоста на суверенитетот, која датира од Аугсбуршкиот мир од 1555 година, со кој владетелот добил право да одлучува за религијата на својата земја (cuius regio, eius religio – чија е областа, негова е и верата). Ова право е потврдено и ревидирано со Прашкиот мир од 1635 година и со Вестфалскиот мир од 1648 година, со кој е завршена триесетгодишната верска војна во Европа меѓу католиците и протестантите. Тогаш воспоставениот концепт на државниот суверенитет, по кој никој не е над државата, обединува законски права, по кои сувереноста вклучува политички авторитет заснован на територија и автономија. Територијалноста подразбира право на исклучителен политички авторитет над одреден географски простор (внатрешна сувереност), а автономност значи дека ниту еден надворешен фактор – како што е друга држава – нема авторитет внатре во границите дефинирани од страна на државата (надворешна сувереност).[25]

Самиот поим национална безбедност е во употреба од 1943 година, кога Волтер Липман во своето дело „U.S Foreign Policy“ прв пат го употребил овој термин. По Втората светска војна поимот национална безбедност наоѓа широка примена во политичкиот речник на

[24] Исто., стр. 12-14.

[25] Holsti Kalevi Jaakko, „States and Stateshood“, во: Little Richard, Smith Michael (eds), *Perspectives on World Politics*, Routledge, London-New York 2006., pp.17-24;

современите држави. Во тој контекст тој е употребуван да ги означи внатрешната и надворешната безбедност на државата, односно безбедноста на државата во однос на внатрешни и надворешни извори на загрозување. Се работи за безбедност на една држава која обезбедува нејзин опстанок и нормално дејствување со сите елементи на независност, територијална целовитост и гаранција на уставниот поредок.[26] Според С. Мијалковиќ, ваквата употреба на терминот национална безбедност не е сосема адекватна, имајќи предвид дека со неа се дефинира безбедност на државата, а не на нацијата, која најчесто опфаќа пошироко географско подрачје од државата. Според овој автор, во таа смисла дури и називот државна безбедност бил поточен, бидејќи со неа се обележувала безбедноста на државните вредности и интереси, пред сè суверенитет, опстанок, уставното уредување и поредок на власта, при што грижата за секојдневна безбедност на луѓето е ставана во втор план.[27] Во врска со тоа, основните разлики помеѓу концептот на безбедноста на луѓето и безбедноста на државата се однесуваат на: ентитет кој е предмет на безбедносна грижа т.е индивудуални луѓе кои егзистираат во одредено општествено опкружување и политичко-административните единици спроти државата; доминантна референтна вредност на која и се дава заштита, т.е опстанок и достоинство на луѓето наспроти опстанокот на државата, односно заштита и промоција на човековите права наспроти заштитата и промоцијата на државните права – суверенитет и изразеност на субјективизмот (психолошки компоненти) во сфаќање на човековата безбедност кои се операционализираат како „слобода од стравот“ и „слобода од стискањето“.[28]

Одредени теоретичари националната безбедност ја дефинираат како отсуство на каков било страв од напад, загрозување на интересите или заканите од друга држава или други држави.[29] Во „Меѓународната енциклопедија на општествените науки“ националната безбедност е дефинирана како способност на државата (наци-

[26] Според: Masleša R., *Teorije i sistemi sigurnosti*, Magistrat, Sarajevo, 2001., str. 37.

[27] Мијалковић Саша, „Национална безбедност – од вестфалског концепта до хладноратовског“, *Војно дело* бр. 2/2009, Министарство одбране Републике Србије, Београд 2009., стр. 60.

[28] *Индикатори људске безбедности у Србији – Извештај за 2004*, Факултет цивилне одбране, Београд 2005., стр. 12.

[29] Според: Vukadinović Radovan, *Međunarodni politički odnosi*, Barbat, Zagreb 1998., str.159.

јата) своите внатрешни вредности да ги заштити од надворешните опасности.[30] А. Хеведи ја толкува националната безбедност како функција на националните држави, со помош на која, во согласност со сопствените можности сега и во иднина, а почитувајќи ги глобалните промени и развојот во светот, го штитат сопствениот идентитет, опстанокот и интересите,[31] додека Божидар Јаворовиќ ја разгледува како глобална безбедност на една политичка заедница и како посебна безбедност во рамките на меѓународната заедница. Под националната безбедност тој подразбира внатрешна и надворешна безбедност на државата, односно безбедноста на државата во однос на внатрешните и надворешните видови на загрозување, која обезбедува опстанок и нејзино нормално функционирање.[32] Како што истакнуваат Кегли и Виткоф, „националната безбедност е психолошка слобода на земјата од стравот дека државата нема да биде во состојба да им се спротистави на заканите по нејзиниот опстанок и по националните вредности кои доаѓаат без разлика од надвор или од внатре.[33]

Во врска со тоа, Бери Базан националната безбедност ја разгледува на три нивоа (индивидуална, државна/национална и меѓународна безбедност), вклучувајќи неколку важни подрачја на човековата дејност, првенствено воено, политичко, економско, општествено и еколошко окружување. Според мислењето на овој автор, државното (национално) ниво е најважно, бидејќи ги одредува другите две нивоа на безбедност.[34] Како што истакнува американскиот теоретичар Џозеф Нај,[35] националната безбедност во значителна мера ја детерминира моќта и потенцијалот на државата. Според него, моќ е способност на државата да изнуди одредено

[30] Според: Sills L.David, Merton K. Robert (eds), *internacional Encyclopedia of the Social Sciences*, vol.XI, MacMillan Publishing Company, New York 1968, p.40.

[31] Hewedy Amin, *Militarization and Security in the Middle East*, Printer Publishers, London 1989., p.16.

[32] Според: Javorović Božidar, „Terorizam“, во: *Policija i sigurnost*, br.1-2, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, siječanj-travanj 1997., str.6.

[33] Кегли В. Чарлс Јуниор, Виткоф Р. Јуџин, *Светска политика*, Факултет политичких наука & Дипломатска академија МСП, Београд 2004., стр. 655.

[34] Buzan Barry, *People, States and Fear: An agenda for International Security Studies in the Post-Cold War Era*, Harvester Wheatsheaf, London 1991, pp. 19-20.

[35] Според: Nye S. Joseph Jr, „Limits of American Power“, in: Political Science, Vol. 117, No. 4., The Academy of Political Science, New York 2002/2003, p. 548.

однесување на друга држава или други субјекти кон кој е насочена моќта, додека потенцијал претставуваат капацитетите на државата на коишто се темели нејзината моќ. Во овој контекст, Роберт Арт,[36] говори дека во современиот свет за определување на моќта на државата не се веќе пресудни само големината на територијата, бројот на жители, воената сила, богатство во основните суровини или извори на енергија. Значаен извор на моќта на државата се и степенот на нејзиниот техничко-технолошки развој, образовната и старосната структура на населението, но и влијанието кое го има државата за донесување на одлуките во меѓународните организации. Во однос на моќта на државата, Збигњев-Бжежински смета дека таа е производ на повеќе видови моќ, а пред сè: *воената моќ,* односно поседување на мобилни и на обучени човечки и респективни материјални воени капацитети кои се способни во конфликт со противничката сила да извојуваат победа и да ја покорат, наметнувајќи ѝ ја волјата на својата влада; *економско-енергетската моќ,* односно поседување на сировински, стручни, кадровски, производни, енергетски, финансиски и слични капацитети кои ја чинат државата богата, а на нејзините граѓани им го гарантираат задололувачкиот животен стандард; *културната моќ,* односно развиеност на културата, традицијата, националната свест, националниот идентитет и безбедносната култура, со што зедницата станува модерна, сложна и хармонична целина способна да се спротистави на безбедносните проблеми и да допринесе за нивни решавање; *политичката моќ,* која се јавува како резултат на наведените видови моќ на државата, а се состои и во способноста на државата да доминира или барем рамноправно да учествува во случувањата на меѓународната сцена; и *моќта на знаењето и технолошко-информационата моќ,* односно континуираниот развој на науката, техниката и технологијата со која се унапредуваат образовните, производните, комуникациските, истражувачките и животните процеси, но и воената и економската моќ на државата.[37]

Во рамките на концептот на национална безбедност, особено место им припаѓа на сегментите приватна безбедност и корпорациска безбедност. *Приватната безбедност* е израз на општата тенденци-

[36] Art J. Robert, „The Fungibility of Force", in: Art J. Robert, Waltz N. Kenneth (eds.), *The Use of Force - Military Power and International Politics*, Rowman & Littlefield Publishers Inc., Oxford 2004., pp. 8-15.

[37] Бжежински-Збигњев, *Велика шаховска табла*, ЦИД, Подгорица 2001., стр. 28-29.

ја во светот за зголемување на приватизација на безбедносниот сектор. Постојат само мал број држави во кои не се одвива овој процес на приватизација. Зголемувањето на бројот и значењето на приватните компании кои даваат услуги од воен и од безбедносен карактер и услуги во делот на физичко-техничките обезбедувања претставуваат глобален феномен кон крајот на XX век и почетокот на XXI век. Со тоа, државата и нејзините институции не се веќе единствени субјекти кои се грижат за надворешната и за внатрешната безбедност на своите граѓани.[38] Во овој контекст, постојаната ерозија на државниот монопол над сите форми на организирано насилство е предизвикана од неможноста државата на традиционален начин ефикасно да одговори на современите предизвици, ризици и закани настанати по завршувањето на Студената војна.[39] На ова треба да се надоврзе и фактот дека по завршувањето на Студената војна се јавува процес на масовни отпуштања на персоналот во одбранбениот сектор (потребата од мал персонал и помали вооружени сили) за да се намалат државните трошоци поврзани со безбедноста. Намалувањето на бројниот сооднос на персоналот во безбедносниот сектор ја зголеми понудата од обучена и висококвалификувана работна сила која потоа со нетрпение е барана од страна на приватните компании заинтересирани за безбедносниот бизнис. Исто така, интересот за одредени региони во светот, појавата на нови војни во земјите во развој во текот на 90-тите години на минатиот век и тенденцијата за користење услуги од военообучените лица резултирале со вклучување на приватниот безбедносен сектор како сериозен играч во поширокиот безбедносен контекст и негово прераснување во сериозен актер.[40]

За повеќето луѓе сликата за приватната безбедност е онаа претстава во која има оклопни возила пред банките или униформирани чувари кои патролираат низ трговските центри. Тука, исто така, влегуваат и инсталираните аларми и брави, приватните истражувачи и производителите на безбедносната опрема. При-

[38] Schreier F. and Caparini M., *Privatising Security: Law, Practise and Governance of Private Military and Security Companies*, Geneva, DCAF, 2005, p. 1.

[39] Small M., *Privatisation of Security and Military Functions and the Demise of the Modern Nationstate in Africa*. Durban, African Centre for the Constructive Resolution of Disputes, 2006, p. 4.

[40] Nyamuya M., et.al. *Private Military Companies & International Law: Building New Leaders of Legal Accountability & Responsibility,* 2009, pp. 99-104.

ватната безбедност, сепак, опфаќа многу повеќе од тоа. Добра аналогија за приватната безбедносна индустрија е познатиот брег, со високопрофилниот униформиран сектор малку над површината и остатокот од индустријата долу под површината.[41]

Идентично како и приватната безбедност и *корпорациската безбедност* без сомнение е нов концепт и тој се фокусира на прашањата врзани за безбедноста во компаниите, односно корпорациската безбедност е насочена кон детектирање на криминал, измама и прекршоци во корпорацијата. Тоа значи дека со постоење на ефикасен систем на корпорациска безбедност компанијата ќе биде заштитена од различни опасности кои можат да попречат во нормалното работење на корпорацијата, како и заштита на имотот, на бизнисот, на сопствениците и на вработените од различни ризици и закани кои се составен дел на современото живеење. Корпорациската безбедност ќе биде и во фокусот на интерес на овој труд и заради тоа ние нема да ги разгледуваме основните аспекти на корпоративната безбедност во овој дел, туку тоа ќе го оставиме за во наредните глави во кои корпоративната безбедност ќе биде разгледувана интегрално во сите нејзини фази и димензии.

На трето место е **концептот на меѓународна безбедност**. Генезата на меѓународната безбедност можеме да ја следиме уште од дамнешни времиња. Таа е во директна корелација со оформувањето на првите територијално организирани заедници, но со лабави внатрешностуктурални односи. Всушност, недоволната организираност на тие едноставни сегментарни заедници (збир на луѓе – племиња) и нивното однесување кое произлегувало од тогашните предвидливости како и од односите кои главно се базирале на водење војни, отвориле низа прашања на теоретска, на политичка и на филозофска основа, за различни временски периоди. Раната регулација била базирана на нормативни правила кои имале врвен карактер и како такви биле вечно непроменливи. Во тој период сите размислувања биле фокусирани на проблемите војна и мир. Тоа е сосема разбирливо од едноставна причина, што тогашните воспоставени политички заедници својата безбедност и физичко одржување можеле да го осигураат само ако биле военоспособни за одбрана, односно за водење на војна.[42] За разлика од минатото,

[41] Bruce G. and Button Mark, *Private Security*, Palgrave Macmillan, New York, 2004, pp. 7-10.

[42] Masleša R., *Teorije i sistemi sigurnosti,* Magistrat, Sarajevo, 2001 str. 39.

денес, меѓународната безбедност првенствено треба да се заснова врз соработка на државите (но и на определени општествени групи, поединци и организации) односно од најниско ниво на индивидуална безбедност преку регионалната и националната до меѓународната безбедност, со цел да се постигне оптимална безбедност на секој поединечно и на сите заедно.[43]

Терминолошката разновидност која се сретнува во теоријата и практиката покажува дека и покрај традиционалната доминација на безбедносниот дискурс во меѓународните односи, сепак тешко е да се говори за изграден конзистентен теориски концепт за тоа што претставува меѓународната безбедност. Извонредно богатата научна литература која се занимава со глобалните аспекти на безбедноста забележливо избегнува да се врзе за конкретен и за изграден термин за означување на концептот на меѓународна безбедност. И тука реликтите од минатото се очигледни и присутни. Најчесто споменуван е изразот меѓународна безбедност. Како и во контекст на дефинирањето на меѓународните односи, така и тука суштинско, но и најпроблематично е прашањето што точно претставува „меѓународно". Обидот за елаборација е осуден на неуспех, затоа што терминот „меѓународната безбедност" е одомаќинет колку заради интелектуална инерција, толку и заради неуспехот да се изгради конзистентен светски систем и/или концепт на безбедност. Станува збор за терминологија која изразува статичка концепција, врзана за постулатите на реализмот или на неореализмот во меѓународните односи, а во крајна линија врзана за опстанокот и функционирањето на системот на државите во светски рамки.[44]

Меѓународната безбедност одамна излезе од универзитетските кругови и стратегиски и воени естаблишменти, па така престанала да биде само поле на научно истражување и на практична државна (т.н. висока) политика. Денес се вели дека секој поединец, секој од нас, на дневна основа, на еден или на друг начин, учествува во меѓународните односи, и повеќе или помалку ги чувствува ефектите од меѓународната (не)безбедност. Меѓутоа, во практика меѓународната безбедност е вградена во животите на поединците на сосема различни начини, но заедничка карактеристика меѓу нив

[43] Котовчевски М., *Национална безбедност на Република Македонија*, прв дел, Македонска цивилизација, Скопје, 2000, стр. 31-33.

[44] Ванковска Б., *Меѓународна безбедност*, Филозофски факултет, Скопје, 2011, стр. 20-21.

лежи во фактот што светското мнозинство е повеќе објект, отколку активен субјект во сферата на креирањето на безбедносната политика или во носењето на најважните одлуки кои имаат директно влијание врз нивните животи.[45]

Во основа, меѓународната безбедност не претставува само обичен збир на националните безбедности (безбедност на националните држави), туку подразбира и усвојување определени вредности како во меѓународните односи, така и во односите во самата држава. Исто така, меѓународната безбедност претставува збир на мерки што им го осигуруваат (обезбедуваат) опстанокот на сите држави, што претставува темелен предуслов за опстанокот и за развојот на меѓународната заедница.[46] Исто така, „меѓународната безбедност би требало да значи дека сите членови на меѓународната заедница како целина се чувствуваат безбедни и дека во меѓународниот политички систем постојат такви односи, или такви механизми, кои овозможуваат на сите држави да им се гарантира и во практиката да им се обезбеди безбедност".[47]

Значи, централната идеја за меѓународната безбедност е да се создаде чувство на заеднички интерес за опстанокот на човештвото. Постоеа различни приоди за остварување на оваа цел, од „балансот на сила" меѓу главните актери преку создавањето на наднационални тела, до комбинација на овие приоди преку создавањето алијанси. Меѓутоа, најиздржан се покажа приодот за создавање супранационални тела и промовирањето на концептот за заемна безбедност. Таа може да се смета како сознание на државите дека сите заедно се подложни на заеднички закани за нивната безбедноста. За да се справат со заканите по заедничката безбедност државите воспоставуваат одредени механизми, кои можат да бидат договори за колективна безбедност или пактови за колективна одбрана. Двата концепта го подразбираат постоењето или перцепцијата за „регионот", како група на држави кои се лоцирани во географска блискост една до друга.

Секоја држава на извесен начин се препознава во овие досегашно изнесени концепти, но исто така секоја држава во својата национална безбедносна агенда има јасно дефинирани интереси и задачи, како што се: способноста да ја штити својата територија и

[45] Исто., стр. 24-25.

[46] Славески С., *Безбедносен систем*, Европски универзитет, Скопје, 2009.

[47] Vukadinović R., *Teorije o međunarodnim odnosima*, Zagreb, 1978.

главната национална инфраструктура заедно со националните интереси; да ги брани своите граници од илегален и насилен влез или излез на лица и стоки; да ја обезбеди потребната физичка сигурност на граѓаните и на нивниот имот итн. Секоја од овие задачи мора да биде доделена како јасно дефинирана мисија на посебна компонента од безбедносната структура на земјата – од вооружените сили до полицијата. Тие различни посебни мисии треба, идеално, да се базираат врз сеопфатна национална безбедносна политика – јавен документ дефиниран и усвоен од политичкото раководство, т.е. владата и парламентот, по широка јавна дебата, вклучувајќи ги сите политички партии и цивилното општество. Така, мисијата доделена на секоја компонента од националната безбедносна структура мора да биде јасна, специфична и единствена. Тие мора да ги адресираат сите аспекти на национална безбедност, и внатрешни и надворешни. Секоја компонента на безбедносните структури мора да биде одговорна не само за ефикасно извршување на доделената мисија туку и одговорна за неуспехот таа да се изврши. Одговорноста бара транспарентност во извршувањето на доделената мисија. Двојното барање на транспарентност и одговорност цврсто го поврзува концептот на реформи во безбедноста со оној на добро владеење и со заштита на човековите права.[48]

[48] *Security Sector Reform: Institutions, Society and Good Governance,* Bryden Alan and Fluri Philipp (eds.), Nomos Verlagsgesellschaft, Baden-Baden, 2003, pp.16-17.

II глава

КОРПОРАЦИСКА БЕЗБЕДНОСТ

1. ОПШТО ЗА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Корпорацијата[49] (англ. corporation, германски körperschaft/ korporation, шпански corporación, италијански corporazione) претставува најразвиен современ облик на работење на деловните системи во развиените земји со пазарни стопанства и еден од правните облици на тие општества.[50] Според „Оксфордскиот речник за висок степен на учење", поимот корпорација подразбира голема деловна компанија, односно организација или група на организации со закон признати како правно лице, која има слични права како и физичкото лице, со цел соединување и групирање на деловните интереси, а кои како такви се најчест облик на деловно здружување.[51]

Корпорацијата успеала да ги отстрани сите дотогашни слабости на ортачките општества, особено оние што се однесуваат на ризиците, бидејќи во случај на банкрот на корпорацијата сопственикот на акции го губи само она што во неа го вложил. Корпорацијата претставува друштво на капитал, кое до средствата за формирање и работење доаѓа со издавање на обврзници. Паричниот износ потребен за

[49] Во коренот на зборот корпорација е латински израз corpus (тело)

[50] Термините корпоративизам и корпоративен систем постојат и во политиколошката теорија, но таму имаат сосема друго значење, бидејќи со нив се означува популистички концепт на замена на парламентарната демократија со корпоративни тела, односно заеднички институции на работниците, работодавците и државата, а под државно-партиско туторство. Таквата пирамида на локална, обласна и национална бирократија во најчист вид била воспоставена во Италија во текот на фашистичкиот режим на Бенито Мусолини (1922-1943 година), кој прокламирал дека „корпоративизмот го менува социјализмот и либерализмот и создава нова синтеза". Сличен облик на корпоративен систем постоел и во првите деценииии на авторитарниот режим на Франциско Франко во Шпанија, а имало и обиди да се воспостави и во уште некои профашистички диктатури. Види во: *Florinsky Michael, Faschism and National Socialism – A Study of the Economic and Social Policies of the Totalitarian State, Macmillan, New York 1936., pp. 83-105; Sarti Roland, Fascism and the Industrial Leadership in Italy, University of California Press, Berkeley 1971., pp. 80-96.*

[51] Според: *Oxford Advanced Learners Dictionary*, Oxford University Press, 6th Edition, New York 2000., p. 279.

формирање и работа на корпорацијата се вика основна главница која се дели на одреден број акции. Акциите се наоѓаат во рацете на акционерите, сопственици на корпорацијата, а нивната вредност ја одредува берзата. Во гигантските корпорации бројот на акционери достигнува стотини илјади, а во некои случаи, и повеќе од милион. Корпорацијата претставува еден од најсовршените начини на прибирање капитал, особено во оние дејности во кои природата на процесот на производство бара големи средства. Корпорациите имаат сложена организациска структура, со поголем број претпријатија (ќерки) во својот состав.[52]

Американскиот теоретичар Алфред Чендлер смета дека современата корпорација, како нов организациски облик на претпријатие, е најважна иновација на XX век. Според него, корпорациите овозможиле круцијален поттик за забрзување на економскиот раст на националните стопанства, влијаеле на ефикасната алокација на ресурсите, во голема мера придонесле за создавање нови технологии, производи и услуги и за зголемување на продуктивноста. Модерната корпорација инаку е термин кој се однесува на облик на претпријатие во кое сопствениците не се одговорни за обврските кои деловните субјекти ги создаваат и во кои доаѓа до одвојување на функцијата „сопственишство“ од функцијата „управување“ со ресурсите на компанијата. Основното барање што се поставува пред модерната корпорација е создавање профит за сопствениците и другите интересни групи на одговорен начин. Заради исполнување на својата економска цел, корпорација мора да ги усогласи разновидните интереси.[53]

А. Берле и Г. Минс укажуваат дека корпорациите потекнуваат од периодот на развојот на работењето во САД од почетокот на XX век кој подразбирал автоматско приспособување на технолошкиот предизвик на модерното масовно производство. Тогаш големите компании ја поттикнувале вертикалната интеграција заради минимизирање на трошоците и отстранување на зависностите од други компании. За да обезбедат сигурно и непречено движење на стоки, многу од нив се одлучувале за интеграција „наназад“ за да може во рамките на своето работење да го воведат и експлоатирањето

[52] Марковиќ Слободан, op. cit. стр. 148-149.

[53] Пошироко види: Chandler D. Alfred Jr, *Scale and Scope: The Dynamics of Industrial Capitalism*, The Belknap Press of Harvard University Press, Cambridge MA 1994., pp. 224-226.

суровини. Во воените индустрии во кои сè уште не била воспоставена дистрибуцијата, производителот прифатил и инсталација на услуги, а подоцна и одржување. Тоа водело кон интеграција „нанапред“ на транспортни и на дистрибутивни мрежи, вклучувајќи и малопродажни синџири и услужни гранки.[54] На тој начин, модерното индустриско претприемаштво го интегрирало масовното производство со масовната дистрибуција „во рамките на една деловна фирма“. Растот на компанијата предизвикал и промени во сопственичката структура, а довел и до помасовни вработувања на обучени стручњаци од сите профили, до централизирана администрација, како и еднообразен книговодствен и статистички систем, а подоцна и до целосно повлекување на сопствениците од управување со корпорациите и препуштање на тие дејности на платени менаџери.[55]

Поимот транснационална корпорација подразбира деловна компанија која е легално домицилирана во повеќе од една држава и чии што комерцијални активности се со доволно голем обем да имаат значително влијание на стопанството, како во земјата од која што потекнува корпорацијата, така и во државата во која има свои филијали. За дефинирањето на мултинационалната корпорација важни се следните елементи: постоење матична компанија која остварува сопственишство, т.е. контролира и управува со работењето и производството во странство преку сопствени ограноци лоцирани во повеќе земји; настојување да се оствари таква политика во рамките на производството и на маркетингот, финансирањето и други работи, која ќе ги надмине границите меѓу државите и ќе придонесе за реализацијата на геоцентричната ориентација на корпорациите.[56]

Создавањето сложени мултифункционални компании поделени во повеќе сектори неминовно водело кон интеграции надвор од државните граници, односно до создавање и развој на големи мултинационални корпорации, кои од средината на 60-тите години на XX век станале вистински деловни царства со раширени меѓународни мрежи.[57] Според податоците на Лорен Идн, на преминот

[54] Berle Adolf, Means Gardiner, *The Modern Corporation and Private Property*, Transaction Publishers, Piscataway NJ 1932., pp. 44-46.

[55] Chandler D. Alfred Jr, *The Visible Hand: The Managerial Revolution in American Business*, The Belknap Press of Harvard University Press, Cambridge MA 1977., pp. 416-417.

[56] Марковиќ Слободан.op.cit. стр. 23.

[57] Wilkins Mira, *The Emergence of Multinational Enterprise*, Harvard University Press, Cambridge MA 1970., pp. 212-213.

од XX во XXI век, од 100 водечки светски корпорациии, 75 биле изворно американски, јапонски и германски, 11 биле британски, додека на другите развиени земји отпаѓаат само 14. На крај, постои и посебна листа од 10 финансиски установи кои се сметаат за „светска суперкорпорација". Меѓу нив се познатите банки Vagslauy, Merrill Lynch, JR Morgan Chase, UBS, но и помалку познатите инвестициски фондови, како што се Capital Group Companies, FMR Corporation, AXA или State Street Corporation.[58]

Трендовите присутни од 50-те години на XX век укажуваат на глобално пренесување на економската и на политичката моќ од државата и нејзините институции на корпорациите и деловниот свет. Според студијата која ја објавиле Сара Андерсон и Џон Кавано, еден од показателите на тој тренд е и самата количина на капитал што се концентрира во современите корпорации, така што Microsoft има поголем приход од 31 најнеразвиена земја во светот заедно.[59] Некои други истражувања покажуваат дека „на листата на стотината најголеми економии на светот, 51 место заземаат корпорации, а само 49 државите".[60] Како што истакнува Р. Радоњиќ, „несомнена е потребата на современиот човек преку глобалното поврзување на светот што поскоро да го реши, или макар да го ублажи, делот на т.н. развојни проблеми, особено во отстранувањето на регионалните диспропорции, т.е. рационалното користење на ресурсите, намалувањето на трошоците на транспорт и комуникација, односно економско и пазарно поврзување на стандардизираното, за сите народи и земји прифатливи и корисни образци на производство и потрошувачка. Тоа барање, меѓутоа, главно се остварува со посредство на мултинационалните корпорации, кои според логиката на нивната припадност на сферата на профитабилното упатени на тоа да сите работи и задачи ги вршат првенствено водејќи сметка за остварување на сопствените цели и интереси.[61]

---

[58] Според: Eden Lorraine, „Bringing the Firm Back In - Multinationals in International Political Economy", in: Efiggott Richard, Payne Anthony (eds), *The New Political Economy of Globalization*, tom I, Edward Elgar, Cheltenham 2000., p. 341.

[59] Anderson Sarah, Cavanagh John, *The Top 200: The Rise of Global Corporate Power*, Institute for Policy studies, Washington DC, 2000., pp. 6-8.

[60] Види: Weissbrodt David, Kruger Muria, „Human Rights Responsibilities of Businesses as Non-State Actors", in: Alston Philip (ed.), *Non-State Actors and Human Rights*, Oxford University Press, Oxford 2005., p. 318, fn 15.

[61] Според: Радоњић Радован, „Лидерство – фељтон/13", *Побједа*, Подгорица, 27. април 2008.

Според годишната анализа направена од страна на SEENews и консултантските куќи A. T. Kearney и Euromonitor International, на листата на 100 најголеми корпорации во Југоисточна Европа во 2010 година, првите десет места ги заземале: OMV Petrom (Романија – 3,6 милијарди € приход), INA (Хрватска – 3,2 милијарди € приход), Lukoil Neftochim Burgas (Бугарија – 2,7 милијарди € приход), Automobile Dacia (Романија – 2,7 милијарди € приход), Petrol (Словенија – 2,4 милијарди € приход), Rompetrol (Романија – 1,9 милијарди € приход), Autorubis Bulgaria (Бугарија – 1,9 милијарди € приход), Konzum (Хрватска – 1,7 милијарди € приход), NIS (Србија – 1,7 милијарди € приход) и Lukoil Bulgaria (Бугарија – 1,7 милијарди € приход).[62]

Некои автори укажуваат и на различни правни и етички проблеми кои ја направила експанзијата на мултинационалните корпорации како што се: прашањето на сопственоста, усогласувањето на правните регулативи на државите во кои корпорацијата го остварува своето работење, изедначување на цените во разни земји, конкуренцијата меѓу големите деловни субјекти и создавање олигополи, формирање цени кои можат негативно да влијаат на стопанската рамнотежа на земјата во која се наоѓа филијалата на корпорацијата, различните правни норми и локални обичаи, еколошки проблеми и друго.[63]

2. ПОИМ ЗА КОРПОРАЦИСКА БЕЗБЕДНОСТ

Во безбедносната теорија и практика присутни се суштински разлики во поимното определување на корпоративната безбедност, а со самото тоа и во поглед на нејзината содржина. Со толкување на определени сфаќања во оваа сфера, може да се заклучи дека еден број автори содржините на корпорацискатa безбедност некогаш во целост ги изедначуваат со содржините на приватната безбедност. Во таа смисла карактеристична е дефиницијата која ја дава Љ. Стајиќ според која „приватната (корпорациска) безбедност е планска, организирана и врз основа на закон формирана самостојна или заедничка дејност и функција на организациите, приватни и(ли) професионални агенции, насочени кон сопствена заштита

[62] Според: Zibret Branko, van der Oord Jan, „Moving toward higher value-added economies" (http: www.top100.seenews.com/companies).

[63] Види: Šimleša Dražen, *Snaga utopije*, Što čitaš, Zagreb 2005., str. 43.

или заштита на други, како и заштита на соодветни лица, простори, објекти, работења или дејности, а кои не се покриени со ексклузивна заштита од страна на државните органи".[64]

Корпорацискатa безбедност без сомнение е нов концепт кој се грижи за работите поврзани со безбедноста во компаниите и којшто едноставно го дефинираат како заштита на имотот и работењето на компаниите со што би се постигнала поголема превенција и намалување на материјалните загуби заради осигурување на интересите на сопствениците, профитот и имотот од различни опасности.

Покрај наведеното размислување, во литературата може да се сретнат и следните размислувања за корпорацискатa безбедност.

Според Кристофер Кјубиг и Дејвид Брукс, корпорацискатa безбедност е насочена кон детектирање измама и прекршоци, а ги проучува и вистинските случаи на корпоративна криза, криминалот, како и другите злодела за кои професионалците во корпорацискатa безбедност треба да бидат свесни за да обезбедат ефикасна заштита на луѓето, на операциите и на средствата.[65]

Мајкл Генсер смета дека корпорацискатa безбедност е приспособена да одговори на структуралните ризици за компанијата, преку примена на определени модели на симулација за спроведување на најдобрата безбедносна практика во компанијата.[66]

Никол Детелхоф и Клаус Вулф во нивната компилација на уредување на материјали корпорацискатa безбедност е насочена кон корпорациска безбедносна одговорност која е фокусирана на улогата на приватниот бизнис во зоните на конфликтот. Тоа ја обезбедува сликата за видовите придонес кон мирот и кон безбедноста од страна на транснационалните корпорации.[67]

Питер Рајд смета дека корпорацискатa безбедност треба да ја обезбеди потребната избалансираност меѓу нивото на безбедност

[64] Стајић Љубомир, „Правни оквир приватне безбедности", *Зборник радова Правног факултета у Новом Саду*, бр. 1-2/2008, стр. 383.

[65] Christopher J. Cubbage and David J. Brooks, *Corporate Security in the Asia-Pacific Region: Crisis, Crime, Fraud, and Misconduct,* CRC Press, 2012, pp.3-16.

[66] Michael Genser, *A Structural Framework for the Pricing of Corporate Securities: Economic and Empirical Issues,* Springer-Verlag New York, LLC, 2005, pp. 196-238.

[67] Nicole Deitelhoff, Klaus Dieter Wolf (Editor), *Corporate Security Responsibility?: Corporate Governance Contributions to Peace and Security in Zones of Conflict*, Palgrave Macmillan, 2010, pp. 2-20.

во корпорацијата, бизнисот и конвенционалните барања на работа надополнета со мудрост, и на таков начин се нуди радикален, но инспириран предлог за успех. Во таа насока треба да биде и истражувањето на компаниите со здрав разум и логика кон подобра бизнис конзистентност.[68]

Некои размислувања одат во насока дека корпорациската безбедност се смета како дел од обезбедувањето на безбедноста на една организација. Како и да е, таа е заедничка за многу функции на безбедноста. Овде може да бидат вклучени проверките на вработувањето, тимот чувари на организациските сајтови, анализа на ризикот на земјата итн. За обезбедување на овие услуги, квалитетот треба да биде контролиран од страна на директорот (носот и грлото) на компарациска безбедност.[69] Во овој контекст, според учебникот за Корпорациски менаџмент во безбедноста улогата на менаџерот за безбедност е исто така детаљно помагање на менаџерите, во добивање стручна помош кога таа им е потребна во однос на ризикот од криминална активност, индустриска шпионажа и вандализам.[70]

Милан Милошевиќ укажува дека корпорациската безбедност по својата дефиниција е интегрирана, бидејќи опфаќа вршење на повеќе различни функции кои треба да се синхронизираат. Како таква, таа претставува функција на корпорацијата која контролира и која управува со координацијата на сите дејности внатре во деловниот субјект а кои што се однесуваат на безбедноста, континуитетот и сигурноста. Постоењето ефикасен систем на корпорациска безбедност ја штити компанијата од сите загрозувачки дејствувања, воспоставува основа за донесување управувачки одлуки, му обезбедува на врвниот менаџмент пристап до тајни информации и формира процеси и процедури кои оневозможуваат одлевање заштитени податоци од корпорацијата.[71]

Ивандиќ, Карловиќ и Остојиќ корпорациската безбедност ја дефинираат како стратегиска функција на компанијата, која има за

---

[68] Peter Reid, *How to Land a Top-Paying Corporate securities research analysts Job,* Emereo Pty Ltd, 2012, pp. 5-25.

[69] http://www.closeprotectionworld.com/security-guarding-forum/29093-definition-corporate-security-commercial-security.html

[70] *Corporate Manager's Security Handbook*, AuthorHouse, 2012.

[71] Милошевиђ Милан, „Појам и садржаји корпоративне безбедности", у: *Научни скуп «Дани безбједности» на тему: „Корпоративна безбједност – ризици, пријетње и мјере заштите" (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2010., стр. 59-60.

цел остварување на сигурноста на деловниот успех на корпорацијата, што подразбира: елиминација на сите ризици и загрозувања кои можат да влијаат на деловните активности и остварувањето на деловниот успех; сведување на загрозувачките фактори на најмала можна мера; деловно функционирање во услови на криза, т.е. надминување на кризата и воспоставување повторно нормално работење.[72]

Одредени дефиниции се многу пошироки во својот поглед, сметајќи ја корпорациската безбедност како дел на националната безбедност во контекст на реализирање на т.н. цивилна безбедност. Во тој контекст, Марковиќ смета дека корпорациската безбедност е потсистем на националната безбедност и таа претставува дел од безбедносните структури со збир на општествени цели, кои ги насочуваат деловните активности на стопанските субјекти и ја мерат нивната општествена одговорност во согласност со стандардите и со законот.[73]

Од изнесените размислувања за корпорациската безбедност може да се заклучи дека има недостаток на прецизна дефиниција за овој поим. Се смета дека дефинирањето на овој термин е исклучително тешко, затоа што вистинската природа и опфатот на полето на корпорациската безбедност е тешко да се утврди. Исто така, дефинирањето е тешко да се направи, затоа што постои одредена поделеност во размислувањата и деференцијација за тоа што треба да биде поле на интерес на корпорациската безбедност, а притоа да не се навлезе на полето на интерес на приватната безбедност. Во тој контекст одредени автори дури и ги поистоветуваат овие два поима, додека, пак, други сметаат дека определени безбедносни менаџери треба да преземаат конкретни безбедносни улоги за да бидат претпознатливи за корпорациската безбедност. На пример, директорот за корпорациска безбедност треба да му припаѓа на највисокото ниво на средниот менаџмент на корпорацијата и неговите задачи треба да бидат поставување цели, стратегиско планирање и осигурување на безбедноста во компанијата.

Општиот впечаток е дека полето на корпорациската безбедност е доста значајно и суштинско во работата на самата корпорација. Оваа констатација нè упатува на нашата генерализација

[72] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, *Korporativna sigurnost*, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb 2011., str. 34.

[73] Марковиђ И. Слободан, op. cit. стр. 21.

дека корпорацискатa безбедност е фокусирана на процесите и состојбите во определена корпорација, односно подоброто управување со безбедноста, ќе значи носење релевантни одлуки за тоа како да се заштитат сопствениците и менаџерите, вработените, средствата и имотот од определени форми на криминал, кражба на деловни тајни, фактори на ризик итн.

2.1. ОДНОСОТ НА КОРПОРАЦИСКАТА И НА ПРИВАТНАТА БЕЗБЕДНОСТ

За државата и нејзините органи традиционално е резервиран монополот на употреба на легитимна сила и единствено таа е одговорна за осигурување на безбедноста, внатрешната безбедност и одбраната на земјата од надворешни закани. Меѓутоа, сè поголемата сложеност на современите внатрешни конфликти предизвика појава на нов феномен познат како приватизација на безбедносните функции. Во таа насока, компаративната практика укажува на процеси на приватизација на безбедносните функции во различни области кои во претходните периоди биле резервирани за воените, за безбедносните и за полициските структури, а чиј обем во различни држави зависи од законските рамки, безбедносните закани и предизвици, како и од институционалните капацитети на земјата. Во тој контекст, новиот феномен претставува корпорациска безбедност и безбедност во рамките на деловните субјекти.

Во теоријата често не се прави доволна дистинкција меѓу приватната и корпорацискатa безбедност, при што заедничките именители во дефинициите за корпорацискатa безбедност се сведуваат на тоа дека станува збор за планска, организирана и врз основа на закон заснована самостојна или заедничка дејност и функција на организацијата насочена кон сопствена заштита или заштита на други, како и на заштита на соодветни лица, простори, објекти итн. Извесно е, меѓутоа, дека корпорацискатa безбедност (corporate security) не може да се поистовети со приватната безбедност (private security), пред сè поради тоа што приватната безбедност[74] е

[74] М. Даничиќ и Љ. Стајиќ „Системот на приватна безбедност претставува облик на организирање и функционирање на корпорацијата во спроведување мерки и активности на превентивен и на репресивен план кои се преземаат заради зачувување на безбедноста на лица, имот и работење, а заради зачувување на економската и на социјалната функција на корпорацијата, како и заштита на сите други вредности на корпорацијата од сите облици и носители на загрозувањето“.

реално поширок поим од корпорацискатa безбедност. Имено, покрај работите на приватно обезбедување на лица, работење и имот (објекти, простори и вредности), приватната безбедност опфаќа и работи врзани со приватните воени компании и многу други фирми кои на комерцијална основа реализираат бројни работи поврзани со безбедноста.[75] Тоа значи дека субјектите на приватната безбедност реално не можат да се стават во рамките на приватните и(ли) на професионалните агенции насочени кон сопствена заштита или заштита на други, како и заштита на определени лица, простории, објекти, работа или дејности, ниту нивната активност се исцрпува во заштита и самозаштита, па ниту пак, детективска дејност.[76]

Поимот корпорациска безбедност не може да се изедначува со поимот приватно обезбедување, ниту пак неговите содржини можат да се поистоветуваат со работите и задачите на интерните служби за обезбедување во објектите кои задолжително се обезбедуваат, односно во јавните претпријатија и во големите техничко-технолошки системи. Според насоките од Европската унија, корпорацискатa безбедност во корпорациите се дефинира како интегрална безбедност,[77] која во себе опфаќа работи од безбедноста (security) и заштитата (safety), што пак вклучува собирање на информации, безбедносни процени и процени на ризик, информатичка заштита, кризен менаџмент, заштита од пожари, експлозии и хаварии, заштита на безбедноста и здравјето на работа и друго.

Нема сомневање дека во државите на Балканот значаен дел од актуелното функционирање на корпорацискатa безбедност внатре во деловните субјекти и понатаму е поврзан за работи кои во најширока смисла се однесуваат на физичкото и на техничкото обезбедување лица, имот и работење на стопанските друштва, интерните чинители кои тие работи ги организираат и ги насочуваат, како и ангажираните екстерни или интерни субјекти кои тоа го спроведуваат во практика. Може да се претпостави дека моменталниот „епицентар“ на корпорацискатa безбедност на овие простори претставува самозаштитна дејност во големите техничко-

[75] Според: Матић Горан, „Правни аспекти физичко-техничког обезбеђења у приватном сектору безбедности“, Правни информатор бр. 9, Београд 2006., стр. 61.

[76] Кесић Зоран, *Приватни сектор у контроли криминалитета*, Досије студио, Нови Сад, 2009, стр. 12-15.

[77] Ivandić Vidović Darija, Karlović Ludija, Ostojić Alen, op.cit.стр.68.

технолошки системи, што доведува до грешки во дефинирањето на поимот корпоративна безбедност и одредувањето на неговите содржини. Проблемот станува уште посложен и поради фактот што некои од деловните субјекти кои задолжително се обезбедуваат (банки, пошти и друго) можат да ги имаат застапено речиси во сите категории на услуги од приватното обезбедување, односно заштитните или самозаштитните дејности.

3. СОДРЖИНА И ОСНОВНИ КАРАКТЕРИСТИКИ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Современите корпорации и другите деловни системи денес се позагрозени отколку порано поради длабоките општествени промени на преминот од XX во XXI век, што особено се однесува на државите во транзиција и на т.н. „млади демократии". Кон тоа треба да се додаде и порастот на бројот на организации, групи и поединци кои имаат интерес да го загрозат опстанокот, растот и развојот на корпорацијата, без разлика дали тоа го прават од економски, од политички, од идеолошки или од верски причини, како и појавата на нови методи и средства за загрозување, што севкупно ги прави задачите на службите задолжени за безбедност[78] на корпорациите сè потешки.

Покрај работите на физичко и техничко обезбедување лица, имот и работење, корпорациската безбедност мора да ги опфати и сите други аспекти на безбедноста и заштитата, вклучувајќи ги и работите врзани за собирање информации и процена на ризици, заштита од пожари, експлозии и хаварии, заштита на безбедноста и здравјето при работа итн. Суштината е во тоа дека во деловните субјекти, а пред сè во големите техничко-технолошки системи, мора да се обединат сите работи врзани за безбедноста и заштитата. Во согласност со насоките од Европската унија, во таквите колективи се инсистира на интегрална безбедност, која во себе ги опфаќа работите од обезбедување во најширока смисла (security) и работите врзани

[78] Според: Стајић Љубомир „Изазови корпоративне безбедности у светлу савременог схватања појма безбедности" *Први међународни научни скуп «Приватна безбедност – стање и перспективе» (Зборник радова)*, Факултет за правне и пословне студије, Нови Сад 2008., стр. 29.

за заштитата (safety).[79] Се смета дека само со поврзување на сите такви работи, било тоа да е во иста организациона единица или во вид на управување од страна на единствен менаџер за безбедност, се придонесува за поделотворна организација, координација и контрола на дадените работи, а со самото тоа и за рационализација и унапредување на севкупното работење.

Корпорациската безбедност во современи услови стана стратегиска функција на деловните субјекти и како таква ја дефинира интегрираната безбедносна политика на корпорацијата и нејзиното единствено спроведување во практика. Во врска со тоа, дефинициите на одделни автори укажуваат дека во основните карактеристики на корпорациската безбедност спаѓаат: вкупната безбедност на корпорациите; одговорноста на стручњаците за корпорациска безбедност, кои денес се соочуваат со тешки задачи истовремено да ги поддржуваат растечките потреби на деловните субјекти од една страна и од друга страна да ги оневозможуваат сè пософистицираните напади на корпорациите; професионалната етика, односно припадноста на професијата и настојување на сите професионалци во областа на корпорациската безбедност да го даваат максимум од себе.[80]

3.1. ИНТЕГРАЛНА БЕЗБЕДНОСТ ВО КОРПОРАЦИИТЕ

Корпорациската безбедност во западните земји стана дополнителен важен феномен покрај имотно-правното раздвојување во практика на титуларното сопственишто и на менаџерско-правната функција на водење на претпријатието. Овој феномен во практиката е особено врзан за т.н. постиндустриско општество кое егзистира во последните неколку децении.[81] Тоа особено доаѓало до израз во случаите на акционерскиот капитал, задругарството, ортаклукот или здружувањето на два или повеќе сопственика, одредени облици на диригирани друштва, подружници на мултинационални корпорации, картели и трустови, мешовити облици на сопственост

[79] За поимите безбедност (обезбедување), сигурност и заштита, пошироко кај : Остојић Момир, „Научни проблем теоријске дефиниције безбедности као основе за дефинисање приватне безбедности“, *Приватна безбедност - стање и перспективе (зборник радова),* Факултет за правне и пословне студије, Нови Сад, 2008, стр. 181 - 201.

[80] Види: Murray Tonita; McKim Erica, *The policy issues in policing and private security*, Canadian Association of Chiefs of Police Publication, Ottawa 2000., p. 6.

[81] Види: Дракер Питер, *Постиндустријско друштво,* Грмеч; Привредни преглед, Београд 1995.

и сл. Во такви случаи, кои во практиката се сè почести, важна е разликата во располагањето и сопственоста, како и управувањето на компанијата во однос на случаите на претежно иконосни сопственици (а најчесто и управувачи кои биле исти лица или од исти фамилии, или на некој друг непотистички начин меѓусебно дополнително поврзани, што создавало дополнителна доверба) или двајца ортаци, што порано бил доминантен облик на сопственост, но и на управување со повеќето претпријатија. Независно од тоа, ефикасната, високопрофесионализирана служба за обезбедување, која има извесна дистанца и самостојност во однос на внатрешната хиерархија на организацијата на работа и на вработените во тој процес, станува сè поизразена потреба со цел поголем квалитет на корпорациската безбедност. Покрај надворешното загрозување на безбедноста на претпријатието и неговиот имот, особено е висок ризикот од внатрешните фактори на загрозување на безбедноста, а некогаш овие фактори се и поврзани.[82]

Основен предуслов за осигурување на корпорациската безбедност, односно функционирањето на службата за обезбедување на деловниот субјект е исполнувањето на неговата крајна намена – зголемување на профитот и непречена работа на компанијата преку ефикасна заштита на имотот, лицата и работењето. Ова претставува императив на врвните менаџери и на сопствениците на капиталот за неопходноста од постоење и функционирање на службите за обезбедување на имот, лица и работење. Оваа претпоставка во најголем дел е условена од конкретните користи кои корпорацијата, установата, односно сопственикот може да ги има од службата за обезбедување имотот, лицата и работењето.[83] Корпорациската безбедност на компанијата се остварува низ два облика на дејствување: превентивно, при што со своето постоење претставува инструмент на одвраќање од сите облици и извори на загрозување, и репресивно, што подразбира отстранување на причините на загрозување и елиминирање на носителите со помош на сила, на правно дозволен начин.

Безбедносниот менаџмент во конотација претставува субјект на организирање и управување со системот за обезбедување на лицата и имотот на корпорацијата. Во негова надлежност е одредувањето на целите, планирањето, организирањето, издавањето наредби, контролата, координацијата и одговарноста за безбедна работа на

[82] Петровиќ Драган, оп. цит. стр. 247-254.

[83] Според: Петровиќ Предраг, „Приватизација безбедности у Србији“, *Безбедност Западног Балкана*, бр. 4/2007, Београд 2007., стр. 14.

компанијата. Менаџмент е тој што го осмислува целокупниот систем на обезбедување, го усогласува со работата на другите делови од компанијата, заради остварување на целите на корпорациската безбедност без да прави штети врз процесот на работа. Имено претераното и непотребно инсистирање на безбедносни процедури таму каде тоа не е неопходно, може да ја забави работата на други делови на компанијата во процесот на производството. Безбедносниот менаџмент, исто така, е одговорен за почитување на правните прописи и за обученоста на работниците за обезбедување, како и за грешките кои тие во својата работа ќе ги направат.[84]

Независно од тоа дали корпорациската безбедност се спроведува со дејности на своите сопствени организациски единици во составот на корпорацијата или со ангажирање одредени специјализирани субјекти надвор од неа, важно е да се анализира организацијата на корпорацијата во доменот на безбедноста, и навремено и стручно, според одредени потреби да се вклучат и релевантни научни институции, за да се изготви безбедносна процена за корпорацијата, но и прогноза за можните ризици и закани за корпорациската безбедност, што значи дека мора да се оди во пресрет на можните загрозувачки фактори.[85]

Задачите на корпорациската безбедност се да ги воочува и во раната фаза ефективно да го спречува секој развој на заканите кои ја загрозуваат корпорацијата и нејзиното работење. Така разбрана корпорациската безбедност не опфаќа само работи за физичка и за техничка заштита на компанијата, туку и заштита на информатичкиот систем, интелектуалното сопственишто, стоковите марки и слично, нешто што светските корпорации помасовно започнале да го применуваат од осумдесеттите години на XX век. Во врска со тоа, современиот концепт за безбедност на деловните субјекти поаѓа од три основни претпоставки: 1) недостаток на свест за постоење на загрозеност на корпорациите и потреба за воспоставување соодветни безбедносни механизми; 2) интегралната безбедност не е само техничко, туку е и стратегиско прашање; 3) надминувањето на концентрацијата

[84] Види: Даничић Милан, Стајић Љубомир, *Приватна безбједност*, Висока школа унутрашњих послова, Бања Лука 2008., стр. 28.

[85] Според: Бошковић Мићо, Бошковић Александар, „Неки актуелни проблеми од значаја за безбедност и заштиту корпорација", у: *Научни скуп «Дани безбједности» на тему: „Развој система безбједности и заштите корпорација" (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 18.

само на надворешни извори на загрозување (инсајдерите како причина на кршење на безбедносните процедури се појавуваат во 80% од сите случаи). Исто така, досегашниот концепт на безбедност на компаниите беше со најголем дел насочен на воспоставување на механизми на информациска безбедност (во 70% случаи на губење на информации причина бил човечки фактор, а не информатичката технологија).[86]

Идејата за модел на обединета, односно интегрална функција на безбедност, која дава можност за единствена процена на ризиците, дефинирањето на единствени мерки на заштита и единствено постапување во остварувањето на корпорациските цели во областа на безбедноста станува присутна и на просторите на ЈИЕ. Ваквиот модел дава шанси за усвојување единствена безбедносна политика како интегрален дел од вкупната деловна политика, а од друга страна, тоа ќе значи обединета национална политика на безбедност, како и нејзина реализација во практика.[87]

3.2. ОБЛИЦИ НА ЗАГРОЗУВАЊЕ НА БЕЗБЕДНОСТА НА КОМПАНИИТЕ

Поимот загрозување[88] најчесто подразбира општ израз за ситуација во која се јавува опасност дека на некој или некому ќе му биде одземен животот, оштетено здравјето, уништена или оштетена материјална, финансиска или друга сопственост. Изворите на такво загрозување, односно доведување во опасност, може да бидат природни, вештачки и општествени (а според други автори надворешни, внатрешни и комбинирани).[89]

---

[86] Според: Bilandžić Mirko, „Korporativna sigurnost u Hrvatskoj: mit ili uvjet bez kojeg se ne može poslovati", *Druga međunarodna konferencija «Korporativna sigurnost u vrijeme recesije»*, Poslovni tjednik Lider & MBOS, Zagreb, 02.04.2009.

[87] Кешетовић Желимир, Симоновић Бранислав, „Сектор корпоративне и приватне безбедности у Србији", Годишњак факултета безбедности, Београд 2009., стр. 166.

[88] Даничић Милан, Стајић Љубомир, op. cit. стр. 49-50.

[89] Одредени автори употребуваат и поим за закана (опасност) под кој подразбираат можност дека нешто или некој ќе предизвика штетни последици врз одреден систем во форма на оштетување, измени, откритија. Таа опасност може да се изразува во облик за веројатност дека нешто ќе се случи. Во врска со тоа, се користи и израз за повредливост – слабост која може да биде искористена за да се оствари некоја закана. Види: Кековић Зоран, Савић Сузана, Комазец Ненад, Милошевић Младен, Јовановић Драгиша, *Процена ризика у заштити лица, имовине и пословања*, Центар за анализу ризика и управљање кризама, Београд 2011., стр. 30-31.

Природните извори на загрозување се поврзани со стихијно дејствување на природните сили и тие не подлежат под влијание и насоки од страна на човекот. Вештачки или технички извори на загрозување се предмети кои се резултат на човековата активност кои се користат во човековото општење и работа. Носители на општествените извори на загрозување се секогаш општествени субјекти со одредени својства, кои по правило се насочени на одземање животи или нанесување повреди на други лица, односно нанесување материјална штета со различен интензитет.

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

Природни, односно елементарни несреќи може да се дефинираат како деструктивни и/или антропогени појави, односно како процес со големи размери што претставува опасност за животот и здравјето на луѓето, а може да доведе и до уништување на материјалните добра и на животната средина. Иако природните опасности не може да се избегнат, интеграцијата за процена на ризикот и навременото предупредување, во мерките на превенција и намалување, може да спречат нивно преминување во катастрофа, што значи дека може да се преземаат акции со цел значително намалување на сите последици[90]. Во природни непогоди спаѓаат: земјотреси, поплави, цунами, вулкански ерупции, лизгање земјиште,

[90] Според: Powell L. Jason, Edwards Margaret, „Risk and Youth: A Critical Sociological Harrative in: International Journal of Sociology and Social Policy Vol. 23, Issue 12, Emerald Group Publishing Limited, Bingley UK 2003., pp. 84-85.

одрони, урагани, масовни шумски пожари, снежни наноси и лавини, поплави и суши, обилни врнежи, тешки мразови, епидемии, епизоотии,[91] масовно ширење шумски и полски штетници. Силата на земјотресот сама по себе не е доволна да ги одреди големината на загубите, бидејќи ниту големите катастрофи во услови на слаба ранливост и добрата подготвеност на населението како и одличниот менаџмент не подразбираат големи загуби.[92] Во врска со тоа, на специфичноста на проектирање објекти и инфраструктурата на корпорациите, на сеизмички трусни подрачја се состои од потребата за одредување максимално очекуваниот интензитет на земјотресот како и вклучувањето на овие проценi во проектот за изградба.

Како пожар се смета секој оган што настанал надвор од контролирано огниште, или оган што го напуштил ова место и е способен да се развива со сопствена сила, при што нанесува материјална штета.[5] Пожарот често е последица на елементарни непогоди, а може да се јави во објект на корпорацијата како последица на несреќи или прекин на електрични и други инсталации. Ако во деловниот објект не се преземаат адекватни мерки на заштита од ширење и пренесување пожари, постои опасност и мали пожари да прераснат во катастрофа. Пожар во деловен субјект може да биде предизвикан и со умисла или од невнимание на луѓето и тогаш претставува криминален акт кој содржи некое од кривичните дела кои можат да се предизвикаат со пожарот. Намерно предизвиканиот пожар во криминалистичката терминологија се нарекува подметнување пожар и претставува кривично дело извршено со намера. Мотивите на намерно предизвиканиот пожар може да бидат различни: освета, користољубие, фингирање пожар за да се прикрие некое друго претходно извршено кривично дело, но и екстремистички побуди и тероризам.

Диверзијата (лат. diversio – одвраќање, свртување внимание, промена на правец) претставува смислена, прикриена и неочекувана акција, која се состои од предизвикување пожари и експлозии или опфаќа преземање на некоја друга опасна активност заради загрозување на човечки животи, уништување или оштетување објекти и друг вреден имот од поголемо значење за корпорацијата.[93]

---

[91] Епидемии кај животните.

[92] Кековиħ Зоран, Савиħ Сузана, Комазец Ненад, Милошевиħ Младен, Јовановиħ Драгиша, op. cit. стр. 32.

[93] Поширко види: Мијалковиħ Саша, *Национална безбедност*, Криминалистичко-полицијска академија, Београд 2009., стр. 257.

Како причинители на техногени хаварии во корпорациите може да бидат надворешни природни фактори, проектно-производни неисправности на опремата, како и непочитување на технолошките процеси, правилата при експлоатацијата, транспортот на уреди, машини, механизами итн. Во практика најчести примери на вакви хаварии е човечкиот фактор, непочитување на технолошкиот процес, нормите и правилата на техничката безбедност.[94]

Поимот антропогена катастрофа подразбира квалитативна промена во средината до која се дошло под дејство на фактор настанат од човековата активност, што има штетно влијание врз луѓето, животните, растителниот свет и животната средина во целина. Во загрозувања од еколошки карактер спаѓаат: деградација на земјиштето и загадување на почвата со тешки метали (кадмиум, олово, жива, хром итн.), загадувањето на атмосферата (уништување на озонската обвивка, кисел дожд, температурни инверзии над индустриските градови, загадување и црпење на водените резерви, влошување на квалитетот на водата за пиење и слично) што ги влошува условите за живот на луѓето и го нарушува нивното здравје.[95]

Под саботажа се подразбира смислена и прикриена, спонтана или организирана дејност на поединци или групи при што за кратко или за подолго време се оневозможува нормалната работа на корпорацијата и посредно или непосредно се предизвикува материјална или друга штета. За разлика од тероризмот и диверзиите извршители на саботажа се лица кои се вработени во деловниот субјект врз кој му се нанесува материјална штета, при што саботерите настојуваат таа штета да ја прикажат како последица на случајност, невнимание, негрижа, неодговорност, неисправни и дотраени средства за работа или неквалитетни репроматеријали.[96]

Потенцијален внатрешен извор на загрозување на корпорацијата претставуваат сите вработени кои може да нанесат штета на вредностите и на интересите на компанијата свесно или несвесно по пат на саботажа, различни облици на кражба, затајување, проневера, измама или други облици на негативно

[94] Види: Савић Андреја, Стајић Љубомир, *Основи цивилне безбедности*, Факултет за правне и пословне студије, Нови Сад 2006., стр. 86.

[95] Според: Cifrić Ivan, *Socijalna ekologija: Prilozi zasnivanju discipline*, Globus, Zagreb 1989., str. 203.

[96] Мијалковић Саша, *Национална безбедност*, op. cit. стр. 258-259.

однесување. Можноста претставува најважен момент на одлука и извесност со која на вработените може да им се нанесе штетно, забрането или кривично дело, а да се смета дека нема да биде откриено. Факт е дека вработените кои подолго работат во корпорацијата истовремено се и најмногу информирани за начинот на работа и слабостите во функционирањето на корпоративната безбедност во компанијата, што секако дека би можеле да го искористат тоа за свои цели. Мотивите за внатрешно загрозување, одделни автори[97] ги наоѓаат во деструктивното човековото однесување, кое може да биде детерминирано од условите на живеење на носителот на загрозувањето, неговите недоразбирање со себеси, недоразбирањата со други лица, со општествени групи, со организации или со општеството во целост. Најчесто таквото однесување е резултат на судири на поединечни или заеднички интереси, несогласување помеѓу желбите, потребата и можностите на нивното задоволување, резултат на некој потрес или излез од кризата, негативното решавање на некои конфликти или стресни ситуации, акт на непромисленост или проектирање болни имагинации или халуцинации.

Одредени автори укажуваат на резултатите од спроведени истражувања според кои повеќе од една четвртина на вкупните штети кои корпорациите ги трпат од различни видови загрозувања, настануваат поради незаконско дејствување на групи и поединци надвор од корпорацијата (надворешен заговор – извршител надвор од компанијата) и внатре во корпорацијата (внатрешен заговор) учесници кои се вработени во корпорацијата. Според тие истражувања, односот помеѓу надворешниот и внатрешниот облик на загрозување на корпорацијата е приближно 80% : 20%. Меѓутоа, висината на штетата која за компанијата настанува во поглед на споменатите видови на загрозување има обратен однос, така што штетата која ја предизвикуваат вработените учествуваа со речиси 80% од вкупниот износ. Компаративните искуства укажуваат на фактот дека вработените со подолг стаж во компанијата почесто се решаваат за вршење противзаконски дејства бидејќи ги знаат слабостите на работата на организацискиот процес и имаат изграден однос на доверба со менаџментот на деловниот субјект. Мотиви за дејствување

[97] Според: Јовановић Љубиша, *Кривично право I* – Општи део, Полицијска академија, Београд 1995., стр. 89.

на штета на корпорацијата би можеле да бидат: нееднаквоста помеѓу сопствените финансиски и статусни желби и можноста за нивно легално реализирање, од претходно искажаната наклонетост кон вршење кривични дела, зависност од алкохол и од наркотици, клептоманија или болест.[98] Наспроти тоа постојат и мислења дека главни внатрешни извори на загрозување на корпорацијата се поврзани со менаџментот, односно за нивните погрешни деловни и други одлуки кои се за околу 70% основна причина за пропаѓање одредени компании.[99]

Во поглед на предноста, односно погодноста која во извршување различни кривични дела на штета на компанијата ја имаат извршителите „(напади однатре во однос на напади однадвор)“ се укажува на следното: извршителите од редовите на вработените се запознаени со системите на техничка и на физичка заштита на компанијата; тие немаат временско и просторно ограничување за противзаконско дејствување, лицата кои компанијата ја загрозуваат однатре може да го одложат времето за дознавање на штетата, односно тоа дека се извршила противзаконска активност, а штетата можат да ја прикажат како последица на одвивање друг процес или исклучување; внатрешно загрозување на корпорацијата може да се одвива во спрега со повеќе извршители внатре, еден или повеќе поврзани работни процеси. Фактори кои во корпорацијата може да предвидат настанување вакви видови загрозување се: недоволен надзор на вработени во процесот на работа и отсуство на постојана контрола на нивниот работен ефект и однесување; нејасно одредување и разделување на функционалните и извршните одговорности во компанијата, и отсуство или издавање лоши или неадекватни работни задачи.[100]

Според М. Даничиќ, најчест, а истовремено и најопасен облик на загрозување на имотот на вработените во компанијата се криминалитетот и други социопатолошки појави (алкохолизам, употреба на опојни дроги и др.) Деловните субјекти се загрозени и со прекршоци од областа на јавниот ред и мир, и тоа на различни начини: уништување и оштетување на имотот, нанесување

[98] Според: Laušić Mate, Petar Saša, Marjanović Bono, „Ulaganje u sigurnost kompanije – investicija ili trošak“, u: *Druga znanstveno-stručna konferencija s međunarodnim sudjelovanjem «Menadžment i sigurnost - M&S 2007» (zbornik radova)*, Hrvatsko društvo inženjera sigurnosti & Visoka škola za sigurnost, Zagreb 2007., str. 316.

[99] Töpfer Armin, *Plötzliche Unternehmenskrisen: Gefahr Oder Chance?* Luchterhand Literaturverlag, München 1999., pp. 28-29.

[100] Laušić Mate, Petar Saša, Marjanović Bono, op. cit. str. 317.

повреди и вознемирување на вработените и на лицата кои доаѓаат во компанијата, создавање атмосфера на лична несигурност, прекинување на работата, губење на угледот на компанијата во работната средина и сл. Се смета дека последиците на овие работи некогаш може да бидат подеднакво негативни како и за оние што настануваат со вршење кривични дела. Поради тоа во спречување и откривање на прекршоците и на другите недозволени дела не се занимава само полицијата и агенциите за обезбедување на лица и имот, туку тоа го прават и други државни органи, односно други стручни служби и менаџментот на корпорацијата. Имено, криминалитетот што ги загрозува лицата и имотот на компаниите е истиот тој кој го загрозува општеството во целина, а чии носители најчесто се мотивирани од користољубие или желба да се нанесе штета како на компанијата така и на општествено-економскиот систем на земјата. Сепак, тешко е прецизно да се изрази вистинскиот обем на криминалитет на штета на корпорацијата поради високите „црни бројки на криминалитетот“ во оваа област.[101]

Комбинирани извори на загрозување на корпорацијата може да се најдат во разни форми, најчесто како комбинација на елементарни непогоди и човечки фактор, но и како заедничко штетно дејство против виталните интереси на компаниите од страна на лица кои се вработени во неа, како и на лица однадвор, чиј мотив е стекнување материјална корист. Комбинираниот облик на загрозување на компаниите задолжително ја карактеризира спрегата меѓу надворешното и внатрешното загрозување, која мора да постои како свесна постапка на вработените. Многу важен и присутен комбиниран извор на загрозување на корпорацијата претставуваат и штрајковите на вработените.[102]

Во последно време, особено по терористичките напади во САД во септември 2001 година, во стручната литературата во почеста употреба се користи терминот „критична инфраструктура“ (Critical Infrastructure).[103] Иако помеѓу авторите не постои целосна

[101] Според: Даничић Милан, *Обезбеђење лица и имовине предузећа у Републици Српској*, Висока школа унутрашњих послова, Бања Лука 2006., стр. 59-60.

[102] Даничић Милан, Стајић Љубомир, op. cit. стр. 62.

[103] Според: Rinaldi M. Steven, Peerenboom P. James, Kelly K. Terrence, „Complex Networks – Identifying, Understanding and Analyzing Critical Infrastructure Interdependiencies““, in: IEEE Control Systems Magazine, IEEE Control Systems Society, Ann Arbor MI, December 2001., p. 13.

усогласеност за содржината на тој поим и концепт, сепак под овој назив најчесто се подразбираат природни и материјални добра, имот, технички системи, комуникации, деловните активности и служби кои се од особено значење за државата и чие уништување или прекин на функционирањето би ја загрозило националната безбедност, националната економија, виталните општествени функции, здравјето на населението, јавниот ред и заштитата на националните интереси.[104] Станува збор за производство и пренос на електрична енергија, хемиска индустрија и нуклеарни централи, производство, транспорт и дистрибуција на нафта и природен гас, систем за телекомуникации, ресурси на вода за пиење, производство на основни животни продукти, системи на греење, објекти и служби на јавното здравство, системи на јавен транспорт, органи на државна власт, финансиски и безбедносни институции. Во врска со тоа, Европската унија врз основа на директивата на Европската комисија – EU COM (2006) 786 final ја усвои Европската програма за заштита на клучната инфраструктура, која содржи и Европска листа на критична инфраструктура (ECI) изработена врз основа на доставени предлози на земјите членки.[105]

3.3. ПРОЦЕНА НА РИЗИК И ПРОЦЕНА НА БЕЗБЕДНОСТА НА РАБОТЕЊЕТО ВО КОРПОРАЦИЈАТА

Во современата литература не постои единствена дефиниција за тоа што е ризик. Одредени автори сметаат дека ризик претставува „ситуација во која постои можност од отстапување во однос на посакуваниот резултат“[106], за други тоа е „мерка на веројатност е дека последиците штетни по животот, здравјето, сопственоста и /или животната средина да се појават како резултат на некои одредени опасности“[107], трети дека ризик е „комплексната особина со која се

[104] Види кај: Čaleta Denis, „A Comprehensive Approach to the Management of Risks Related to the Protection of Critical Infrastructure: Public-Private Partnership“, in: Čaleta Denis, Shemella Paul (eds), Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection, Institute for Corporative Security Studies (ICS) & Center for Civil-Military Relations, Ljubljana-Monterey CA 2011., pp. 16-17.

[105] Според: Council Directive (EC) No. 114/2008 of 8 December 2008.

[106] Пошироко види: Vaughan J. Emmett, *Risk Management,* John Wiley & Sons Inc, New York 1996., p. 23.

[107] Sage P. Andrew, „Systems Engineering for Risk Management“, in: Beroggi E. G. Giampiero, Wallace A. William (eds), *Computer Supported Risk Management, Kluwer Academis Publishers,* Norwell MA 1995., p. 4.

опишува веројатност од настанување штетни настани и очекувана големина на последици од тие настани за сиот систем и за време на утврдената должина на временскиот интервал или за време на одредена мисија".[108] Одредени размислувања одат во насока дека тоа е „Мерка за веројатност на настанување на техногени или природни појави кои се карактеризираат со настанок, формирање и дејство на опасности, како и социјални, економски, еколошки и други видови загуби и штета"[109], додека други размислувања посочуваат дека тоа е „Можност потенцијалната опасност да се реализира во случај и во услови на користење и/или изложувања и можното значење на штетата". [110]

Според некои дефиниции ризикот претставува неможност да се предвиди резултатот од идните случувања со целосната сигурност. Во врска со тоа треба да се има предвид дека претприемачите и менаџерите на корпорациите по правило донесуваат ризични деловни одлуки врз основа на веројатноста од настанување во идните случувања. Ако е сигурноста ситуација во која нивните очекувања ќе бидат исполнети, тогаш несигурноста може да се мери како веројатност дека вистинскиот резултат ќе отстапува од очекуваното или од планираното.[111] Од тие причини, изработката и имплементацијата на проценатa на ризик и вградувањето резултати од проценатa и од одлуките од изборот на видот и начинот на функционирање на интегрираниот систем на безбедносна заштита на корпорациите сведочат за професионалноста на нејзиниот пристап кон проблемот за заштита на лицата, имотот и работата. Проценатa на ризик вклучува примена на повеќе логички и систематски методи за комуникација и консултација за време на овој процес, како и за воспоставување на организацискиот контекст за идентификација, анализа, процена, третман и контрола на ризикот

[108] Според: Вукићевић Душанка, Видовић Данило, „Могућности оптимизације улагања у превентиву и интерес осигуравајућих компанија за та улагања", *Превентивно инжењерство*, год. III, бр. 1, Превинг, Београд 1995., стр. 5.

[109] Цхадая Д. Николай, Подосенова С. Нина, Управление безопасностью труда, ЦентрЛитНефтеГаз, Москва 2008., стр. 9-10.

[110] Луковић Славољуб, *Приручник за процену професионалних ризика*, Заштита, Београд 2000., стр. 10.

[111] Види: Fisher N. Irving, Hall R. George, „Risk and Corporate Rates of Return", *Quarterly Journal of Economics*, Vol. 83, No. 1, Oxford University Press, Oxford UK 1969., pp. 79-80.

врзан за активностите, производите, функциите и процесите, со цел адекватно известување и архивирање во врска со резултатите на проценатa. [112]

Основна цел на секоја процена е настојувањето да се предвиди и делумно да се одреди иднината, односно да се предвиди, а во некои елементи и да се одредат идните случувања. Смислата на тоа е со доаѓање до одредени информации и нивна анализа да се обезбеди влијание на насоката и интензитетот на одредени активности како сопствени, така и на што потекнуваат од носителите на загрозувањето.[113] Во таа насока, безбедносна процена претставува интегративно и логично поврзување на фактите и на сознанијата за одделни елементи на предметот (субјекти на процена) со цел стекнување сознание за можноста и веројатноста од настанување опасност, можност на спречување или, ако тоа не е можно, смалување (ублажување) и/или отстранување на штетата, односно контрола на опасноста. При разгледување на безбедносната ситуација се оценуваат разни латентни или моментни конфликтни состојби, нивните причини и можниот развој. Во заклучниот дел на проценатa потребно е да се искаже прогноза на идните однесувања и активности на носителите на загрозувачките дејности и задачите на надлежните служби во превенција и спротивставување на тие појави.[114]

Според Д. Пајковиќ, под безбедносна процена се подразбира, збир од сознание и заклучоци до кои доаѓаат надлежни субјекти за безбедност во корпорациите кои се одговорни за состојбата на безбедност која се оценува во соодветна постапка. Во таа смисла, безбедносната процена е аналитичко синтетички заклучок за моментната состојба на безбедноста во корпорацијата која ги опфаќа сите значајни елементи за оценување на безбедносната состојба (веројатност и облици на појава на опасности од потенцијален извор на загрозување и др).[115]

---

[112] Според: Кесеровић Драгомир, „Одређивање контекста – кључна фаза процене ризика корпорација“, у: *Научни скуп «Дани безбједности» на тему: „Развој система безбједности и заштите корпорација“ (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 241.

[113] *Војна енциклопедија*, Војноиздавачки завод, Београд 1974, стр. 696.

[114] Ђорђевић Обрен, *Лексикон безбедности*, Привредапублик, Београд 1989., стр. 380-381.

[115] Според: Пајковић Драгић, *Обезбеђење одређених личности и објеката*, МУП Републике Србије, Београд 2003., стр. 88.

Во врска со безбедносните процени З. Драгишиќ го воведува и поимот на безбедносна појава, дефинирајќи го како општествена појава која со својата насоченост, цели и ефекти во поголема или во помала мера ги загрозува националната и другите видови на безбедност, вклучувајќи ја и корпорациската безбедност. Според степенот на општествена опасност, тој ги дели во три категории, и тоа: безбедносни појави со висок интензитет (тероризам, верски национален екстремизам, организиран криминал, шпионажа, атентати и др.), безбедносни појави со среден интензитет кои ги загрозуваат важните вредности на општеството, слободите и правата на граѓаните, животот и имотот на луѓето, безбедноста во сообраќајот, и безбедносни појави со низок интензитет, кои ги загрозуваат општествениот морал и личните интереси на луѓето, (мали облици на општ криминалитет).[116]

Состојбата на безбедносно работење на корпорациите е резултат од дејствувањето негативни и позитивни безбедносни појави кои во крајна линија се појавуваат како вкупно загрозување на деловниот субјект и на неговите капацитети да одговорат на тие загрозувања. Преку истражување на состојбата на безбедно работење треба да се утврдат трендови и нови појавни облици на безбедносни закани, законитости во исполнување на негативни безбедносни појави и причини за нивно појавување. Состојбата на безбедност се утврдува со примена на методи за изработка на безбедносна процена кои во начело се статистички методи, методи на анализа, синтеза и сл.[117]

За време на вршење на безбедносни процени на загрозеност и процена на безбедното работење на корпорациите, се идентификуваат бројни закани и ризици со различно потекло. Во таа смисла, одговорноста на вработените, а особено на оние што се задолжени за безбедност на корпорациите врзана е за менаџмент на ризиците кои вклучуваат и анализи на ризикот, како средство кое го олеснува комплетирањето на следните задачи: идентификација на лица, објекти и имот кои вредат да се заштитат; идентификација на закани кои можат да доведат до загрозување на безбедноста на имотот, лицата и работењето на корпорацијата; процена на веројатноста да дојде до штетни случувања, влијанието на заканите на процена

[116] Види: Драгишиђ Зоран, Безбедносни менаџмент (скрипта), Факултет безбедности, Београд 2006., стр. 35-36.

[117] Исто., стр. 37.

на; можноста за управување со заканите и идентификација на контрамерките на овие закани.[118]

Идентификацијата на лицата, објектите и деловните ресурси е поврзана со утврдувањето на основаноста на заканите кон корпорацијата и дефинирањето дали нејзината загрозеност може битно да влијае на одредени појави на општеството и на државата. Идентификацијата на екстерни и на интерни закани[119] опфаќа препознавање на намерите на способноста на потенцијалните носители на загрозувањето. Екстерните закани се движат од екстремно загрозувачки настани, како што се терористичките напади и киднапирањето, до нешто помалку драстични како провала во објекти. Интерните закани вклучуваат кражби, саботажи, насилство, вандализам и издавање на чуствителни информации. Екстерните закани, исто така, вклучуваат индустриска шпионажа, контаминација на производи, уцени, јавни немири, пожари, временски непогоди, земјотреси и други видови природни катастрофи. Проценатa на можноста да се случи настанот тргнува од прашањето колкава е можноста да се дојде до одреден заканувачки настан. Процена на можноста бара ментална концентрација и не се заснова на математички модели или формули. Прецизните бројки никогаш не се мерило кога се работи за фактор на кој влијае единствено човечкото однесување. Повеќето вакви анализи доаѓаат од познавање на природата на криминалните закани, искуството и здраворазумското размислување.

Анализата на безбедносните закани, загрозувања и ризици, претставува процена на секоја реална или потенцијална закана за корпорацијата која може да предизвика повреда или смрт на лица и/или уништување (губење) на имотот на компанијата и/или смалување на профитот, односно финансиски загуби без разлика на нивната големина. Се однесува на постепена и системска анализа на работата и постапки кои произлегуваат од процесот на работа на корпорацијата со цел идентификација на ризик или закана на компанијата и изработка на проактивни препораки, решенија и

[118] Кековиќ Зоран, Савиќ Сузана, Комазец Ненад, Милошевиќ Младен, Јовановиќ Драгиша, op. cit. стр. 53.

[119] Заканата е индикација, околност или настан која може да предизвика загуба во работењето или штета на имотот, како и смрт, повредување или пречки во работата на високите раководители и други запослени во корпорацијата.

процедури за нивна елиминација и/или ублажување на последиците во случај на остварување на заканата во текот на работата на корпорацијата.[120] При анализа на секој ризик треба да се одговори на следните критични прашања: „Дали сме свесни дека ризикуваме“?, „Заради што ризикуваме?“, „Колку и кога најмногу ризикуваме?“. Одговорите на овие прашања се значајни од повеќе аспекти, и тоа заради: договарање работи; трошоци и време на реализација на работите или на проектите; квалитет на производите и услугите; управување со буџетот; одлучување.[121]

Некои автори укажуваат дека целта на анализата на безбедносните ризици е одвојување на малите (прифатливи) ризици од оние главните, т.е. доаѓање до релевантни сознанија кои треба да овозможат нивно вреднување, а потоа и управување со ризикот.[122] Во таа насока, анализата е поврзана со одредување на последиците и веројатноста на секој ризик, заради одредување на неговиот степен, додека самиот степен на ризик се одредува со врската меѓу веројатноста (зачестеност или можност) и последиците (влијание и ефект) ако се појави ризикот. Веројатноста на настаните кои се појавуваат и обемот на нивните последици се проценуваат во контекст на постојните контроли. Вреднувањето на ризикот вклучува квалитативно и квантитивно споредување на степенот на ризик одреден за време на процесот на анализа според претходно утврдени критериуми на ризик, односно формирање соодветно степенување.[123] Резултатот од вреднувањето на ризикот е создавање на приоритетна листа на ризик заради преземање на понатамошни мерки во компанијата, односно одлучување дали конкретниот ризик ќе биде прифатлив или во некоја наредна фаза ќе биде активно третиран.[124]

Секоја компанија може да се соочи со голем број ризици и кризи предизвикани од нив при што за менаџмент околу ризиците клучно значење има нивната идентификација, т.е. проценатa на веројатност на појава на кризата (невозможно, скоро невозможно, малку веројатно,

[120] Даничић Милан, Стајић Љубомир, op. cit. стр. 47.

[121] Кековић Зоран, Савић Сузана, Комазец Ненад, Милошевић Младен, Јовановић Драгиша, op. cit. стр. 52.

[122] Sage P. Andrew. op. cit. p. 5.

[123] Пошироко види: Sarin K. Rakesh, Weber Martin, ,,Risk-Value Models“ , in: European Journal of Operational Research, vol. 70, Issue 2, Elsevier, London 1993, pp. 138-140.

[124] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 40.

можно, повеќе од можно/се случувало во конкурентските компании; многу можно/можно е и порано да се случувало во компанијата; предупредувачките знаци се евидентни) и големината на штетата која за корпорацијата може да настане (без штети и сериозни последици; мало оштетување кое лесно може да се поправи; извесна штета; значителна штета; значителна штета која е предмет на медиумите; разурнувачка штета која на насловните страни и во ударни вести може да ја уништи компанијата). По овие фази, следи контрола на ризикот и санирање на последиците од кризата.[125]

Неопходно е внимателно да се анализираат условите во кои потенцијалниот извор на загрозување може да ја изврши својата замисла во однос на работата и мерките кои се преземаат заради заштита на корпорацијата. Ако безбедносно-заштитните мерки се неразвиени а кај изворите на загрозување постои позитивна процена дека без проблем може да ги реализира своите замисли, тогаш веројатно ќе се случи загрозување на безбедноста на корпорацијата. Ако по правилни безбедносни процени, мерките на обезбедување се правилно поставени, кај носителот на загрозување ќе се развие убедување дека не е можно да го спроведе замисленото, па постои можност од злонамерното дејствување да се откаже.[126]

Проценатa на влијанието (последица) на заканата е субјективна процена која се базира на историјата на нападот на корпорациската безбедност и искуството на сродни служби на безбедност во слични ситуации. Мерките на влијанието вообичаено се изразуваат со негативни последици за општеството и државата ако дојде до несакани настани, но се изразува и во пари. Тука спаѓаат и трошоците за замена, поправки, губење на продуктивноста, губење на државните и на деловните можности и друго. Ако последицата вклучува повреда или смрт, загубата се мери со скалата на траума, која не може да се изрази со пари.[127]

Во последниот чекор на анализата на ризикот, безбедносните контрамерки се идентификуваат и потоа се проценуваат според

[125] Види: Петровић Перо, *Менаџмент ризицима на тржишту капитала*, Институт економских наука, Београд 2000, стр.17-18.

[126] Мандић Горан, *Систем обезбеђења и заштите,* op.cit. стр. 42.

[127] Според: Јегеш Мила, „Интегрисани систем безбедности нафтне индустрије А.Д. Нови Сад“, во Први Меѓународни научни скуп „Приватна безбедност – стање и преспективе“ (Зборник радова), Факултет за правне и послевне студије, Нови Сад 2008., стр. 431-432.

соодветноста на трошоците. Изборот на контрамерки е заснован на две информации. Првата е добиена од процесот на анализа на ризик (податоци за идентификација на имот и закани, процена од можноста дека нешто ќе се случи, процена на влијанието и фреквенцијата, како и процена на соодветното управување со ризик. Другата информација се однесува на природата на работата, целта и филозофијата на управување и културата на корпорациската организација. Истражувањета за контрамерките ја насочуваат управата да обрати внимание на следните релевантни прашања: „Дали е секогаш најдобро решение да се спречи настанот"?, „Дали е разумно да се преземат проактивни чекори за да се ублажи ефектот од настанот"?, „Дали е разумно да се комбинираат превенцијата и ублажувањето"?, „Дали е доволно да се биде свесен за заканите и да не се преземе ништо однапред за тие да се спречат или да се ублажат"?, „Дали превенцијата или ублажувањето се вредни"?. Културниот или општествените фактори може да бидат особено важни во објаснувањето зошто консултантите на менаџмент на ризикот понекогаш нудат неможност од препораки.[128]

4. ПРИНЦИПИ НА ФУНКЦИОНИРАЊЕ НА КОРПОРАЦИИТЕ

Работењето на современите корпорации го детерминираат три елементи кои истовремено постојат и се меѓусебно зависни: поволни околности (opportunities), ранливост (vulnerabilities) и зависност (dependencies). Во денешниот отворен пазарен натпревар секој деловен субјект има шанса за деловен успех. Истовремено, тој субјект е ранлив без разлика дали опасностите на кои е изложен се резултат на жестоката пазарна конкуренција или произлегуваат од општата несигурност. Менаџерите на корпорациите во минатото никогаш немале толкава потреба и разбирање за заканите со кои е соочена нивната компанија. За разлика од поранешниот период, денес ниту една корпорација не е во потполност имуна на факторите на изненадување, односно на „ненадејни удари". За тоа сведочат и случаите како што беше пропастот на енергетскиот гигант Enron

[128] Види: Dorfman S. Mark, *Introduction to Risk management and Insurrance*, Prentice Hall, Englewood Cliffs NJ., pp. 393-396.

Corporation во САД или на една од најмоќните светски авиокомпании, швајцарската фирма Swissair. Enron во 2000 година држела 25% од американскиот енергетски пазар, а вредноста на капиталот изнесувала 77 милијарди УСД. Сета таа моќ корпорацијата не ја спасила од пропаст една година подоцна, кога загубите, грешките во сметководството и незаконитостите во работењето ја довеле до распад. Деловните грешки на менаџментот, а пред сè преголемите вложувања во проблематични авиокомпании во Франција и во Белгија, како и ситуацијата во светот по терористичките напади во САД од 11 септември 2001 година, го довеле Swissair на работ на пропаст.[129] Тие примери пожуваат дека корпорациите, ако сакаат успешно да работат во современи услови, мора да ги антиципираат идните настани и закани, а врвниот менаџмент е должен да ги дефинира примарните деловни одговори на сите предизвици. Покрај тоа, работењето на денешните корпорации не може се набљудува изолирано, туку тоа е поврзано и е зависно од редица околности и настани условени од глобализациските трендови во светот.

Според американската авторка, Маргарет Блер, „подрачјето на корпорациското управување опфаќа корпорациска правна рамка и практика на донесување одлуки во надзорните одбори и управи на корпорациите, разни аспекти на корпоративни финансии, закони кои го регулираат работењето со хартии од вредност, стечајни закони, закони кои го регулираат работењето на финансиските институции, односи со вработените, договорно право и теорија, сопственички права, компензациски системи и системи на интерно информирање и контрола“.[130]

Како што истакнува Д. Хрушка, надворешните и внатерешните елементи на корпорациско управување и односите помеѓу нив го дефинираат системот на корпорациско управување. Односите помеѓу елементите во системот на корпорациско управување се одредени со редица причинско-последични врски кои се нарекуваат механизми на корпорациското управување. Основната разлика помеѓу одделните системи на корпоративно управување е позицијата на корпорациска контрола. Елемент на корпорацискиот систем е

[129] Според: Mishkin S. Frederick, Eakins G. Stanley, *Financijska tržišta i institucije*, Mate, Zagreb 2005., str. 380-381.

[130] Види: Blair M. Margaret, *Ownership and Control - Rethinking Corporate Governance for the Twenty-First Century*, The Brookings Institution Press, Washington DC 1995., pp. 3-4.

во позиција на контрола ако своите цели може да ги наметне како цели на корпорацијата. Инаку, целите на корпорацијата можат да бидат разновидни: да се опстои, да се максимизира пазарниот удел, продажбата, профитот, да се минимизираат трошоците и друго. Со други зборови, целта на корпорацијата е сè она што субјектот во позиција на корпоративна контрола го посакува.[131]

Реагирајќи на финансиската криза во државите на Источна Азија во 1997 година, Организацијата за економска соработка и развој (OECD) во 1999 године пристапила кон изработка на принципи за корпорациско управување, кои биле наменети за земјите со пазари во развој. По финансиските скандали во различни корпорации во текот на 2003 година (Enron, WorldCom, Credit Lyonnais, Vivendi, Parmalat и др.) прашањето за квалитетот на корпорациското управување добило на значење не само за земјите во развој, туку и за државите со развиена пазарна економија – токму поради дотогашното недоволно квалитетно корпорациско управување. Споменатите принципи на OECD се ревидирани во 2004 година.[132]

Доброто корпорациско управување подразбира не само начин на кој се управува со компанијата, туку и односите во неа и односите со надворешните учесници на микро и на макро план, како и правна и институционална регулатива. Во таа смисла, корпорациското управување е систем со кој се водат и да се контролираат компаниите. Тој систем го сочинуваат збир на односи помеѓу управата на корпорацијата, нејзиниот одбор, акционерите и други иматели на интереси. Корпорациското управување обезбедува структура низ која се остваруваат целите на компанијата и се утврдуваат средствата за постигнување на тие цели и надгледување на резултатите. Доброто корпорациско управување треба да овозможи и да го поттикне остварувањето на целите, да обезбеди квалитетен менаџмент и економично искористување на ресурсите, што е во интерес не само на компанијата и на акционерите туку и на сите други заинтересирани страни. Корпорациското управување денес е широко прифатено како мисловно средство за воспоставување на

[131] Пошироко кај: Tipurić Darko, Hruška Domagoj, Mešin Marina, *Promjene vrhovnog menadžmenta i korporativno upravljanje*, Sinergija, Zagreb 2011, стр. 182-183.

[132] Види: Stability Pact – South East Europe Compact for Reform, Investment, Integrity and Growth – White Paper on Corporate Governance in South East Europe, South East Corporate Governance Roundtable and the Corporate Affairs Division in Cooperation with the Investment Compact Team, OECD, Paris, June 2003. (http: www.stabilitypact.org).

привлечна инвестициска клима која ја карактеризираат конкурентни компании и ефикасни економски пазари. Во таа смисла, присутна е корелација помеѓу ефикасните економски пазари и стопанскиот раст како на микроекономско, така и на макроекономско ниво, но и поврзаност, условеност и меѓузависност на корпоративното управување и стопанскиот раст.[133]

Различните емпириски истраживања покажуваат дека постои директна корелација помеѓу квалитетот на корпорациското управување и резултатите на компаниите, кои може да се мерат со финансиски показатели, стапка на иновации, зголемување на учеството на пазарот, времето кое е потребно за излегување нови производи на пазар, задоволството на клиентите, на купувачите и на вработените и др. Од изнесеното следи дека квалитетното корпорациско управување е извор на конкурентски предности за компанијата, која на тој начин ќе биде попрофитабила, со обезбеден долгорочен раст и развој.[134]

Во современата практика на корпорациите, две групи механизми го осигуруваат ефикасното управување и помагаат во решавање на судирите на интереси кои се јавуваат во корпоративните структури. Станува збор за интерни и за екстерни механизми на корпорациско управување. Интерните управувачки механизми на корпорациите се: одбори на директори, наградување на менаџментот, концентрација на сопственоста, односот со интересно вклучените групи, финансиска транспарентност и адекватно објавување на релевантни информации. Во екстерни механизми на корпорациското управување спаѓаат: пазар за корпорациска контрола, правната инфраструктура, заштита на малцинските акционери и условите на конкуренција.[135]

Одборот на директори е организациски инструмент со чија помош акционерите, односно сопствениците влијаат на дејствувањето

[133] Види*: Corporate Governance Codes Relevant to the European Union and its member States*, Survey of Corporate Governance Development in OECD Countries, Paris 2003 (http: www.europa.eu.int/comm/internal_market/en).

[134] Според: Tschopp H. Gerry, „Corporate Governance – The Key to Success of Failure", in: *BoardRoom - Magazine for Corporate Governance, Leadership and Quality of Life*, No. 1, New York 2002., pp. 24-29.

[135] Види: Bai Chong-En, Liu Qiao, Song M. Frank, Zhang Junxi Jack, „Corporate Governance and Market Valuation in China", in: *William Davidson Working Paper No. 565*, The William Davidson Institute, University of Michigan Business School, Ann Arbor MI, April 2003., pp. 5-7.

на менаџерите како би обезбедиле корпорацијата да функционира на начин со кој ќе се остварат нивните интереси. Одборите на директори се врска помеѓу сопствениците и менаџерите, и заради тоа имаат клучна улога во корпоративното управување. На нивно чело се, по правило, главниот извршен директор (Shief Executive Officer – CEO), главниот оперативен директор (Shief Operation Officer – COO) и главниот финансиски директор (Shief Finance Officer – CFO). Постојат два начина на организирање на Одборот: постоење еден одбор на директори (The Board of Directors) или постоење два одбора, и тоа: надзорен одбор (Supervisory Board) и управа (Management Board). Независно од организациониот облик, Одборот на директори се занимава со прашања на управување со компанијата за да може во корпорациите да се зголеми ефикасноста на работата на Одборот, често се раздвојуваат функцијата на управување од функцијата на надзор. Честа е и практиката Одборот на директори да формира специјализирани пододбори, како што се: Одбор на неизвршни директори, Извршен одбор, Одбор за наградување, Одбор за ревизија и Одбор за корпорациска безбедност. Одборот на неизвршни директори го сочинуваат лица кои не се менаџери во компанијата и тој има задача да врши надзор и контрола на работата на извршните директори. Одборот за наградување ја утврдува висината на надомест и компензацијата за менаџерите и другиот клучен персонал во корпорацијата. Одборот за ревизија се занимава со квалитетот и точноста на финансиските извештаи. Ова тело мора да биде запознаено со содржината на финансиските извештаи и е одговорно за точноста на податоците во нив. Одборот за именувања предлага нови членови на одборот, ако се појави испразнето место. Одборот на директори често врши и други значајни работи, како што се избор на менаџери и нивно наградување, одлучување за прашања како што се издавање акции и други промени во капиталот на фирмата, пообемни инвестици итн. Добар одбор на директори може значително да го унапреди работењето на корпорацијата, како што лош одбор може да ја остави компанијата на милост и немилост на бескрупулозни или недоволно способни менаџери. Иако Одборот на директори е моќна институција, неговата работа од различни причини често не е доволно ефикасна. Прво, менаџментот често завладува со тоа тело, било со влијание на гласање на собрание на акционери, или подоцна во друга форма. Потоа, членовите на Одборот на директори обично попрво ја прифаќаат советодавната улога од надзорната и управната, што за нив е полесен пристап, главно поврзан со нивната обично мала финансиска заинтересираност за

резултатите од работењето на компанијата. На крај, менаџментот на корпорацијата практично секогаш има подобри информации од членовите на Одборот, поради што тие не успеваат ефикасно да му парираат и кога тоа го сакаат.[136]

Како правна институција, корпорацијата се заснова на приватна сопственост и по тоа, во правен поглед, не се разликува од индивидуалното приватно претпријатие. Меѓутоа, во модерните корпорации сопственоста во смисла на римското право, односно целосното овластување на сопствениците во однос на остатокот, никогаш не е во целост присутно. Во врска со тоа, се поставува прашањето: „Кој освен сопственикот може да ја контролира корпорацијата?“. Сопствениците законски имаат контрола над компанијата и ги одредуваат целите кои таа треба да ги оствари. Тука се поставува прашањето за начинот на остварување на тие цели. Во одредени случаи сопствениците особено ако немаат доволно знаења за да можат успешно да водат така сложен деловен систем вклучуваат односно ангажираат професионалци во администрацијата на работењето, и тоа во улога на менаџери. Во случај на делегирање на овластувањата за управување со деловниот систем од сопствениците кон менаџментот доаѓа до причинско одвојување на сопственоста и на контролата, бидејќи поединци немаат неминовно и менаџерски талент и финансиски капитал. Можноста сопственоста да се одвои од контролата овозможува на сите заинтересирани страни да ја одобрат својата позиција. Во потесна смисла, терминот корпоративно управување го одредува системот кој на сопственикот му го обезбедува врвниот менаџмент, поставен за да ги оствари целите на корпорацијата, и да ги исполни преземените обврски – создавање профит за сопствениците. Сопствениците својата позиција кон менаџментот ја уредуваат со менаџерски договори. Со воспоставувањето на договорните односи се решава проблемот околу усогласеност на интересите помеѓу учесниците во процесите кои се одвиваат во корпорацијата.[137]

А. Берл и Г. Минс корпорациската контрола ја поврзува со односите на релевантните фактори во управувањето со корпорациите (системот на корпорациско управување), кога ги одредуваат механизмите на контрола, посточката правна рамка и нивото на концентрација на сопственоштвото во компанијата. Како такви,

[136] Исто., pp.8-9.

[137] Tipurić Darko, Hruška Domagoj, Mešin Marina, op. cit. str. 184.

системите на корпорациско управување значително се разликуваат од земја до земја. Така истражувачите од англосаксонското деловно подрачје како основен проблем на корпорациско управување го наведуваат спротивното (опортуното) однесување на менаџментот и слабите, дисперзирани сопственици. Така, голем број сопственици со мал удел на капитал ја зголемува одвоеноста на сопственишТвото и контролата, која претставува основна карактеристика на модерните деловни системи – корпорации. Последицата од големата дисперзија на сопственишТво и на непостоење еден голем принцип е создавање преголемо влијание на менаџментот.[138]

Меѓутоа, некои автори укажуваат дека високата дисперзија на сопственишТвото и незаинтересираноста на инвеститорите е карактеристична за американските корпорации, но не и за остатокот на светот. Така во континентална Европа преовладува модел на корпорациска контрола од страна на големите акционери. Во моделот на големи сопственици основен проблем на корпорациското управување не е проблемот на надзор на менаџментот и обезбедување на исполнувањето на интересите на сопствениците. Основните конфликти во системите на корпорациското управување кое што го карактеризира високо ниво на сопственост се тензиите помеѓу големите акционери, кои имаат претставници во надзорниот одбор и учествуваат во поставување на целите на корпорацијата, со други влијателни интересни групи во корпорацијата.[139]

Големите инвеститори во корпорациите дејствуваат преку надзорните одбори. Кога се во состојба да ги поставуваат поголемиот број членови на надзорниот одбор, во позиција се и да можат да го именуваат и да го отпуштаат менаџментот, и да иницираат или да блокираат донесување на клучни одлуки. Самите надзорни одбори инаку се надлежни за имплементацијата на системот на корпорациско управување, додека големите сопственици се одговорни за поставување компетентни и ефикасни членови на надзорните одбори.[140]

---

[138] Според: Berle Adolph, Means Gardiner, *The Modern Corporation and Private Property*, MacMillan, New York 1932, pp. 38-39.

[139] Види пошироко: La Porta Rafael, Lopez-de-Silanes Florencio, Shleifer Andrei, „Corporate Ownership Around the World", in: *Journal of Finance*, Vol. 54, No. 2, Wiley, Hoboken NJ 1999., pp. 491-494.

[140] Cadbury Adrian, *Committee on the Financial Aspects of Corporate Governance - Report*, Gee Publishing, London 1992., pp. 15-16.

4.1. ПРОФИТНА ЕФИКАСНОСТ

Историски гледано ефикасноста на деловните системи долг период се мерела преку финансиската успешност и обемот на промет. Во услови во кои постојат на светскиот пазар на почетокот на XXI век, таквото оценување на корпорациите се покажало неадекватно, а сè поголемиот број научници и стручњаци од практиката ја истакнуваат централната улога на деловните процеси во сите сегменти на работењето, вклучувајќи ги настојувањата да се подобри неговата успешност.[141] Ставањето на деловните процеси во фокусот на мерење на напредокот на компанијата ги става менаџерите на корпорацијата во нова позиција за врз основа на сериозни анализи да ги дефинираат процесите и критериумите на успешноста, врзани за остварување клучни цели на компанијата, а пред сè создавање вредности.[142]

Императив на современите деловни системи во светот е идентификација на деловните процеси, нивна категоризација и моделирање, воведување следење и мерење на деловните процеси според критични фактори на успешноста (Critical Factor of Success – CFS) и клучни показатели на перформансите на работење (Key Performance Indicators – KPI). За таа цел, секоја корпорација развива систем за управување со деловните процеси (Business Process Management System – BPMS), кој овозможува континуирано управување и надзор над деловните процеси.[143]

Резултатите од следењето и мерењето на успешноста на деловните процеси, менаџментот може да ги користи за споредување со конкурентите, за дефинирање на стратегиските цели на компанијата, но и за следење на успешноста за спроведување на стратегијата на корпорацијата, додека сопствениците преземаат корективни активности и предлагаат подобрување на деловните процеси.[144]

---

[141] Види: Tenner R. Arthur, DeToro J. Irving, *Process Redesign: The Implementation Guide for Managers*, Prentice Hall, Upper Saddle River NJ, 2000, p. 75.

[142] Според: Hammer Michael, Stanton A. Steven, *The Reengineering Revolution: A Handbook*, Harper Business, New York 1996., p. 8.

[143] Види: Kueng Peter, „The Effects of Workflow Systems on Organisations", in: van der Aalst Wil, Desel Jörg, Oberweis Andreas (eds), *Business Process Management – Models, Techiques and Empirical Studies*, Springer-Verlag, Berlin, 2000., pp. 301-309.

[144] Според: Willaert Peter, Willems Jurgen, „Setting-Up a Business Process-Support Organization", in: *Managing Worldwide Operations & Communications with Information Technology*, IRMA International Conference, Vancouver, 2007., pp. 1275-1277.

Секоја корпорација настојува да функционира без да го загрози нејзиниот имот, сопствениците, менаџерите и вработените, за непречено да работи и така да ја оствари основната цел на постоењето – остварување профит. Во основа, остварувањето на профитот како стратегискака цел на корпорацијата сè повеќе е загрозена поради изложеноста на различни облици на ризик. Поради тоа сè поголемо внимание е насочено кон идентификацијата, проценатa и управувањето со ризици, но и за заштита, односно имплементација на одбранбените механизми (корпорациска безбедност), за да можат стратегиските цели на компанијата да бидат исполнети. Од аспект на безбедноста и заштитата, некогаш во голем број претпријатија се воочувале главно мали штети кои ги правеле незадоволните поединци. За разлика од тогаш, денес компаниите се соочуваат со напади на организирани групи, чија цел е загрозување на работењето и на имотот на деловниот субјект. Во врска со тоа, се користат најразлични начини и средства за загрозување, кои можат на корпорацииите да им нанесат големи штети. За да се спречи или да се избегне тоа, компаниите се принудени да воспостават ефикасни системи на заштита на сопствените процеси на управување и на деловните процеси.[145]

4.2. HSEC (Health, Safety, Environment Management, Community Relations)

Клучни компоненти на HSEC (принципот) се:

- здравје, што значи промовирање и подобрување на квалитетот на здравјето на вработените во компаниите и околното население;
- сигурност, односно востановување на заштитните вредности и обезбедување на работното окружување за безбедна и сигурна работа на вработените;
- животна средина, под што се подразбира промовирање ефикасно користење на деловните ресурси со намалување на ризикот од загадување на животната средина и зачувување на биолошката разновидност;
- општествената заедница, што вклучува почитување на етичките принципи, придонес кон економскиот просперитет и одржив развој на општествената заедница во опкружувањето и почитување на човековите права.

[145] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 66.

Заговорниците на општествената одговорност на корпорацијата тргнуваат од хипотезата дека деловните субјекти со подобра репутација имаат конкурентска предност над компаниите со помала или со недоволно добра репутација. Според нив, подобра репутација носи профит, ја штити корпорацијата за време на криза и спречува нејзино вовлекување во политички спорови во општеството. Така, според Е. Фримен и Д. Гилберт, основната идеја за корпорациска општествена одговорност е едноставна – компаниите се општествени идентитети, поради што треба да учествуваат во актуелни прашања на заедницата, сериозно да ги разбираат своите обврски кон општеството и да настојуваат да ги остварат.[146]

Сандра Духе во врска со тоа истражувала еден посебен аспект од кој може да се разгледува односот меѓу репутацијата на компанија и на корпорациска општествена одговорност. Имено, општествената одговорност, квалитетното управување и стабилните финансиски корпорации го чинат основниот атрибут на репутацијата, што според студијата на оваа авторка, е поврзано со добро финансиско работење.[147]

Наспроти ова, одделни критичари на корпорацискатa општествена одговорност, како Роберт Рајх, сметаат дека зад политиката на корпорацискатa општествена одговорност, особено јавните изјави со кои компаниите сами се фалат, се крие настојувањето стратегиите на некои корпорации да се претстават како добри и успешни и со самото тоа да се избегнат критиките на нејзина сметка. Тој укажува и на потези како што се наградите кои корпорациите и другите субјекти од деловната сфера си ги доделуваат сами на себе, со честитки за наводно корпорацискатa општествена одговорност. Во врска со тоа, Рајх го поставува прашањето: „Дали тоа е добра практика за управување или обид корпорацијата на лесен начин добро да се позиционира на пазарот?“.[148] Во таа насока,

[146] Според: Freeman R. Edward, Gilbert R. Daniel, *Corporate Strategy and Search for Ethics*, Prentice Hall, Englewood Cliffs, NJ 1988., p. 89.

[147] Според: Duhé C. Sandra, „Good management, sound, finances and social responsibility: Two decades of US Corporate insider perspectives on reputation and the bottom line”, *Public Relation Review*, Vol. 35, Issue 1, Elsevier Inc, New York, March 2009., pp. 77-78.

[148] Види: Reich B. Robert, *Supercapitalism: The Transformation of Business, Democracy and Everyday Life*, Alfred A. Knopf, New York 2007., pp. 126-127.

Лан Ни и Роберт Хит ја истакнуваат репутација на компанијата која е централен поим во расправите за корпорациска општествена одговорност и во дефинирање на најдобрите практики од таа област, но и дека претставува „меч со две острици". Во врска со тоа, тие го поставуваат следното прашање: „Дали може добрата репутација да ја затскрие вистинската состојба на компанијата која по обелоденувањето може релевантни интересни групи да ги наведе на заклучок дека или корпорацијата или нејзиниот менаџмент не ги исполнуваат најважните стандарди на корпорациската општествена одговорности, како што се претпоставувало?".[149] Ни и Хит, во врска со тоа, укажуваат на различни примери, поврзани за корпорациската општествена одговорност, споменувајќи бројни светски банки кои, како што можеше да се воочи за време на финансиската криза 2008 – 2010 година, со својата кредитна политика придонесле кон создавање услови за работење кои им одеа на рака на големите корпорации и нивните врвни менаџери, додека истовремено е нанесена штета на повеќето даночни обврзници. Овие автори сметаат дека има основа за сомневање дека многу корпорации и банки, како и различни интересни групи, имале корист од создавање и свесно преземање ризик со кој не можеле сами да состават крај со крај кога во 2008 година ескалира економската криза во САД од која, потоа, тие субјекти не можеле да излезат без државна помош. Л. Ни и Р. Хит даваат и пример на компанија за дистрибуција на играчки, кои се продавани или пробале да продаваат производи кои содржеле олово или некои други штетни супстанци. Иако знаеле дека репутацијата им е загрозена, некои од тие компании, не ги тестирале играчките и не запирале со продажбата на штетни производи, сепак се обиделе вината да ја префрлат на производителите на играчките.[150]

Корпорациската општествена одговорност, според извештајот во 2009 година, кој беше подготвен од меѓународната христијанска хуманитарна организација Christian Aid, често се користи за промовирање доброволно корпоративни иницијативи, како алтернатива на дополнителни или поголеми постојни задолжителни правила и норми. Во тој поглед, Меѓународната трговска комора агресивно го промовира концептот на корпоративна одговорност,

[149] Види: Ni Lan, Heath L. Robert, „Community Relations and Corporate Social Responsibility", in: Heath L. Robert (ed.) *The SAGE Handbook of Public Relations*, SAGE Publications, Thousand Oaks CA 2010., p. 559.

[150] Исто., pp. 561-562.

неоптоварен со стандарди, кои им овозможуваат на корпорациите да ги промовираат своите одговорности, без да се исполнат некои минимум стандарди. Во извештајот на Christian Aid, во врска со тоа, се истакнува дека многу невладини организации во светот се скептични кога станува збор за „движење на корпоративната општествена одговорност", која се сведува на корпоративни PR (Public Relations), тие да оценуваат дека тука се работи за начинот да се избегне спроведување на постојните утврдени правила. Во заклучокот на извештајот на Christian Aid, подготвен врз основа на детаљен преглед на документација и податоци за повеќе корпорации, се наведува дека „индустријата која е во процвет, познат како општествено одговорни корпоративни ... сега се смета за клучна алатка за промовирање и подобрување на јавниот имиџ на некои од светските најголеми фирми и корпорации... Тоа создаде превид за мултинационалните компании кои вложуваат напори од светот да направат подобро место за живеење е навистина само илузија ... Потребни се нови закони со кои ќе се принудат корпорациите да ги штитат човековите права и животната средина каде што работат."[151]

Ни и Р. Хит заклучуваат дека „репутацијата е најважна карика во ланецот на корпоративна општествена одговорност, односно дека корпоративната општествена одговорност е најважната карика во репутацискиот ланец. Но тој ланец воопшто не поднесува критика полесна од најслабата критика. Може да се заклучи дека со заговарање на настојувањата да се задоволат стандардите на корпоративните општествени обврски може да биде опасно во јавни дискурси и во репутацискиот менаџмент.[152]

4.3. *BCCM (Business, Crisis and Continuity Management)*

Принципот BCCM вклучува обезбедување работа на корпорацијата под нормални услови, во услови на криза, вонредни ситуации и несреќи, како и обезбедување на континуитетот на работењето по завршување на кризата и вонредните ситуации. За да ѝ се обезбеди работа на бизнис корпорација според овој принцип, потребно е да се дејствува проактивно и реактивно. Проактивно се дејствува во нормални услови на работење, во кои компаниите во текот на своето постоење и функционираат. Во овие услови, управувањето со безбедносните активности главно се врши според

[151] Види: *Getting Back on the Rails - The Private Sector and Development: A Christian Aid Report*, Christian Aid, London, October 2009., pp. 20-21.

[152] Ni Lan, Heath L. Robert, op. cit. p. 564.

строго пропишана методологијата на управување со ризикот (Risk Management).[153] Реактивното дејствување е применливо во кризни и во вонредни ситуации во кои се преземаат соодветни процедурални активности. Сите реактивни процедури се планираат и се извежбуваат во нормалниот режим на работа, што претставува составен дел од проактивното дејствување.

Н. Османагиќ-Беденик смета дека потенцијалната криза не е состојба на криза, туку само можност за нејзино појавување. Во таа смисла, деловните одлуки на менаџментот на корпорацијата, активностите или непреземените мерки, во комбинација со неповолен развој можат да предизвикаат или да ја интензивираат евентуалната криза. Потенцијални причини за бизнис кризи има во ситуација кога индивидуалните ризици и нивното акумулирање, во други околности, ќе станат сериозна закана за остварување на основните бизнис цели. Внимателното планирање и мисловно опфатените активности и нивните последици можеби може да се сметаат за можни ризици. Иако погрешниот развој не може да се избегне, кризниот менаџмент може во раната фаза да открие опасни случувања и да воведе мерки за да се совладаат ризиците или да се овозможи нивно намалување. Потенцијалната криза, како таква, не ја карактеризираат никакви симптоми, тоа е квазинормална состојба.[154]

Некои истражувачи, како Ж. Кешетовиќ и З. Ковиќ, сметаат дека постојат две основни групи причини за појава на криза кои ги погодуваат корпорациите, и тоа:

- надворешни причини, коишто настануваат во компанијата и немаат значително влијание (општи пазарни промени, промени во индустријата, глобалната економска криза. политички промени, промени во законодавството, природни несреќи).
- внатрешни причини, коишто се наоѓаат во рамките на истата корпорација (неадекватен и необучен менаџмент, некомпетентност, неморално лидерство, потценување на

[153] Ризикот е потенцијална мерка за неповолен исход на одреден настан. Претставува комбинација од веројатноста на настаните и нивните последици. Според класичниот американски економист Френк Најт, разликата помеѓу ризикот и неизвесноста е следна: ,,Ако не знаете сигурно што ќе се случи, но ја претпоставувате веројатноста, тоа е ризик. Меѓутоа, ако не ја претпоставувате ниту веројатноста, тогаш тоа е неизвесност“ (Според: Knight Frank, *Risk, Uncertanity and Profit,* Heart, Schaffner & Marx, Boston MA., p.25.)

[154] Bedenik Osmanagić Nidžara, „Krizni menadžment: teorija i praksa“, op. cit. str. 106.

јавното мислење и подредените, неефикасни перформанси на функции за управување, нереални цели и барања на синдикатите, неефикасен систем на комуникација, слаба организациска култура, незадоволство и немотивираност на вработените, отсуство на контрола на вработените, несоодветни организација на работата, постоење на внатрешни неформални групи за акција, несредени односи за работните места).[155]

Според Алфред Крименахер, корпорациските кризи ги имаат следните генерички димензии: претставуваат точка пресвртница во развојот на следните настани и активности; доведуваат до ситуации кога е потребна итна акција; претставуваат закана за корпорациските цели и вредности; од нив произлегуваат значајни последици за иднината; произлегуваат од следот на настани од коишто резултираат нови услови, создавање несигурност во проценатa на ситуацијата и во постигнувањето на потребниот развој на алтернативите, ја намалуваат контролата над настаните и нивните последици, ги зголемуваат тензијата, стресот и стравот; ги прават достапните информации недоволни, временскиот притисок се зголемува; се менуваат односите меѓу вклучените лица во корпорацијата.[156]

За изворите на безбедносните ризици поврзани со бизнис корпорациите, постојат различни научни дефиниции и национални стандарди кои се применуваат во одделни држави. Здружението за стандардите на Австралија во општи извори на ризик за корпорацискатa безбедност ги смета: комерцијалните и правни односи помеѓу компании и други надворешни лица (добавувачи, потрошувачи и други), економските околности, кои можат да бидат присутни во корпорацијата на национално и на меѓународно ниво, т.е. фактори кои влијаат врз овие околности, однесувањето на вработените во компанијата и на лицата во нејзиното опкружување, природните феномени и настани, политичките околности, вклучувајќи ги и промените во законите и факторите кои влијаат на другите извори на ризик, технолошки и технички прашања и проблеми, дејствување на менаџерите и на други поединци во компанијата.[157]

---

[155] Кешетовић Желимир, Кековић Зоран, op. cit. стр. 23.

[156] Krummenacher Alfred, *Krisenmanagement: Leitfaden zum Verhindern und Bewaltigen von Unternehmungskrisen*, Verlag Industrielle Organisation, Zürich 1981., p. 5.

[157] Според: „Risk Management (S/NZS 4360:1999)“, Standards Association of Australia, Starthfield 1999., pp. 30-31.

За да можат бизнис стратегиите да ги задоволат своите основни корпорациски цели, потребно е да бидат идентификувани, спречени или сведени на минимум сите фактори кои му се заканууваат на исполнувањето на тие цели. Овој процес подразбира идентификување, анализа, оценување и обработка на безбедносни закани (ризици) и утврдување степен на дозволена ранливост на приоритетните ресурси, сервис на инфраструктурата и на имотот за да можат компаниите успешно да ги реализираат своите бизнис стратегии. Во утврдувањето на контекстот за управување со безбедносните ризици потребно е да се дефинира врската меѓу деловниот субјект и средината, идентификувајќи ги предностите, недостатоците, приликите и заканите за компанијата. Тој контекст вклучува финансиски, оперативни, конкурентни, политички (јавна перцепција/имиџ), социјални, културни и правни аспекти на функцијата на корпорацијата. Во таа постапка важно е средината да се дефинира на вистинскиот начин, бидејќи таа претставува рамка за одвивање на сиот процес, за да може идните чекори да бидат смислени и целисходни.[158]

Американскиот автор Роберт Сајмонс го вовел терминот стратегиски ризик, кој е дефиниран како неочекуван настан или серија на околности кои значително ја намалуваат способноста на менаџерите за спроведување на предвидените бизнис стратегии. Сајмонс разликува три главни видови стратегиски ризик: оперативен, ризик од оштетување на средства и конкурентен ризик. Првите два вида ризик се поврзани со средствата и со процесите на компанијата. Последниот од овие се однесува на надворешните случувања, односно да се промени во конкурентното опкружување.[159] Оперативниот ризик доаѓа од бизнис операциите на компанијата. Примери на ризици врз здравјето на луѓето и животната средина, кои произлегуваат од деловните операции, најдобро може да се илустрираат со дамката од танкерот Exxon Valdez во Аљаска, во март 1989 година или експлозијата на отровен гас во фабриката Union Carbide во Бопал, Индија, во декември 1984 година. Поради овие причини, повеќето корпорации на Запад имаат разработени процедури и процеси за решавање на оперативниот ризик, вклучувајќи ги и процедурите за управување со кризи.[160]

---

[158] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 37-38.

[159] Според: Simons L. Robert, *A Note on Identifying Strategic Risk*, Harvard Business School, Cambridge MA 1998., p. 4.

[160] Види: Гилад Бен, *Рано упозоравање: Пословне стратегије за контролу ризика*, ХЕСПЕРИАеду, Београд 2009., стр. 39.

5. ЦЕЛИ И ЗАДАЧИ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Во утврдувањето и дефинирањето на целите, задачите, принципите и критериумите за корпорациска безбедност во одредена компанија, покрај клучната улога на врвниот менаџмент на корпорацијата, влијание има и опкружувањето на компанијата, што ја доведува во врска функцијата на целта на планирањето на корпорациската безбедност, и работата на менаџерите за безбедност кои изработуваат соодветни планови на корпорацијата. На тој начин се воспоставува системска врска помеѓу функцијата на секторот за безбедност во корпорацијата и нејзиното опкружување, што укажува на нужноста од постоење на системски пристап при изработката на плановите во корпорациската безбедност.[161] Во таа смисла, како цели на корпоративната безбедност можат да се одредат: превентивно дејствување насочено кон елиминација на сите ризици[162] и загрозувачките фактори кои можат да влијаат на деловните активности и остварување деловен успех на корпорацијата; сведување на загрозувачките дејства на најмала можна мера; деловно функционирање во услови на криза, како и надминување на кризата и повторно нормално работење. За сето да се тоа оствари, потребно е да се воспостави нормативно, организациски и функционален конзистентен систем на безбедност кој ќе овозможи посигурна и поефикасна заштита на лицата, имотот и работењето на корпорацијата.

Целта на корпорациската безбедност е поправање на продуктивноста и поттикнување на конкурентноста, за безбедносните ризици да се намалат на најмала можна мера, како и да се подготват мерки кои се преземаат ако дојде до инциденти, опасности и штети. Вложувањето на деловната организација во безбедносните системи треба да се третира како зголемување на

[161] Види: Cederblom Doug, Pemerl E. Dan, „From Performance Appraisal to Performance Management: One Agency' Experience", in: *Public Personnel Management* Vol. 31, No. 2/2002, International Public Management Association for Human Resources, Alexandria VA 2002., pp. 131-140.

[162] Ризик е веројатноста за појава на нарушување во одреден технички-организациски систем, чии последици се деловно-економски загуби, односно производ на веројатност од случување на несаканиот настан и неговите последици (економски, еколошки и други).

вкупната вредност на таа организација чија цел е зголемување на продуктивноста и на континуитетот на деловните процеси. Освен секојдневните обврски, корпорацискатa безбедност мора да биде вклучена и во процесите на воведување нови технологии за да може да се предвидат безбедносните ризици но и да се предложат мерки со кои ризиците би се свеле на минимум.[163] Притоа, треба да се раководите од правилата според кои безбедноста не може да се импровизира, односно дека безбедноста не е само техничко, туку и стратегиско прашање.

5.1. СОБИРАЊЕ ИНФОРМАЦИИ И ДЕЛОВНО РАЗУЗНУВАЧКО ДЕЈСТВУВАЊЕ

Под поимот деловна информација се подразбираат сите сознанија кои се во функција на внатрешното и на надворешното дејствување на корпорацијата, односно сите информации коишто се потребни за работење и вршење на деловните интереси и цели. Денес, кога работењето не е ограничено само на стопанските субјекти и на економијата како подрачје на човековото дејствување, туку се шири на сите дејности, во такви околности деловните информации не можат да се задржат во својата класична рамка, иако во другите подрачја имаат иста функција. Во таа смисла, деловните информации можат да имаат и политички, правни, социјални, техничко-технолошки, демографски или научен карактер. Тоа во практика значи дека секоја информација, ако има потреба, може да биде и деловна, но и дека ниту една информација не мора да биде деловна ако како таква не е употребена. Информацијата не е деловна според своето настанување или потекло, туку според деловната потреба, намена или употреба. Актуелното постоење огромен број различни информации укажува на два аспекта на деловните информации – релативност (некоја информација на еден деловен субјект е деловна информација, а на друг не е) и релевантност (се бара не каква било информација, туку онаа која на одредена компанија ќе ѝ биде корисна и вредна).[164]

---

[163] Според: Campbell, G. K.: Measures and Metrics in Corporate Security, CSO 06 2006; Brennan, J. Walker, S., Security Careers/Defining Jobs, Compensation, Qualifications (посочено во: Вејић Томислав, „Корпоративна сигурност“, *Пошта* бр. 3/2007, Загреб 2007., стр. 38).

[164] Пошироко: Javorović Božidar, Bilandžić Mirko, *Poslovne informacije i business intelligence*, Golden marketing/tehnička knjiga, Zagreb 2007., str. 116-120.

Кон крајот на 50-тите години од XX век, во САД се појавил изразот Competitive Intelligence,[165] а триесетина години подоцна и Business Intelligence. Во научно-теориска и деловно-практична смисла, во поглед на меѓусебниот однос на поимите Competitive Intelligence и Business Intelligence постојат редица нејаснотии, контроверзи и несогласувања.[166] Така, некои автори, како Вернон Прајор и Јан Херинг, ги сметаат за синоними,[167] додека повеќе теоретичари сметаат дека Competitive Intelligence е составен дел на Business Intelligence.[168]

Без разлика на терминолошките дивергенции факт е дека терминте Competitive Intelligence и Business Intelligence настанале во САД, кои се сметаат за основоположници на претприемачкиот капитализам. Американскиот економски модел го карактеризира дерегулиран, односно слободен пазар, без никакви влијанија на пошироки фактори на дејствување, како што тоа е државата. Во тие околности, конкурентноста (competitiveness), разбрана како деловна способност, односно способност на економијата да произведе стока и услуги кои можат да ги задоволат своите тестирања на меѓународниот пазар и да го подигнат просечното ниво на просперитет и на животниот стандард на луѓето, е одлучувачки фактор кој некого го легитимира на пазарот. Акцентот на конкурентноста, односно на

[165] Поимот competitive intelligence се поврзува со Џералд Албум, кој при истражувањето на американските електроенергетски компании, заклучил дека нивните менаџери располагаат со мал број информации за клиентите и предложил воспоставување механизам за да можат менаџерите врз основа на добиените информации да добијат соодветни знаења за тоа. Види: Albaum Gerald, Competitive Intelligence C.I. Associates, Watertown MA 1959., pp.16-19.

[166] Англискиот збор business значи „работење“ а competitive значи нечија способност, односно, подготвеност за натпреварување и конкуренција.

[167] Според: Prior Vernon, „The Language of Business Intelligence“, *Society of Competitive Intelligence Professionals (SCIP)*, CI Resources, Alexandria VA (http: www.scip.org/ci/languagebi/asp); Herring P. Jan, „Create an Intelligence Program for Current and Future Business Needs“, in: *Competitive Intelligence Magazine*, Vol. 8, No. 5, Alexandria, September-october 2005.

[168] Според: Meyer E. Herbert, *Real-World Intelligence: Organized Information and Executives*, Storm King Press, Washington 1991., pp. 28-30; Sawka A. Kenneth, „Demystifying Business Intelligence“, in: *Management Review*, Vol. 85, No. 10, American Management Association, New York, October 1996., pp. 47-49.; Hammer Michael, Champy James, *Reengineering the Corporation: A Manifesto for Business Revolution*, Nicholas Brealey Publishing, London 1993., pp. 64-66.

поимот competitive, ја условил неговата доминација во американскиот деловен свет, со што се удрени темелите и поистоветувањето на споменатите поими.[169] Независно од различните дефиниции, извесно е дека во теоријата постои согласност во поглед на основните цели на Competitive Intelligence, кои опфаќаат: откривање закани кои на деловниот субјект му доаѓаат од конкуренцијата, елиминирање или ублажување на влијанијата од можните изненадувања, зголемување на сопствената конкурентска предност преку намалување на времето потребно за реакција на заканите и изнаоѓање нови деловни можности за корпорацијата.[170]

Големите промени на меѓународната сцена по распадот на комунистичките режими во Источна и во Централна Европа кон крајот на 80-тите години од минатиот век и забрзувањето на процесот на глобализација создале услови за поинтензивна и посеопфатна употреба на спомнатите поими и за примена на нивната содржина во деловната практика на корпорациите ширум светот.

Во стручните кругови постои неусогласеност и околу преведувањето (толкувањето) на поимот Business Intelligence, поради што и во нив и во јавноста можат да се споменат и изрази, како што се „деловна интелигенција“[171], деловно разузнувачка активност“, „деловно разузнавање“, „деловно истражување“, „деловно разузнавачко дејствување“, „управување со деловни информации“ и слично.

Терминот деловна интелигенција (англиски израз Business Intelligence) претставува збир на методологии и концепти за прибирање, анализа и дистрибуција на информации со помош на различни софтверски алатки, или способност за разбирање и брзо

[169] Види: Murphy Cristopher, „Where is Croatia on the Map of Competitiveness“, *Business Intelligence 2000*, Druga hrvatska konferencija o pribavljanju, organiziranju i uporabi poslovnih informacija, Zavod za poslovna istraživanja, Zagreb 2000.

[170] Според: Kahaner Larry, *Competitive Intelligence: How to Gather, Analyze and Use Information to Move Your Business to the Top*, Touchstone Books, New York 1996., pp. 16-21; Combs E. Richard, Moorhead D. John, *Competitive Intelligence Handbook*, Rowmann & Lttlefield, Lanham MD 1993., pp. 22-29.

[171] Во некои јазици се користат повеќе зборови за да се одреди значењето на англискиот поим intelligence, кој исто така може да означува и интелигенција и разузнавачка дејност. Така, во францускиот јазик Intelligence се однесува исклучиво на човековата интелигенција, додека за разузнавачката функција се користат други зборови, како renseignement. Слично е и во германскиот јазик (Nacrichten).

снаоѓање на менаџментот на одредена компанија во новите услови на работење.[172] Поимот Business Intelligence прв пат бил употребен во 1989 година од страна на Хауард Дреснер, аналитичар на Gartner Group, американска компанија за истражување информатичка технологија и развој, со цел категоризирање на концептите и на методите кои би помагале во полесно донесување на деловните одлуки. Деловната интелигенција претставува една од техниките на деловното информирање, која овозможува пронаоѓање информации потребни за полесно и поисправно донесување деловни одлуки. Некои од методите на деловната интелигенција вклучуваат и ископување податоци (Data Mining), складирање податоци (Data Warehousing) и OLAP мрежна аналитичка обработка на податоците. Business Intelligence еволуирала од систем за поддршка во одлучување кој бил користен во американските корпорации во 60-тите години на XX век.[173]

Хрватскиот автор Мирко Биланџиќ, во својот пристап на проблематиката на корпоративна безбедност, го користи терминот Business Intelligence, под кој подразбира легално прибирање деловни информации, односно јавно достапни податоци, обработка на тие информации во деловни анализи заради давање поддршка на менаџментот на корпорацијата во донесувањето и реализацијата на што поквалитетни деловни одлуки за зачувување на нејзината положба во деловното опкружување. Според М. Биланџиќ, поимот Business Intelligence, не е секогаш со исто значење, а во светот е во употреба повеќе од 20 години и се применува во речиси сите поголеми корпорации. Тој термин неретко погрешно се поистоветува со нелегалната и тајна деловна шпионажа, со која нема никакви врски. Основната цел на Business Intelligence е воочување поволни деловни можности пред конкуренцијата, односно рано откривање на изворите на загрозување кои се закануваат од деловното опкружување, за да има доволно време да преземе противакција и отстранување на опасностите.[174]

---

[172] Според: Fehringer Dale, Hohhof Bonnie (eds.), *Competitive Intelligence Ethics: Navigating the Gray Zone,* Competitive Intelligence Foundation, Alexandria VA 2006., p. 115.

[173] Види пошироко: Power J. Daniel (ed.), „Decision Support Systems“, 2002., pp. 27-28 (www.businessexperts.com).

[174] „Во Хрватска со корпорациска безбедност работат помлади референти – разговор со Mirko Bilandzic“, *Lider* br.126, Zagreb, 28 февруари 2008 година.

Според Мирко Биланџиќ, Business Intelligence е најважното подрачје на истражување на меѓународната економија, а во услови на глобализиран и хиперконкурентски пазар, еден од најважните стратегиски менаџерски ресурси и единствен кој не може да се имитира. Овој автор споменатото подрачје на корпорацискатa безбедност го дефинира како деловен радар кој предупредува на тоа каде се наоѓа компанијата на внатрешниот и на меѓународниот пазар, во каков однос е кон своите конкуренти, клиенти, добавувачи и деловни партнери, каде се поволните пазари, кои се попрофитабилни клиенти, во кој правец корпорацијата треба да се развива и како да ја остварува деловната стратегија и цели. За важноста на Business Intelligence сведочи и податокот дека во земјите на Европската унија се применува во рамките од 73% од компаниите во Норвешка, до 96% во Германија, додека во САД оваа функција е институционализирана во речиси сите посериозни компании. М. Биланџиќ истакнува дека предмет на Business Intelligence не се само информации од областа на економијата, туку и сите други податоци кои можат да дадат јасна претстава за потенцијалните потрошувачи и деловниот амбиент. Така, за процена на целисходноста од инвестирање во одредена земја е неопходна комплетна анализа на внатрешната политичка ситуација, социокултурниот амбиент на дадената држава, функционирањето на нејзиниот правен систем, техничко-технолошката развиеност, можностите за приспособување кон потенцијалните купувачи и друго.[175]

За Виктор Радун, Business Intelligence претставува дејност на следење на надворешното опкружување на компанијата во потрага по информации кои се релевантни за процесот на одлучување во рамките на деловниот субјект. Покрај истражувањата на актуелните конкуренти, Business Intelligence опфаќа и анализа на некои други области од опкружувањето, како што се потенцијалните процеси на припојување и интеграција или процена на ризиците за вложување во одредена земја.[176]

Ерол Мујановиќ ја дефинира Business Intelligence или Competitive Intelligence како процес на собирање, третирање, анализирање и користење стратегиски информации за некоја компанија. Притоа не се работи за прибирање интерни информации од компанијата, туку

[175] Исто., Mirko Bilandzic", *Lider* br.126, Zagreb, 28 февруари 2008 година.

[176] Според: Радун Виктор, *Конкуренција на нишану – Теоријски и практични аспекти истраживања конкуренције*, ХЕСПЕРИАеду, Београд 2008., стр. 95.

за информации за надворешните фактори кои влијаат врз нејзиното работење. Според Мујановиќ, станува збор за легален и за етички допуштен начин на собирање информации, кој се врши со помош на користење современа технологија или ангажирање на човечки фактор. Во таа смисла, постои граница помеѓу Business Intelligence и индустриската шпионажа, која го разделува легалниот начин на прибирање на информации од нелегалниот. Во дефиницијата Business Intelligence, важен е и сегментот за третирањето на собраните информации, бидејќи, ако податокот до кој се дошло не е употреблив за доносителот на одлуката во корпорацијата, истиот не е вреден, што всушност е и основната разлика помеѓу податокот и информацијата. Е. Мујановиќ, сепак, прави разлика помеѓу Competitive Intelligence и Business Intelligence укажувајќи дека првиот поим е многу широк и во себе ги опфаќа Business Intelligence, кој е повеќе фокусиран на софтверот и на информатичките алатки.[177]

Здравко Баздан смета дека „деловната разузнувачка дејност" или Business Intelligence, односно деловната разузнувачка служба (Business Intelligence Service), има примарна задача да ги спроведува и да ги реализира економските цели на врвниот менаџмент на корпорацијата, на чело со главниот извршен директор, со примена на легални методи на работење, а секундарна задача ѝ е да ја штити тајноста на податоците, процесите и постапките во кои се создаваат иновации, нови производи и нови технологии во компанијата. Исто така, задачи на деловната разузнувачката дејност се и заштита од неовластени упади во информатичката инфраструктура, спречување „уфрлање кртови" и сите други видови субверзивни дејствувања кои можат да ги преземат конкурентските деловни субјекти, но и органите на државата на чија територији се наоѓа корпорацијата. Во таа смисла, според овој автор, потребно е да се воспостави Центар за деловна разузнувачка служба во компанијата, и тоа како инвестиција, а не како трошок. Баздан укажува и на светските искуства во оваа област, наведувајќи дека транснационалните и мултинационалните компании веќе со децении имаат такви разузнувачки јадра, кои имаат многу важна улога во креирањето и во спроведувањето на деловните стратегии на корпорацијата.[178]

[177] Види: „Business Intelligence и индустријска шпијунажа - Пословање по моделу ЦИА-е", *Дани* бр. 608, Сарајево, 06.02.2009.

[178] Според: Bazdan Zdravko, „Menadžeri moraju znati: poslovno obavještajna djelatnost kreira najvažniji resurs upravljanja", во: *Poslovna izvrsnost*, god. III, br. 2, Hrvatski institut za kvalitetu, Zagreb 2009., str. 62.

Укажувајќи на значењето на деловните информации и улогата на Business Intelligence во нивното прибирање и откривање, Баздан наведува дека и во минатото се преземале операции (дури и воени) за да се дојде до клучни информации, или по секоја цена да се оневозможи „другата страна“ во истата таква намера. Според него, „војната за информации“ е израз кој се користел и кој ќе се користи сè додека постојат менаџери и работење. Како пример на изнесеното, Баздан го наведува случајот на германскиот пронаоѓач Рудолф Дизел, кој во 1897 година го патентирал дизел моторот, а во 1908 година и дизел моторот за надморско возење подморница. Дизел во ноќта наспроти 29/30 септември 1913 година исчезнал во текот на бродското патување за Велика Британија. Се смета дека од бродот го фрлиле припадници на германската тајна служба, од страв дека својот проект за подморници би можел да го продаде на Англичаните. Како друг пример, Баздан ја наведува посетата на советските инженери на фабриката „Боинг“ во Тахома, САД, до која дошло во 1974 година во рамките на културно-техничката соработка на двете земји. Овие инженери во текот на посетата на фабриката за чевли, успеале со помош на нивните ѓонови кои биле премачкани со лепак, да соберат метални струготини од авионските легури. Во овој втор случај, станува збор за неетичко, противзаконско прибирање информации, што спаѓа во рамките на деловната шпионажа (Business Espionage), односно индустриска шпиунажа (Industrial Espionage).[179]

Како што истакнуваат одделни автори, прибирањето навремени, точни и ажурирани информации само по себе не е доволно, бидејќи тие информации треба да се поврзат, да се стават во соодветен контекст и врз нивна основа да се изведат заклучоци кои ќе овозможат акција и на крај остварување профит на корпорацијата. Во услови на пренатрупаност со информации што е карактеристично за денешниот пазар, на поединците и на корпорациите им треба радар (Business Intelligence) кој треба да им овозможи навремено воочување релевантни информации, како и спречување загуби, но и на сето тоа што долгорочно не им носи добивка.[180]

[179] Bazdan Zdravko, op. cit. str. 64.

[180] Види: Singer Slavica, Alpeza Mirela, Bakić Smirna, „Corporate Entrepreneurship: Is Entrepreneurial Behaviour Possible in a Large Company“, in: Rebernik Miroslav, Bradač Barbara, Rus Matej (eds), *The Winning Products – Proceedings of the 29th Conference on Entrepreneurship and Innovation Maribor*, Institute for Entrepreneurship Research, Maribor 2009., p. 220.

Business Intelligence е активност од цикличен карактер и се состои од следните основни фази: планирање и управување со циклусот (planning and direction); прибирање податоци (collection); обработка и анализа на податоците/изработка на разузнавачки анализи (processing and analysis); дистрибуција на готовите разузнавачки производи и нивно користење (dissemination). Сите овие фази се меѓусебно поврзани и се одвиваат паралелно, а со завршувањето на сиот процес циклусот се повторува.[181] За успех на процесот Business Intelligence потребно е секоја од наведените фази да биде остварена на задоволувачки начин, при што секоја наредна фаза може да започне дури откако претходната во целост ќе биде завршена. Тоа значи дека ниту една од нив не доаѓа сама од себе, што значи дека секоја сама по себе бара грижливо планирање и систематско реализирање.[182]

Општо земено, не постои стандардна категоризација на податоците. Тие можат да се поделат според нивниот карактер (јавни и тајни), според средствата и начините на собирање, според изворите, содржината итн. Во тој контекст, не постои ниту категоризација на податоци на која во поглед на собирањето е насочена Business Intelligence. Сепак, податоците можат логички да се структурираат во три општи категории, и тоа: *јавни*, кои по правило се отворени и достапни на сите; *приватни* (персонални) податоци кои ги поседуваат поединци, односно податоци за кои поединци имаат одредени знаења, како и *тајни* податоци.[183] Собирањето податоци во рамките на Business Intelligence се однесува на јавните, на отворените и на сите достапни податоци, како и на податоците за кои поединци имаат одредени знаења.[184]

Во поглед на средствата кои се користат за прибирање податоци, односно „зоните" во кои можат да се прибираат податоци, исто така, постојат три категории и тоа: „бела зона", која подразбира

[181] Радун Виктор, op. cit. стр. 364.

[182] Види: Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 72.

[183] Проценитe на некои американски автори укажуваат дека 80% од сите податоци кои им се потребни на менаџерите на корпорациите за донесување квалитетни одлуки, се наоѓаат во нивните компании (Види: Boni William, Kovacich L. Gerald, *Netspionage: The Global Threat to Information,* Butterworth Heinemann, Boston/Oxford 2000., p. 74

[184] Види: Meyer E. Herbert, *Real-World Intelligence: Organized Information and Executives*, Storm King Press, Washington 1991., pp. 36-37.

употреба на законски и на етички средства при собирањето на податоците; „сива зона“, во која се користат неетички, но законски средства и „црна зона“, која вклучува употреба на незаконски и на неетички средства.[185] Business Intelligence првенствено се ориентира на дејствување во „белата зона“, иако во практиката постојат случаи кои укажуваат и на активности во рамките и на „сивата зона“. „Црната зона“ е надвор од рамките на Business Intelligence и спаѓа во доменот на шпионажата.[186]

Постојат два вида начини на собирање јавно достапни податоци, и тоа од примарни извори и од секундарни извори. Примарни извори се: интернет, финансиски извештаи, говори, деловни настани, саеми, лични и телефонски интервјуа, како и јавно достапни публикаци. Секундарни извори се: online и дигитални бази на податоци, книги, написи во весници и списанија, ТВ и радио програми и аналитички извештаи. На овој начин добиените податоци имаат ограничена вредност, бидејќи претежно зборуваат за минатата или во најдобар случај за сегашна состојба, а квалитетна деловна одлука не може се донесе ако е исклучиво заснована на минатото или на сегашноста. Поради тоа е потребно да се имаат и податоци за она што ќе се случи во иднина, за што незаменлив е „човечкиот извор“ – ресурс кој се наоѓа внатре или надвор од деловниот субјект, а кој поседува информации од значење за корпорацијата.[187]

Гледано од аспект на информатичката инфраструктура, секој Business Intelligence систем започнува со изградба на архиви на податоци – централна база во која се слеваат сите податоци кои настануваат во компанијата, без разлика на тоа дали извор на тие податоци е некоја трансакциска апликација или други, т.н. индивидуални апликации кои се наоѓаат во персоналните компјутери на вработените, како, на пример, дадотеки во Exsel или во Access, или тоа се податоци собрани надвор од компанијата.[188]

---

[185] Boni William, Kovacich L. Gerald, op. cit. pp. 149-150.

[186] Bilandžić M., *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op.cit. str. 74.

[187] Пошироко кај: Nolan John, „Building an Effective and Inexpensive Internal Business Intelligence Network“, *Business Intelligence 2000*, Druga hrvatska konferencija o pribavljanju, organiziranju i uporabi poslovnih informacija, Zavod za poslovna istraživanja, Zagreb 2000.

[188] Види пошироко: McKenney Peter, „CI in Action: Key Steps to Building an Internal CI Function”, *Competitive Intelligence Magazine*, Vol. 8, No. 6, Alexandria VA, November-December 2005., pp. 10-13.

Во текот на фазата собирање на податоци, се собираат голем број разновидни „сурови“ податоци и сознанија. За тие податоци да се одвојат важни од неважни и да се разрешат нивните меѓусебни противречности, сите добиени сознанија се анализираат, се проценуваат, се интерпретираат и се обединуваат. Една од првите работи во процесот на обработка на податоците е нивно класифицирање според заедничките карактеристики. По класификацијата, собраните податоци подлежат на проверка и процена, односно утврдување на нивната сигурност и точност, имајќи предвид од кои извори се добиени. Во тој процес податоците се споредуваат со постојните сознанија и со податоците добиени од други извори. Аналитичката обработка на податоците подразбира употреба на различни методи (анализа, синтеза, компарација, индукција, дедукција и др.) со цел од низата фрагментарни сознанија да се добие јасна слика.[189]

Анализата и интеграцијата, пред сè се мисловен процес кој речиси целосно се потпира на човековата процена, расудување и интуиција, така што ова претставува критична точка во разузнавачкиот циклус. И покрај развојот на техничката поддршка во современата разузнавачка работа, сè уште нема замена за искуството, способноста за расудување и интуитивноста на аналитичарите. Способноста на луѓето да донесуваат судови и процени, заедно со интуицијата се клучни за успешно извршување на фазата на обработка на податоците. Тоа е основа за интерпретација на информациите и донесување заклучоци, како и за остварување на крајната цел на аналитичкото дејствување – продукција на финалниот разузнавачки производ кој содржи процени, заклучоци, проекции и алтернативни можности, а кој е наменет за крајниот корисник.

За да може крајниот разузнавачки производ да ја изврши својата функција, тој мора да биде навремен, што значи да вреди онолку колку што е употреблив за корисникот, бидејќи секое доцнење доведува до губење на можноста деловниот субјект навремено да реагира на заканата. Во услови кога постојат кратки рокови, а не се располага со сите потребни сознанија, се прави финална разузнавачка информација заснована на достапните податоци и по скратена процедура, при што се нагласуваат условите

[189] Пошироко види: Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 76.

во кои е настаната, со цел крајниот корисник да може да ја третира со одредена доза на резерва; да биде адекватен, што значи дека треба да ги задоволува барањата и потребите на корисникот, да биде разбирлив и достапен и да биде презентиран во бараната форма. По донесувањето соодветни деловни одлуки и по поминување на определено време, можно е прецизно да се одредат и да се оценат актуелните резултати од деловниот субјект со процени и заклучоци кои биле содржани во финалниот разузнавачки производ.[190]

Од европските земји на планот на научното истражување на процесите на Business Intelligence и општата општествена поддршка на тој концепт најдалеку е отидено во Шведска, првенствено благодарејќи на ангажирањето на Стеван Дедијер, кој со своите соработници во 1992 година ја формирал и првата мрежа во таа област – BISNES (Business Intelligence & Strategy Nework Scandinavia).[191] Во првата половина на 90-тите години на XX век, слични програми на државна разузнавачка поддршка на компаниите воспоставени се и во Франција, во Руската Федерација и во Јапонија.[192] Во развиените земји речиси секоја сериозна компанија се служи со деловна интелигенција (Business Intelligence). На тој начин менаџерите дознаваат за важни деловни информации, кои ќе се искористат за донесување клучни одлуки при изборот на најцелисходни деловни стратегии.[193]

Имајќи предвид дека Business Intelligence е феномен на поновото време и дека на одреден начин претставува новина во вкупното работење на корпорациите, неговата примена во деловните системи сè уште се соочува со различни отпори и негирања.[194] Резултатите од различни истражувања во САД и во земјите на

---

[190] Види: Bernhardt Douglas, *Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence*, Prentice Hall Financial Times, London 2003., p. 59.

[191] Dedijer Stevan, „Development & Intelligence 2003-2053“, *Working Paper Series*, Lund Institute of Economic Research - Infoforum Business Intelligence Conference, Zagreb 25-26 september 2003., p. 15 (http:www.lri.lu.se).

[192] Пошироко види: Joyal M. Paul, „Industrial Espionage Today and Information Wars Tomorrow“, in: *19th National Information Systems Security Conference*, Baltimore, October 1996., pp. 141-143.

[193] Bezdan Zdravko, op. cit. str. 75.

[194] Види: Blenkhorn L. David, Fleisher S. Craig, „Outsource Competitive Intelligence? A Viable Option“, in: *Competitive Intelligence Magazine*, Vol. 8, No. 6, Alexandria VA, November-December 2005., pp. 14-18.

Западна Европа укажуваат на тоа дека околу 90% од проблемите на воведување на Business Intelligence во компаниите било предизвикано од човечкиот фактор, односно од арогантни или игнорантски ставови на менаџментот. Околу 25% од корпорациите во САД и понатаму во својата работа не ги користат услугите на Business Intelligence, со образложение дека не им се потребни, односно дека не знаат како би ги примениле во процесот на донесување деловни одлуки.[195] Некои автори укажуваат и на други контроверзи на односите менаџмент – Business Intelligence а кои првенствено се однесуваат во одредувањето на деловните стратегии и цели. Имено, ако тие цели не се јасно одредени, односно ако врвните менаџери не знаат во која насока деловниот систем би требало да се движи, тогаш ниту најквалитетниот Business Intelligence нема значење. Истиот резултат ќе биде и ако целите на корпорацијата не се целосно и јасно артикулирани, односно ако менаџментот во одредена мерка ги крие од професионалците кои за потребите на дадената компанија се занимаваат Business Intelligence. Од друга страна, професионалната етика на лицата вклучени во BI им налага да ги поддржуваат деловните цели на компанијата и сопствените сознанија до кои ќе дојдат да не ги злоупотребуваат.[196]

Според Јан Херинг, еден од најзначајните теоретичари на проблематиката врзана за Business Intelligence, критериумите по кои Business Intelligence во одредена корпорација функционира на вистински и на ефикасен начин се следните:

- врвните менаџери располагаат со елементарни знаења за Business Intelligence, го поддржуваат дејствувањето на Business Intelligence внатре во компанијата и ги користат нејзините резултати во процесот на донесување и реализација на деловните одлуки;
- на чело на Business Intelligence одделението на корпорацијата се наоѓа врвен стручњак за тоа подрачје кој ужива доверба кај врвните менаџери;
- Business Intelligence оделението на корпорацијата континуирано дејствува најмалку пет години и е составено од врвни професионалци препуштени на својата компанија;

[195] Според: Sawka Kenneth, „Intelligence Ostriches and Eagles: Why Some Companies Soar at Competitive Intelligence and Why Others Don't Get It", in: *2006 SCIP International Annual Conference & Exhibition*, Orlando FL, April 2006., pp. 53-54.

[196] Meyer E. Herbert, op. cit. p. 46.

– Business Intelligence е дел од деловната култура на сите вработени во корпорацијата, кои Business Intelligence го прифаќаат како легитимна и неопходна деловна функција на денашниот глобален конкурентски пазар;
– Business Intelligence операциите професионално се планираат и се извршуваат во согласност со деловната политика, стратегија и плановите на компанијата;
– Business Intelligence програмите се остваруваат во согласност со законските и со етичките норми кои се составен дел на кодексот на конкретната компанија;
– Business Intelligence одделението на корпорацијата на професионален начин собира податоци од расположливите внатрешни и надворешни (отворени) извори, со помош на технички средства и од човечки извори;
– Business Intelligence анализите мора да дадат одговор на прашањето каде се наоѓа корпорацијата во однос на деловното опкружување и каква е нејзината позиција кон конкурентите, како и да го предвидат развојот на идните настани за да можат врвните менаџери да донесуваат примарни деловни одлуки;
– континуирано се спроведуваат Business Counterintelligence операции, со цел спречување intelligence операции од други деловни субјекти во деловното опкружување и заштита на интелектуалната сопственост и на деловните информации на корпорацијата;
– за собирање, архивирање, пребарување и дистрибуција на собраните податоци и информации се користи информатичка технологија.[197]

За разлика од Деринг во аргументацијата на Бен Гилад, во однос на Business Intelligence стои дека тоа е мерка на способноста на корпорацијата да го разбере конкурентското опкружување и ефикасно да се приспособува на сите промени во тоа опкружување. Според него, Business Intelligence е знаење на компанијата за сегашната и идната состојба на деловното опкружување, но не е и организациски инструмент за собирање, анализа и дистрибуција на информациите, т.е. донесување деловни одлуки врз основа на

[197] Види пошироко: Herring P. Jan, „World-Class Intelligence Programs“, in: *Competitive Intelligence Magazine*, Vol. 10, No. 2, Issue 3, Alexandria VA, May-June 2006., pp. 20-24.

тие информации, а во согласност со деловните интереси и потреби на корпорацијата. Овој автор Business Intelligence уште пократко го опишал како способност на компанијата да се натпреварува со конкурентите, но на таков начин за да биде од нив поуспешна. Според него, каква било грешка во спроведувањето на Business Intelligence нема да го доведе во прашање опстанокот на корпорацијата, но непостоењето на функцијата Business Intelligence може да доведе до тоа.[198]

Брзото темпо на развој на новите технологии и ширењето на глобалната трговија го условува денешното деловно опкружување кое се менува побрзо од кога било пред тоа. Извршните директори и менаџерите повеќе не мора да си дозволат луксуз во донесувањето на клучните одлуки базирани исклучиво на инстинкт и интуиција, бидејќи последиците од донесувањето на стратегиски лоши одлуки може да доведе до губење на трката на пазарот. Истражувањето кое во 2004 година го спровел MIT (Massachusetts Institute of Technology) на 4.500 менаџери, покажало дека адекватната примена на Business Intelligence ја зголемува ефикасноста на одлучување, бидејќи се намалува ризикот за донесување лоши проценки и погрешни одлуки кои како честа последица ја имаат турбуленцијата на пазарот. Таквиот заклучок го потврдуваат и резултатите од истражувањата кои се направени кон крајот на 2001 година, а ги објавило[199] списанието Business Week. Според тие истражувања, корпорациите кои го применуваат „Business Intelligence", бележат и до 20% поголем раст на приход за разлика од компаниите кои тоа не го прават. Идентични резултати од истражувања се добиени во 2002 година и на примерок од 405 врвни менаџери (CEO) на корпорации во САД, што е објавено во „Price Waterhouse Coopers Barometer Surveys".

Од државите на просторите на поранешна Југославија, прашањата на деловно-разузнавачкото дејствување на корпорациите нешто поголемо внимание се посветува во Република Хрватска. Меѓутоа, и во таа земја според тамошните автори, методите кои подразбираат Business Intelligence недоволно се применуваат, првенствено затоа што повеќето менаџери на хрватски компании за тоа не се информирани на вистински начин. Се случува овие

[198] Според: Gilad Ben, „A letter to CEO", in: *Competitive Intelligence Magazine*, Vol. 1, No. 1, Alexandria VA, April-June 1998., pp. 11-14.

[199] Види: Weiss Arthur, „Justifying CI Activities", in: *Competitive Intelligence Magazine*, Vol. 8, No. 6, Alexandria VA, November-December 2005., pp. 36-37.

компании да не можат на примерен начин да се однесуваат ниту кон странските партнери кои располагаат со речиси сите релевантни податоци, ниту кон домашната конкуренција.[200] Таквата ссостојба во економијата јасно укажува на потребата од отварање квалитетни Business Intelligence агенции кои би ги придвижиле тромите механизми во хрватската економија. Тие агенции би биле предуслов за создавање солидни основи за идно управување со деловните информации. Сепак во Република Хрватска постојат компании како „Плива“, „Адриса“ и „ХТ-а“, кои имаат формално задолжени одделенија за Business Intelligence.[201]

Како што истакнува Мирко Биланџиќ, Business Intelligence има две димензии на дејствување. Покрај офанзивната компонента, постои и дефанзивен, контраразузнавачки аспект (Business Counterintelligence), кој подразбира противразузнавачко дејствување во деловниот свет, насочено кон остварување на безбедноста на корпорацијата и воспоставување механизми за нејзина заштита. Во прашање се активности со кои се настојува кон елиминација или намалување на ефектот на Business Intelligence дејствување на конкурентите, како и мерки за заштита на информациите на деловниот субјект во однос на индустриската шпионажа. Во таа смисла, Business counterintelligence ги има следните основни цели: држење статус кво врзано за позиција на корпорацијата во деловното опкружување, процена на можните опасности и закани како и заштита на корпорацијата од незаконски и од неетички напади на други деловни субјекти.[202]

Во стручната литература се укажува дека степенот на ризик и опасностите на кои се изложени деловните информации на корпорацијата го зголемуваат следните фактори: деловното дејствување на компанијата во странство; децентрализирани информатички системи и мрежи на деловниот субјект; неконтролирана достапност до интернет на вработените; работење поврзано за националната безбедност; висок степен на соработка со конкурентите; значајни „joint venture“ (заеднички) странски и домашни инвестиции; постојните или најавени отпуштања на вработени; користење на висока технологија во работењето; непостоење сопствени Business

[200] Bazdan Zdravko, op. cit. str. 76.

[201] Singer Slavica, Alpeza Mirela, Bakić Smirna, op. cit. str. 222-223.

[202] Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 78.

Intelligence програми кои се во состојба навремено да ги детектираат заканите; непостоење сопствени Business counterintelligence програми на компанијата; широка употреба на електронско работење; партнерство во работењето и друго.[203] Според Џералд Ковачиќ, програмата за заштита на деловните информации има три основни функции: воспоставување контрола на пристапот до тие информации; овозможување исклучиво само индивидуален пристап, со претходна идентификација на секој поединец кој пристапува до доверливите деловни информации способност во секој момент да се утврди кој, кога, како, на кој начин и зошто имал пристап до доверливите информации, со постоење трага (запис) за тоа.[204]

Во современите корпорации прашањето на безбедност на деловните информации е актуелно идентично како и нивното собирање и како такво претставува еден од најголемите предизвици на модерното работење. Многу компании во светот уште од почетокот на 90-тите години на XX век започнале со примена на процесот на заштита на деловните информации кој тогаш се нарекувал „модел на обезбедување компетитивни способности" (Competitive Assurance – CA Model). Теоретската елаборација на тој модел ја дал Џон Нолан, кој сметал дека процесот на обезбедување на компетитивните способности на деловниот субјект се одвива во следните фази: точно утврдување на деловните информации на компанијата кои треба да се заштитат; процена на способностите на конкурентите да дојдат до тие информации; процена на внатрешните слабости на корпорацијата; дефинирање и примена на соодветни противмерки; континуирана анализа на ефикасноста на применетите контрамерки и откривање нови методи кои конкурентите можат да ги развијат заради доаѓање до заштитените деловни информаци.[205]

Појавата на нови видови загрозувања на корпорациите, со проширување на нивниот делокруг на работа, интензитет и краен ефект, довеле до тоа во некои земји да дојде до своевидна симбиоза на напорите на ниво на државата и компаниите

[203] Bonni Willian, Kovacich L. Gerald, op. cit. pp. 171 – 173.

[204] Според: Kovacich L. Gerald, *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*, Butterworth Heinemann, Boston/Oxford 1999., p. 40.

[205] Види: Nolan John, „Confusing Counterintelligence With Security Can Wreck Your Afternoon", *Competitive Intelligence Review*, Vol. 8, No. 3, Alexandria VA, Autumn 1997., pp. 53-57.

насочени кон остварување на оптимален степен на безбедност на деловните субјекти. Така, на ниво на национални разузнавачки системи воспоставени се програми кои укажуваат на изворите на зарозување и обезбедуваат поддршка и помош на корпорациите во остварувањето на нивната безбедност.[206] На тој план Федералното истражно биро (FBI) во САД уште на почетокот на 80-тите години на XX век[207] воспоставило „Програма за развој на свеста во однос на шпионажата, контраразузнавачката дејност и тероризмот" (Development of Espionage Counterintelligence and Counterterrorism Awareness – DECA), како интегрален дел на контраразузнавачкото дејствување на територијата на САД. Таа програма една деценија подоцна е проширени и преименована во „Програма за постоење на свест за прашања и противодговори во подрачјето на националната безбедност" (Awareness of National Security Issues and Response Program – ANSIR).[208] Слична програма за соработка со Централната разузнавачка агенција (CIA) во странство спроведува и Советодавниот совет на Стејт Департментот за прекуморска безбедност. Целта на таа програма е предупредување на американските компании на заканите кои им доаѓаат од земјата и од странство, како и давање помош на корпорациите во остварување на заштитата од потенцијални извори на загрозување, односно во воспоставување механизам неопходен за корпорациската безбедност.[209] За значењето на споменатите програми, но и за сериозноста на заканите на кои се изложени деловните субјекти во САД, сведочат податоците за континуирано зголемување на бројот на корисници на тие програми (во програмата FBI вклучени се околу 25.000 компании, а во програмата на Стејт Департментот учествуваат околу 1.600 американски корпорации кои работат во странство).[210]

---

[206] Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 171.

[207] Целосно оперативен од 1995 година.

[208] За програмата FBI види: *National Counterintelligence Center (NACIC): Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* pp. 10-11. Прикажано на: (http: www.ncix.gov/publications/reports/fecie_all/fecie_2000.pdf).

[209] *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage,* July 1995., p. 14. Преземено од: (http: www.fas.org/sgp/othergov/indust.html).

[210] Според: Vaknin Sam, *The Industrial Spies, Industrial Espionage in the Digital Age*, p. 24. (http: www.samwak.tripod.com/pp144h.html).

5.2. ПОДГОТОВКА НА КОМПАНИЈАТА ЗА РАБОТА ВО ВОНРЕДНИ СИТУАЦИИ

Поимот вонредна состојба потекнува од руската стручна литература од почетокот на XX век, во која е користен терминот *чрезвычайная ситуация* (вонредна т.е. исклучителна состојба). Во таа смисла, вонредната состојба го означува нарушувањето на нормалните услови на живот и работа во објектите или на дадената територија, предизвикани од хаварија, елементарна непогода, катастрофа, еколошки инцидент, епидемија и слично. Исто така, и со примена на расположливите средства кои може да ги употреби потенцијалниот противник, може да се нанесе штета на здравјето на луѓето или на природата и на опкружувањето, како и сериозни материјални загуби и нарушување на животот и на работата на луѓето. Врз основа на тие извори,[211] вонредните состојби може да ги класифицираме на следниот начин: според карактерот на опасноста (технички, природни, биолошки, еколошки и социјални), според степенот на зачестеност: најчести (земјотреси, транспортни хаварии), многу чести (пожари), со умерена зачестеност (хаварии на комуналниот систем, вулкани), најретки (епидемии, еколошки инциденти со големи размери) и според територијална зафатеност (локални, месни-општински, регионални, национални, федерални, меѓудржавни и глобални-транснационални).

Во документот на Министерството за внатрешни работи на Владата на Велика Британија од 1998 година под наслов *Dealing with disaster* (постапување при несреќи),[212] се користи изразот „сложени од големи размери вонредни состојби" (major emergencies), во кои спаѓаат: катастрофи, кризи и големи инциденти. Сложените вонредни состојби се објаснуваат како секој настан или околност (со предупредување или без) кој се заканува или предизвикува смртен исход за луѓето, флората и фауната, прекин на функционирањето на општествената заедница или нанесува толкава штета на добрата и на животната средина што службите за вонредни состојби, локалните власти и другите организации не се во состојба со своите

[211] Види: Мастрюков Б. С., *Безопасность в чрезвычайных ситуациях*, Издательский центр, Академия, Москва 2003., стр. 15-17; Лига, М. Б., *Качество жизни как основа социально безопасности*, Гардарики, Москва, 2006., стр. 10-14.; Архипова И. Надежда, Кульба В. Владимир, *Управление в чрезвычайных ситуациях*, РГГУ, Москва 1998., стр. 13-16.

[212] Според: Dealing with disaster (Third edition), Home Office Communication Directorate, London 1998., pp. 2-3.

редовни активности да ги намалат последиците од тие опасности. Во американската стручна литература вонредните состојби се поделени според објектот на загрозување: опасност по живот, здравјето, јавните добра и животната средина.[213] Повеќето земји во службите задолжени за решавање вонредни состојби ги вбројуваат: полицијата, противпожарните служби и итната помош. Со тек на времето бројот на служби кои се ангажираат се проширил, па во некои земји постојат и посебни министерства за вонредни состојби, како што е во Руската Федерација.

Во Република Хрватска терминот вонредна состојба е изедначен со поимот катастрофа. Слично гледиште има и СР Германија (Katastrophe). И во нивната литература под катастрофа се подразбира ненадеен и брзо развивачки настан, чијшто учинок врз луѓето и врз материјалните вредности е толку разорувачки, што итните служби и погодената заедница, поради недостаток на сила и средства, не се во можност соодветно да одговорат поради што е неопходно воведување вонредни мерки и помош од заедниците во соседството и пошироко. Поимот катастрофа во овој случај значи вонреден настан кој предизвикува прекин на нормалното функционирање на заедницата, големи човечки жртви, материјални разорувања и уништување на животната средина, со што се надминува способноста на погодената заедница сама да ги реши проблемите со употреба на сопствените сили и средства.[214]

Во Република Србија според член 8, став 1, од Законот за вонредни состојби, „вонредна состојба е состојба кога ризиците и заканите или последиците од катастрофата, вонредните настани или други опасности за жителите, животната средина и материјалните добра е во таков обем и интензитет што нивното настанување или нивните последици не може да се спречат или да се отстранат со редовно дејствување на надлежните органи и служби, поради што за нивно ублажување и отстранување неопходно е да се употребат посебни мерки, сили и средства при засилен режим на работење".[215]

Во Република Македонија вонредната состојба ја третира Уставот на Република Македонија во член 125 во кој стои дека

[213] Види: Wahle Thomas, Beatty C. Gregg, *Emergency Management Guide for Business & Industry*, Federal Emergency Management Agency (FEMA), Washington DC 2004., pp. 5-6.

[214] Пошироко кај: Млађан Драган, Кекић Далибор, „Ванредна ситуација – прилог концептуалном одређењу безбедности", у: Наука безбедност, полиција, бр. 3/07, Београд 2007., стр. 63-65.

[215] „Службени гласник РС", бр. 111/2009.

вонредна состојба настанува кога ќе настанат големи природни непогоди или епидемии.

Во стручната литература се смета дека сите вонредни ситуации во својот развој имаат четири карактеристични стадиуми, и тоа: настанување, иницијација, кулминација и смирување:[216]

1) во стадиумот на појава или настанување се создаваат предуслови на идната вонредна состојба (активирање неповолни природни процеси, натрупување на технолошките пропусти и проектно-производни дефекти, преоптоварување на опремата и на вработените, појава на екстремни физички услови на производниот процес, натрупување складирани опасни материи, акумулирање негативни антропогени влијанија на животната средина);
2) во стадиумот на иницијација се појавуваат: технолошки неправилности во врска со промена на параметрите на процесите, неповолни или екстремни временски услови, елементарни несреќи, диверзии и други загрозувачки дејства од страна на човечкиот фактор;
3) стадиумот на кулминација е проследен со ослободување голема количина маса и енергија, при што често незначителен иницијален настан го покренува механизмот на верижни случувања со повеќекратно зголемување на почетната сила и размер на случувањето (т.н. „домино ефект“);
4) стадиумот на смирување на вонредната состојба почнува од моментот на отстранување на изворот на опасноста и трае до целосната елиминација на последиците од вонредната состојба. Траењето на овој стадиум зависи од видот, од интензитетот и од размерот на последиците од вонредната состојба, и може да се мери дури и во децении (пр. Чернобилската катастрофа). Во врска со тоа, фазата на траење и текот на вонредната состојба може да дадат насоки за активностите кои треба да се преземат, со цел надминување на негативните последици на вонредната состојба.

Менаџерите на корпорацијата имаат обврска добро да ги слушнат, да ги воочат и да ги сфатат сигналите за претстојната криза и вонредна состојба. Меѓутоа, постојат бројни проблеми кои ги

[216] Според: Denk Robert, „Frühwarnung als integraler Bestandteil der Controllingkonzeption“, in: Eschenbach Rolf, Risak Johann (Hrsg.) *Die Krise als Normalfall: Aktuelle antworten des Controlling - Österreichischer Controllertag 1996*, Facultas, Wien 1997., p. 28.

спречуваат да ги слушнат и да ги прифатат таквите предупредувања. Тие, имено, секојдневно се бомбардирани со голем број информации и совети, со амбивалентни и со контрадикторни сигнали. Потребно е предупредувачките сигнали да се издвојат од многуте наизглед минорни и безначајни индиции. Исто така, патот на информацијата до менаџерот често е замрсен. На патот на кој лошите вести ќе поминат за да стасаат до највисоките раководители постојат бројни и сериозни пречки, особено во една бирократска организација, во која никој не сака непотребно да го тревожи својот претпоставен или да го понесе епитетот на оној што навестува проблеми. Заради тоа постои опасност врвните менаџери да станат жртви на „молчењето" како комуникациски образец во корпорацијата. Особено е опасна тенденцијата проблемот во настанувањето да не се сфати доволно сериозно. Така, раководството на корпорацијата Intel во 1994 година ја потценила неисправноста на чипот Pentium, која на менаџментот им ја укажал еден професор по информатика. Започнала размена на информации помеѓу експертите, која прераснала во лавина од пораки, а целата афера стигнала и до медиумите. Последицата била гнев на клиентите, предизвикан не само од грешката на чипот, туку и од игнорирањето на проблемот од страна на Intel.[217]

Преголемата самоувереност, исто така, е опасна за успешната корпорација, затоа што го поттикнува самозадоволството и буди чувство на неранливост што ги заслепува менаџерите кои не ги воочуваат знаците на доаѓање на опасностите и на вонредните состојби. За тоа сведочи случајот со автомобилската индустрија од почетокот на 80-тите години на XX век. Имено, тогаш се објавени резултати од истражување на мислењето на купувачите во поглед на квалитетот на возилата од различни светски производители на автомобили. Според тие резултати, јапонските возила ги заземале водечките места на ранг листата, а американската компанија General Motors се нашла на нејзиното дно. Податоците и други извори, исто така, укажувале на проблеми со квалитетот на возилата на General Motors. Раководството на најголемиот производител на автомобили во светот овие предупредувања ги занемарило, што резултирало со тоа што никогаш веќе не го надоместиле губитокот во уделот на светскиот пазар.[218]

---

[217] Види: Growe S. Andrew, *Only the Paranoid Survive*, Currency Doubleday, New York 1996., pp. 3-4.

[218] Според: Sorkin A. Ross, „A Bridge Loan: U.S. Should Guide G.M. in a Chapter 11", *New York Times*, 17 November 2008.

Системите за управување со ризикот во вонредни состојби се системи за управување чија цел е планирање, контрола и редукција на ризикот. Разновидноста и сложеноста на задачите кои се јавуваат при појавата и развојот на ризичниот/вонреден настан, како и неопходноста од негово брзо разрешување, бараат декомпозиција на системот на управување на низа меѓусебно координирани потсистеми.[219] Во врска со тоа, неопходно е да се обезбеди оптималност на декомпозицијата во смисла на задоволување на целта на системот.[220]

Во системите за управување со ризикот и вонредните состојби најчесто се користи декомпозиција по фазите на управување, кои подразбираат поделба на управувањето на планирање на ризикот (стратегиско планирање) и намалување на ризикот (оперативно управување со ризикот).[221] Структурата на овие потсистеми е одредена со целите и со критериумите на системот и со ограничувањата. Значаен дел во двете фази имаат податоците за потенцијалните фактори на ризик. Заради тоа за имплементација на системот за управување со ризици и со вонредни состојби неопходна е реализација на модулот за евиденција на факторите на ризик.[222]

5.3. ОБЕЗБЕДУВАЊЕ И ЗАШТИТА НА ВИТАЛНИТЕ ИНТЕРЕСИ НА КОРПОРАЦИЈАТА

Клучни вредности на корпорацијата се: репутација на компанијата на пазарот, нејзин корпорациски имиџ (углед), морал и мотивираност на вработените, стратегиските планови за развој, анализа на конкуренцијата. За воспоставување на овие вредности потребна е долготрајна работа и давање квалитетни услуги, како и

[219] Види: Trim R. J. Peter, „An Integrative Approach to disaster Management and Planning“, in: Disaster Prevention and Management Vol. 13, Issue 3, Emerald Group Publishing Limited, Bingley UK 2004., pp. 218-221.

[220] Kash J. Toby, Darling R. John, „Crisis Management Prevention, Diagnosis and Intervention“, in: Leadership & Organization Development, Vol. 19, Issue 4, Emerald Group Publishing Limited, Bingley UK 1998., pp. 179-183.

[221] Според: Yusko P. Kenneth, Goldstein W. Harold, „Selecting and Developing Crisis Leaders Using Competence-Based Simulations“, in: Journal of Contingencies and Crisis Management, Vol. 5, Issue 4, Vrije Universiteit, Amsterdam 1997., pp. 220-222.

[222] Според: Crichton T. Margaret, Flin Rhona, Rattray A. R. William, „Training Decision makers – Tactical Decision Games“, in: Journal of Contingencies and Crisis Management, Vol. 8, Issue 4, Vrije Universiteit, Amsterdam 2000., pp. 208-209.

постојано присуство на корпорацијата на пазарот. Корпорацискиот имиџ на компанијата, како и неговата репутација на пазарот, е од одлучувачко влијание за опстанокот и развојот на корпорацијата. Една од најважните дејности, кога е во прашање градењето и зачувувањето на корпорацискиот имиџ, секако е оценување на квалитетот на производите кои учествуваат на одделни манифестации.[223]

Како што истакнуваат одредени автори, заканите врз угледот на корпорацијата се проценуваат во процесот кој се состои од две фази, од кои првата е поврзана за препознавање на облиците на загрозување, односно видот на кризата, додека втората фаза вклучува стратегија на насоченост кон јавноста како одговор на кризата. Во тој случај, стратегиите се она што одговорните лица во компаниите го говорат и го прават по настанатата криза, а со цел заштита на репутацијата на деловниот субјект. Споменатите стратегии се разликуваат според степенот на одговорност за кризата која се прифаќа во корпорацијата, како и кон интересот за последиците. Така, стратегиите на непризнавање се базираат на тврдења дека ризик не постои, или на обидот за докажување дека корпорацијата нема одговорност кон кризата. Стратегијата за намалување настојува да ја минимизира одговорноста на компанијата и/или сериозноста на кризата. Стратегијата на повторна изградба нуди надомест и/или извинување на корпорацијата поради настанатата криза. Најпосле, стратегиите на зајакнување се појавуваат како дополнителни и вклучуваат изјави за успешното дејствување на компанијата во текот на кризата и самопофалување на субјектите кои биле зафатени со неа.[224]

5.4. ПРЕВЕНЦИЈА НА ИНЦИДЕНТНИ СОСТОЈБИ

Во стручната литература под безбедносен инцидент се подразбира секој непредвиден настан или случај кој може да предизвика значително оштетување на имотот, односно повреда или смрт на лица и/или да предизвика директни или индиректни загуби во приходите и профитот на корпорацијата.[225] Во службените

[223] Пошироко види: Bentele Günther, Fröhlich Romy, Szyszka Peter, *Handbuch der Public Relations: Wissenschaftliche Grundlagen und berufliches Handeln*, Verlag für Sozialwissenschaften, Wiesbaden 2005., S. 604-605.

[224] Според: Heath L. Robert, Coombs W. Timothy, 2006.: *Today's Public Relations*, Thousand Oaks, London 2006., pp. 205-206.

[225] Harms-Ringdahl Lars, *Safety Analysis: Principles and Practice in Occupational Safety*, Taylor & Francis Inc., New York 2001., p. 12.

документи на Европската унија за овој сегмент се користи терминот „голем инцидент“ (major accident), под што се подразбираат штетни емисии во големи размери, како и пожари и експлозии кои се резултат од неконтролиран развој на настани во одреден систем, кои за последица имаат сериозна опасност по човековото здравје и/или околина, веднаш или со одложено дејство, внатре или надвор од границите на набљудуваниот систем и кои вклучуваат една или повеќе опасни ситуации.[226]

Во тој контекст, некои автори го користат и поимот несреќа, под кој се подразбира настан кој е предизвикан од ненадејно дејствување на природните сили, техничко-технолошки или други фактори, а кој го загрозува здравјето и животот на луѓето, односно предизвикува штета во имотот на корпорацијата и загрозување на нејзиното природно опкружување. Несреќа од големи размери, по оваа дефиниција се смета настан кој со својот можен развој може да поприми облик на катастрофа. Можат да бидат предизвикани големи несреќи од неконтролиран развој на настаните и од несреќите по пат на ослободување штетни материи во голем обем, оган или експлозија во постројките во кои се произведуваат опасните материи, складираат или со истите се ракува, а чијашто емисија може да има директни или индиректни последици врз животот и здравјето на луѓето и животната средина.[227]

Кога е во прашање односот на корпорациите кон можните кризи, се споменуваат пет нивоа (степени) на нивна подготвеност, и тоа:

1) компании кои се склони на криза (немаат систем за рано предупредување, планови за ограничување на штетата ретко постојат пред да се случи криза, а системи за закрепнување сè уште не се воспоставени);
2) компании кои стравуваат од криза (често имаат програми за различни видови катастрофи, но не и за други видови кризи, пред сè надворешни економски удари или информатички напади);
3) корпорации приспособени на криза (имаат разработени планови и процедури за ограничен број нарушувања, како што се: проблеми со функционирање на компјутерите, сериозни грешки на операторите или поголеми безбедносни

[226] Види: „Control of Major Accident Hazards Involving Dangerous Substances“, *Council Directive 96/82/EC*, Council of the European Union, Brussels 1996.

[227] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 338.

пропусти, но сè уште не ги сфаќаат комплексните односи кои придонесуваат за настанување криза);
4) кризно зајакнати компании (не претставуваат напредок во смисла на видовите кризи кои ги идентификуваат и на планот на спроведување на превентивни акции, но имаат подобрено управување со фазите на кризата – поради воспоставување проактивен кризен менаџмент);
5) корпорации подготвени на криза (имаат разработени правила и процедури за кои експлицитно ги земаат предвид сите критични системи кои предизвикуваат или кои спречуваат поголеми кризи, како и поголем степен на свест за постоење организациска култура и нејзиното позитивно или негативно влијание на кризниот менаџмент).[228]

5.5. УПРАВУВАЊЕ СО РИЗИЦИ ВО КОРПОРАЦИЈАТА

Управувањето со ризиците може да се дефинира како преземање активности креирани за минимизирање на негативното влијание кое ризикот може да го има врз очекуваниот работен резултат. Со оглед на тоа дека управувањето со ризиците е активност која често бара вложување средства, треба да се знае дека намалувањето на негативното влијание што произлегува од изложеноста на работењето на компанијата на некој од ризикот нема нужно и да го елиминира тој ризик. Според тоа, на менаџментот е да одлучи помеѓу алтернативните стратегии на управување со ризиците како би се избалансирало намалувањето на ризиците и на трошоците поврзани за активноста на управување со ризиците. Одбраната стратегија пред сè ќе зависи од карактеристиките на корпорацијата и од нејзината изложеност на одделни видови корпорациски ризици, но и од начинот на размислување на нејзините водечки луѓе за тоа како да се интегрираат функциите за управување со ризици во работните процеси на компанијата.[229]

Управувањето со ризици спаѓа меѓу најстарите забележани човекови активности. Уште Аристотел говорел дека „секогаш треба да се очекува нешто неочекувано“[230], додека кинеската книга

[228] Кешетовиќ Желимир, Кековиќ Зоран, op. cit. стр. 30-31.

[229] Види: Schmit T. Joan, Roth Kendall, „Cost Effectiveness of Risk Management Practices“, in: *Journal of Risk and Insurance*, Vol. 57, No. 3, American Risk and Insurrance Association, Malvern PA 1990., pp. 458-460.

[230] Според: Аристотел, *О песничкој уметности* (XIV глава), Бојковиќ, Београд 1935.

на промени (Ји-Џинг) претставува еден од најстарите алати за донесување одлуки кој сè уште е во употреба и денес. Во современа смисла, под управување со ризик се подразбира процес на мерење или процена на ризикот и развој на стратегија за излегување на крај со ризикот. Се работи за идентификација на тоа колку некоја корпорација е изложена на потенцијални загуби т.е. избор на најадекватен начин на постапување со таквите изложености. Генерално, некои од стратегиите кои се применуваат се префрлање на ризикот на друг, избегнување на ризикот, намалување на негативниот ефект на ризикот, и прифаќање некои или сите последици на определен ризик. Традиционалниот risk management е фокусиран на оние ризици кои произлегуваат од физички или од правни извори (природни катастрофи, пожари, инциденти, смртни случаи, судски процеси, итн). Од друга страна, финансиски risk management се фокусира на ризици на кои е можно да се управува со помош на размена на финансиски инструменти. Без разлика на видот на ризик, сите големи корпорации имаат тимови и мали групи за risk management и го практикуваат и неформално и формално.

Според американскиот автор Емет Вон, управувањето со ризикот е аспект на управување на квалитетот кој има поддржувачка улога во остварување на саканиот квалитет на системот. Во таа смисла, основна цел на управување со квалитетот е таква имплементација на стратегискиот план на управување со која се обезбедува саканиот квалитет на системот, додека цел на управување на ризикот е задржување на квалитетот на системот и негово функционирање во континуитет при разни случувања.[231]

Менаџментот на технолошкиот ризик опфаќа три широки подрачја, и тоа: мерки, кои се насочени кон намалување на потенцијалот за настанување на научно-технолошкиот акцидент, како и последиците ако предизвиканата криза дојде до нив; процедури, чија цел е предупредување за секој настан кој може да биде поттикнувач на технолошкиот инцидент; мерки за ублажување на ефектот на катастрофата предизвикана од некој вид инцидент (евакуација, згрижување и слично). Најкомплетни превентивни мерки на овој вид инцидент се забраната или доброволното повлекување одредени производи. Меѓутоа, како начини за смалување на овие облици на загрозување се и користење алтернативна технологија или намалувавање на резервите на опасни материи на минимум

[231] Vauhan J.Emmett, op.cit.p.25.

кој е неопходен во текот на производството. Други превентивни мерки вклучуваат внимателно дизајнирање на машините и одбирање добра локација за корпорацијата, редовни безбедносни инспекции и контроли, детаљно планирање во случај на криза и редовно тренирање. Неовластено постапување, игнорирање на предупредувањата, несоодветно или неодговорно однесување и носење лоши одлуки за компанијата се карактеристични составни елементи на настаните коишто доведуваат до појава на научнотехнолошки инцидент.

До 90-тите години на XX век во повеќето компании не е посветувано доволно внимание на хармонизација на практиката на управување на корпоративните ризици со основната цел на деловниот субјект – зголемување на пазарна вредност и богатството на сопственикот. Оттогаш во голема мера се размислува дали одлуките за управување со ризици се компатибилни со деловната стратегија на компанијата, а на управувањето на корпорацијата со ризиците почнало да се гледа како на процес кој ја поврзува корпоративната стратегија, луѓето, технологијата и знаењето со цел на подобро вреднување и управување со ризиците на кои компанијата е изложена во остварување на својата основна цел. Овој начин на размислување за функцијата на управување со ризици е сеопфатен, свртен кон иднината и ориентиран е на процеси, при што се фокусира на управување на сите корпоративни ризици, а не само на пазарните или на оперативните, со цел да се зголеми пазарната вредност на компанијата. Притоа поефикасно управување со корпоративните ризици може да се постигне на следните начини: со намалување на очекуваните трошоци за финансиски проблеми, намалување на можни конфликти помеѓу кредиторот и сопственикот на компанијата, намалување на отпорот на менаџерот спрема ризикот, намалување на даночните обврски, како и намалување на можностите на пропуштање на профитабилни инвестиции со осигурување доволна количина на интерни средства за финансирање.[232]

Меѓународната организација за стандардизација ISO во 2009 година го објавила стандардот ISO 31000, Risk Management – Principles and Guidelines on Implementation (Управување со ризици – начела и насока за примена). Во согласност со стандардот ISO 31000,

[232] Види: Miloš-Sprčić Danijela, Tekavčič Metka, Šević Željko, „The Relevance of Corporate Risk Management Function and Its Influence on the Company's Value", in: *Računovodstvo, Revizija i Financije*, br. 5-6, RriF Plus, Zagreb 2007., str. 15-16.

ризикот се дефинира како „ефект на несигурност во постигнување на планираните цели“.[233] Управувањето со ризикот според овој меѓународен стандард претставува процес со кој се опфатени следните елементи:

- комуникација и консултација со интерни и со екстерни партнери, односно заинтересирани страни, на технолошки примерен начин и на секој степен на процес на управување со ризик, со разгледување на процесот како целина;
- утврдување екстерен, интерен и контекст на управување со ризик, односно утврдување критериум според кој ќе се проценува ризикот и ќе се дефинира структурата на анализата;
- идентификација на ризикот (каде, кога, зашто и како неповолниот развој на настаните би можел да се спречи, да се намали, да се одложи или да ги зголеми трошоците за постигнување на планираните цели);
- анализа на ризик, што опфаќа идентификација и процена на постојната стратегија, одредување на веројатност, подрачје на појавување, нивоа и можни последици на ризик;
- процена на ризик, односно споредување на проценетите нивоа на ризик со претходно утврдени критериуми и разгледување каква е рамнотежата меѓу потенцијалната корист и неповолните резултати, што овозможува донесување одлука според обемот и природата на потребните активности и приоритетите;
- обработка на ризик, која опфаќа изработка и примена на ефикасна и економски исплатлива стратегија и акциски планови за зголемување на можностите за добивка и намалување на потенцијалните трошоци;
- следење и преиспитување, што подразбира согледување спроводливост и ефикасност на сите чекори на процесот на управување со ризикот, со нивно постојано подобрување.[234]

[233] Пошироко за дефинициите по стандардот ISO 31000 види во: „ISO/IEC Guide 73: Risk Management – Vocabulary“, International Organization for Standardization, Geneva 2009. (http: www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651).

[234] Пошироко за процесот на управување со ризик види во: „ISO/DIS 31000: Risk Management – Principles and guidelines on implementation“, International Organization for Standardization, Geneva 2009. (http: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170).

На спроведување на ISO 31000 стандардот упатени се корпорациите кои според природата на деловните активности работат во услови на зголемен ризик. Често се случува одделни компании да не чувствуваат потреба за негова примена, или бавно ги воведуваат начелата и насоките потребни за управување на ризикот во согласност со овој стандард. Тоа меѓутоа, не значи дека различни деловни субјекти не користат некои од одделните елементи на управување со ризици за планирање и спроведување на своите деловни цели.

Со помош на ISO 31000 стандардот се добива комплетно заокружување на процесот на управување со ризици и се создава реална основа за континуирано подобрување на безбедносните услови за работа во компанијата. Според овој стандард, управувањето се ризикот треба да ги содржи следните принципи:[235] учество во создавање на вишокот на вредности; вклученост во дугите деловни процеси; учество во носење одлуки; конкретно адресирање на изворот на загрозување; систематичност, структурираност и правовременост; организираност и реализација врз основа на најквалитетни достапни информации; приспособеност на потребите на деловниот субјект и на дејноста во којашто се применува; водење сметка за расположливите човечки ресурси и културолошки специфичности; транспарентност, инклузивност, динамичност, интерактивност; давање одговор на промени и овозможување постојано унапредување и подобрување на функционирањето на организацијата. Ако целокупниот систем на управување со ризици експлицитно не ги поддржува наведените принципи, тогаш примената на ISO 31000 за наведената корпорација не е ниту применлива ниту корисна.[236]

Управување со ризиците претставува исклучително важен дел во целокупното управување на корпорацијата и нејзините активности. Практично не постои компанија која не користи некој облик на процена на ризик, иако често не е ниту свесна за тоа. ISO 31000 дава можност да се дефинира принципот на управување со ризици, односно деловниот процес со сите елементи на систематичност и документираност. Исклучителната вредност на ISO

[235] За принципите на управување со ризици види пошироко во: „Committee Draft of ISO 31000 Risk Management", International Organization for Standardization, Geneva 2009 (http: www.nsai.ie/uploads/file/N047_ Committee_Draft_of_ISO_31000.pdf).

[236] Според: Hubbard W. Douglas, *The Failure of Risk Management: Why It's Broken and How to Fix It,* John Wiley & Sons Inc, Hoboken NJ 2009., pp. 46-47.

31000 стандардот е во тоа тој во основа да го нормира меѓународниот консензус во смисла на применливост. Тој стандард е хармонизиран со другите ISO норми, како што се ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, итн., што значи дека тој стандард дава релативно едноставна можност на интеграција во IMS (Integrated Menagement System).[237]

Последиците од инцидентните ситуации често се разгледуваат како дисфункционални, непожелни и лоши, а зад нив останува одредена материјална и нематеријална штета. Кризата која довела до инцидентна ситуација создава потреба за стабилност, за нова рамнотежа или за привремена состојба на статус кво. Во таа смисла, ако крајот на инцидентната ситуација е јасен и недвосмислен, менаџерот за корпорациска безбедност мора тој крај да го објави на состанок на компанијата, на веб страницата или по пат на некој друг медиум. Без разлика на избраниот метод, односно начинот на прогласување крај на инцидентната ситуација, менаџерот треба кратко да се осврне на изминатата криза, да објасни што и поради што се случила, но и да објасни како инцидентната ситуација е решена и каква штета е нанесена на корпорацијата, потоа сликовито да ја прикаже моменталната ситуација, да образложи план за враќање на редовните активности и план за закрепнување на компанијата со потсетување на нејзините стратегиски цели и да го охрабри секој да даде целосен придонес на тоа закрепнување. Идеално гледано, постојат три можни решенија за излез од криза предизвикани со инцидентна ситуација, и тоа: компанијата престанува со работењето, можно е да биде тужена, а нејзините раководители обвинети за кривични дела; компанијата останува да работи, со нарушен углед и оштетен имиџ во очите на јавноста и со финансиски губитоци, по напорна работа, корпорацијата ја повратила или дури и ја унапредила својата позиција во очите на јавноста.[238]

Кога инцидентните ситуации ќе поминат, истражувањето кое се прави по сето тоа, помалку е поврзано за учење од грешките, а повеќе за утврдување на вината (blame game). Бидејќи вработените и јавноста очекува некој да сноси одговорност за пропустите и недостатоците кои довеле до криза, се усовршуваат одбранбените рутини, како што се барање прифатливо негирање и унапредување на вештина на комуникација со јавноста. Што повеќе време се

[237] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 36.

[238] Кешетовић Желимир, Кековић Зоран, op. cit. стр. 92.

посветува на овие механизми, на раководителите им останува помалку време да се искористи потенцијалот за да се стави крај на инцидентните ситуации за учење, а вистинските напори за подобрување на системот на превенција и заштита често се губат во посткризната политика. Ако посткризното учење воопшто и се случува, тоа е главно на долги патеки и станува збор за мачен процес со кој се управува далеку од очите на медиумите, политичките и судските постапки против највисоките менаџери. Тоа учење најчесто се сведува на проектирање технолошки подобрувања и приспособувања на постојните процедури.[239]

Преземањето и управувањето со ризикот е дел од редовното работење на денешните корпорации, насочени кон остварување профит за своите акционери. Бројните деловни неуспеси од компаративната практика укажуваат дека компаниите сепак не управуваат доволно добро со ризикот или не го разбираат ризикот што го преземаат. Од таквите проблеми не се имуни ниту големите корпорации, за што сведочи анализата на петгодишните перформанси на околу 200 водечки финансиски компании во САД, која ја спровел MsKinsey Global Institute (MGI). Таа анализа покажала дека во 90 набљудувани корпорации пронајдени се вкупно 150 случаи на значајни финансиски нарушувања, предизвикани од различни видови на ризик. Други истражувања на MGI покажале дека околу 36% од менаџерите во корпорациите не го разбираат во целост ризикот, а 24% сметаат дека сите процеси во кои управните одбори ги проценуваат ризиците се неефикасни, додека 19% од нив сметаат дека одборите немаат дефинирани процеси на управување со ризикот. Неупатеноста во проблемите на ризик главно ја покажуваат високи менаџери на корпорацијата кои традиционално се концентрираат на поедноставната матрица како приход на компанијата по одаточувањето, заработка по акција или очекување раст на акциите на берза, додека перформансите кои би се зеле предвид ретко се појавуваат како предмет на нивната анализа. Од тие причини, неопходна е поактивна улога на управниот одбор на корпорацијата, како и инкорпорирање на управувањето со ризикот во секојдневното одлучување. Компаниите кои не успеваат да ги подобрат процесите на управување со ризикот по правило имаат

[239] Според: Hart Paul, Rosenthal Uriel, Kouzmin Alexander, „Crisis Decision Making: The Centralisation Thesis Revisited“, in: *Administration and Society*, Vol. 25, No 1, SAGE Publications, Thousand Oaks CA, May 1993., pp. 42-43.

проблем со друг вид на ризик – неочекуван, а некогаш може да придонесува да се направат значајни финансиски загуби.[240]

Некои корпорации заземаат став кој е во голема мера повнимателен во поглед на ризикот, со цел заштита од падот на вредноста и на профитот. Таков пристап генерално не е добар, затоа што подготвеноста на преземање ризик е основа за доаѓање до профит на пазарот. Во таа смисла, потребно е да се настојува кон постигнување рамнотежа помеѓу состојбата што корпорацијата ја штити од финансиски нарушувања, и којашто остава доволно простор за претприемништвото. За да може тоа да се оствари, менаџментот на компанијата треба да работи во услови во кои потенцијалните добивки од донесените деловни одлуки се споредуваат со ризикот што се презема. Во такво опкружување, компанијата не само што го штити работењето од непредвидливи ризици, туку постигнува и сè поголема компетитивна предност, бидејќи презема ризик со неопходно внимание. Современите корпорации сериозно пристапуваат кон инвестирање во процесот на управување со ризици, а во тој поглед предничат финансиските институции, кои се мотивирани со регулаторни притисоци.[241]

Бен Гилад, во врска со неадекватното реагирање на компаниите на ризици и кризи, односно отсуство на навремено дејствување, идентификувал три такви вида менаџмент во корпорациите, и тоа: вид „Полжав темпо": менаџментот хронично дејствува бавно во поглед на ризикот; вид „Мажино линија": менаџментот дејствува, но неговата акција не е доволна, било да го сопре ризикот, било да ја искористи можноста (овој вид е наречен по неславната француска одбранбена линија која не успела да ја запре германската инвазија на Франција во Втората светска војна) и вид „Црна дупка": менаџментот е „парализиран со анализа" и воопшто не дејствува, ниту има одговор на ризиците.[242]

[240] Види: Brancato Kay Carolyn, Tonello Matteo, Hexter Ellen, *The Role of U.S. Corporate Boards In Enterprise Risk Management (Project Report)*, McKinsey & Company, New York 2006., pp. 17-22.

[241] Според: Lacković Marko, „Upravljanje rizikom: Koliko ga se treba bojati u poslovanju?", Empiria Magna d.o.o., Zagreb 25.02.2009 (http: www.ebizmags.com/kako-upravljati-rizikom-u-poslovanju/).

[242] Гилад Бен, op. cit. стр. 207-208.

6. ФУНКЦИИ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Во согласност со доктрината и со практиката на европските земји со високоразвиена пазарна економија и стабилна демократија, функциите на корпорациската безбедност опфаќаат:

- административна безбедност (Administrative Security) – процедури и политика во областа на информатичката заштита;
- физичка и техничка безбедност (Out-Source/Proprietary) – машини, постројки и објекти;
- безбедност на имотот и надворешни партнерства (Personnel Security);
- лична безбедност (Protective Security) – заштита на лица и заштита при работа;
- заштита од пожари (Fire Security);
- работа во вонредни ситуации (Contingency Planning)
- информатичка безбедност (Informattion Security);
- безбедност на менаџерот (Executive Security);
- безбедност на различни деловни случувања (Event Security);
- безбедност на договорени работи со државни структури;
- истраги (Investigations) – програма за заштита од криминалитет и
- програма за едукација и развој на безбедносната култура на вработените (Security Education Awareness and Training Program).[243]

Според тоа, корпорациската безбедност е перманентно вклучена во механизмите на деловното управување така што таа го штити нормалното одвивање на деловните процеси, отстранува акутни безбедносни проблеми и на вработените им создава безбедносни услови за работа. Поконкретно гледано, корпорациската безбедност работи на создавање планови и спроведување мерки чија цел е: заштита на корисникот на услуги, заштита на вработените во деловната организација, заштита на имотот во сопственост на деловните организации, заштита на информациите и на репутацијата на деловната организација од материјални штети, криминални дејности итн. Со тоа корпорациската безбедност е составен дел на процесот со кој се управуваат деловните ризици внатре во деловниот субјект.

[243] Види: Kovacich L. Gerald, Halibozek P. Edward, *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*, Butterworth-Heinemann, Boston MA 2002., pp. 161-162.

6.1. АДМИНИСТРАТИВНА БЕЗБЕДНОСТ

Административната безбедност на корпорацијата, според Стипе Баљкас, ги опфаќа следните компоненти: политика (правила на однесување, заштита на имотот и стопанисувањето, информатичката безбедност, деловна етика, конфликт на интереси и друго); планови (контрола на пристап, користење, евакуација, противпожарна заштита, техничка заштита итн); процедури (стандарди, превенција и избегнување напад, однесување во случај на загрозување, користење тајни податоци, безбедно користење на информатичкиот систем и друго). Во врска со тоа, дефинирањето, развојот и реализацијата на административната безбедност е задача на сите нивоа на одлучување во корпорацијата, а не само на организациските единици за корпорациска безбедност.[244]

6.2. ФИЗИЧКА И ТЕХНИЧКА БЕЗБЕДНОСТ

Под физичка и техничка безбедност се подразбира ангажирање специјализирани работници на работи за спроведување и стручна контрола на безбедносна заштита, примена на посебни мерки при складирање и чување оружје и муниција, посебно обезбедување при чување и транспорт на пари и скапоцености, физичко и техничко обезбедување зграда, особено простории во кои се сместени виталните погони и машини, систем на техничко обезбедување на објекти и простори, издавање службени легитимации и безбедносно-пропусни документи и друго. Со тоа во целина се унапредува извршувањето на работите околу обезбедување на корпорацијата, а со тоа се придонесува и кон јакнење на личната и безбедноста на имотот како едно од основните слободи и права на граѓаните на кои се темели современото општество. Со безбедносна едукација на сите вработени и со професионализација на службата за обезбедување се придонесува кон унапредување на безбедноста на работењето на корпорацијата, како и кон поголема сигурност на имотот и лица во пошироки рамки.

Физичката безбедност во компанијата се остварува со работењето на службата за обезбедување, која се состои од одреден број извршители (постојано вработени лица или ангажирани припадници на специјализирани агенции за давање услуги за

[244] Според: Baljkas Stipe, „Projektiranje sustava korporativne sigurnosti“, *Četvrta konferencija o korporativnoj sigurnosti «Korporativna sigurnost 2011»*, Lider & MBOS, Zagreb, 10.03.2011.

обезбедување), кои носат оружје и чија задача е заштита на објекти и лица во нив. Техничката заштита подразбира механичка, електронска и оптоелектронска заштита на објектот на корпорациите и на лицата во нив и организациски најчесто е поставена во рамка на службата за обезбедување во оние компании во кои таква служба е организирана.[245]

Некои автори во мерките на физичкото и техничко обезбедување ги набројуваат: обезбедувањето на сите лица за време на престојот во компанијата, а особено на менаџментот на корпорацијата; обезбедување на сите објекти и простори на корпорацијата; обезбедување на сите видови собири кои се организираат во просториите или на просторот на компанијата, особено оние на коишто се појавуваат одредени важни личности од менаџментот на корпорацијата или личности однадвор; обезбедување специјален транспорт за потреби на компанијата; обезбедување и заштита на информатичките системи, податоци и документација на корпорацијата.[246]

6.3. БЕЗБЕДНОСТ НА СОПСТВЕНОСТА И НА НАДВОРЕШНИТЕ ПАРТНЕРСТВА

За периодот по 2000-та година карактеристично е масовното пристигнување странски капитал и инвестиции во земјите од поранешните комунистички режими во кои странските фирми отвораат банки, фабрики, различни компании и агенции. Странските корпорации кои се присутни на домашните пазари воведуваат свои стандарди на организациите за корпорациска безбедност, но и нудат работи за обезбедување домашни фирми кои можат да ги исполнат меѓународните стандарди на безбедноста. Оваа појава значајно влијаела на унапредувањето на недржавниот сектор на безбедноста, а домашните фирми од овие области започнале да ги прифаќаат меѓународните стандарди кои се однесуваат на организацијата, на техниката и на обуките на своите кадри, благодарејќи на отворените тендери што ги добивале работите за заштита на дипломатско-

[245] Даничић Милан, Стајић Љубомир, оп. цит. стр. 22.

[246] Види: Скакавац Здравко, Малиновић Драгана, „Улога менаџмента безбедности у заштити корпорације од криминалитета“, у: *Научни скуп «Дани безбједности» на тема: „Развој система безбједности и заштите корпорација“ (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 59.

конзуларните претставништва и обезбедување на меѓународни спортски натпреварувања. Овој процес во голема мера влијаел и на затворање, т.е. на неможноста да се одржат на сè поотворениот пазар, полукриминални приватни агенциии за обезбедување, кои биле формирани во поранешните социјалистички држави во текот на 90-тите години на минатиот век. На тој начин доаѓањето на странските компании во овие земји во голема мера влијаело на подигање на квалитетот и обемот на услугите на обезбедување.

6.4. ЗАШТИТА НА ЛИЦА И ЗАШТИТА НА РАБОТА

Под поимот заштита при работа се подразбира збир на технички, здравствени, правни, социјални и други мерки и активности чија цел е спречување и отстранување опасности и штетни влијанија коишто можат да го загрозат живот и здравјето на вработените. Со оглед на тоа дека повредите на работа и професионалните болести нанесуваат штета не само на вработените и на нивните семејства, туку и на деловниот субјект и на поширокатa општествена заедница, заштитата при работа се спроведува како организирана дејност чија цел е да се обезбедат услови за работа во кои нема да постои опасност по животот и здравјето, односно услови во кои тие опасности ќе бидат сведени на најмала можна мера.[247]

Во основа, според позитивните законски прописи работодавачот не може да го упати вработениот на кој по мислење на надлежниот здравствен орган, би му било загрозено здравјето. Исто така, вработените со здравствени проблеми, утврдени од страна на надлежен здравствен орган, не можат да извршуваат работи кои би предизвикале влошување на нивната здравствена состојба или би довеле до последици опасни за нивната околина. Исто така, работодавачот е должен да обезбеди извршување на работите во текот на денот ако, според мислење на надлежниот здравствен орган, ноќната работа би довела до влошување на здравствената состојба на вработениот.

6.5. ЗАШТИТА ОД ПОЖАРИ

Поимот пожар подразбира неконтролирано согорување материја, предизвикано од природен причинител (гром, влијание на Сонцето, земјотрес) и со дејство предизвикано од човекот случајно и смислено. Намерно, односно смислено предизвикан

[247] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 257.

пожар се нарекува палење. Кај палењата сторителот секогаш има за цел проширување на пожарот и отежнување на неговото гасење или локализирање, односно уништување или нанесување на што поголема штета на имотот каде што е запален. За таа цел, сторителот на пожарот често поставува повеќе жаришта кои природно не се поврзани, што може да се утврди во текот на увидот со соодветно вештачење. Ако палењата се извршени во затворен простор, сторителот заради полесно согорување и ширења на пожарот често ја остава отворена вратата или прозорците и други отвори, за да може кислородот полесно да продре со што би се влијаело на понатамошното ширење на оганот, што исто така може да се утврди во текот на увидот.[248]

Штетата од пожар, како што наведува Д. Млаѓан, може да се класификува според различни карактеристики. Класификација во однос на последиците на настанот може да биде извршена според местото и времето на манифестирање на последиците предизвикани со дејствување на опасности, во зависност од задачата која треба да се реши, според објектите на кои дејствува опасноста и според обемот (влијае на финансиската стабилност на организацијата). Директна штета од пожарот е непосредна штета за здравјето, имотот или сопственичките интереси. Таа ги опфаќа сите загуби и штети кои ги претрпеле сите објекти важни за животот и работата на човекот, а кои се нашле во зони на влијание на опасноста. Посредната штета е сочинета од загубите, пропуштената заработка и дополнителните трошоци, кои ќе ги имаат објектите кои не успеале во зоната на дејствување на опасноста да се заштитат, а штети коишто се предизвикани со нарушувања и промени во новонастаната структура на деловните врски, инфраструктура, како и дополнителни трошоци настанати заради потребата од спроведување мерки на отстранување на последиците од настаните. Конкретни облици на последици од пожар, хаварија и експлозија можат да бидат: загуба на живот или телесна повреда; загуба на средства за работа; штета на имотот; уништување на инфраструктура; оштетување на животната средина; финансиски загуби; издвојување дополнителни средства; епидемија; миграција; раселени лица или избеглици; недостаток на храна, несигурност и друго.[249]

---

[248] Види: *Разјашњење узрока пожара, експлозија и хаварија* (зборник радова), МУП Републике Србије – Управа за сузбијање криминалитета, Београд 1993., стр. 13-22.

[249] Млађан Драган, op. cit. стр. 20-21.

Појавата на пожари е постојана опасност што ја следи секоја компанија. Во таа смисла, преземање мерки за заштита од пожари претставува нивна законска обврска, а организациски овие мерки се спроведуваат или од страна на посебни служби за заштита од пожари или во рамките на службата за внатрешно обезбедување. Без разлика на организациската форма, противпожарната заштита претставува составен дел од корпорациската безбедност, при што постои и законска обврска за обучување на работниците од противпожарната заштита како општа превентива наменета на вработените.[250] Секоја сериозна компанија која сака да дејствува во насока на превентивна заштита од пожари посветува големо внимание на организациските, на техничките и на други мерки и работи насочени кон отстранување опасности од настанување пожари, нивно рано откривање и спречување на ширење, како и ефикасно гасење. Системот за заштита од пожар подразбира планирање, пропишување мерки на заштита на градбите, организирање субјекти на заштита од пожари, финансирање на тие работи, оспособување и обука на извршителите и нормативно уредување на противпожарната заштита, со цел заштита на животот, здравјето и безбедноста на луѓето и имотот, околината и природата од пожар, при општествено и економски прифатлив ризик.[251]

Заштитата од пожари подразбира проверка и одржување инсталација во објектите на корпорацијата и преземање соодветни превентивно-технички мерки со цел спречувања појава на пожар внатре во тие објекти. Тоа, пред сè подразбира одржување во исправна состојба на уредите, на опремата и на средствата за гасење пожар, како и на уредите и инсталацијата за детекција на пожари. Исто така, во мерки за заштита од пожари спаѓаат и: одржувањето во исправна состојба на електрични, вентилациски, топлотни и други инсталации и на простории за складирање лесно запаливи материјали, како и периодични прегледи и сертификација на опрема од страна на стручни и овластени служби. Од голема важност е во објектите на компанијата да бидат вградени системи за автоматска дојава на пожар, првенствено заради нивна заштита од пожари, експлозија или земјотрес. Со вградување на дојавувачот на пожар во овие објекти и негово поврзување со противпожарна централа која се наоѓа на пријавница на објектот, секој пожар би бил забележан во својата почетна фаза и би бил брзо локализиран. Секојдневното

[250] Даничић Милан, Стајић Љубомир, op. cit. стр. 22.

[251] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 303

следење на состојбата и преземањето потребни мерки на безбедност ја вршат овластени припадници на службата за обезбедување на компанијата, со потребна асистенција на противпожарните служби, според пропишани процедури.

Сите земји членки на Европската унија имаат свои национални закони од областа на заштитата од пожари, но се должни меѓусебно да ги хармонизираат. Стандардите, како технички документи, се хармонизираат уште во текот на нивната изработка, бидејќи постои соработка на референтни лаборатории на европските земји (EGOLF) и национални организации за стандардизација. Постои обврска на земјите членки 80% од стандардот да биде кратко време имплементиран и идентичен со европски стандарди. Таа цел е сè уште далеку од остварувањето дури и за Германија и за Франција, но општата ориентација е јасна, а тоа е дека она што треба прво да се направи е да се хармонизираат стандардите од областа за заштита од пожари. Практично, еден од првите донесени европски стандарди (EN 3) се однесува на противпожарните апарати.[252]

6.6. РАБОТА ВО КРИЗНИ ВОНРЕДНИ СИТУАЦИИ

Успешно дејствување, координација и контрола во вонредни ситуации, иако првенствено бараат одбранбени и реактивни потези, бара и мерки на антиципирање, а менаџерите во тие ситуации значи дека тие ќе оперираат во „трикратни временски фази“, и тоа: додека се носат со некоја вонредна ситуација, проценуваат акции кои ги презеле, спроведуваат акции кои се неопходни во тој момент и ги планираат следните акции кои ќе мора да се преземат.

Како што истакнуваат Ж. Кешетовиќ и З. Кековиќ, вонредната ситуација создава тензија и притисок на менаџерите кои не се сигурни, но мора брзо да решат, што може да предизвика чувство на немоќ и констернација. Во тие околности, носителите на таа одлука можат да го компензираат своето чувство на несигурност, со ригидна, а некогаш и со опсесивна преокупација само со едно можно решение на настанатата криза. Најчесто се размислува по аналогија, а референтна точка е последната вонредна ситуација. Бидејќи слични ситуации ретко се повторуваат, различни и неконзистентни мерки донесени врз основа на ваквото размислување можат да бидат контрапродуктивни. Во вонредни ситуации менаџерите имаат големи проблеми во редефинирање на ситуацијата и често се предаваат на групно мислење кое што се јавува во многу кохезивни

[252] Млађан Драган, op. cit. стр. 27.

групи кои настанале по заеднички искуства како и од потребата да се обединат пред заканата. Некогаш се работи и за „колективно лудило“ во кое на зачувувањето на групната хармонија и на односот меѓу членовите, надвладува способноста на групата критички да ги проценува проблемите поврзани со носењето одлука, да ги прифаќа и да ги проследува стратегиски информации и рационално да го избира правецот на акција. Ова често им служи на менаџерите и на советниците од себе да ја отфрлат одговорноста на групата.[253] Во литературата главно постои согласност за пет основни фази на одговор на настаната вонредна ситуација, и тоа: предупредување и известување, узбуна, заштита на животот и имотот, обезбедување на јавното добро и обновување. Должината на секоја од тие фази зависи од природата на кризната ситуација, така што предупредување и известување во случај на оркан или поплава може да трае по неколку дена, а во случај на торнадо или експлозија неколку минути.

Вонредната ситуација бара брзо и одлучно дејствување, затоа што во спротивно последиците можат да бидат од поголеми размери. Пример за такво дејствување е постапката на компанијата Nike, која во јуни 1997 године лансирала нов дизајн на кошаркарски патики „Летен скок“, користејќи го зборот воздух (air) напишан со огнени букви. Се потврдило дека тој натпис визуелно многу е сличен на зборот „Алах“ на арапски јазик. Согледувајќи ги можните последици, компанијата повлекла од продажба 38.000 пари патики од таа серија и ја прекинала линијата на нивното производство.[254]

Иако многу важни за корпорацијата, материјалните добра за разлика од човечките животи можат да се надоместат. Затоа во вонредена ситуација потребно е да се ризикуваат и трошоците и загубите, заради заштита на луѓето. Така, корпорацијата Johnson & Johnson во 1982 година повлекла 22 милиони шишенца лек Tylenol од своите аптеки, веднаш кога ја забележале врската помеѓу земањето на овој лек и смртта на пациентите. Овој потег на споменатата компанија ја чинело повеќе стотина милиони долари, но сочуван е главниот капитал, угледот на корпорацијата, на која човечките животи ѝ се поважни од профитот. Истовремено, спречени се и нови потенцијални жртви.[255]

---

[253] Кештовиќ Желимир, Кековиќ Зоран, op. cit. стр. 86.

[254] Види: Awad Nihad, „Nike and Islamic Group end Logo Logjam“, *CNN U.S.*, Atlanta GA, 21 November 1998.

[255] Според: Yang Lynn Jia, „Getting a Handle on a Scandal“, *CNNMoney*, Atlanta GA, 22 May 2007.

Еден од основните поими кои се споменуваат во врска со дејствување во вонредни ситуации е кризниот менаџмент, кој се дефинира како активност насочена кон надминување ситуации опасни по опстанокот на корпорацијата, т.е. како планирање и спроведување мерки за обезбедување на основните цели на компанијата.[256] Важни карактеристики на кризниот менаџмент се поинтензивно користење на средствата и на методите потребни за спречување, воспоставување контрола и надминување вонредни ситуации. Ако станува збор за активности за спречување криза, тогаш се зборува за превентивен или за антиципативен кризен менаџмент, т.е. систем за рано предупредување, анализи на потенцијалите, управување со ризиците и политиката на флексибилност како клучен, но не и единствен, инструмент на превентивното управување. За реактивниот кризен менаџмент се зборува во смисла на обезбедување основни, егзистенцијални варијабли по појавата на криза. Тој вид кризен менаџмент го карактеризираат јасни цели, како што се: остварување одредена ликвидност или корист, како и користење инструменти за идентификација на кризата. Кризниот менаџмент не треба да се разбере како нешто непожелно, туку како важен и составен дел на одговорниот дел на управување со корпорацијата, во кој од повеќето деловни одлуки се проценува ризикот и шансите, особено кога заради зголемена несигурност и брзи промени не може да се исклучи кризна, односно вонредна ситуација. Во тој процес препознавањето на постојните интерни потенцијали, покрај согледувањето на грешките и недостатоците се одлучувачки за надминување на кризната ситуација.[257]

Моделот на кризен менаџмент што го развила американската Федерална агенција за управување со кризни ситуации (Federal Emergency Menagement Agency-FEMA), опфаќа активности на подготовки за вонредни ситуации кои се групират во четири временски одвоени фази, и тоа:

– Ограничување (спречување, избегнување), коешто вклучува активности за елиминирање или намалување на шансите да дојде до вонредна ситуација, односно до намалување на нејзините ефекти. Ако е невозможно да се спречи вонредната

[256] Krummenacher Alfred, op. cit. p. 13.

[257] Види: Osmanagić-Bedenik Nedžara, *Kriza kao šansa: kroz poslovnu krizu do poslovnog uspjeha*, Drugo promijenjeno izdanje, Školska knjiga, Zagreb 2007., str. XXX.

ситуација, тогаш може да се намали нејзиниот разорен потенцијал. На пример, зајакнување на покривите на објектите ќе го намали оштетувањето од силните ветрови, а системот на одводни канали ќе ги намали последиците од поплава.

– Подготовка, којашто се однесува на планирање на одговор на тоа кога ќе се случи вонредна ситуација и на распоредување на ресурсите во функција на соодветен ефективен одговор на истата. Овие активности помагаат да се спасат животи и да се минимизираат оштетувањата на објектите и на имотот, така што човечките ресурси се подготвуваат адекватно да одговорат кога вонредната ситуација е неизбежна или таа веќе се случила.
– Одговор (опфаќа период на тек на траења или непосредно по појавата на вонредната ситуација), којшто се состои во укажување неопходна итна помош на загрозените и во настојувањата да се намали веројатноста на идните штети и загуби.
– Закрепнување, коешто трае додека сите системи не дојдат во состојба на речиси нормално функционирање. Краткотрајното закрепнување се однесува на враќање на виталните системи во минимални оперативни услови, а долготрајното е поврзано за враќање во претходната состојба, односно за мерки кои ќе влијаат и ќе придонесат за помала изложеност на вонредни ситуации во иднина.[258]

6.7. ЗАШТИТА ОД ИНДУСТРИСКА ДЕЛОВНА ШПИОНАЖА

Во светските стручни кругови не постои целосна согласност околу дефиницијата на поимот деловна (индустриска, економска, стопанска, информатичка) шпионажа и апаратот на нејзината содржина. Поради тоа различни феномени се дефинираат на ист начин (на пр., индустриска и стопанска шпионажа) или во тоа подрачје се вметнуваат поими како саботажа, која не спаѓа во рамките на тој феномен. Често одредени поими се дефинираат од аспект на подрачје на дејствување (индустриска шпионажа), а други од аспект на методи и средства за остварување на целите на шпионажа (информатичка шпионажа).[259]

[258] *FEMA – Plan for Emergencies* (http: www.fema.gov/plan/prepare/plan.shtm).

[259] Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 141.

Канадскиот автор Е. Потер укажува дека во таа област постојат три основни поими: разузнавачка дејност во подрачје на стопанството, односно економијата (economic intelligence), економска шпионажа (economic espionage) и индустриска шпионажа (industrial espionage). Тој укажува дека поимот economic intelligence е најширок и дека истиот во себе ги вклучува останатите два поима. Според него, поимот economic intelligence опфаќа политика или комерцијално релевантни информации, вклучувајќи ги и податоците со кои располагаат органите на државните власти, и информации од областа за финансиите и трговијата, а кои се од значење за националните интереси, односно за поддршка на унапредување на продуктивноста и конкурентноста на националните економии во светот. Од друга страна, економската шпионажа опфаќа тајни и недозволени настојувања на одделни држави кои, заради сопствените економски интереси, можат да се служат и со саботажи и со други противзаконски средства и на тој начин да допрат во економската безбедност на други земји. На крајот, поимот индустриска шпионажа Потер го дефинира како употреба на илегални, потајни, принудни или измамнички начини и методи да се дојде до одредени информација за стопанските субјекти во приватниот сектор.[260]

Американското Федерално истражно биро (Federal Bureau of Investigation – FBI) во своите интерни документи стопанската шпионажа ја одредуваат како активност управувана од државата, која ја спроведуваат разузнавачки институции и кои со употреба на легални, но и на нелегални средства и методи собираат податоци за економските потенцијали и способности на другите држави и нивниот економски субјекти како таа држава или нејзиниот деловен сектор би имале поголема конкурентност во меѓународните економски односи и на светскиот пазар. Федералното истражно биро ја дефинира индустриската шпионажа како разузнавачка активност со која не управува државата туку приватни стопански субјекти, со цел постигнување конкурентски предности.[261]

Највисокото тело на САД за координација на контраразузнавачки работи во сферата на економијата, Национално биро за контраразузнавачките работи (Office of the National Counterintelligence

[260] Пошироко види: Potter H. Evan (ed.), *Economic Intelligence and National Security*, Carleton University Press & The Center for Trade Policy and Law, Ottawa 1998., pp. 11-14.

[261] Boni William, Kovacich L. Gerald, op. cit. p. 48.

Executive - ONCIX), во своите официјални документи економската шпионажа ја одредуваат како незаконско и тајно прибирање доверливи финансиски и деловни информации, како и информации кои се однесуваат на економската политика, прашања поврзани со сопственоста на корпорациите или заштитените технологии. Според дефиницијата на ONCIX, индустриската шпионажа е активност која ја преземаат странски влади или компании, со цел прибирање деловни тајни.[262]

Американските автори Џон Квин и Џон Нолан, поимите индустриска и економска шпионажа ги одредуваат единствено како тајно прибирање чуствителни, доверливи, рестриктивни или посебно класифицирани информации, при што индустриската шпионажа опфаќа и кражба на информации од конкурентите.[263]

Имајќи ги предвид наведените поимни неусогласености и поаѓајќи од ставот дека економијата и индустријата во суштини претставуваат стопанисување, т.е. економската и индустриска шпионажа се случуваат во светот на стопанисувањето, М. Биланџиќ го застапува ставот дека тие два термина треба да се стават под заеднички поим деловна шпионажа.[264] Според неговото размислување, штетните директни и индиректни последици од индустриска шпионажа за некоја корпорација може да значи губење на пазарите, послаб пласман на сопствените производи, опаѓање на бројот на работни места, намалување на профитот, а во драстични случаи и банкрот на компанијата. Според Биланџиќ, дејствувањето на економската шпионажа можат да ја почувствуваат цели гранки на стопанството, па дури и целокупната економија на одредена држава, а последиците можат да значат и намалување на бруто националниот производ.[265]

Во поглед на штетните последици кои корпорациите и националните стопанства ги имаат заради дејствувањето на индус-

[262] Види: *Office of the National Counterintelligence Executive Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, Washington DC 2009., pp. 7-8. (http: www.ncix.gov/publiations/reports/fecie_all/fecie_2008/2008, FECIE_Blue.pdf).

[263] Според: Nolan A. John, Quinn F. John, „Intelligence and Security: The Counterintelligence Approach“, in: Miller P. Jerry, Leonard M. Fuld, *Millenium Intelligence – Understanding and Conducting Competitive Intelligence in the Digital Era*, Information Today Inc., Medford NJ 2000, pp. 208-209.

[264] Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 143.

[265] Исто, стр. 147.

триската/стопанската шпионажа, во стручната литература постојат различни мислења, првенствено околу дилемата дали штетата од таков вид воопшто е можно да се согледа во целина. Така, одделни автори укажуваат дека штетните последици од економската/индустриска шпионажа многу тешко може да се проценат, првенствено затоа што жртвите не се ниту свесни дека се жртви, поради што во овие случаи нема жалби, нема инциденти и нема основа за поведување постапка за барања на обештетување.[266] Во врска со тоа, проценатa на Националното биро за контраразузнавачки работи на Соединетите Американски Држави (ONCIX), укажува дека дури 42% од инцидентите поврзани за стопанска шпионажа во кои се оштетени американските корпорации остануваат скриени од јавноста поради стравот дека изнесувањето такви податоци би можело да ја ослабне нивната репутацијата на оштетената компанија на пазарот, односно да доведе до пад на вредноста на нивните акции.[267]

На состанокот на Светскиот економски форум, кој е одржан кон крајот на јануари 1998 година во Давос, Швајцарија, понудени се повеќе објаснувања, поради што инцидентите кои се поврзани со стопанската шпионажа во најголем број случаи не ѝ се откриваат на јавноста. Како причина за тоа, се наведени, меѓу другото: страв дека тоа би предизвикало негативни реакции на акционерите и на клиентите на оштетената компанија; страв дека корпорацијата би можела да изгуби одредени зделки; страв дека би се откриле слабостите на компанијата на конкурентите; привлекување негативен публицитет кој би можел да влијае на конкурентноста на корпорацијата.[268]

Поаѓајќи од оценатa дека терминот контраразузнавачко дејствување на корпорацијата на планот на заштита и спротивставување на индустриската, односно стопанската шпионажа предизвикува негативни асоцијации, со оглед на тоа дека на вработените во рамките на стопанскиот субјект им наметнува одредени ограничувања и правила на однесување, а што во одредена мерка е во спротивност со отвореноста и слободата на пазарот,

[266] Според: Fialka J. John, *War by Other Means: Economic Espionage in America*, W.W.Norton & Company, New York 1997., p. 15.

[267] *Office of the National Counterintelligence Executive Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, op. cit. p. 15.

[268] Според: Vaknin Sam, „The Industrious Spies: Industrial Espionage in the Digital Era“ (http: www. samvak.tripod.com/pp144.html).

одделни автори предлагаат наместо поимот counterintelligence, да се користи терминот „обезбедување компетитивни способности“ (competitive assurance).[269] Исто така, одделни автори наместо counterintelligence да го користат поимот „дефанзивно разузнавачко дејствување“ (defensive intelligence).[270]

6.8. ИНФОРМАТИЧКА БЕЗБЕДНОСТ

Информатичката безбедност се дефинира како состојба на доверливост, целовитост и располагање со информации, независно од тоа во кој облик егзистираат. Таа состојба се постигнува со соодветни мерки и стандарди на информатичка безбедност, како и со организациска поддршка на работите на планирање, на спроведување, на проверка и на доработка на тие мерки и стандарди. Доверливоста на информацијата значи дека таа е достапна само на оние лица што се овластени да ја користат. Интегритетот подразбира заштита на податоците од намерно или случајно менување, додека достапноста е гаранција на овластените корисници на системот дека ќе им бидат достапни во секој момент кога ќе имаат потреба од нив. Информацискатa безбедност и информатичката безбедност не се синоними, затоа што информацискатa безбедност опфаќа заштитата на сите информации, без разлика на тоа во кој облик се наоѓаат.[271]

Според дефинициите на одделни автори, односот помеѓу информацискатa безбедност и работењето на корпорацијата има четири различни аспекти. Првиот се однесува на процесот на прибирање на работните информации за конкурентите, а вториот е во проблемот на чување деловни информации во базите на податоци. Економскиот аспект на информацискатa безбедност, односно „цена на чинење“ на системите за заштита на информациите и „цена на губитокот“, поради нивната неадекватна заштита на информациите, претставува третиот аспект на тој однос. Како четврт аспект, овие

[269] Nolan, John, „The Worldwide growth of Competitive Intelligence: Who's Doing What To Whom and How Well“, *Business Intelligence 2000*, Druga Hrvatska konferencija o pribavljanju, organiziranju i uporabi poslovnih informacija, Zavod za poslovna istraživanja, Zagreb 2000;

[270] Види: Comai Alessandro, „Global Code of Ethics and Competitive Intelligence Purposes: an Ethical Perspective on Competitors“, in: *Journal of Competitive Intelligence and Management*, Vol. 2, No. 1, Society of Competitive Intelligence Professionals (SCIP), Alexandria VA, Spring 2004., pp. 27-28.

[271] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 94.

автори го наведуваат информациско-аналитичкото обезбедување на работењето на корпорациите. Имено, секоја држава, со цел обезбедување сопствен економски развој, мора да се создадат оптимални услови на планот на обезбедување транспарентност на одвивање на економските процеси и максимална информираност на сите учесници за состојбата на пазарот, т.е. спречување од бирократската злоупотреба и нелојалната конкуренција.[272]

6.9. БЕЗБЕДНОСТ НА МЕНАЏЕРОТ

Најчести видови на лична загрозеност со која се соочени сопствениците, директорите, менаџерите и другите раководители во корпорацијата врзани се за различни кривични дела, вклучувајќи потенцијални грабнувања, уцени, разбојништва, провали, физички напади и вознемирувања од страна на непријателски расположени лица од различни категории – од незадоволни меѓу вработените, преку активисти на „зелените“, до припадници на бизнис конкуренцијата. Ако дејноста на корпорацијата е врзана за некоја специфична област (хемиски, фармацевски, биолошки истражувања, нуклеарна енергија, воено-индустриски комплекс, електроника, информатика) челниците на тие компании можат да навлечат и да имаат против себе бројни непријателски расположени анонимни фанатици со кои всушност немаат никакви лични контакти. Безбедносната заштита на менџерот во практика најчесто се сведува на превезување на штитеното лице (и/или неговото семејство) на работни и на други состаноци, настани, собири, ручеци/вечери и слично, а самите тие неретко кон таа заштита се однесуваат како кон нешто што им е нужност, но и оптоварување.[273]

6.10. БЕЗБЕДНОСТ НА РАЗЛИЧНИ ДЕЛОВНИ НАСТАНИ

Планирањето на мерките за безбедност и заштита на различни деловни/работни настани започнува со правење соодветна безбедносна процена, чија содржина зависи од повеќе фактори, првенствено од бројот и структурата на учесниците и од тоа дали работниот собир (конференција, манифестација) се одржува во

[272] Според: Синковски Стеван, Лучић Бранислав, „Информациона безбедност – основа безбедног бизниса“, *Саветовање „Злоупотребе информационих технологија и заштита (Ziteh '06)Ч*, Удружење судских вештака за информационе технологије ИТ Вештак, Тара, 07. – 10.11.2006. године.

[273] Според: Vrbanc Darko, *Osobna zaštita,* Zagreb štit -Vrbanc, Zagreb 2002., str. 9.

затворен или на отворен простор. Со планот за заштита се одредуваат носителите на задачите од секторот за безбедност на корпорацијата, кои утврдуваат конкретни мерки и активности кои ќе бидат спроведени со цел остварување на потребното ниво на безбедност и намалување на ризикот за учесниците.[274]

Со цел заштита од насилен или од таен упад во објектите и на просторот каде се одвиваат работните настани, заради остварување на општата безбедност на учесниците на тие собири, се преземаат и неопходни противдиверзиски мерки, мерки на противпожарна заштита, како и мерки на техничка заштита кои опфаќаат: надворешен и внатрешен видео надзор, механичка заштита, алармен систем и видео интерфонски систем. Ако е потребно и ако е можно, во зависност од природата на работниот настан, може да се спроведат и мерки на противприслушувачка заштита.[275]

6.11. БЕЗБЕДНОСТ НА ДОГОВОРЕНИ РАБОТИ СО ДРЖАВНИТЕ СТРУКТУРИ

Некои од безбедносните ризици со кои се соочуваат современите корпорации можат да произлегуваат и од склучените деловни договори. Имено, условите на договорот можат да создадат обврска која деловниот субјект не е во состојба да ја исполни. За да се намалат тие ризици, потребно е во корпорацијата да биде развиен и да се примени план со кој би се обезбедила потребната комуникација со заинтересираните екстерни и интерни субјекти. Тој план би требало да опфати: комуникација со заинтересираните страни во случај на криза или штетен настан, ангажирање соодветни екстерни заинтересирани страни и овозможување ефективна размена на информации; интерно известување за влијанието и за ефектите од проценетиот ризик врз односот со заинтересираните страни; достапност на информациите во согласност со законот; обезбедување повратна информација во процесите на комуникација; обезбедување транспаретност во работењето и градење на доверба внатре во корпорацијата итн.[276]

---

[274] Види: Smith A. Lee, „Corporate Event Security" (http: www.eazinearticles.com/?Corporate-Event-Security&id=3868394).

[275] Рађеновић Рајко, *Безбедност личности и објеката*, МДД систем, Београд 2003., стр. 66-69.

[276] Кековић Зоран, Савић Сузана, Комазец Ненад, Милошевић Младен, Јовановић Драгиша, op. cit. стр. 77-78.

6.12. ПРОГРАМА НА ЗАШТИТА ОД КРИМИНАЛИТЕТ

Економскиот криминалитет, со кој најчесто се соочуваат корпорациите, според некои свои карактеристики се разликува од останатите видови на криминалитет. Станува збор, меѓу другото, за следното:

- постоење „црна бројка" – кривичното дело и извршителот за време на извршувањето најчесто не се откриени, односно се непознати. Кривичното дело е инфилтрирано во редовното и регуларно работење, а однесувањето на извршителот е нормално и вообичаено;
- временско растојание – од моментот на извршување на кривичното дело до неговото воочување, т.е. детектирање, по правило поминува долго време, понекогаш и повеќе месеци или години. Причините се нетранспарентни последици од кривичното дело, непријавување од страна на оштетениот или на трети лица, недоволно ниво на соработка на деловниот субјект и надлежните полициски служби и друго;
- стручност на извршителите, кои често се високообразовани поединци, експерти, професионалци, претприемачи, менаџери, сопственици и носители на работната дејност, т.е. лица кои поседуваат специфични знаења и вештини во врска со економското работење и правните рамки на дејноста со која се занимаваат;[277]
- сложеност – економијата е специфично подрачје на човековото дејствување, а работните движења се комплексни, па затоа и економскиот криминалитет е специфичен и сложен. Разноликоста и сложеноста на правната регулатива која ги одредува рамките на работење на деловните субјекти логично води до појава на компликувани modus operandi на овие деликти;[278]
- организираност – врските на високопозиционирани поединци од деловниот, општествениот и политичкиот живот во заедницата кои ја злоупотребуваат својата положба и

[277] Според: Janowsky Thomas, „Ermittlungen in Wirtschaftsstrafsachen", *Kriminalistik,* Teil 1, Heft 4, Kriminalistik Verlag, Heidelberg 1998., p. 269.

[278] Според: Greiner Georges, „Akkusationsprinzip und Wirtschaftsstrafsachen", *Schweizerische Zeitschrift fűr Strafrecht*, 1/2005, Stämpfli Verlag AG, Bern 2005., p. 102.

општественото влијание, ги прават особено опасни облици на криминалитет (т.н. „криминал на белите вратоврски“);
- масовност – економскиот криминалитет е релативно фреквентна појава во современите општества, а кривичните дела од оваа област по правило учествуваат со околу 10% во вкупниот криминалитет;
- противправната имотна корист (односно предизвикана штета) е значително поголема отколку што е тоа случај кај класичниот криминалитет, а негативните последици, освен оштетеното правно лице, се рефлектираат на економскиот систем, како и на поширокатa општествена заедница;[279]
- приспособливост и инвентивност на извршителите – економскиот криминал е област со голем потенцијал на иновации, менување на начинот на извршување на кривичното дело, т.е. приспособување на новите околности, на измените на прописите и на развојот на техничките средства, што во голема мера го отежнува неговото откривање и докажување;[280]
- имотниот статус на обвинетите, кој им носи подобра можност за одбрана (ангажирање повеќе бранители, т.е. можност на неформално истражување на фактичката состојба, односно спроведување неформална, „приватна истрага“ на одбраната);
- во голем број случаи непостоењето „класичен“ оштетен, на пример, кај некои случаи на корупциски кривични дела, го отежнува нивното откривање и докажување.[281]

За да се обезбеди адекватно функционирање на корпорацијата и заштита од криминални однесувања, потребно е во континуитет да се преземаат бројни превентивни тактичко-технички мерки и работи за да се спречи какво било загрозување. Затоа неопходно е безбедносниот менаџмент да биде адекватно стручно оспособен, што вклучува и познавање на криминалистичките мерки и работи. Во врска со тоа, во превентивно криминалистичките работи и мер-

[279] See Hans, Spoo Eckart (Hrsg.), *Wirtschaftskriminalität – kriminelle Wirtschaft*, Distel Verlag, Heilbronn 1997., pp. 23-24.

[280] Види: Lindemann Michael, „Strukturelle Probleme der strafrechtlichen Aufarbeitung von Wirtschaftskriminalität“, *Kriminalistik,* Teil 59, Heft 8-9, Kriminalistik Verlag, Heidelberg 2005., pp. 507-508.

[281] Orlović Ante, Pajčić Matko, „Policijski izvidi kaznenih djela gospodarskog kriminaliteta“, *Hrvatski ljetopis za kazneno pravo i praksu*, Vol. 14, br. 2, Zagreb 2007., str. 703-705.

ки на корпорацискатa безбедност спаѓаат: легитимирање лица и утврдување на идентитетот; преглед и претресување лица, објекти, превозни средства и отворен простор; привремено одземање предмети; набљудување и следење; полиграфско тестирање и криминалистичка проверка; заседа и друго. По сознанието дека е направен криминален настан, се преземаат следните итни мерки: известување на врвниот менаџмент за настанот; известување на надлежните државни органи заради вршење увид; обезбедување на местото на настанот; давање итна медицинска помош; спречување бегство на сторителот на кривичното дело и негово задржување до предавање на надлежните органи и слично.[282]

6.13. ПРОГРАМА ЗА ЕДУКАЦИЈА И РАЗВОЈ НА БЕЗБЕДНОСНАТА КУЛТУРА НА ВРАБОТЕНИТЕ

Различни автори укажуваат дека системската едукација на вработените со цел подигање на нивното ниво на свест и безбедносна култура е незаменлив фактор во намалување на штетата која ѝ се заканува на корпорацијата од различните видови загрозувања и закани. Во врска со тоа, се истакнува дека едукацијата мора да биде спроведена како во фазата на вработување, така и во континуитет во текот на работењето во компанијата. Во практична смисла, важно е програмите за едукација на вработените да бидат насочени кон тоа пропишаните процеси и процедури на корпорацијата да се реализираат во практика, а да не претставуваат „мртов текст на хартија“. Исто така, кај вработените мора да се поттикнуваат иницијативи за промена на процесите и на процедурите, особено во случаи кога постојните се неприменливи во пракса и кога е неопходно донесување нови, првенствено поради новонастанати ситуации, предизвикани од промените на технологијата и унапредувањето во одвивање на работните процеси. Вработените во корпорацијата мора да бидат едуцирани и стимулирани за да може соодветно да реагираат и да постапуваат во однос на воочените неправилности и пропусти, т.е. итно да ги известуваат повисоките нивоа на раководење во компанијата за вооченото и постапеното. Повисоките менаџери во компанијата се должни врз основа на воочените пропусти и неправилности да наложат проверка на одвивањето на работните процеси и да идентификуваат исти или слични загрозувачки ситуации на другите објекти или простори на корпорацијата. По завршување на

[282] Скакавац Здравко, Малиновић Драгана, op. cit. стр. 59-60.

постапката на проверка на одвивањето на одреден работен процес, потребно е да се донесе заклучок и одлука дали регистрираниот безбедносен настан е предизвикан од спореден пропуст или од вообичаениот модел на однесување, дали неговата причина е субјективен став на поединците или е објективен факт, кој настанал како редица на непредвидливи околности и ситуации, т.е. дали важечките работни правила и другите безбедносни процедури не се во согласност со реалноста, а со самото тоа се и неприменливи.[283]

7. СТРУКТУРА НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Во дефинирањето на соодветното ниво на корпорациската безбедност неопходно е предходно да се утврдат и да се формулираат следните елементи:

- актуелни разлики, причини и облици на загрозување лица, имот и работење на корпорацијата кои треба да се очекуваат во идниот период;
- прецизирање на надлежностите и овластувањата на лицата кои работат во компанијата на работи околу заштита на нејзините витални вредности и утврдување на состојбата на нивната стручност и мотивираност;
- организација и дејствување на физичко-техничкото обезбедување на сите објекти кои ѝ припаѓаат на компанијата;
- мерки на заштита поврзани за безбедноста и здравјето, заштита на животната средина, заштита од пожари, хаварии и експлозии;
- мерки на заштита на работењето на корпорацијата од сите облици на корупција, различни видови злоупотреба, проневери, измами и други методи на отуѓување и присвојување на нејзиниот имот;
- прецизирање на мерките на заштита на деловна и на службена тајна;
- конкретизирање на мерките во однос на контрола на движењето и престојувањето на надворешни лица во објектите и на просторот кој припаѓа на деловниот субјект;
- организација и функционирање на информациските системи и обезбедување на лицата, имотот и работењето

[283] Laušić Mate, Petar Saša, Marjanović Bono, op. cit. str. 319-320.

на корпорацијата, особено на мерките за заштита на информациите;
– хармонизација на нормативните акти во сите сегменти на безбедноста, со националните прописи и стандардите на ЕУ;
– оцена на степенот на загрозеност на лицата кои во корпорацијата извршуваат работи поврзани со заштита на нејзините витални вредности.[284]

7.1. НАЧЕЛА НА ФУНКЦИОНИРАЊЕ И РАЗВОЈ НА СИСТЕМОТ НА КОРПОРАЦИСКА БЕЗБЕДНОСТ

Корпорациската безбедност се развива преку воспоставен систем, според следните начела:
– *единственост* (сите елементи и актери на системот на корпорациско ниво и во делови на компаниите се развиваат според истите начела, функционално се поврзани и обединети во извршната функција на ниво на корпорацијата со почитување на субординацијата и обврската на спроведување на налогот на повисокото ниво на одлучување);
– *рационалност* (вклучување во функција на безбедноста на сите расположливи човечки, материјални и организациски ресурси на компанијата, формирање оперативни и високостручни служби за безбедносни работи кои ефикасно ќе го планираат, ќе го насочуваат, ќе го усогласуваат, ќе го следат и ќе го контролираат функционирањето на сите сегменти на системот);
– *сеопфатност* (организациско и функционално уредување кое ќе овозможи ефикасно отстранување на последиците од сите проценети реални извори и облици на загрозување и истовремено ангажирање во повеќе правци за да се остварат најдобрите ефекти);
– *селективност* (прецизно и концизно дефинирање, делегирање и дистрибуција на елементите на системот на корпорациска безбедност);
– *приспособливост* (можност за брзо и за ефикасно пренесување на тежиштето на дејствување на актерите и прераспоредување на елементите на системот на безбедност во согласност со промената на условите на дејствување, изворите и облиците на загрозување);

[284] Види: Barney Jay, Hesterly S. William, *Strategic Management and Competitive Advantage*, Prentice Hall, London 2005., pp. 432-435.

– *доверливост* (способност на системот да биде во постојана функционална состојба независно од чија било поединечна желба и способност да ги стимулира актерите на пожелно и пропишано однесување).[285]

Имајќи ја предвид значајноста на корпорациската безбедност за остварување на стратегиските цели на компанијата, организацискатa единица која ќе ги извршува тие работи треба да се престрои така да поседува јасни одговорности и прецизни овластувања во исполнување на своите основни задачи. Ако се работи за корпорација со голем број вработени, или компанија која работи на различни локации, тоа треба да биде организациска единица на прво ниво на поделбата на работите. Во малите компании, потребно е да се воспостави одбор за безбедност или да се именува менаџер за безбедност кој ќе биде непосредно одговорен за врвниот менаџмент. Во случај тоа да не е економски исплатливо, еден од врвните менаџери на компанијата мора да ја преземе улогата на менаџер за безбедност.[286] Во врска со тоа, треба да се потенцира дека во стандардната организација овие работи, во согласност со насоките од Европската унија, во големите корпорации се користи поимот интегрална безбедност, кој понатаму се расчленува на работи на безбедност (security), заштита (safety) на работата, заштита од пожари, заштита на околината. Ако тие работи се групираат во една организациска единица, компанијата добива рационална и ефикасна организација со воспоставена координација и контрола над сите работи врзани со безбедноста.[287]

7.2. ОДГОВОРНОСТ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Организациската структура која се воспоставува во рамките на корпорацијата се базира на расчленување на нејзините вкупни задачи на поединечни задачи, на формирање организациска единица како носител на извршувањето на одредени заеднички задачи, т.е. воспоставување на такви механизми на координација кои овозможуваат извршување задачи на сите нивоа на поврзување на работните процеси. Структурата на така воспоставената органи-

[285] Според: *Chief Security Officer Guidelines* (GDL CSO 06 2004), ASIS International Commission on Guidelines, Alexandria VA 2006., pp. 6-7.

[286] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 68.

[287] Според: Banner K. David, *Designing Effective Organizations: Traditional & Transformational Views*, SAGE Publications, Thousand Oaks CA 1995., p. 320.

зација е резултат на организацискиот дизајн во кој се врши поделба на задачите и нивно групирање, односно синтеза во соодветната организациска единица.[288] Во таква организациска структура на компанијата, одговорноста за корпорациската безбедност на компанијата ја носат: врвните менаџери (Управата) и раководителите на сите нивоа на одлучување; надзорен комитет, односно експертско тело чија задача е да ги следи и да ги унапредува безбедносните аспекти на работењето; менаџери за безбедност (CSO – Chief Security Officer), CSO оперативните тимови, проектанти и реализатори на компонентите на безбедносните работни принципи; како и сите вработени во компанијата. Некои автори во оваа структура ја додаваат и функцијата директор за безбедност, на кој му припаѓа највисокото ниво на среден менаџмент или ниското ниво на врвниот менаџмент на корпорацијата, чијашто задача е да поставува цели, стратегиски да планира, да предлага алтернативни решенија на проблемите, да ја претставува корпорацијата во јавноста заедно со центарот за односи со јавноста, да ги насочува и да ги следи активностите на лицата кои во компанијата се задолжени за работите врзани за корпорациската безбедност, да го поттикнува и да го охрабрува професионалниот развој на потчинетите.[289]

Менаџерот за безбедност ги координира и ги раководи работите на системот на обезбедување на лица, имоти и работењето на корпорацијата. Во хиерархијата на раководење со компанијата, неговото место е (ако во компанијата не постои функција директор за безбедност) непосредно покрај генералниот директор, односно сопственикот на капиталот. Сложената и одговорна работа на работите на системот на обезбедување бара одговарачко ниво на образование, мултидисциплинарни знаења и специфични особини на личноста кои се неопходни за извршување на оваа работа. Менаџерите за безбедност повеќе се занимаваат со луѓето и човековата деструкција, а помалку со системите во техничка смисла на зборот. Целокупниот систем на корпорациска безбедност во најголема мерка служи за проактивно спречување на човечката

[288] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 67.

[289] Според: Даничић Милан, Радаковић Ненад, „Преглед стања модерног менаџмента у корпоративној безбједности“, у: *Научни скуп «Дани безбједности» на тему: „Развој система безбједности и заштите корпорација“ (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 226-227.

деструкција, а само мал дел од тој систем е наменет да се спротивстави на загрозувањата кои произлегуваат од природните непогоди, земјотреси и пожари. Од тие причини, работите на менаџерот за безбедност налагаат секојдневно ангажирање и перманентна едукација. Успешна подготовка на менаџерот за безбедност подразбира постојано, во континуитет иновирано знаење за облиците и изворите на загрозување на компанијата, конкуренцијата, деловните партнери и клиентите.[290]

Менаџерот за безбедност своите задачи ги извршува секојдневно во интерактивен однос со надворешено и со внатрешно опкружување. Работите ги врши главно самоиницијативно или по барање на врвниот менаџмент. За да одговори на добиените налози, тој мора добро да ја познава компанијата, нејзиното работење и деловната гранка на која ѝ припаѓа. Затоа неопходни му се знаење, вештини, способности и лични карактеристики кои мора да ги поседува и да ги демонстрира. Во прашање се трајни квалитети кои е можно да ги разгледувате, да ги мерите и да ги развивате. Знаењето на менаџерот за безбедност, кое се стекнува со искуство, со учење или со истражување, подразбира специфични факти, идеи, информираност и разбирање внатре во одредено подрачје. Способностите се трајни карактеристики кои поединецот ги поседува, а коишто се важни за успешно извршување на задачите со примена на знаење и вештини. Вештините подразбираат можност за извршување физички или ментални активности кои водат кон ефикасно рашавање на задачите, додека личните карактеристики ја дефинираат личноста на менаџерот за безбедност, неговиот темперамент, академските квалификации, интересите и работните навики.[291] Во врска со тоа, се укажува дека компетенциите не ги вклучуваат „основните“ вештини и знаења, покрај очекуваната успешност во извршување на наложените задачи или умеење да се напише извештај, ниту вообичаените работи и задачи кои допридонесуваат за успехот на поединецот. Компетенциите подразбираат само однесувања кои демонстрираат натпросечност и супериорност, односно „применето“ знаење кое резултирало со успех, и манифестирање на вештините кои доведуваат до успех на компанијата.

Покрај стандардните услови, како што се соодветна стручна подготовка, работен стаж и работно искуство на работи врзани

[290] Даничић Милан, Стајић Љубомир, оп. цит. стр. 186.

[291] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 69-70.

со безбедноста, на менаџерот на корпорацискатa безбедност му се потребни и менаџерски вештини, односно лидерски способности, одговорност, харизматичност, ориентираност кон целите (SMART[292] начелата), способност за управување со тимовите, емоционална интелигенција, чесност, интегритет и морални начела, комуникативност, упорност во совладување на пречките, способност на препознавање на проблемите и можните решенија, како и познавање на теоријата на мотивација и примена во работата на различни мотивациски техники. Раководењето, кое е најважната карактеристика на менаџментот, опфаќа голем број активности – од визии, дефинирање на целите, планирање и дефинирање на задачите, мотивирање и придобивање на вработените за акции, координирање, насочување и следење на извршувањето на задачите, до наградување и преземање мерки на унапредување, при што се користат различни техники. Во врска со тоа, се истакнува дека постојат неколку видови раководење, со оглед на начинот на користење на авторитетот: автократски, демократски или партиципативен и стилот на лидер на одврзани раце. Постојат и приспособени видови на раководење, во зависност од ситуацијата во која се наоѓа компанијата, раководителот (менаџер) или неговите следбеници и потчинети.[293]

Менаџерите на сите нивоа, во сите области на системот за безбедност во корпорациите донесуваат одлуки, т.е. прават избор од две или од повеќе алтернативи. На пример, менаџерите од највисокото ниво донесуваат одлуки за целите на корпорацискатa безбедност, локациите на производствените објекти, елементите на системот на заштита, безбедност на финансиското работење и друго. Менаџерите на средните и ниските нивоа донесуваат одлуки за неделната или за месечната работа на службеното лице за обезбедување и за употребата на средствата за техничка заштита, за настанатите проблеми во работата на системот на безбедност, за зголемување на нивото на безбедност. Може да се утврди дека менаџерите донесуваат одлуки, но сепак за менаџерот во секторот за безбедност во корпорациите, како носител на одлуки, сè уште не се знае доволно, а всушност не се знае како се донесуваат одлуките во секторот за безбедност во корпорациите. Често одлуката која

[292] Целта мора да биде специфична, мерлива, остварлива, релевантна, временски ограничена.

[293] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 71.

се донесува е поврзана со висок степен на ризик. Притиснати со временските рокови менаџерите за безбедност се склони анализата да ја вршат површно. Донесувањето одлука бара да се врши организирано, и таа да се базира на современите принципи на менаџментот. Недопустливо е површно решавање на проблемите од безбедносна природа, што менаџерите за безбедност ги принудува во процесот на донесување на одлуки многу подлабоко да навлезат во причините на проблемот и да ги истражат сите можни решенија.[294]

Во литературата како клучни одговорности на менаџерот за корпорациска безбедност се наведуваат: развој и примена на безбедносна стратегија која покажува разбирање на природата на настанување вонредни случувања кои би можеле да имаат негативно влијание на општо ниво на безбедност во компанијата (безбедносна политиката, програми и процедури, планови за превенција и дејствување во вонредни ситуации); управување со процесите на корпорациска безбедност на деловниот субјект; прибирање информации и процена на ризици (ранливост) на корпорацијата; одржување подготвеност на организацијата (обезбедување на подготвеност на корпорацијата за можност од напад, од катастрофални случувања или од организирани безбедносни инциденти – разбојништва, измами, нелојалност на вработените, намерен/ненамерен инцидент и др.); превенција на инциденти; заштита на работниците, на клучните работни функции, на информатичкиот систем, на податоците, на информациите и на репутацијата на компанијата; одговор на инциденти, управување со ризиците и заздравување; координација на работите со државните институции и тела.[295]

Менаџерот за безбедност претставува витална алка во хиерархиската структура на корпорацијата, и најчесто се наоѓа меѓу службениците од една и врвниот менаџмент од друга страна. Во таа позиција, тој ги застапува ставовите и барањата на менаџерите во компанијата, но истовремено тој е одговорен и за презентирање на ставовите, потребите и проблемите на потчинетите службеници на менаџментот на корпорацијата.[296]

---

[294] Види: Триван Драган, „Одлучивање у корпоративној безбедности“, у: *Корпоративна безбједност – ризици, пријетње и мјере заштите* (зборник радова), Факултет за безбједност и заштиту, Универзитет Синергија, Бања Лука 2010., стр. 399-400.

[295] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 72-73.

[296] Даничић Милан, Радаковић Ненад, op. cit. стр. 231-232.

Како основни услуги кои менаџерите на корпорациска безбедност ги даваат на раководството на корпорацијата се наведуваат: безбедносна стратегија, идентификација и анализа на ризиците, процена и тестирање на ризикот, политиката, програми и процедури на безбедноста, заштита на технологијата и на инфраструктурата, раководење со информацискиот ризик, управување со континуитетот на работење, раководење со кризниот менаџмент и одговор на кризни ситуации, подигнување на свеста на вработените за ризиците, операции врзани за безбедност на работните места, истражување на работното однесување и неговата усогласеност со законите, заштита на раководството на корпорацијата, работи Business Intelligence и Business Counterintelligence, проверка на информациите добиени од извори во корпорацијата, форензички и истражни услуги, заштита на документацијата.[297]

Во секторот за безбедност во корпорациите, одлуките се донесуваат на ниво на управен одбор, директор на секторот за безбедност, одделни оддели на секторот за безбедност, но одлуки донесува и секој поединечен менаџер во рамките на една организациска единица од секторот за безбедност. Донесувањето на одлуката е од исклучителна важност за работата на менаџерот и е составен дел на другите четири менаџерски функции. Затоа менаџерите и кога планираат, организираат, водат (издаваат наредби) и контролираат се нарекуваат донесувачи на одлуки. Може да се рече дека донесувањето одлуки за корпорациска безбедност, всушност е синоним за менаџерство. Факт е дека речиси сè што прават менаџерите за безбедност подразбира донесување на одлуки, но тоа не значи дека одлуките се долготрајни, комплексни или јасни за надворешен набљудувач. Оваа тема може да се разгледува со согледување на следните основни принципи и начини на донесување одлуки во секторот за безбедност на корпорацијата: рационалност, ограничена рационалност и интуиција. Се претпоставува дека менаџерското донесување одлука е рационално. Под ова се подразбира менаџерите доследно да вршат избор и максимално да придонесуваат за зголемување на вредноста на безбедноста во рамките на одредени безбедносни ограничувања.[298] Се смета дека во системот на корпорациска безбедност во компаниите треба да

[297] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 73.

[298] Триван Драган, „Одлучивање у корпоративној безбедности“, op. cit. стр. 401.

постои принцип на едностарешинство, под што се подразбира во раководењето со секој потчинет како раководител да се појавува само еден претпоставен (исклучок се вонредни ситуации и пропусти на менаџерот за безбедност кои можат да ги загрозат стратегиските цели и репутацијата на корпорацијата).[299]

Се укажува дека донесувачот на одлуките кој е целосно рационален ќе биде и потполно објективен и логичен, дека внимателно ќе го дефинира проблемот и ќе има јасна и специфична цел. Покрај тоа, донесувањето одлука со примена на рационалност води до избор на алтернатива која максимално ја зголемува веројатноста за постигнување на таа цел. Претпоставките на рационалност се применуваат на која било одлука во секторот на безбедност – тимска или менаџерска. Рационално менаџерско донесување на одлука подразбира одлуките да се донесуваат со цел да се оствари најдобар интерес за безбедноста на корпорацијата. Тоа значи дека донесувачот на одлуката мора максимално да ги согледува безбедносните интереси на корпорацијата, а не сопствените интереси на секторот за безбедносност. Донесувањето одлука за корпорациската безбедност може да биде рационална ако се исполнети следните услови: безбедносниот менаџер е соочен со едноставен проблем во кој целите се јасни, а алтернативите ограничени, во кој временскиот притисок е минимален, а трошоците за пронаоѓање решение и процени на алтернативите се мали, во кој организациската култура поддржува иновација и преземање ризик и во кој исходот од применетите мерки на безбедност се релативно конкретни и мерливи. Но повеќето од одлуките со кои се соочуваат безбедносните менаџери во корпорациите не ги исполнуваат овие услови. Поради тоа повеќето одлуки во секторот за безбедност во корпорациите се донесуваат со концептот на ограничена рационалност.[300]

М. Даничиќ и Љ. Стајиќ сметаат дека вработените претставуваат важен интерен субјект на безбедноста во компанијата, при што основниот облик се исполнува преку нивните активности, поаѓајќи од самозаштита, како една од појдовните основи во функционирање на системот на обезбедување. Според нив, современите трендови неминовно укажуваат дека обезбедувањето на компаниите не може да функционира на вистинскиот начин ако се потпира само на лицата кои професионално ја работат оваа работа, туку мора да ги опфати и ги опфаќа сите поединци кои се заинтересирани за посигурни и за

[299] Даничић Милан, Радаковић Ненад, op. cit. стр. 233-234.

[300] Триван Драган, „Одлучивање у корпоративној безбедности“, op. cit. стр. 402.

побезбедни работни услови. Во текот на секојдневните активности и извршување на работните задачи, вработените во корпорацијата, како и работите и работните места на кои работат, се изложени на разни облици на загрозувања, кои можат негативно да влијаат, како на нивниот физички интегритет, така и на работниот имиџ и углед на компанијата. Лицата кои професионално се ангажирани на работите поврзани со безбедноста често не се во можност физички да бидат присутни на сите места и локации во компанијата каде што постојат потенцијални опасности и ризици, поради што другите вработени често се препуштени сами на себе. Споменатите автори укажуваат на самозаштитната компонента на корпорацискатa безбедност, која првенствено се однесува во проактивните мерки кои вработените ги спроведуваат во текот, а често и надвор од работното време. Од тие причини, потребно е со интерни акти на компанијата прецизно да се дефинираат мерките во доменот на самозаштита кои секој поединец кој е вработен во неа е должен да ги спроведува. Непочитувањето на овие мерки би требало да претставува тешка повреда на работната дисциплина и да повлече адекватни санкции.[295]

7.3. АКТИВНОСТИ НА ОРГАНИЗАЦИСКИТЕ ЕДИНИЦИ ЗА КОРПОРАЦИСКА БЕЗБЕДНОСТ

Организациската структура на секторот за безбедност во корпорациите е симбиоза од човечки и од материјални ресурси, така што на оптимален начин придонесува за успешна реализација на своите задачи. Каква организациска структура на секторот за безбедност во корпорацијата ќе биде избрана зависи од редица фактори, при што основниот критериум е успешно реализирање на стратегијата или конечната цел на корпорацискатa безбедност. Во врска со тоа, потребно е најнапред да се анализираат расположливите начини на организирање на секторот на безбедност во корпорациите или модели на формирање на организациските структури. Британскиот теоретичар Маси го застапува ставот дека ефективната примена на стратегијата бара од менаџерите да разработуваат бројни клучни влијанија, додека лидерот има улога да одреди како ќе ја структуира организацијата за реализација на стратегијата и како треба да управува со луѓето и со средствата за да се реализираат дефинираните организациски планови.[301]

[301] Massie L. Joseph, *Essential of Management,* Prentice Hall International, London 1987., pp. 41-42.

Управите на корпорацијата при идентификувањето и при дефинирањето на елементите на организациската структура на секторот за корпорациска безбедност се соочуваат со четири основни прашања: „Кои делови од секторот за безбедност треба да бидат организациски единици?“, „Кои работи од безбедноста треба да се групираат, а кои да се раздвојат?“, „Која големина и облик одговара на различните организациски единици во секторот за безбедност?“, „Како да се распоредат безбедносните менаџери и службеници и како меѓусебно да се поврзат различните организациски единици?“. На овие прашања не постојат однапред дадени одговори, но врз основа на определени принципи, критериуми, методи и правила во секој конкретен случај може да се дефинира ефективната организациска структура. За да може да се дојде до неа, потребно е да се анализираат: клучните активности кои се очекуваат од секторот за безбедност во корпорациите и нивните цели; придонес кон постигнување на потребната состојба на корпорациската безбедност; активности за произведување мерливи резултати; активности за поддршка и општи работи, т.е. правење рационална анализа заради утврдување на позицијата на поединечните компоненти на секторот безбедност.

Според мислењето на Т.Веиќ, организациската единица за корпорациска безбедност по правило треба да биде воспоставена како интерна служба на корпорацијата за работи на безбедност и заштита, а евентуално може да биде и професионална агенција која постапува според плановите на менаџерот за безбедност на компанијата. Работите на таа единица треба да ги опфаќаат следните активности:

а) *Собирање информации и процена на ризикот.* Единицата за корпорациска безбедност е одговорна за собирање на релевантни информации од областа на безбедноста и заштитата, коишто можат битно да влијаат на безбедноста и заштитата на вработените, на странките, на репутацијата и на конкурентноста на работната организација. Врз основа на така собраните податоци потребно е да се направи процена на ризикот.

б) *Подготовките на организацијата за вонредни состојби.* Единицата за корпорациска безбедност одговорна е и за подготвеноста на организацијата да се заштити во случаи на големи измами, напади, катастрофални случувања, „минирање“ на производството од страна на конкурентните фирми или поединци и сл. Во таа смисла, постојано треба да се контролираат безбедносните мерки и планови и да се обучуваат вработените.

в) *Обезбедување и заштита на виталните интереси на организацијата*. Обезбедување на интегритетот на организацијата, вработените, процесите и недвижностите од штета и загуби, исто така, е една од клучните одговорности на единицата за корпорациска безбедност. Притоа, оваа единица ги штити недвижностите и финансиите на организацијата, но и на интелектуалната сопственост, трговската марка, репутацијата, службените тајни (договори и сл.) итн.

г) *Превенција на инцидентни состојби.* Клучна одговорност е анализа на инфомациите и координирање на активностите со лицата во организацијата и во државните институции за да се предвидат можните напади врз организацијата, односно како да се направат превентивните процедури. Во таа смисла, единицата за корпорациска безбедност мора да биде во состојба да ги разбере конкретните извори на безбедносните проблеми и да изнајде адекватни решенија за нивно отстранување.

д) *Реагирање и управување со инцидентни состојби и санирање на последиците.* Единицата за корпорациска безбедност мора да посвети максимално внимание за враќање на организацијата во нормална работна состојба по инцидентни и акцидентни состојби. Таквото враќање на организацијата во нормална состојба мора да се координира со надлежните институции (полиција, војска, итна помош итн.).[302]

Во согласност со насоките од Европската унија, во големите корпорации денес се користи поимот интегрална безбедност. Во тој контекст, некои автори го предлагаат следниот модел на организациска единица на интегрална безбедност, на чело со главен менаџер, во чиј состав би биле:

- организациска единица за корпорациска безбедност (раководител на организационата единица, менаџер за информациска безбедност, специјалист за безбедност при работа, специјалист за работно обезбедување личности, специјалист за одбранбени подготовки);
- организациска единица за заштита при работа, заштита од пожари и заштита на животната средина (раководител на организациската единица, специјалист за заштита при работа и заштита од пожари, специјалист за заштита на животната средина).[303]

[302] Veić Tomislav, „Korporativna sigurnost“, во: *Pošta*, godište II, broj 3, Zagreb, veljača 2007., str. 41-42.

[303] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 74.

Одредени автори, како Г. Максимовиќ, сметаат дека во составот на организациската единица за интегрална безбедност треба да има и интегриран оперативен центар (ИОЦ) како централен елемент за раководење и управување со безбедносниот систем на корпорацијата. ИОЦ би бил одговорен за спроведување на мерките на приправност и рано предупредување, како и обезбедување на континуитет во водењето на работата и процесите во работниот субјект. Во таа смисла, задачите на интегрираниот оперативен центар би биле: следење на состојбите, прибирање и анализирање на податоци, донесување одлуки кои имаат за цел заштита на животите и имотот, одржување континуитет до дејствувањето на корпорацијата во рамките на важечките прописи и дистрибуирање на одлуките за сите учесници кои се ангажирани во извршување на конкретната задача.[304]

Во рамките на работите за интегрална безбедност на корпорацијата, задача на менаџерот за информатичка безбедност би биле врзани за премостување на јазот меѓу информатиката, безбедноста, работните единици внатре во корпорацијата и врвниот менаџмент. Во таа смисла, тој би бил задолжен за: развој и примена на стратегијата за безбедност и безбедносната архитектура на информатичкиот систем; процена на ризикот на безбедност на информатичкиот систем; одредување безбедносни цели во согласност со стратегијата на информатичкиот систем на корпорацијата; развој на политика за безбедност на информатичкиот систем, стандарди, процедури, насоки и други интерни акти на корпорацијата со цел достигнување и одржување на задоволително ниво на безбедност; анализирање на безбедносните потреби и во согласност со тоа предлагање, планирање, имплементација, тестирање и надзор на активностите за подобрување на безбедноста на информатичкиот систем; планирање и координирање со анализите на исплатливост на препорачаните и на постојните безбедносни решенија; контрола на спроведувањето на политиката за безбедност на информатичкиот систем и другите интерни акти на корпорацијата кои се однесуваат на тоа; давање насоки за обучување на сите вработени кои го користат информатичкиот систем на корпорацијата, а се однесуваат на безбедноста на тој систем. Надлежностите на специјалистите

[304] *Научни скуп «Дани безбједности» на тему: „Развој система безбједности и заштите корпорација“ (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 304-305.

за деловна безбедност во организацискатa единица за интегрална безбедност на корпорацијата би опфатиле: оперативно спроведување на дефинираните политики на корпорацискатa безбедност; непосредно организирање превентивни мерки за противправни и инцидентни однесувања насочени кон работата на компанијата; предлагање мерки и активности во функција на совладување на пречките, санација на негативните последици за излез на компанијата од евентуалната криза во работењето; предлагање превентивни мерки за физичко-техничка заштита на вработените и на имотот на компанијата, како и програма за оспособување и подигнување на свеста на вработените; контрола на спроведување на политиката, програмата и процедурите за безбедност.[305]

Имајќи ја предвид сериозноста на последиците од загрозување „на критичка клучна инфраструктура", во литературата се присутни заложби во нивната заштита да се применува интегриран модел на корпорациска безбедност, со препуштање на одделни помалку чувствителни функции (физичка и техничка безбедност) на тој систем на надворешни специјализирани давачи на услуги од таа област (outsourcing). Тој интегриран модел во системот Critical Infrastructure, кога од него би се изземале функциите на корпорацискатa безбедност кои можат да бидат предмет outsourcing, според Марин Вршец може да го опфати: главниот менаџер за безбедност и на него потчинетите оперативни безбедносни менаџери; организацискатa единица за безбедност и заштита (заштита од природни, индустриски, транспортни и други катастрофи, заштита на лица, тајни податоци и службени тајни, заштита на информациите и на архивите, заштита на електронските комуникации, заштита на патенти, жигови и заштита на угледот на компанијата, заштита од пожари и опасни материи и заштита при работа); организациска единица за безбедност на документи; организациска единица за информатичка заштита; организациска единица за оперативно дејствување и безбедносен контролен центар.[306]

[305] Муравъева Ирина, „Новый взгляд на службу информационной безопасности компании" (http: www.bre.ru/security/20033.html).

[306] Vršec Miran, „The Role and Risks of Outsourcing in the Processes of Providing Corporate Security in Critical Infrastructure", in: Čaleta Denis, Shemella Paul (eds), Counter-Terrorism Challenges Regarding the Processes of Critical Infrastructure Protection, Institute for Corporative Security Studies (ICS) & Center for Civil-Military Relations, Ljubljana-Monterey CA 2011., pp. 59-60.

8. НАДВОРЕШНА КОНТРОЛА НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Со развојот на демократските процеси во светот, на надворешната контрола на корпорацискатa безбедност ѝ се придава сè поголемо значење. Надворешната контрола на овој сектор најчесто се остварува како: а) парламентарна и владина, б) судска, в) цивилна, и г) контрола на јавното мислење. *Парламентарната* и владината контрола на корпорацискатa безбедност ја остваруваат надлежните владини и собранискиорганиорган, најчесто парламентарни одбори и комисии за безбедност, но и непосредно Собранието и Владата, на кои надлежното министерство им поднесува извештаи од работата на разгледување и усвојување. *Судската контрола* на корпорацискатa безбедност се остварува со обврска на секој вработен во корпорацискатa безбедност во врска со службената должност да учествува во покренатa судска постапка во која се утврдува негова или туѓа одговорност, ако тоа се побара од него. *Цивилната контрола* на корпорацискатa безбедност се остварува преку соодветни невладини организации, локални заедници (независни комисии за контрола и надзор и сл.). *Контролата на јавното мислење* се обезбедува преку обврската на овластениот припадник за корпорациска безбедност во компанијата редовно да ја информира јавноста за безбедносната состојба, тежишните задачи, мерки кои се превземаат и резултати од работата.

9. СОСТОЈБА НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО ВИСОКОРАЗВИЕНИТЕ ЕКОНОМИИ

Актуелен тренд во развиените замји на Европа е зголемување на бројот на вработени во недржавниот сектор за безбедност, вклучувајќи ги и вработените во корпорацискатa безбедност, додека бројот на редовните полициски сили се намалува, така што односот помеѓу бројот на припадници во полицијата и пресоналот во службите за безбедност во корпорациите и во компаниите кои даваат услуги за приватно обезбедување сега е приближно 1:1. Споредувајќи ги коренсподирачкиот број припадници на недржавниот сектор за безбедност на 100.000 жители се добиваат следните показатели: во

Шведска – 184, во Литванија – 75, во Луксембург – 201, во Данска – 193, а во Велика Британија дури 273.[307]

Во споменатите држави недржавниот сектор за безбедност настојува да ги заштити правата и легалните интереси на своите клиенти, со што би ја осигурал нивната безбедност и би го одржал редот. Дејствувајќи кон остварување на таа цел, субјектите на корпорациската безбедност ги формулираат основните насоки на активноста, кои потоа се регулираат со законодавни норми. Покрај тоа, развојот на технологијата и на обликот на производство и услугите неминовно ја услови појавата на бројни нестандардни безбедносни системи и процедури во функција на заштитата, што значи дека кругот на традиционалните работи за обезбедување се проширил и на други, незаштитни функции, кои побаруваат работа на сиот систем на корпорациска безбедност.[308]

10. ПРОБЛЕМИ СО КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО ЗЕМЈИТЕ ОД БАЛКАНОТ

Сè поизразените проблеми на корпорациската безбедност, според Љ. Стаиќ,[309] можат да се сведат на новите, изменети околности (економски услови, политички односи на меѓународен и на регионален план, поврзување на економските субјекти, безбедносните стандарди на корпорацијата, правната регулатива, средствата и методите за заштита, оддалеченоста на седиштето на корпорацијата и др.); на интернационализацијата и на глобализацијата на: односите, условите, потребата од комуникација, производството, транспортот, прописите, финансиските услови, работната сила, пазарот, на идеите; постојана регионализација на корпорациите (промена на бројот на организациски единици, нивна географска дисперзија); на нови стандарди (нужност од забрзување на работите на воведување на меѓународните стандарди во областа на корпорациската безбедност).

[307] Kalesnykas Raimundas, The Place and Role of Private Security in Policing: A State in Transition, in: *Science, Security, Police (NBP)*, Vol. 8, No. 2, Belgrade 2003., p. 31.

[308] Даничиќ Милан, Стајиќ Љубомир, op. cit. стр. 239.

[309] Стајиќ Љубомир, „Изазови корпоративне безбедности у светлу савременог схватања појма безбедности“, op. cit. стр. 28-29.

Како еден од проблемите во функционирањето на корпорацискатa безбедност се појавува и хронична незаинтересираност на компаниите за ефикасно извршување на безбедносните функции внатре во нив. Причините за тоа се различни – тежнеењето на раководителот во компанијата за неконфронтирање, по линија на помал отпор, се настојува да се спречи разоткривањето на недозволените работи на менаџментот, страв од можното компромитирање на компанијата ако внатрешните проблеми бидат предмет на медиумски презентации и друго.[310] Видот на дејност, односно припадноста на компанијата на одредена работна гранка или индустрија, ја детерминира природата на работа во безбедноста и специфичностите на организацијата на корпорацискатa безбедност. Најважните индустриски гранки во смисла на просторот на Балканот поврзани се со експлоатација на нафта, гас, руда и на други природни ресурси, вклучувајќи ја и водата. Работењето на корпорациите во тие области бара големи инвестиции и генерира големи приходи кои треба да се делат со локалната власт, што често станува извор на спорови и недоразбирања внатре во државата и помеѓу државите. Од менаџерот за безбедност во тие околности се очекува да демонстрира респективно ниво на комуникација со опкружувањето. Корпорацискатa практика укажува на големото влијание што овие компании можат да го имаат на локалното опкружување и неговите постојни карактеристики (еколошки, демографски, техничко-технолошки) во смисла на степенот на заштита на природните расурси и намалување на различните видови загадување. Корпорацискатa безбедност во ваквите корпорации има големо значење во ситуации врзани за изградбата и функционирањето на големите инфраструктурни проекти, особено на оние што налагаат раселување и преместување на локалните жители, заради остварување полесен пристап до природните ресурси коишто се предмет на експлоатација. Рударството, нафтените дупчења и слични активности кои ги деградираат природните ресурси, често можат да ја влошат локалната безбедносна ситуација, особено ако не се даваат информации за потенцијалните здравствени загрозувања.[311]

[310] Кешетовиќ Желимир, Симоновиќ Бранислав, op. cit. стр. 155.
[311] Даничиќ Милан, Стајиќ Љубомир, оп. цит. стр. 167.

На актуелната состојба на безбедност во корпорациите во државите на Балканот битно влијаат следните услови:

– непостоење адекватни законски и подзаконски акти кои би требало да ја регулираат работата на секторот на корпорацискатa безбедност;
– неусогласеност на постојните организациски структури на секторот за безбедност во корпорациите со целите на корпорацискатa безбедност;
– непостоење на пропишани постапки за извршување на безбедносни работи и примена на мерките за безбедносна заштита;
– преклопување на задачите на секторот за безбедност во корпорациите со задачите на другите организациски единици на корпорацијата;
– недоволно познавање на организациските структури на странските служби за безбедност во корпорациите;
– недоволна соработка на секторот за безбедност во корпорациите со истакнати домашни и странски експерти кои се занимаваат со проектирање на организациските структури на секторот за безбедност и работите на корпорацискатa безбедност;
– непостоење стручно оспособен кадар за проектирање на организацискатa структура на секторот за безбедност;
– непостоење едукација на безбедносните менаџери за оформување на организацискатa структура на секторот за безбедност во корпорациите;
– непостоење современа информатичка опрема, софтверски апликации, други материјални и парични средства заради подготовка и реализација на процесот на оформување на организацискатa структура на секторот за безбедност во корпорациите.

III глава

ВЛИЈАНИЕТО НА КОРПОРАЦИСКАТА ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ ОД АСПЕКТ НА ЕКОНОМИЈАТА

1. НАЦИОНАЛЕН ЕКОНОМСКИ ИНТЕРЕС И ЕКОНОМСКАТА МОЌ НА ДРЖАВАТА

Економската благосостојба во вкупната развиеност на државите, ниската стапка на невработеност и високиот животен стандард, спаѓаат во најголемите гаранции за националната безбедност. Економската моќ на државите лежи во нејзиното богатство, природните ресурси, капацитетот на производи, работната сила, трговијата и сл. Богатството на нациите е централен фактор за национална безбедност од најмалку две причини: прво, државата мора да им овозможи на своите граѓани прифатлив стандард на живот и второ, повисок степен на развој и повеќе богатство, овозможувајќи со тоа поголеми вложувања во оние инструменти на национална безбедност што се директно одговорни за нејзино остварување или за спречување и елиминирање на различни видови загрозувања. Од аспект на насоченост кон странство (национален интерес во потесна смисла), националните економски интереси, вклучуваат унапредување на меѓународната трговија на една држава, нејзиниот пристап до материјални и до финансиски ресурси и пазари, како и заштита на приватните интереси во друга држава.[312]

Составен дел на вкупната моќ[313] на една држава е нејзината економска моќ, која ѝ стои на расплагање за остварување на некои други интереси кон странски држави (политички, воени, економски, разузнавачки), односно за слабеење или за зајакнување на потенцијалот на други држави – во зависност од сопствените цели и интереси. Економската моќ може да даде огромен придонес на националната безбедност, така што во случај на економска војна, државите ги прават неповредливи. Поради тоа, низ историјата се сметало дека „економската самодоволност“ (економска независност,

[312] Tatalović Siniša, Bilandžić Mirko, оп. цит. стр. 79.

[313] Моќта е способност за остварување на сопствените намери и цели, способност и вештина за контролирање на други, односно способност другите да се принудени на однесување во согласност со сопствениот пазар, во: *Енциклопедија политичке културе*, Савремена администрација, Београд 1993 стр.685.

односно постоење доволни сопствени суровини и производни капацитети и доволни сопствени пазари, независност на економијата од увоз и извоз) се средство за успешна одбрана, односно заштита на националната безбедност.[314]

Преку економската моќ може во голема мера да се влијае на однесувањето на другите држави, користејќи низа расположливи инструменти, почнувајќи од „економски влијанија“ до „економска војна“.[315] Поради сложените и хетерогени меѓународни економски односи,[316] на државите им стојат на располагање редици техники од спектарот на економски инструменти кои можат да се употребат со цел да се задржи постојниот однос на државите или да се промени тоа однесување. Споменатите техники можат да бидат од позитивен (награди) или од негативен (санкции, присила) карактер. Некои од тие техники се: даноци, квоти, бојкот, ембарго, блокада, заеми, кредити и монетарна манипулација, црна листа, контрола на увоз/извоз, замрзнување средства и капитал, давање или одземање странска помош. Одлуката на државите која од овие техники ќе биде применета зависи од: целта што сакаат да ја постигнат, од споредбата на трошоците и ризиците применети од различни техники (економските санкции можат да создадат трошок, а потоа и незадоволство на домашната јавност во земјата која се обидува да ги наметне), можни противмерки на целната држава, нејзината можност за излез на алтернативен пазар и пронаоѓање други трговски партнери, т.е. однесувањетото на државите во меѓународната заедница. Наведените економски инструменти можат да бидат поефикасни ако се користат во комбинација со другите инструменти на националната безбедност (политички, дипломатски, воени, разузнавачки, пропагандни). Притоа, потребно е при примена на некои од нив (ембарго) кон „проблематични“ држави да учествуваат сите држави членки на меѓународната заедница.[317]

---

[314] Види: Мијалковић Саша, Бошковић Горан, „Угрожавање корпоративне безбедности и последице по националну безбедност“, во: *Научни скуп «Дани безбједности» на тему: „Корпоративна безбједност – ризици, пријетње и мјере заштите“ (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2010., стр. 289.

[315] Tatalović Siniša, Bilandžić Mirko, оп. цит. стр. 80.

[316] Според: Mileta Vlatko, *Uvod u međunarodne ekonomske odnose*, Narodne novine, Zagreb 1988., str. 25-27.

[317] Tatalović Sinisa, Bilandžić Mirko, op.cit. str. 82.

2. ЕКОНОМСКИ ИНСТРУМЕНТИ НА НАЦИОНАЛНАТА БЕЗБЕДНОСТ

Анализата за примена на економските инструменти на националната безбедност првенствено насочени кон надвор (странство), упатува на заклучокот дека тие првенствено се применливи и ефикасни во односите развиени-неразвиени држави.[318] Во тие односи нивната успешност зависи од неколку услови кои мора да бидат исполнети, и тоа: целната земја во споредба со земјата која се обидува врз неа да влијае, мора да биде економски ранлива; за целната земја не смеат да бидат достапни алтернативни пазари, извори на снабдување и донатори. Во поглед на домашните ресурси, таа мора да биде дефицитарна во тоа што се сака да се скрати; мора да постои критична маса на незадоволство на домашната јавност која поради наметнатите санкции влијае на промена на политиката на целната држава; постоење целосна координација со другите инструменти на националната безбедност (полициски, воени, разузнавачки); во целната земја мора да постои економски потенцијал за развој во случај на примена на техники од спектарот наградување итн. Економскиот инструмент постигнува најголема ефикасност ако целната земја се карактеризира со големи слабости (нестабилност, внатрешна поделба и др.) и со ограничени можности. Во тој случај, нивната координирана употреба може да влијае на промена или останување на постојните политички ставови на целната земја во согласност со тежнеењето на државите кои ги преземаат таквите инструменти.

Покрај доминантното применување на економски инструменти од страна на економски развиени држави кон неразвиени земји, современата историја на меѓународните односи сведочи дека и малите и слаби држави можат да се здружат и да дејствуваат на слабите точки на големите и моќни земји, да влијаат на нивното надворешно политичко однесување. Пример за тоа се случаите на почетокот на 70-тите години на XX век, кога сите западновисокоразвиени земји биле зависни од изворите на нафта од Блискиот и од Средниот Исток. Земјите на производители на нафта од тоа подрачје (Organization of Petroleum Exporting Countries – OPEC), биле незадоволни од фактот дека државите

[318] Постојат примери дека сите овие инструменти, дури и на ниво на „економска војна“ ги применуваат дури и економски развиените земји.

на развиениот Запад застанале на страната на Израел со кој арапскиот свет бил во воен конфликт. Во таа насока, формирале заеднички блок насочен кон западните влади. Земјите членки на OPEC тогаш вовеле 5% месечно намалување на производството на нафта, а потоа и ембарго за извоз на нафта во одделни западни држави, како во САД и во Холандија. Нивната цел била да создадат енергетска пореметеност во високоразвиените западни држави со тоа што на тој начин би влијаеле на промената на политиката на тие земји кон блискоисточните прашања. Во таа ситуација, прва попуштила Јапонија која во состав на барањата на арапките држави, ја суспендирала дипломатската поддршка за Израел. Иако индиректно, својата надворешна политика кон Блискиот Исток, под востство на државниот секретар Хенри Кисинџер, ја промениле и САД, кои ја задржале дотогашната воена и политичката поддршка на Израел, но паралелно почнале да вршат притисок на Владата на Израел да пристапи на одредени територијални отстапки на спорните подрачја кон арапските соседи.[319]

3. ЗНАЧЕЊЕТО НА КОРПОРАЦИИТЕ ЗА ЕКОНОМСКАТА СТАБИЛНОСТ НА ДРЖАВИТЕ

Процесот на глобализација во претходната деценија довел до огромни економски меѓузависности на земјоделските субјекти од различните земји и на самата национална економија, како и во поглед на сè поголемиот обем и на сè поразгранетите форми на трансакција на добрата, на услугите и на капиталот, така и на сè побрзото ширење на дифузиите на технологијата.[320] Основната идеја што го наметнала таквото опкружување е во фактот што концептот на суверенитетот на националната држава и на економијата е нарушен и дека во светот се формираат нови регионални и транснационални сојузи и системи како регулатори на глобалната економија, меѓу кои клучни се големите транснационални корпорации.

Постои мислење дека денешното корпорациско насочувано глобално деловно опкружување во голем дел е глуво на принципите на

[319] Пошироко кај: Yergin Daniel, *The Prize: The Epic Quest for Oil, Money and Power*, Simon & Shuster, New York 1991., pp. 587-589.

[320] Според: *World Economic Outlook*, International Monetary Fund, Washington DC 1997., p. 94.

општествената праведност и солидарност, а ефиктите од досегашната коорпорациска глобализација се познати и препознатливи, како меѓу богатите, така и меѓу сиромашните делови на светот, но и меѓу општествените групи и слоеви во внатрешноста на секоја национална економија. Меѓутоа, истовремено, појавата на глобалното светско управување што го спроведуваат транснационалните корпорации, коренспондира и со развојот на „глобалните цивилни општества", односно со појавата и вмрежувањето илјадници доброволни, невладини асоцијации насекаде во светот како ATTAC, Amnesty International, Greenpeace и многу други. Оние што непосредно го чувствуваат економскиот, политичкиот и општествениот ефект на глобалното бизнис опкружување како и сè помоќните, покажуваат подготвеност да му се спротистават на сето тоа.[321]

Некои автори укажуваат на тоа дека корпорациите имале клучна улога во трансформацијата на меѓународната економија, и, во продолжение, на светската монетарна криза од 2008 година, и тоа на различни начини: како трговци, инвеститори, актери кои ја шират технологијата и поттикнуваат луѓе и ги динамизираат врските помеѓу различните пазари. Извесно е дека мултинационалните коорпорации успеале и во услови на светска криза да го консолидираат своето производство на сè повеќе дерегулираниот глобален пазар и во околности на постоење ефтина работна сила, капитал и поволни производствени услови на неразвиениот светски Југ, дополнително ја зајакнуваат профитабилноста на капиталот. Нивната можност да го уништат производниот процес преку редица посебни, дисклоцирани фази во светот ја промени природата на глобалното производство.

Глобалната мрежа на транснационалното производство им овозможила на корпорациите, како што се: Nike, General Motors или Volkswagen, да произведуваат, да дистрибуираат и да ги пласираат своите производи на глобално ниво. Исто така, овие транснационални производни мрежи ја јакнат силата на глобалниот капитализам така што им олеснуваат транснационалните компании да ги заобиколат националните работнички синдикати кои треба да ги штитат интересите на вработените во поглед на висината на дневницата и условите на нивната работа.[322]

---

[321] Види: Blomstrom Magnus, Hettne Bjorn, *Development Theory in Transition: The Dependency Theory and Beyond -Third World Responses*, Zed Books, London 1998., pp. 59-62.

[322] Ђурић Кузмановић Татјана, Вуковић Марија, оп. цит. стр. 34.

Во врска со проценатa на влијанието на корпорацијата на економска стабилност на државата, Анри-Мишел Буше дефинирал општ ризик на земјите како симбиоза на различности поврзани со инвестициите на корпорациите во одредена држава. Во таа смисла, сите бизнис трансакции на компаниите вклучуваат и одреден степен на ризик што е поврзан за повраќање на вложените средства и профитабилност на трансакцијата или инвестицијата. Трансакцијата на капиталот надвор од границата на една земја носи со себе одредени дополнителни ризици, кои се поинакви од ризиците кои ги имаат во домашните економски субјекти. Во тој контекст, основните компоненти на ризици на земјите на бизнис корпорација Бише ги дели на две групи: компонента која е можно да се квантифицира и да се процени (економски ризик, финансиски ризик и ризик на промена на девизниот курс) и компонента која се опишува како квалитативна и чија што процена е комплексна (политички ризик, културолошки ризик, ризик поврзан со правната рамка на земјата, регионален ризик и системски ризик – глобална криза).[323]

4. ВЛИЈАНИЕТО НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВРЗ ЕКОНОМСКАТА СТАБИЛНОСТ НА ДРЖАВАТА

Според Ж. Добрановиќ, воведувањето на пазарната економија во земјите во транзиција води кон ширење на приватната сопственост, пораст на економската размена, појава на нова работа, создавање средна и виша класа, зголемување на странската инвестиција и приватизирање на претпријатијата. Сите тие промени се ранливи на криминал и на други облици на загрозување и оттука потребата за услуги на корпорацискатa и на приватната безбедност. Во понови околности, претприемачите и компаниите ангажираат телохранители, финансиските институции бараат физичка заштита на своите објекти и блиндирани автомобили за транспорт на пари, припадниците на средната класа купуваат електронски алармен систем за своите домови, а корпорациите ангажираат консултанти за развивање на системот за безбедност и заштита. Во тоа земјите во транзиција не се разликуваат многу од земјите на развиената

[323] Види: Bouchet Henry-Michel, „Country Risk Analysis“, *Master in International Finance (MscIF)*, Global Finance Center & University of Westminster, London 2008., pp. 6-11.

демократија, затоа што заедничка цел им е да се изнајдат мерки, системи и начини за спречување евентуални загуби.[324]

4.1. ФУНКЦИОНИРАЊЕ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО НОРМАЛНИ ЕКОНОМСКИ УСЛОВИ

Според оценатa на М. Даничиќ и Љ. Стајиќ, еден од приоритетите во работата на секоја современа корпорација е обезбедување соодветна заштита на вработените, на менаџментот, ма имотот и на бизнисот на компанијата. За таа цел, внатре во деловниот субјект се воспоставува соодветен „систем на обезбедување" што треба да овозможи ефикасна заштита на компанијата од сите извори и носители на загрозување. Во состав на тој систем на корпорациска безбедност, надлежните субјекти дејствуваат на превентивен и на репресивен начин, за да се спречат различни облици на криминал и асоцијални активности и да се откријат кривични дела, т.е. отстранување други закани и облици на загрозување на имотот. Врз основа на тоа, системот за обезбедување на корпорацијата, според овие автори, претставува составен дел од системот за безбедност во општеството, што се состои од повеќе потсистеми на безбедност и во чии рамки субјектите на системот за обезбедување остваруваат соработка со цел заштита на виталните вредности.[325] Исто така, Даничиќ и Стајиќ наведуваат дека внатрешните и надворешните обезбедувања во компаниите на просторот на Балканот, најчесто организациски се поставени во облик на служба за физичко обезбедување, што ја сочинуваат раководен кадар и непосредни извршители. Таа служба се состои од одреден број обучени лица кои поседуваат оружје и соодветна опрема и нејзината задача е обезбедување на имотот и на работата на компанијата со сите нејзини вредности и интереси. Во таа смисла, физичката заштита претставува заштита на лица, имот и на работењето од уништување, оштетување, присвојување и други облици на дејствување кои се опасност за здравјето и животот на луѓето, и за материјалната и за нематеријална сопственост на компаниите. Под работи на техничкото обезбедување на компаниите, овие автори подразбираат механичка, електронска и оптоелектронска заштита на лица и имот. Наведените работи, најчесто се организациско поставени во рамките

[324] Добрановић Жељко, оп. цит. стр. 227.

[325] Даничић Милан, Стајић Љубомир, *Приватна безбједност*, оп. цит. стр. 19.

на службата за безбедност во компаниите каде што се организирани такви служби. Техничка компонента на безбедност се спроведува со примена на механички и на електронски средства на заштита и опрема наменета за таа потреба.[326]

Г. Мандиќ укажува на тоа дека безбедносниот менаџмент на корпорацијата функционално ги поврзува физичката и техничката компонента на системот за обезбедување во компаниите, давајќи им нови содржини кои квалитетно го подигаат на повисоко ниво целокупниот систем на обезбедување на имот и работењето на деловниот субјект. Овој вид зашита е насочен кон човекот како важен фактор на секој систем за обезбедување и неговите односи кон внатрешното и надворешното опкружување. Во таа смисла, безбедносниот менаџмент, според Мандиќ, ја опфаќа заштитата на имотот и на целокупното работење на компаниите, влучувајќи ја организацијата и правната регулатива. Тој смета дека предметот на интерес на безбедносниот менаџмент го сочинуваат: субјекти на обезбедување, носители и облици на загрозување, метод на прием на нови вработени, превенција – спречување насилство на работното место, проактивни и реактивни мерки на обезбедување на лица и имот, култура на работна заштита и комуникација која опфаќа правила на работен бон-тон со сегменти на заштита, зашита на информации и на информатичкиот систем, безбедносна процедура, заштита на интелектуална сопственост, обука на раководиот кадар и на сите вработени, задолжителна проверка на бонитетот, заштита на називот и заштитниот знак на фирмата и др.[327]

4.2. КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО УСЛОВИ НА ЕМБАРГО

Според дефинициите на некои автори, економските санкции претставуваат унилатерални принудни мерки со кои од политички, од економски или од воено-стратегиски причини се казнува одредена држава, најчесто спротивно на основните принципи на Повелбата на Обединетите нации.[328] Најчести политички цели за воведување санкции се дестабилизација или сквернавење на некоја странска влада, додека економски причини можат да бидат казнување на некоја земја поради нејзиниот пробив на одреден пазар или заштита

[326] Исто., стр. 20.

[327] Мандиќ Горан, *Системи обезбеђења и заштите*, оп. цит. стр. 177-178.

[328] Стајиќ Љубомир, Гаћиновиќ Радослав, op. cit. стр. 273.

на домашното производство. Меѓу најважните воено-стратегиски причини за воведување надворешни економски санкции спаѓаат зачувување на сопствениот монопол за прозводство на вооружување и воена опрема, слабеење на воениот потенцијал на земјата која е жртва на казнените мерки, како и спречување продажба на воено-стратегиски материјали на други земји.[329]

Со меѓународни или со унилатерални економски санкции, кои можат да опфатат различни мерки – од трговска блокада, забрана за меѓународен воздушен сообраќај, преку блокирање монетарни резерви во странски банки и запленување превозни средства и имот во странство, до оспорување членство во меѓународни економски, финансиски и политички организации, општо земено, се настојува на одредена држава да ѝ се оневозможи пристап кон стоки, технологија, услуги, пазар и капитал. Понови примери на спроведување вакви мерки биле делумни или целосни економски санкции кои од страна на Обединетите нации беа воведени за Родезија (1966-1979 година), за Јужна Африка во текот на владеењето на режимот на апартхејдот (1963-1994 година), за Либиска Џамахирија (1989-2003 година), за Ирак (1989-2005 година), за Сојузна Република Југославија (1992-2000 година), за Северна Кореја (од 2006 година) и за некои други земји.[330] Критичарите на економските санкции укажуваат дека тие не ги постигнуваат редовно прокламираните цели во вистинска насока. На пример, соборување недемократски режим (почесто ја зацврстува државата), но затоа во голема мера санкциите ја гушат економската самостојност на државата, придонесувајќи кон слабеење и уништување на националното стопанство, непосредно влијаат на падот на општествениот производ и на зголемување на невработеноста, на осиромашувањето на широките народни маси и загрозување на социјалниот мир.[331]

Ембаргото (од шпанскиот збор embargar – затворање) претставува забрана за тргување со одредени вредности, т.е. делумно или целосно престанување на стопанските односи со некоја држава, како вид казнување на таа земја во меѓународната

[329] Пошироко кај: Ковач Оскар, „Утицај санкција на функционисање и реформу привреде Југославије“, *Економска мисао* бр. 34, Београд 1994., стр. 118-121.

[330] Според: Cortright David, Lopez A. George, *The Sanctions Decade: Assessing UN Strategies in the 1990s*, Lynne Rienner, Boulder CO 2000., pp. 221-223.

[331] Стајић Љубомир, Гаћиновић Радослав, op. cit. стр. 275.

политика. Во практика, најчест е случајот група од неколку држави, обединети според принципот на зеднички интерес или идеологија, да објават ембарго на некоја друга држава, со намера да ѝ создадат тешка економска состојба и така да ја присилат на одредени отстапки кои се однесуваат на внатрешната или на надворешната политика. Таквите унилатерални казнени мерки, кои немаат поддршка во меѓународното јавно право, се воведуваат за да се оствари одредена конкретена надворешнополитичка цел на земјите кои ја покренуваат таа мерка.[332]

Меѓу воено-стратегиските причини за воведување ембарго кон некоја држава, се извојува чувањето на сопствениот монопол за производство на оружје и воена опрема, слабеење на воениот потенцијал на земјата која е жртва на мерките, како и спречување продажба на воено-стратегиски материјал на други земји.[333] Најзначајните последици од ембаргото се: задушување на економската самостојност на земјата, а со самото тоа и намалување на нејзината политичка самостојност, пад на општественото производство, осиромашување на населението и загрозување на социјалната стабилност на државата изложена на ембарго, хронична невработеност која, ако потрае, го загрозува економскиот и политичкиот систем на земјата, што е цел на оние што го покренале ембаргото.[334]

Историски гледано, помеѓу државите кои воведувале ембарго водат САД. Според истражувањето што го спровеле G.C.Hufbauer, J.J.Schott и K.A.Elliott, во периодот од 1914 до 1983 година од 100 случаи на економско ембарго кон други држави, 53 вовеле САД.[335] Образложението за ембарго главно било „воспоставување

[332] Види пошироко: Smeets Maarten, „Conflicting Goals: Economic Sanctions and the WTO", in: *Global Dialogue*, Vol. 2, No. 3, Centre for World Dialogue, Nicosia, Cyprus, Summer 2000 (http: www.worlddialogue.org/content.php?id=100).

[333] Види: Ковач Оскар, „Утицај санкција на функционисање и реформу привреде Југославије", *Економска мисао* бр. 34, Београд 1994., стр. 124-126.

[334] Савић Андреја, Стајић Љубомир, оп. цит. стр. 178.

[335] САД во тој период покренале економско ембарго (против некои земји и повеќе пати) кон: Јапонија, Аргентина, Холандија, Советскиот Сојуз, Кина, Северна Кореја, Иран, Израел, Велика Британија, Франција, Лаос, Виетнам, Доминиканската Република, Куба, Цејлон, Бразил, Обединетите Арапски Емирати, Индонезија, Чиле, Индија, Перу, Пакистан, Уганда. Јужна Кореја, Турција, Јужна Африка, Камбоџа, Уругвај, Тајван, Етиопија, Парагвај, Гватемала, Никарагва, Ел Салвадор, Либија, Ирак и Полска.

демократија" и „постигнување напредок на планот на остварување на човековите права", а причини за пристапување кон казнени мерки во најголем број случаи биле дестабилизирање на владите на тие земји и постигнување на сопствени надворешнополитички интереси.[336]

Денес во стручната и во политичката јавност сè повеќе се поставува прашањето за оправданост и ефикасност на ембаргото како начин на борба против режимот во одредена држава, бидејќи тој во практиката не ја погодува владејачката елита, туку главно доведува до пораст на криминалот и корупцијата, како и до пад на стандардот на ниските и на средните слоеви на општеството во земјата кон која се воведува ембарго. Исто така, ембаргото често се користи како средство со кое големите и моќни држави културно, економски, воено и на други начини ги потчинуваат малите земји. Определени автори[337] укажуваат дека досегашните искуства со примената на санкција покажуваат дека тие не ја поткопуваат поддршката на режимот против кој се насочени, туку често и ја зголемуваат, за што сведочат и современите примери на Куба, Ирак, Мјанмар, Северна Кореја, Либија, но и примерот на некогашната Италија на Мусолини, против која, исто така, своевремено биле воведени санкции од тогашната Лига на народите.[338]

Како што истакнува Александар Лојпур, „нема ниту еден пример во светот дека целната политичка група го сменила своето однесување поради санкциите, а во историјата не постои пример трговските ембарга или некоја слична економска мерка да се покажале успешни, без разлика на намерите на оние што ги воведуваа санкциите".[339] Според него, „санкциите ја чинат секоја комерцијална активност нелегална и му овозможуваат на режимот да ги малтретира сопствениците и деловните луѓе, при што корумпирањето е единствен начин да се одвиваат работите во

[336] Според: Hufbauer C. Gary, Schott J. Jeffrey, Elliott A. Kimberly, *Economic Sanctions in Support of Foreign Policy Goals*, Institute for International Economics, Washington DC 1983., p. 53.

[337] Според: Бранковић Србобран, „Санкције и став Запада према Србији", во: *Економске санкције УН – упоредна анализа и случај Југославије*, Институт за европске студије, Београд 1998., стр. 28.

[338] Howse L. Robert, Genser M. Jared, „Are EU Trade Sanctions on Burma Compatible with WTO Law", in: *Michigan Journal of International Law*, Vol. 29, No. 2, University of Michigan Law School, Ann Arbor MI 2008., pp. 186-195.

[339] Види: Лојпур Александар, „Девет добрих разлога за укидање санкција", *Време* број 466, Београд, 11. децембар 1999.

услови на ембарго“. Исто така, „владеењето на сивата економија и на корупцијата доведува до морално распаѓање на општеството во целост, а во такви околности целниот режим може само да профитира“. Според Лојпур, „нема транзиција од затворено во отворено општество без директно изложување на економијата на тоа општество на странски инвестиции и конкурентност на пазарот; санкциите секоја инвестиција од овој вид ја претвораат во криминал, а извозот го прават целосно невозможен, што не само што ја спречува транзицијата, туку и ја уништува економијата на државата која е под санкции“.[340]

4.3. КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО УСЛОВИ НА БОЈКОТ

Како што истакнува С. Мијалковиќ, политиката на економскиот протекционизам е насочена кон настојување на државната власт под паролата „заштита“ на сопствениот пазар, кај сопственото население и стопанските субјекти да фаворизира купување домашни, со повикување на бојкот на странски производи и суровини. Повиците на бојкот може да бидат насочени и кон само една држава, а во тој случај се даваат други образложенија.[341]

Терминот бојкот подразбира избегнување на увозот и купување на одделни или сите стоки кои доаѓаат од некоја држава, како и тргување со истата и некористење на нејзините услужни дејности. Актуелен пример за тоа е од пред 50 години, речиси целосен американски бојкот на кубанските стоки и услуги (составен дел на трговското ембарго на САД кон Куба, кое се применува од 1961 година).[342]

Познати историски примери на помалку или на повеќе успешни бојкоти биле прекин на увоз и избегнување на купување на британска стока од страна на американски доселеници во текот на војната за независност на Соединетите Американски Држави во текот на 70-тите и 80-тите години на XVIII век, повеќегодишниот бојкот на британската текстилна индустрија, покренат во колонијалната

[340] Исто, Лојпур Александар.

[341] Мијалковић Саша, *Национална безбедност*, оп. цит. стр. 220.

[342] Според: Schulz E. Donald, „The United States and Cuba: From a Strategy of Conflict to Constructive Engagement“, in: *Journal of Interamerican Studies and World Affairs*, Vol. 35, No. 2, Center for Latin American Studies, Miami FL, Summer 1993., pp. 91-93.

Индија од страна на движењето Swaraj на Махатма Ганди,[343] кој придонел за стекнување независност на таа земја, бојкотот на јапонската стока во Кина по Првата светска војна, антисемитскиот бојкот на еврејските фирми во нацистичката Германија од 30-тите години на XX век,[344] бојкотот на корпорацијата Ford од страна на Евреите во САД, во текот на 20-тите години на XX век поради антисемитизмот на нејзиниот основач Хенри Форд и други.

4.4. КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО УСЛОВИ НА ЕКОНОМСКА БЛОКАДА

Економската блокада вклучува употреба или закана за употреба на воена сила за некоја земја или за нејзин дел и да се оневозможи нејзино снабдување со клучни материјални добра (храна, енергенси, сировини, оружје, воена опрема, современа технологија и друго). Блокадата не треба да се меша со ембаргото и со економските санкции, кои претставуваат правни пречки на слободната трговија, ниту пак со опсадата, која по правило се однесува на ограничени локации. Во текот на историјата, речиси сите економски блокади се спроведени од море,[345] но во последно време блокадите се спроведуваат и преку земјен прекуграничен транспорт, како и преку националниот воздушен простор. Можност за воведување меѓународна економска блокада врз основа на одлуката на Советот за безбедност на Обединетите нации, е предвидена во член 42 од Повелбата на ООН. Во пракса тоа било применето за време на Корејската војна (1950-1953 година).[346]

Еден од најпознатите историски примери за економска блокада е целосната забрана за трговија т.н. континентална блокада на Велика Британија (Blocus Continental), која е спроведена од 1806 до 1814 година, со цел таа земја да се присили на потпишување мир. Споменатата блокада ја иницирала Франција, со која владеел Наполеон I, а во неа учествувале повеќе земји од континентална

[343] Види: Parel Anthony, *Hind Swaraj and Other Writings of M.K.Gandhi*, Cambridge University Press, Cambridge UK 1997., pp. 189-190.

[344] Erenreich Eric, *The Nazi Ancestral Proof*, Indiana University Press, Bloomington IN 2007., pp. 165-167.

[345] Пошироко види: Reynolds G. Clark, *Navies in History*, Naval Institute Press, Annapolis MD 1998., pp. 237-238.

[346] Според: D'Amato A. Anthony, *International Law and Political Reality: Collected Papers (Volume One)*, Kluwer Law International, The Hague NL 1995., p. 138

Европа. Спроведената блокада на Велика Британија во основа била неуспешна, а од неа значителна штета претрпеле токму земјите од европскиот континент кои учествувале во неа.[347] Најнов пример на унилатерална економска блокада претставуваат сеопфатните мерки кои во текот на 2010 и 2011 година ги спроведува Израел во појасот Газа.

[347] Hecksher F. Eli, „Continental Blockade“, in: Westergaard Harald (ed.), *The Continental System: An Economic Interpretation*, Clarendon Press, Oxford UK 1922., pp. 82-84.

IV глава

ВЛИЈАНИЕТО НА КОРПОРАЦИСКАТА ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ ВО ДОМЕНОТ НА СПРЕЧУВАЊЕ ОРГАНИЗИРАН КРИМИНАЛ

1. ЕВОЛУЦИЈА И ПОСЛЕДИЦИ ОД ОРГАНИЗИРАНИОТ КРИМИНАЛ ВРЗ НАЦИОНАЛНАТА И ВРЗ КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Организираниот криминал и покрај тоа што долг период бил поврзан само со одредени нации и со специфични географски подрачја, во последните децении на XX век, почнува да се третира како вистински меѓународен проблем, што го привлече вниманието на бројни меѓународни организации, на државни институции и на јавното мислење во многу земји, што резултира со многубројни иницијативи за одлучна и ефикасна борба против оваа појава. Изразот организираниот криминал се до крајот на 80-тите години од минатиот век во светот се користел како фраза со која се означува ескалација и загриженост на националните институции и поединци, во врска со експанзија на внатрешни и на меѓународни криминални пазари, со сè поголемата мобилност на носителите на криминално дејствување преку националните граници и штетата која организираниот криминал ја нанесува на легалното работење и на економските движења како и криминалното рушење на демократските политички институции.[348]

Со злоупотреба на технолошкиот развој се појавуваат нови видови организиран криминал (компјутерски криминал и др.) или се усовршува самиот modus operandi. Развојот на современата телекомуникација им овозможува на организираните криминални групи договор и злосторничко планирање и на најголеми далечини, притоа неоставајќи никаква трага. Во која мера криминалците ќе ја злоупотребат техниката, меѓу другото, зависи и од обемот на материјалните средства со кои располагаат.Тој обем во денешно време е енормно голем, дури и во оние земји во кои националниот приход е низок. Во рацете на припадниците на организираниот

[348] Според: Paoli Letizia, Fijnaut Cyrille, „Organised Crime in Europe: General Introduction“, in: Paoli Letizia, Fijnaut Cyrille (eds.), *Organised Crime in Europe: Manifestations and Policies in the European Union Beyond*, Springer, Dordrecht NL, 2003., pp.1-2.

криминал се слева сè поголем капитал. Со тоа и нивното настојување да ја освојат власта, притоа не бирајќи средства за таа цел.[349]

Во Југоисточна Европа даночните и царинските измами и криминалот во приватизацијата имале поголемо значење отколку традиционалниот организиран криминал. Разликата меѓу легалниот деловен субјект што се служи со нелегални економски средства и приходи од криминални активности инвестира во нешто што изгледа дека е законска економска активност, од една страна, додека организираните криминални групи формирани со цел извршување стопански криминал од друга страна не се истакнати. Дополнителното инвестирање на приходите од криминалните активности во легалната економија е проследено со корупција, со што се поставува сериозно прашање за легитимноста на управувачките структури на овие земји. Во повеќе држави од просторите на поранешна СФРЈ во почетокот на 90-тите години од XX век значаен дел од производните стопански капацитети е уништен во војни или е сериозно запуштен, што за последица имало губење на меѓународните пазари што тие капацитети некогаш ги снабдувале. „Изгубената деценија" во таа област ставила поголем акцент на трговијата со легална и со илегална стока, додека трошоците на регионалната трговија исклучително пораснале. Порастот на учеството на криумчарење во трговијата го следи истиот тренд, создавајќи погодна средина за организиран криминал, што во последната деценија од минатиот век се претворил во клучен механизам за незаконска прераспределба на националните богатства во Југоисточна Европа.[350]

Организираните криминални групи на просторот на ЈИЕ и понатаму се присутни во секторите на: градежништвото и трговијата со недвижности, продажбата на автомобили, игрите на среќа, забавата, коцкањето и проституцијата, фирмите за обезбедување, транспортот, компаниите за увоз и извоз, а особено се заинтересирани за секоја можност на профитабилна приватизација со оглед на тоа дека за сите горенаведени работи е карактеристичен

[349] Пошироко кај: Кривокапић Владимир, „Општа разматрања о организованом криминалитету и његовој превенцији", во: Маринковић Дарко (прир.), *Место и улога полиције у превенцији криминалитета – актуелно стање и могућности унапређења*, Криминалистичко-полицијска академија, Београд 2007., стр. 27.

[350] *CARPO Regional Project: Situation Report on Organised and Economic Crime in South-eastern Europe*, op. cit. p. 14.

интензивниот прилив на готови пари. Криминалните организации се сè повеќе софистицирани и професионални и се во состојба да го шират своето работење, вклучувајќи и инвестирање во акции на странски компании, креирање политики или учествување во финансиски холдинзи, до кредитирање или инвестирање во одредена компанија заради нејзино евентуално подоцнежно преземање.[351]

1.1. ИЛЕГАЛНИ ЕКОНОМСКИ АКТИВНОСТИ

Според Б. Добовшек најголемата опасност од дејствувањето на современиот криминалитет се манифестира во инвестирањето криминално стекнати пари во легални бизниси преку перење пари и корупција. Организираниот криминал настојува да влезе во легалната сфера на економијата и да стане нејзина конкуренција. На таквите криминални фирми не им е потребен почетен капитал за производство, а инвестициите се покриваат со пари стекнати од криминални активности. Таквите компании се конкурентни и полека ги уништуваат здравите фирми или пак ги купуваат. Преку политички притисоци, како и со други мерки државата овозможува овие компании да имаат разни поволности, односно победуваат на тендерите за јавна набавка. Ако се земе предвид, за повеќето активности од криминалниот спектар не плаќаат данок, тие стануваат невидливи и со тоа причинуваат голема штета на државата.[352]

Според Л. Шели, модерните криминални организации се профитабилно ориентирани и пазарно насочени, што во комбинација со криминалните методи, но и со методите што ги користат современите деловни организации, им се овозможува професионалност и ефикасност во дејствувањето. Евидентен е продорот на организираниот криминал во економската активност, односно вршење кривични дела од економскиот криминал со елементи на организирање и создавање криминални корпорации. Продорот во легалните економски движења им овозможува „учење“ и злоупотреба на современите техники на работење, што придонесува за софистицирано дејствување и ширење на сферата на влијание. На тој начин, економската моќ на организираниот криминал се користи за стекнување политичка моќ, а политичката моќ повратно се користи за остварување криминални цели. Така,

[351] Ibid., pp. 18-19.

[352] Добовшек Бојан, op. cit. стр. 3.

економскиот криминал станува закана за меѓународната и за националната безбедност. Со неговата интернационализација, последиците се поштетни, бидејќи криминалните организации брзо се приспособуваат на условите на меѓународното економско опкружување. Во тие околности на криминалните корпорации им се обезбедуваат редица погодности првенствено за пристап кон светските финансиски текови, различните криминални пазари, офшор финансиските центри и создаваат можност за процена на сопствениот ризик од кривично гонење за одделни категории на направени или планирани злосторства.[353]

Даночното олеснување што им се дава за странски инвестиции во земјите во транзиција се многу погодни за разни облици на криминал и корупција со цел избегнување на даночните обврски. Така, за време на траењето на ваквите олеснувања некои фирми се регистрираат како константни инвеститори во одредена област само додека траат олеснувањата за потоа да се пререгистрираат на ново име. Оваа појава е карактеристична за деловните субјекти на чие чело се наоѓаат граѓани со двојно државјанство, бидејќи ги искористуваат недоволно дефинираните прописи со цел да создадат вонредни приходи и неплаќање на данок на остварена добивка.[354]

1.2. ПОТТИКНУВАЊЕ НА КОРУПЦИЈАТА И ИНФИЛТРИРАЊЕ ВО ИНСТИТУЦИИТЕ НА СИСТЕМОТ

Организираниот криминалитет претставува еден вид класичен криминалитет во смисла дека крајната цел е постоење и дејствување организирани криминални групи за противправно стекнување профит. Тој вид криминал е од неидеолошки карактер, поради тоа тој не смее да се поистовети со некои облици на политички криминал, како што е тероризмот.[355] Од друга страна, организираниот криминал се обидува на различни начини да се инфилтрира во политичкиот систем на државата. Тоа првенствено го прави со финансирање политички и предизборни кампањи на одредени кандидати или

[353] Shelley I. Louise, „Transnational Organized Crime: An Imminent Threat to the Nation-State“, *Columbia Journal of International Affairs*, No. 48, Columbia University, New York 1995, p. 464.

[354] Бошковиќ Миѓо, Бошковиќ Александар, op. cit. стр. 68.

[355] Види: Шкулиќ Милан, *Организовани криминалитет*, Досије, Београд 2003., стр. 39.

партии и корумпирање на гласачкото тело на изборите, по пат на корупција или застрашување на активните политички фактори во државата.[356]

Корупцијата често се појавува како начин кој во извршувањето на криминалните работи го користи организираниот криминал со цел воспоставување и одржување на криминалните врски со влијателни поединци во политичката структура, во државни органи и во други области во општественото живеење. Притоа, организираниот криминал продира до одредени центри на политичка, на економска и на финансиска моќ, а на неговите шефови им овозможува стекнување моќ и им дава поголем општествен статус. Од тоа следуваат бенифиции да можат да вршат влијание врз политичките структури и врз државните органи (полиција, правосудство, царина и др.) и на тој начин да обезбедат нелегална активност на криминалните организации. Кога ќе се склучи договор меѓу државните службеници и криминалците службениците стануваат нивни клиенти, пред сè во смисла на финансиска поддршка и на физичка заштита.[357] Истовремено, криминалната организација станува клиент на корумпираниот службеник во смисла на административно фаворизирање и заштита на информациите. Меѓутоа, кога некоја страна, најчесто тоа е јавниот службеник, сака да го напушти криминалниот однос, доаѓа до проблеми бидејќи напушањето на која било страна го доведува до потенцијална опасност другиот. Ризикот државните службеници да бидат демаскирани од оние од кои примаат мито е мал, и на тој начин се стекнуваат со високи заработки.

Појавата на корупција кај државните службеници покажува дека државата ефикасно не управува со доверените стоки и услуги. Корупцијата нанесува двократна штета на државата бидејќи ги намалува нејзините приходи и го нарушува нејзиниот углед. Граѓаните кои имаат пари да платат мито, ја зголемуваат цената на стоките и на услугите, а оние што не можат да го платат митото, остануваат без стоки и услуги иако имаат право на нив.

Некои автори укажуваат дека една од суштинските карактеристики на организираниот криминал е неговото постоење како посебен општествен потсистем, односно налик на културна, економска и социјална диференцијација во современото оштество

[356] Савиќ Андреја, Стајиќ Љубомир, op. cit. стр. 161.
[357] Теофиловиќ Небојша, op. cit. стр. 545.

или дел на поширокиот општествен, економски и политички систем. Во рамките на тие карактеристики особено е важно настојувањето на организираниот криминал да извршува квази државни функции, како што се давање физичка заштита или нелагално даночење преку рекет, и на тој начин да биде сурогат на државната власт.[358]

1.3. ВНАТРЕШНИ ОПШТЕСТВЕНИ И ПОЛИТИЧКИ ПОСЛЕДИЦИ ОД ДЕЈСТВУВАЊЕТО НА ОРГАНИЗИРАНИОТ КРИМИНАЛ

Британскиот автор Питер Лупша направил типологија на опасности за државата од организираниот криминал, прикажувајќи го еволутивниот однос меѓу субјектите на организираниот криминал и државата, распоредени во три фази:

1) предаторска фаза, во која колективитетите на организираниот криминал постепено влегуваат во општествените движења на одредени држави, заобиколувајќи ги легитимните пазарни структури;
2) паразитска фаза во која криминалците влегуваат во деловниот свет, во локалниот и во регионалниот политички живот, со создавање „сива" зона во економијата и со постепено преземање на задачите од сличните државни функции.
3) симбиотска фаза, во која криминалните групи се целосни интегрирани во економските и во политичките институции на државата и поседуваат значајна политичка моќ.[359]

Според некои оцени, во текот 90-тите години од XX век, организираниот криминал во државите од Балканот според степенот на развиеност и според спрегата со властите, достигнал такво ниво што неговото потиснување се поставило како услов за опстанок, не само на владата, туку и на државата во целост.[360] Распространетата мрежа на организираниот криминал на Балканот си ги поставила како цели: избегнувањето контрола, зголемувањето на сопствената моќ, непочитувањето на законите, освојувањето

[358] Види: Von Lampe Klaus, „Critical Review of Conceptual Approaches", in: *Assessing Organised Crime (Research project)*, Freie Universität, Berlin 2004., p. 13.

[359] Lupsha Peter, „Transnational Organised Crime versus the Nation-State", in: *Transnational Organized Crime*, Vol. 2, No.1, Routledge, London 1996., pp. 31-38.

[360] Според: Лазић Младен, *Рачји ход: Србија у трансформацијским процесима*, Филип Вишњић, Београд 2000., стр. 36.

на власта во три етапи и претворање на дотогашните конкуренти во клиенти. Тоа го подразбирало следното: наместо замена за неказнување да им се помогне на политичарите во предизборните кампањи, првенствено во убедување на гласачите да гласаат за нив, со користење разни средства – од примена на сила до бесплатен превоз до гласачките места; обликување на моќта по завршување на изборите, преку спонзорство и уфрлување свои луѓе во партиската централа и во завршната фаза на оформување на моќта, правење фузија со политичарите и со носителите на големи бизниси, заради остварување влијание на одлуките на власта и остварување на своите нелегални интереси.[361]

2. КОРПОРАЦИСКАТА БЕЗБЕДНОСТ И СОЗДАВАЊЕТО КРИМИНАЛНИ КОРПОРАЦИИ

Процесите на глобализација, технолошкиот развој, либерализацијата и забрзување на протокот на информации, стоки, услуги и луѓе во глобални размери влијаеле и на промените на структурата на современото криминално организирање. Традиционалните форми на криминалните организации од мафијашки тип оддамна се заменети со структури кои овозможуваат дејствување на организираниот криминал во модерното опкружување и во глобални размери. Овие наведени тенденции особено се изразени во областа на финансиското работење, бидејќи криминалните организации во тие области најбрзо се приспособуваат на современото економско опкружување. Поради тоа криминалните структури во таа област најчесто се комплексни мрежни структури, во организациска смисла, и многу се блиску до класичните корпорации.[362] Некои автори укажуваат на тоа дека денешните криминални организации се профитно ориентирани и пазарно насочени, а нивните методи на работа се комбинација од криминални методи и методи на работа на современата организација, што ги прави многу поопасни за самото општество. Амбициите на таквите „нови“ криминални организации се движат од вршење влијание

[361] Марковиќ И. Слободан, op. cit. стр. 67

[362] Според: Di Nicola Andrea, Scartezzini Alessandro, „When Economic Crime Becomes Organized: The Roll of Information Technologies: A Case Study“, in: *Current Issue in Criminal Justice - Journal of the Institute of Criminology*, Vol. 11, No. 3, University of Sidney - Faculty of Law, Sydney 2000., p. 2.

на власта па сè до оформување на државата и редефинирање како и приспособување на нејзините функции со потфати за остварување на криминалните намери и цели.[363]

Организираниот криминал во современите услови тежнее кон користење на стопанскиот и на финансискиот сектор со цел да се замагли границата меѓу легални и нелегални активности, а со тоа би се овозможила интеграција на криминалниот профит во легалните економски движења. Во врска со тоа, одредени истражувања спроведени во Белгија укажуваат на тоа дека 75% од криминалните организации кои ѝ се познати на полицијата, кои дејствуваат во таа земја, во своите активности како покритие користат легални деловни структури, а во 49,1% случаи станува збор за легални стопански субјекти кои се формирани од страна на криминални организации кои се занимаваат и со легални и со нелегални активности.[364]

Модерните криминални корпорации се закана за многу земји кои преку приватизација спроведуваат економски реформи. Криминалните организации се способни преку аукција да ги исфрлат легитимните купувачи на претпријатија во државна сопственост, бидејќи нудат многу повеќе (валкани) пари и користат уцена, насилство и корупција. Преку откуп на претпријатијата, организираниот криминал го зголемува својот потенцијал за дополнителни криминални активности и корупција, а на земјата и го скратува легитимното пазарно заосновано стопанство кое плаќа данок. Приходите на криминалните корпорации, многу вешто се провлекуваат низ националните и меѓународните финансиски системи. Особено се значајни економските и социјални консеквенци на земјите во транзиција. Нивните пазари најчесто се мали и подложни на нарушувања кои можат да настанат преку криминалните активности. Ранливоста им е изразена и поради фактот што има и недоволно изградени институции во економско-финансискиот систем, немоќ на финансиските институции да применат мерки за идентификација и спречување на прикривање на потеклото и вложувањето во криминалниот профит, низок степен на мерки кои се имплементирани за сузбивање на организираниот криминал или нивна недоволна, односно селективна имплементација, неефикасни казни, вклучувајќи ги и одредбите за конфискација на незаконски стекнат приход кои тешко се спроведуваат, како и низок степен

[363] Види: Adamoli Sabrina, Di Nicola Andrea, Savona U. Ernesto, Zoffi Paola, *Organised Crime Around the World*, HEUNI, Helsinki 1998., p. 5.

[364] Бошковиќ Горан, op. cit. стр. 40.

на обученост и стручност на органите надлежни за сузбивање на економскиот криминал.[365]

2.1. КОРПОРАЦИСКИОТ КРИМИНАЛИТЕТ ВО ФУНКЦИЈА НА ОСТВАРУВАЊЕ НА ДЕЛОВНИТЕ ЦЕЛИ И ПРИДОБИВКИ НА КОМПАНИИТЕ

И покрај тоа што во литературата не постои општоприфатена дефиниција за корпорацискиот криминал, значен број автори тој феномен го сметаат за вид имотен криминалитет и криминалитет на „белите вратоврски", бидејќи криминалните дела се вршат на сличен начин, во сродна област, иако од различни мотиви. Поради тоа, Ѓорѓе Игњатовиќ смета дека корпорацискиот криминал и криминалот на „белите вратоврски" спаѓаат под широкиот поим на имотен криминалитет. Меѓутоа, додека кај криминалот на „белите вратоврски" преовладуваат личните користољубиви побуди, користа од делата на корпорацискиот криминал оди во компанијата, а не само кај извршителот.[366] Слично на него, Грунер смета дека корпорацискиот криминал е еден од облиците на извршување на криминалот на „белите вратоврски", додека другиот вид криминал се врши во делокругот на професијата (occupational crime).[367]

Злата Ѓорѓевиќ оценува дека подрачјата во кои се врши криминалната работа на корпорациите се хетерогени, т.е. тој вид криминалитет најчесто се врши во областа на економското работење (затајување данок, проневери, фалсификување пари, злоупотреба на стечај, кредитни и сметководствени измами, фалсификување деловна документација со цел измама на акционерите, кршење на правата на конкурентноста, перење пари, insider trading, трговска корупција и слично.) Таа укажува и на т.н. погоден организиран криминал, односно ситуации во кои повеќе деловни субјекти, кои работат законски, во дадена околност, заеднички и плански вршат одредени видови организирани криминални активности.[368]

---

[365] Повеќе види: Bartlett L. Brent, „Negative Effects of Money Laundering on Economic Development", *Economic Research Report for Asian Development Bank*, Asian Development Bank, Manila 2002., p. 31.

[366] Игњатовић Ђорђе, *Криминологија* (десето измењено и допуњено издање), Правни факултет, Београд 2010., стр. 110-112.

[367] Види: Gruner S. Richard, *Corporate Criminal Liability and Prevention*, ALM Properties Inc., Law Journal Press, New York 2005., p. 6.

[368] Đurđević Zlata, „Kaznena odgovornost i kazneni postupak prema pravnim osobama u Republici Hrvatskoj", *Hrvatski ljetopis za kazneno pravo i praksu*, Vol. 10, br. 2, Pravni fakultet, Zagreb 2003., str. 722-725.

Според Р. Кремер, корпорацискиот криминалитет е подвид на криминалот на „белите вратоврски“ и претставува криминален чин кој што е разултат на одлука на оние што во деловните субјекти се на менаџерски или на извршни позиции. Таквите одлуки организациски се формираат врз правилата на работење, на стандардната оперативна процедура и на општите норми на организацијата и се насочени кон остварување профит на корпорацијата.[369] Суштината на корпорацискиот криминал се согледува во планираните незаконски активности со цел зголемување на профитот преку директно или индиректно кршење на законите. Проблемот е во тоа што многу криминални активности во таа област не можат да се подведат во постојната инкриминација, а сторителите на тие дела го користат својот статус за да избегнат кривична одговорност. Профитно ориентираната економија најчесто не смета дека таквото кршење на законите има иста тежина како и кршењето на законот со „обични“ кривични дела, при што учесниците во легалното работење настојуваат на дискретен начин да направат одредени нелегални активности, бидејќи самото работење и тргување претрпува штета која е настаната со интервенција од органите за кривично гонење и јавниот публицитет.[370]

Посебна област на корпорацискиот криминал од меѓународен карактер е врзана со илегалниот увоз и производство на генетски модификувана храна. Впрочем, со генетското инженерство, финансирано од страна на мултинационалните корпорации,[371] се добиваат химерични конструкти, комбинации на структурни и регулаторни гени, често и од несродни организми, кои често ги заобиколуваат сите ограничувања на видот. На тој начин може да се комбинираат со гените на ниските и на високите видови билки, микроорганизми, инсекти и животни. Такви резултати не може да се добијат ниту со најнапредните конвенционални методи за исхрана. Според некои податоци, генетски модификуваните билки се произведуваат во 25 држави во светот, со тренд на постојано зголемување на површини кои се под овие култури (1.7 милиони

[369] Kramer C. Ronald, „Corporate Criminality: The Development of an Idea“, in: Hochstedler Ellen (ed.), *Corporations as Criminals*, Sage Publications, Beverly Hills CA 1984., p. 87.

[370] Според: Мршевић Зорица, *Организовани криминал*, Институт за криминолошка и социолошка истраживања, Београд 1993., стр. 95.

[371] Monsanto, Sandoz, Aventis, Novartis и друге.

хектари во 1996 година, во споредба со 134 милиони хектари во 2009 година). Импресивното ширење на споменатата технологија предизвика глобална, по својот обем, незапамтена дебата, поларизирајќи ги научниците, корпорациите и другите производувачи на храна, потрошувачите, интересните групи и државните елити.[372]

Постојат големи несогласувања во врска со еколошките, здравствените и општествено – економските последици од употребата на генетски модифицираната храна, при што поборниците на „теоријата на завера" дури сметаат дека некои од модифицираните билки (пченката, пред сè) е ново биолошко оружје, кое САД го користат во борбата против непријателот, а со цел остварување на целта за светска депопулација, под изреката за намалување на бројот на гладните.[373]

Според некои автори, во последната деценија во земјите на Европската унија е присутен развојот на еколошкиот криминал, односно активности почнати со намера да се предизвика или потенцијално да настане штета на еколошките и/или биолошките системи заради постигнување деловно или приватно богатство. Станува збор за неколку области на илегално дејствување во кои се вмешани и легални компании за: сечење и трговија со шумска граѓа, непријавено рибарење, превоз и истовар на ризичен отпад (расипан, биомедицински, хемиски и метален отпад). Растот на овој вид криминално дејствување е предизвикан од зголемените трошоци за законско отстранување на ризичниот отпад и недостатокот на слободен простор на постојните регистрирани места наменети за исфрање отпад. Според одредени процени, во Европската унија годишно остануваат околу 150 милиони тони високоризичен токсичен отпад, од кој само 15% се рециклира и се исфрла во складовите според постојните прописи.[374]

---

[372] Види: Папиќ-Бранков Татјана, Ловре Ковиљко, Тањевиќ Наташа, „Принципи анализа ризика у производњи генетски модификоване хране", *Ecologica*, вол. 17, бр. 57, Научно – стручно друштво за заштиту животне средине Србије – Ecologica, Београд 2009., стр. 27-29

[373] Папић Татјана, Ловре Ковиљко, „Политика мултинациналних компанија у производњи генетски модификованих биљних култура", *Економика пољопривреде,* vol. 55, бр. 4, Институт за економику пољопривреде, Београд 2008., стр. 391–394.

[374] Според: Clifford Mary, *Environmental Crime: Enforcement, Policy, and Social Responsibility*, Aspen Publishers, Gaithersburg, MD 1998., pp. 26-27.

Одредени автори[375] укажуваат дека стапката на смртни случаи во светот предизвикани од корпорациите е шест пати поголема од стапката на смртните случаи предизвикани од уличниот криминал, а стапката на повреда на работно место, која нема смртен исход, е околу 30 пати поголема од стапката на улични кражби, од што може да се заклучи дека работниците се многу посигурни на улица отколку на своето работно место. Се истакнува и дека работите поврзани со корпорацискиот криминалитет се доста замрсени, се комплексни и се доста софистицирани начини на кршење на законите, кои многу тешко се разоткриваат поради многу сложената внатрешна организациска структурна мрежа на овој вид криминал, како и поради можноста за манипулирање со временските рокови во кои ваквите случаи се обелоденуваат, често придонесуваат за консензуална природа на незаконско однесување и многу дифузен карактер на виктимизација.[376]

Во основа, корпорацискиот криминал, најчесто ги погодува земјите од т.н. Трет свет, кои често се изложени на дампинг производи, забранети стандарди кои се применуваат во развиениот свет, насилни корпорации поради аерозагадување и други видови еколошки криминалитет.[377] Во врска со ова, американскиот online магазин Newsweek/The Daily Beast од Њујорк, во јуни во 2010 година, објави листа на 13 најомразени корпорации во историјата[378], изработена во соработка со група еминентни историчари: Standard Oil – монопол; Union Carbid – имаат отруено повеќе од десетина илјади луѓе во Индија; Exxon – еколошка катастрофа на Аљаска; United Fruit Company – подмитување политичари; International Telephone & Telegraph – подмитување на политичари; British Petroleum – еколошка катастрофа во Мексиканскиот залив; Microsoft – монопол; Goldman Sachs – измама на инвеститори; Nestle – труење бебиња во Африка од млеко во прав; Blackwater – силување и убивање цивили во Ирак; Monsanto – еколошка катастрофа; Halliburton – воено профитерство; Drexer Burnham – измами во тргување со акции.

---

[375] Schwartz Martin, Dekeseredy Walter, *Contemporary Criminology*, Wadsworth Publishing Company, Belmont CA 1996., p. 367.

[376] Според: Reiman Jeffrey, *The Rich Get Richer and the Poor Get Prison: Ideology, Crime and Criminal Justice*, Allyn & Bacon, Boston 1995., pp. 55-56.

[377] Кековиќ Зоран, оп. цит. стр. 224.

[378] „History's 13 Most Hated Companies", (http:www.thedailybeast.com/articles/2010/06/22/the-most-hated-companies-everhow-did-bp-score.html)

На врвот на споменатата листа се нашла нафтената компанија Standard Oil која е формирана од Џон Рокфелер. Иако денес претставува синоним за алчноста на големите корпорации, на крајот од XIX век, оваа компанија била мошне почитувана и според тоа ги „голтала“ помалите фирми и на тој начин создала монопол. Впрочем, Standard Oil ги поткупувала клучните играчи за преработка, за транспорт и за продажба на нафтени деривати и на тој начин го заокружила целиот процес од вадењето на нафтата до продажбата на дериватите на крајните потрошувачи. Поради монополскиот статус, со интервенција на Американската влада, корпорацијата во 1911 година била поделена на 34 помали фирми што значело и крај на царството на Standard Oil. На втората позиција се наоѓа Union Carbid, компанија која е одговорна за најсмртоносната индустриска катастрофа во историјата. Всушност, во 1984 година, од хемиска фабрика во индискиот град Бопал истекле околу 45.000 тони отровен гас, кој веднаш по истекувањето усмртил 5000 луѓе. Во наредните години како последица од труењето умреле помеѓу 15000-20000 лица, а претпоставките се дека околу 100000 граѓани на Индија и ден-денес имаат здравствени проблеми како последица од тоа труење.

Трето место на листата на најомразените се наоѓа нафтената компанија Exxon од чиј танкер „Exxon Valdez“ во 1989 година покрај брегот на Аљаска се излеале повеќе од 270.000 барели нафта покривајќи површина со големина од 11.000 квадратни милји. Сè до експлозијата на нафтената платформа на British Petroleum во Мексиканскиот Залив, на крајот од април 2010 година, тоа била најтешка нафтена катастрофа во американската историја, која таа компанија ја чинело околу 10 милијарди долари и која вовела нови прописи за транспорт на „црното злато“.

Корпорацијата United Fruit Company која е позиционирана на четвртото место, Newsweek/The Daily Beast, го создала поимот „банана република“. Впрочем, таа компанија вршела константен притисок на владите во државите во Јужна Америка со цел тие да бидат пријателски настроени кон нивната работа во тргувањето со овошје, а во Гватемала дури организирале и политички преврат. Уште една корпорација поврзана со јужноамериканскиот континент се наоѓа на листата, а тоа е телекомуникацискиот гигант International Telephone & Telegraph (ITT). Таа компанија, која се наоѓа на петтото место на листата била сопственик на чилеанската фирма Chilteco, преку која го финансирала противничкиот кандидат на претседателот Салвадор Алјенде. Кога по три години Алјенде, кој ги добил изборите, бил соборен и убиен, откриено е дека во сè била вмешана ITT.

Корпорацијата British Petroleum (BP), која се наоѓа на шесто место, одговорна е за најголемата еколошка катастрофа во светската историја. Аналитичарите проценуваат дека BP мора да исплати повеќе од 20 милијарди долари оштета заради тоа што дозволила повеќе од 900.000 тона нафта да се излеат во Мексиканскиот Залив. На седмо место е Microsoft, компанија на најбогатиот човек во САД, Бил Гејтс, поради монопол на светскиот пазар. Оперативниот систем на Microsoft не е компатибилен со другите компјутерски системи. Оваа корпорација има ексклузивни договори со продавниците на компјутерска опрема а има контрола врз цената и врз пазарната доминација на глобално ниво. Седма на листата се наоѓа инвестициската компанија Goldman Sachs, која моментално се наоѓа под истрага на Американската влада, бидејќи е откриено дека ги притискала своите клиенти на ризични вложувања, за подоцна да се клади дека инвестициите на нивните клиенти ќе пропаднат.

Прехранбената индустрија Nestle го зазема деветтото место на оваа листа на светски најомразени корпорации поради аферата во 1977 година со млеко во прав за бебиња. Оваа корпорација е тужена дека нејзиното млеко во африканските земји предизвикало смрт кај доенчињата. Десетото место е резервирано за приватната воена компанија Blackwater, чии агенти биле поврзани со низа контроверзи, од тужби за силување во Ирак па сè до неконтролирано отворање оган кон цивилното население. Компанијата Monsanto (испитување и производство на генетски модифицирани оранизми) се наоѓа на единаесетото место поради излевање на 80.000 литри отровни хемикалии за обработка на дрва во реката Мисури во САД. Компанијата Halliburton на поранешниот потпретседател на САД, Дик Чејни, го завзема дванаесетото место, бидејќи во Ирак, веднаш по почетокот на војната, меѓу другото продавала и WC-школки за цена од 1.000 долари, а чекани за цена од 600 долари. Оваа корпорација набрзо потоа стана синоним за воено профитерство. На последно, тринаесето место на оваа листа се наоѓа инвестиционата банка, Drexel Burnham, чиј финансиски тајкун Мајкл Милкен во 1986 година е осуден за измама во трговијата со меници. Банката потоа и банкротирала, а Милкен послужил како инспирација за главен лик во филмот Wallstreet.

2.2. ДАНОЧЕН КРИМИНАЛ ПРЕКУ ИЗМАМИ ВО ФИНАНСИСКИТЕ ИЗВЕШТАИ

Ефикасноста и ликвидноста на работењето на компаниите во финансиските пазари е условена од бројни фактори. Некои од нив се резултат на објективни околности, додека пак, други се од

субјективна природа, но сепак треба да се нагласи дека како ќе успее корпорацијата да се одржи на пазарот зависи од нејзините финансиски перформанси кои се значаен индикатор за тоа што значи компанијата и во која насока ќе оди нејзиниот развој. За да ја прикрие објективната реалност имаме ситуации во кои корпорациите преку нивните финансиски извештаи ги искривуваат бројките за да се создаде лажна претстава за успешноста на компанијата со цел да не се загрози нејзината позиција на пазарот. Кога се прави определена измама секогаш се настојува да се постигне очекуваното, а тоа е фингирање на: приходите, добивката, загубите, трошоците итн. Значи, од една страна постои нагласување на приходната страна, побарувањата, добивката и друго, додека од друга страна има условно истиснување конкретни бројки како реални показатели во однос на загубите, на трошоците и на обврските кои ги има компанијата кон договорените странки.

Генерално прифатена дефиниција за измамите во финансиските извештаи е намерно погрешно претставување на финансиската состојба во која се наоѓа корпорацијата, преку намерно погрешно прикажување или испуштање на износи или обелоденувања со цел да се измамат корисниците на финансиските извештаи. Измамата, исто така, вклучува фалсификување, промена или манипулација со финансиски записи, документи или бизнис трансакции, материјални намерни пропусти или погрешни интерпретации на настаните, на трансакциите или на сметките и на други значајни информации од кои што се подготвени финансиските извештаи. Како измама се смета и неправилната примена и апликација на сметководствените принципи, политики и процедури кои се користат за да се измерат, да се препознаат и да се објават економските настани и бизнис трансакции. Измамата на раководниот менаџмент често се смета како синоним за измамите во финансиските извештаи бидејќи подготвувањето на финансиските извештаи и нивната презентација е одговорност на раководниот менаџмент. Ако има измама во финансискиот извештај менаџментот речиси секогаш знае за неа.[379]

Секоја измама има три основни елементи, и тоа: 1). осознаен притисок, 2). осознаена можност и 3). способност да ја рационализираме измамата како прифатлива. Без разлика дали станува збор за измама против компанијата како проневера од

[379] Everett E. Colby, B. *Financial statement fraud*, part 1, Professional Development Network, 2011, pp.1-2.

работници или измама во име на компанијата како измама во финансиските извештаи овие три елементи секогаш се појавуваат и се познати како триаголник на измами.[380]

2.3. ВОЕНО ПРОФИТЕРСТВО

Историјата на XX век содржи повеќе примери на корпорациски криминал, врзан за компаниите кои ги користеле воените конфликти за стекнување нелегален профит. Така, новинарите на британската телевизиска мрежа BBC, истражувајќи врз основа на податоци добиени од владините извори во Ирак и во САД, во јуни 2008 година, утврдиле дека за време на воената кампања на западните сојузници во Ирак, започната во 2003 година, во таа земја се проневерени или украдени околу 23 милијарди УСД. Иако во врска со тоа се подигнати повеќе од 70 истражни постапки поради воено профитерство против голем број американски корпорации, од врвот на власта на САД се спречени понатамошни процесирања, па така ниту една американска компанија не е изведена пред суд поради проневера или поради измама во текот на интервенцијата во Ирак. Се наведува и дека еден од челните луѓе на Пентагон за време на кампањата во Ирак, поради судир на интереси, се спротивставил на потпишувањето договор вреден седум милијарди долари со корпорацијата Halliburton на чие чело, до преземањето на функцијата потпретседател на САД, бил Дик Чејни. И покрај противењата од Вашингтон, компанијата Halliburton се пријавила на тендерот и победила.[381]

2.4. ДАМПИНГ ПРОИЗВОДИ СПОРЕД ЗАБРАНЕТИ СТАНДАРДИ КОИ СЕ ПРИМЕНУВААТ ВО ЕКОНОМСКОРАЗВИЕНИТЕ ЗЕМЈИ

Дампингот претставува корпорациски извоз по цена која е пониска од трошокот, или продажба на производи на странските пазари по цена која е пониска од домашната цена. Дампингот се класификува како постојан, прикриен или повремен. Постојан дампинг, или меѓународно дискриминирање на цената, претставува непрекината склоност на домашната монополистичка корпорација

[380] T.W. Singleton, A.J. Singleton, *Fraud Auditing and Forensic Accounting,* 4th edition. John Wiley & Sons, New Jersey , 2010, pp.44-45.

[381] Повеќе види во: Cray Charlie, „Time to Stop Iraq War Profiteers", *Global Beat Syndicate*, New York University's Center for War, Peace and the News Media, New York, 25 November 2003.

да го максимизира вкупниот профит со продажба на производите по повисоки цени на домашниот пазар, кој е ослободен од транспортни трошоци и од трговски пречки, за разлика од странскиот, кој се соочува со конкуренција на странски производители.[382] Прикриениот дампинг е привремена продажба на производите под производствените трошоци или по пониска цена во странство, со цел да се исфрлат странските производители од бизнисот, по што цената расте за да стекне предност од здобиената монополска позиција во странство. Привремениот дампинг претставува повремена продажба на производите под цената на чинење или по пониска цена во странство отколку на домашниот пазар за да се олеснат непредвидени и привремени вишоци на производи без да се намалат домашните цени.[383]

Ограничувањето на трговијата со цел спротивставување на „прикриениот дампинг" е оправдано и дозволено како заштита на домашните индустрии од некоректната конкуренција од странство. Овие рестрикции обично имаат облик на антидампинг давачки за да се надомести разликата во цените, или облик на закани дека ќе се воведат вакви давачки. Меѓутоа, тешко е да се одреди за каков дампинг станува збор, зашто и домашните производители редовно бараат заштита против сите видови дампинг. Со тоа, тие го обесхрабруваат увозот зголемувајќи го сопственото производство и профит. Во одредени случаи на константен и повремен дампинг, користа што ја имаат потрошувачите од ниските цени може во реалноста да ги надмине можните загуби во производството на домашните производители. Во последните децении на XX век, јапонските корпорации биле обвинувани за дампинг на челик и на телевизори во САД,[384] а Европската унија за дампинг на автомобили, на челик и на други производи.

Многу индустриски земји, особено членките на ЕУ, се склони постојано да вршат дампинг на своите земјоделски производи поради својата програма за поддршка на фармерите. Кога дампингот ќе се

[382] Пошироко кај: Ђорђевић Милена, „Дампинг", *Право и привреда*, бр. 9-12/06, Удружење правника у привреди Србије, Београд 2006., стр. 55-56.

[383] Според: Plahutnik Andrej, *Konkurenca, Monopol in povezane ter prijateljske družbe: Gradivo za Borzni fokus*, Ljubljanska borza, Ljubljana 2002., str. 13.

[384] Stern M. Robert (ed.), *Issues and Options for U.S. – Japan Trade Policies*, Studies in International Economics, University of Michigan Press, Ann Arbor MI 2002., pp. 111-112.

докаже, фирмата или земјата што го врши обично се одлучува за зголемување на своите цени за да не бидат соочени со антидампинг давачки. Во 1980 година, само осум држави имале закони против дампинг. Кон крајот на 2001 година, имало 97, вклучувајќи и многу земји во развој.[385]

Постои тврдење дека голем број корпорации од државите членки на ЕУ, со цел да го прошират својот бизнис на нови пазари, спроведуваат дискриминаторски однос спрема потрошувачите во Источна и во Југоисточна Европа, извезувајќи во земјите од тие простори производи од препознатливи брендови, со ист назив и пакување, а со полош квалитет во однос на оние што се продаваат на пазарите во ЕУ. Првенствено станува збор за производи од прехранбената индустрија, чии декларации покажуваат дека нивниот состав не е идентичен со производите што се наменети за потрошувачите во членките на ЕУ. Од друга страна, производите од компаниите од Источна и од Југоисточна Европа што се извезуваат во Европската унија, мора да исполнуваат доста ригорозни стандарди, а наидуваат и на многу пречки и тешко добиваат можност за пристап до потрошувачите на државите од ЕУ.[386]

2.5. АЕРОЗАГАДУВАЊЕ И ДРУГИ ВИДОВИ ЕКОЛОШКИ КРИМИНАЛ

Поимот екологија води потекло од грчкиот збор oikos (дом, живеалиште). Прв пат зборот екологија го употребил германскиот зоолог и еволуционист Ернест Хекел во 1867 година во книгата Природа на историја на создавањето (The Natural History of Creation). Како наука, екологијата првобитно настанала како гранка на зоологијата, и тоа како истражување на односот меѓу животинските видови и нивната органска и неорганска средина.[387] Иако односите меѓу живите суштества и другата природа ги разгледувале и грчките филозофи Аристотел, Теофраст и Хипократ, римскиот поет Вергилие и филозофот Лукреције, екологијата во вистинска смисла на зборот се појавува релативно доцна, дури во втората

[385] Пошироко види: Farah Paolo, Soprano Roberto, „Dumping e Anti-Dumping“, *Il Sole 24 Ore*, Milano, novembre 2009., pp. 163-165.

[386] Според: Драговић Зорица, „Европски шкарт затрпао БиХ”, *Независне новине*, Бања Лука, 14.10.2011.

[387] Види: Марковић Ж.Данило, *Социјална екологија*, Завод за уџбенике и наставна средства, Београд 2005., стр. 29.

половина на XIX век, а посилно се развива дури кон средината на XX век. Екологијата се создава тогаш кога економската активност на човекот ја деградира природната околина, доведувајќи го во опасност опстанокот на човекот. Развојот на екологијата бил условен од сознанието дека економскиот развој дошол во судир со општествениот развој кој притоа е проследен со низа економски појави. Терминот хумана екологија првпат го употребиле Барџес и Парк во 1921 година со значење на медицинска наука која го изучува влијанието на средината врз човекот, неговото здравје и врз нивната меѓузависност. Хуманата екологија како наука ги изучува специфичните односи меѓу човекот и неговата околина. Целта на хуманата екологија е да воспостави рамнотежа во природата и во општеството, со акцент на општествените фактори.[388]

Поимот животна средина изобилува со многубројни теоретски поставки и дефиниции од различни автори. Различните преводи на англиските поими environment или human environment не мора да значи дека под сите нив се подразбира само животна средина. Британскиот закон од 1990 година, со кој оваа област се регулира, наведува дека животната средина се состои од воздух, од вода и од земја, од просторот во зградите и природните или со работа создадените структури над или под земјиштето. Речникот на американската Агенција за заштита на животната средина, поимот environment го одредува како збир од екстерни услови кои влијаат на животот, развојот и преживувањето на организмите.

Големото интензивирање на користењето на природните богатства во текот на „индустриската револуција" довело до забрзана деградација на животната средина. Во врска со тоа, во последните два века се јавуваат различни филозофски и социолошки теории и предлози на модели за излегување од еколошката криза. Почетоците на теоретските прегледи во оваа област се појавиле во средината на XIX век во Велика Британија, која била најразвиената индустриска држава во тоа време. Сите тие теории давале парцијални решенија за излегување од кризната ситуација, а дури со нивна синтеза може да се согледа големината на проблемот. Меѓу нив најпознати се:

- Теорија на бентамистите, која ја добила името според Џеремиј Бентам (1748-1832), британски филозоф и основач

[388] Според: Надиђ Дарко, „Политичка екологија - Прилог заснивању политиколошке дисциплине", во: Годишњак 2010, година IV, број 4, Факултет политичких наука, Београд, децембар 2010., стр. 176.

на утилитаризмот.[389] Бентам, меѓу другото, се залагал за подобрување на хигиенските услови во работничките квартови, поради што противниците му замериле дека главна цел на неговите залагања било остварување поефикасна експлоатација на работниците. Некои од неговите идеи одекнале во книжевноста (романот „Оливер Твист").

- Малтузијанска теорија, наречена според Томас Малтус, кој го предвидел исчезнувањето на човештвото во случај да не дојде до рамнотежа меѓу бројот на жителите и производството на храна. Т. Малтус, меѓу другото ги спомнал војните како едно од средствата за воспоставување рамнотежа и предлагал склопување бракови во подоцнежни години и сексуална воздржливост, контрола на раѓањето во работничката класа и во другите пониски социјални слоеви.[390]
- Теорија позната како „Тивка пролет", според истоимената книга на Рејчел Карсон,[391] врзана меѓу другото, за критиката на масовната употреба на пестициди, односно хлориран јаглеводород, кои се користени во текот на 50-тите години на XX век за да се зголемат приносите во земјоделството. Меѓутоа, земјоделските приноси со текот на времето се намалувале поради загадувањето на околината.
- Теорија „цена на економски раст", објавена во 1967 година во истоимената книга на Е. Мишан,[392] кој се залагал за стабилна и урамнотежена економија и укажувал дека во производството и при формирањето цени на производите мора да се води сметка за загадувањето на животната средина, што се јавува како последица на зголемен индустриски раст.
- Теорија „граница на раст", поврзана со деформирањето на меѓународната невладина организација „Римски клуб" во 1968 година, според чии ставови проблемот со загаденоста на животната средина и брзиот демографски раст имаат светски

[389] Моралниот и филозофскиот систем кој се заснова на идејата дека човечкото битие е рационално, себично суштество и како такво тежнее да оствари сè поголема корист.

[390] Види: *Enciklopedija Leksikografskog zavoda*, tom 5, Zagreb 1961., str. 27-28.

[391] Carson Rachel, *Silent Spring*, Houghton Mifflin Company, Boston 1962., pp. 16-25.

[392] Mishan J. Ezra, *The Costs of Economic Growth*, Stapples Press, London 1967., pp. 95-102.

карактер, поради што мора да се решава на глобално ниво. Од 33 објавени извештаи на „Римскиот клуб“ за иднината на човештвото, два се директно посветени на проблемите на животната средина. Во првиот се наведува дека еколошка катастрофа може да се спречи единствено со намалување на стапката на раѓање, ако е потребно и на драстични начини, а вториот извештај наведува дека економскиот раст ги исцрпува ресурсите, што како последица го има наглото опаѓање на производството на храна.[393]

3. ОДНОСОТ МЕЃУ КОРПОРАЦИСКАТА БЕЗБЕДНОСТ И ПЕРЕЊЕТО ПАРИ

3.1. ПОИМ, СОДРЖИНА И НАЧИНИ НА ПЕРЕЊЕ ПАРИ

Поимот „перење пари“ потекнува од САД и е врзан за периодот на т.н. Прохибиција од 1920 до 1933 година, кога било забрането точење алкохол. Во тоа време криминалните организации се занимавале со илегално производство и криумчарење алкохолни пијалаци, стекнувајќи на тој начин енормно висока заработка. За да ја легализираат така стекнатата добивка, криминалните организации прибегнувале кон разни начини на прикажување на тие пари како приходи стекнати со легална работа, поради што таа појава во јавноста е позната како перење пари. Повеќето автори под перење пари го подразбираат секое прикривање на изворите на противправно стекнат капитал, за тој да биде искористен за вршење на некоја законски дозволена дејност или стекнување сопствена корист. Со перењето пари не се прикрива само незаконски остварен профит, туку и криминалната дејност на субјектите кои во секојдневниот живот се претставуваат како чесни, угледни и економски моќни граѓани.

Во постапката перење пари организираниот криминалитет постојано ги усовршува модусите, при што во прилог му одат современиот технички и технолошки напредок и развојот на економските и на финансиските односи на меѓународен план. Исто така, организираните криминални групи настојуваат да воспостават

[393] Според: Meadows H. Donella, Meadows L. Dennis, Randers Jørgen, Behrens W. William III, *The Limits to Growth*, Universe Books, New York 1972., pp. 60-73.

соодветни врски со државните и со финансиските органи, за да ја искористат нивната положба, функција и углед и на што посигурен начин да ги легализираат „валканите пари".

3.2. ТРЕНД НА ПРЕМИНУВАЊЕ НА ВАЛКАНИТЕ ПАРИ ВО ЛЕГАЛНАТА СФЕРА

Според Б. Добовшек, перењето пари е секундарна фаза во дејствувањето на организираните криминални групи кои настојуваат нелегално стекнатите пари да ги вложат во законска сфера на работење и на тој начин себеси да си обезбедат легалност, станувајќи директори на компании, а неретко и политичари. Трендот на преминување од организиран криминал во легална сфера е присутен во речиси сите земји. Во таа смисла, перење пари е секоја техника насочена кон претворање на нечесно или незаконски стекнато богатство на начин на кој тоа ќе се прикаже како чесен и легален приход. Примарна цел при перењето пари е да се прикрие откривање на финансиските малверзации, плаќањето данок и неговото пласирање во легалниот економски и финансиски систем. Бидејќи перењето пари е компликувана операција, во спротивставувањето на тој вид организиран криминал мора да учествуваат сите државни институции (полиција, судство, банки, даночни институции).[394]

Иако според теоретските објаснувања присутна е аргументација дека организираниот криминал, сфатен како компанија односно индустрија, не настојува да го дестабилизира или да го сруши поредокот во рамките во кои непречено стекнува профит, тешко може да се прифати, зашто инсајдерското малцинство со „приватизацијата" на јавните дејности им го одзема граѓанското право на маргинализираното мнозинство. [395]

Последица од учеството на државното раководство во корупција е појава на феноменот „заробени држави", под кој се подразбира противзаконско плаќање поединци од врвот на власта за да се оствари влијание на изработка и усвојување закони и административни прописи, како и на содржината на одлуките на

[394] Добовшек Бојан, оп. цит. стр. 4.

[395] Види: Berenskoetter Felix, „Under Construction: ESDP and the «Fight Against Organised Crime»", in: Challenge Working Pape*r, Work Package 2: Securitization beyond borders, 5 July 2006*, International Relations Department of London School of Economics & Political Science, London 2006.

органите на власта.[396] Превласта на влијанието на криминалните интереси на изборните резултати, формирањето влади и креирањето јавна политика го обесмислува демократското владеење кое се заснова на согласност и посредно или непосредно учество на граѓаните во јавните работи. Краен резултат од политичката корупција е општествена нееднаквост и нарушување на начелата на одговорност на сите нивоа на власт. Негативните ефекти од организираниот криминал во легалните економски движења најчесто се манифестираат преку општиот раст на степенот на криминал и корупција; нечесната конкуренција; намалувањето на даночните приходи поради движењето на парите низ нелегални финансиски текови; нарушената репутација на земјата во меѓународни рамки; слабеењето на финансиските институции и рушењето на нивниот кредибилитет; компромитираната економија и приватниот сектор.[397]

3.3. СПРЕЧУВАЊЕ НА ПОЈАВАТА ПЕРЕЊЕ ПАРИ НА МЕЃУНАРОДЕН ПЛАН

Според J. B. Дајк најчесто користени методи на перење пари во Европската унија се: системот за трансфер на пари во готовина (Cash Deposit System), т.н. подземно банкарство (undergraund banking) базирано на мрежи од тајни посредници, пренос со посредување на курири, легални коцкарници, вложување во недвижности и законско работење претежно со голем обрт на готовина. Значителен број легално формирани компании се наоѓаат во делумна или целосна сопственост на криминалци или нивни блиски соработници. Тие фирми, според проценитe на Европол, повеќето регистрирани групи на организиран криминал ги (зло)употребуваат при извршувањето противзаконски дејства. Не ретко се случува како параван да се користат туристички агенции и угостителски објекти, шпедиторски, извозни-увозни и транспортни компании и складишта, особено за трговија со жени поради сексуално искористување и за криумчарење недозволена роба и илегални емигранти. Организираниот криминал со помош на контролираните компании има пристап до значајни средства од национални или од наднационални фондови,

[396] Според: Кораћ Срђан, „Организовани криминал као безбедносна претња Европској унији“, во: Фатић Александар, Бановић Божидар (ур.), *Друштвени аспекти организованог криминала*, Институт за међународну политику и привреду, Београд 2011., стр. 438.

[397] Бошковиќ Горан, op. cit. стр. 45.

наменети за развој на сиромашните региони на Европската унија, по примерот на поранешната практика на мафијата во јужните делови на Италија. Високото присуство на класичниот криминал како една од гранките на „индустријата" на организиран криминал ги нарушува движењата во стопанството и пазарните механизми со поскапувањето на работењето, што резултира со непосредни загуби во вид на украдени ресурси, потреба за дополнителни вложувања во безбедносни системи и создавање негативна претстава за состојбата на безбедноста во одредено подрачје, што може да ги одбие потенцијалните инвеститори и туристи.[398]

Спротиставувањето на раширената појава перење пари на меѓународен план се заснова на подготовка и усвојување конвенции и други акти кои ги носат релевантни меѓународни организации. Така, со Конвенцијата на ООН против незаконската трговија со опојни дроги (т.н. Виенска конвенција)[399] предвидени се мерки за сузбивање недозволена трговија со дроги, но и обврска на државите во своите кривични закони да воведат кривично дело перење пари.

За време на усвојување на споменатата конвенција поимот перење пари главно се однесува на пари добиени од недозволена трговија со дрога и психотропни супстанции.

Конвенцијата, исто така, предвидува одземање на предметите кои се стекнати со недозволена трговија со дроги и со неа се исклучува можноста за повикување на банкарска тајна при идентификација, запленување и конфискација на добивката која е остварена со кривичното дело недозволена трговија со дроги и психоактивни супстанции.

На Конференцијата на претседатели на држави и влади на групата Г-7 најразвиени земји од 1989 година разгледувана е проблематиката на перење пари и со цел подобрување на борбата против оваа појава на меѓународен план формирана е група за финансиски акции, која во текот на 1990 година изработила документ со наслов „Четириесет препораки за борба против перењето пари", а кои содржат стратегиски елементи и упатуваат на основните правци за сузбивање на тоа кривично дело.

[398] Пошироко види: Van Dijk Jan, „Organized Crime and Collective Victimization", in: *Paper for International Conference «Corruption and Organized Crime: Bridging Criminal and Economic Policies», Sofia, 23-24 June 2006*, Center for the Study of Democracy, Sofia 2006.

[399] Донесена во Виена на 19 декември 1988 година.

Значаен меѓународен придонес во борбата против перење пари претставува и Конвенцијата на Советот на Европа за перење, следење, привремено одземање и одземање приходи стекнати со кривично дело која е донесена на 8 септември 1990 година во Стразбург. Во преамбулата на Конвенцијата укажано е на потребата од законско регулирање на спречувањето перење пари, и во тој контекст, со цел постигнување што поголемо единство меѓу државите потписнички, како неопходно е истакнато: водење заедничка казнена политика насочена кон заштита на општествената заедница со користење современи методи на меѓународно ниво во борба против тешките кривични дела, коишто сè повеќе стануваат меѓународен проблем; одземање на приходите на сторителите на кривични дела стекнати со кривичното дело и воспоставување ефикасен систем на меѓународна соработка во таа област.

Во член 12 став 2 од Конвенцијата на Советот на Европа внесена е обврска на државите потписнички со сите расположливи средства да дадат помош во идентификацијата, влегувањето во трага, замрзнувањето или заплена поради евентуална конфискација на приходите стекнати со криминал или во врска со криминал. Член 4 од споменатата Конвенција предвидува можност за остварување на предвидените цели со: следење, надгледување, прислушкување на телекомуникациите, пристап до компјутерските системи, како и налог за изработување одредени документи. Исто така, предвидена е и можност, ако сторителот не ја надомести штетата барањето да може да се реализира на кој било достапен имот.[400]

Советот на Европа на собранието во Луксембург одржано на 10 јуни 1991 година донел насоки за спречување на користење на финансискиот систем со цел перење пари. Со овој документ е регулирана обврската на државите членки да го инкриминираат перењето пари во кривичните закони т.е. да се обврзат на усвојување одредени мерки и да го санкционираат неговото непочитување, со што би се овозможило остварување на низа барања од насоките на Советот на Европа кои се однесуваат на кредитните, финансиските и банкарските институции, а коишто се поврзани со идентификација на клиентите; чување најмалку пет години оригинали или фотокопии

[400] Во рамките на наведената конференција под сопственост се подразбира сопственост или имот во каква било смисла, дали е тоа материјална или нематеријална, движна или недвижна, како правен документ или инструмент со кој се докажува сопственоста или интерес во однос на таквата сопственост.

од документите кои можат да послужат како доказ во постапка за кривично дело перење пари; особено внимателен однос во испитување трансакции за кои постои сомневање дека се во врска со перењето пари; соработка со органите надлежни за спречување перење пари и нивно информирање во врска со сите факти кои можат да укажат на перење пари; избегнување трансакции за кои се знае или се соменва дека се во врска со перењето пари, додека надлежните не извршат процена; забрана на клиентот или на некое друго лице да биде известено дека е во тек постапка во врска со кривичното дело перење пари, преземање мерки од страна на надлежните институции за спроведување соодветни интерни контроли и облици на соработка со цел спречување перење пари; организирање соодветни програми за стручно оспособување на вработените, за да може навремено да ги забележат и да ги препознаат дејствата со кои се врши перење пари како и да реагираат на пропишан начин.

Советот на Европска унија на 3 декември 1998 година усвои заедничка акција за перење пари, утврдување, следење, замрзнување заплена, конфискација на средствата и приходите од криминал чиј предмет бил елиминирање на ограничувањата во идентификација, следење, заплена и конфискација на приходи од организираниот криминал по конвенцијата на Советот на Европа од 1990 година, како и постигнување поголема компатибилност при постапување преку јакнење на меѓусебната соработка меѓу државите. Со тој документ е создадена правна основа за воспоставување Европска соработка во конфискација на приходи стекнати со правење дела кои се казниви со даночното законодавство.

Советот на Европска унија на 26 јуни 2001 година донесе *рамкова одлука за перење пари, пронаоѓање, утврдување, замрзнување, заплена и одземање средства и приходи од криминал*, со која ги обврза државите членки за кривичните дела од член 6 став 1 точка а и б од конвенцијата од 1990 година да предвидат во своите закони казни лишување од слобода со максимум од најмалку четири години, како и можност да исклучат одземање имотна вредност во случаи кога таа е помала од 4000 евра.

Покрај наведените акти, значајна е и Конвенцијата на ЕУ за заштита на нејзините финансиски интереси донесена во месец јули 1995 година со која подетаљно се дефинирани финансиските измами.

Со конвенцијата на ООН за борба против транснационалниот организиран криминал, усвоени во Палермо во 2000 година предвидена е обврска на државите потписнички во своите

национални закони, покрај другите кривични дела од областа на организираниот криминал, да пропишуваат и кривично дело перење пари. Конвенцијата од Палермо под тоа кривично дело не подразбира само готови пари произлезени од криминални дејства, туку и сите облици на имот што претставува добивка од извршените кривични дела. Исто така, во член 12 од Конвенцијата предвидено е и конфискација и одземање пари или имот кои се стекнати со криминално дејствување или се користени во тие цели, па во тој контекст упатува на меѓународна соработка. Одредбите на Конвенцијата бараат од државите потписнички да преземат и низа други мерки со кои ќе се спречуваат финансиски и други трансакции со кои се врши перење пари и ќе се придонесе за поуспешно откривање, како и поефикасна постапка против сите лица кои учествувале во перењето пари. Со Конвенцијата од Палермо се регулира и располагањето со заробени средства од страна на државата која ги стекнала, при што е предвидено тие да можат да се поделат и со други држави, како на пример, плаќање компензации или оштети на жртвите, или да се дадат како прилог на некои меѓународни тела кои се борат против транснационалниот организиран криминал. Со член 13 став 7 од Конвенцијата предвидени се и случаи кога може да се одбие или одложи давањето правна помош која се однесува на конфискација на криминално стекнатиот имот.

Како што истакнува Н. Куракис, ако некоја држава стекне репутација на прибежиште на организиран криминал и перење пари, тоа само по себе може да доведе до значајни негативни последици за нејзиниот развој. Во тие ситуации странските финансиски институции може да ги ограничат своите трансакции со институциите на земјите кои се скривалишта за перењето пари, да ги вратат тие трансакции на дополнителна опсервација, што ќе ги направи поскапи или сосема да ги прекинат кореспондентните или заемните односи со нив. Дури и легалните компании од тие земји може да трпат последици поради отежнатиот пристап до светските пазари или достапност на тие пазари по повисоки цени поради дополнителниот степен на внимание на странските субјекти во однос на нивната сопственост, организација или систем на контрола.[401]

[401] Види: Courakis Nestor, „Financial Crime Today: Greece as a European Case Study“, in: *European Journal on Criminal Policy and Research*, Vol. 9, No. 2, Springer, Heidelberg 2001., p. 212.

3.4. ПРИДОНЕС НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО СПРЕЧУВАЊЕТО НА ПЕРЕЊЕ ПАРИ

Перењето пари е изворен облик на појава на организиран криминалитет, а произлегува од една од неговите основни цели – остварување криминален профит. Со оглед на тоа дека основен проблем на вака стекнатиот капитал е неговата легализација, перењето пари, како збир на разни методи на финансиски трансакции, фалсикување документи и деловни манипулации го решава овој проблем кај многу видови организирани криминални активности, како што се: профити од трговија со наркотици, луѓе и оружја, даночни затајувања, проституција, коцка и рекет. Во суштина перењето пари во организираните облици на криминалитет е во конверзијата или во преносот на имотот кој претставува незаконски приход, односно прикривање или маскирање на правната природа на сопственста на средствата од незаконско потекло, како и нивно вклучување во легални финансиски институции и вложување.

Специфичноста на перењето пари и неговите спреги (врски) со организираниот криминал се гледа во тоа што истовремено се појавува и како производ и како претпоставка за постоење на другите видови организиран криминал. Кривичното дело перење пари е последица на претходни сторени кривични дела со елементи на организиран криминал, но без перење пари криминалната активност не би можела успешно да се продолжи. Непреченото финансиско јакнење ѝ овозможува на криминалната група да ја подобри сопствената способност во однос на конкурентските криминални структури, било со техничко опремување или со влијание на одделни припадници на власта со помош на корупцијата. Корупцијата во овој случај се појавува како еден од „трошоците на работењето“, неопходен за безбедносно преминување од „црни“ или „сиви“ зони во области регулирани со правни норми.[402]

Посебен проблем претствуваат ситуациите кога организираниот криминалитет ќе успее големи количини на криминално стекнати пари да ги уфрли во финансискиот систем, со што себеси се доведува во позиција низ различни вложувања да контролира одредени сектори на стопанското работење, при што со создадените економски и политички влијанија би ги ослабнале демократските институции на системот и би довеле до нарушување на етичките вредности во општестовото. Процесот на приватизација во земјите во транзиција дава шанса преку вложување „нечист“ капитал, со

[402] Кораћ Срђан, op. cit. стр. 424.

корумпирање на претставниците на надлежните институции, да се купуваат поранешни државни претпријатија што претставува еден од ефикасните методи на перење пари.[403]

Во начините на перење пари спаѓа и формирањето фиктивно стопанско општество коешто не се занимава со никакви деловни активности туку служи само за легализација на „нечистите пари". Во овој случај перењето пари се врши на тој начин што преку сметките коишто обично се отвораат во повеќе банки се врши уплата и префрлување на незаконските пари, коишто сопственикот подоцна ги подигал. Со редица трансакции преку овие сметки се прикрива изворот на парите. Сличен случај е и со злоупотреба на (off shore) компаниите коишто се формираат во оние подрачја каде што има многу либерални закони во поглед на стопанисувањето, отворањето банки и фирми, како и ниски даночни ставки, загарантирана тајност на банкарските сметки. Иако формирањето off shore компанија чија основна цел е избегнување плаќање данок во својата земја не е незаконско, тој облик на дејствување овозможува дејности кои го вклучуваат и перењето пари.[404]

За да се спречат или барем да се ублажат последиците од перење пари, од големо значење е секое правно лице да изработи анализа на ризик од перење пари. Таа анализа треба да содржи процена на ризикот за секаква група или вид услуги кои објектот ги нуди во рамките на своето работење или трансакции по што тие групи и видови треба да се систематизираат според степенот на различност.[405]

4. ВЛИЈАНИЕТО НА КОРПОРАЦИСКАТА ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ ВО ДОМЕНОТ НА ИНТЕРНАЦИОНАЛИЗАЦИЈАТА И НА ГЛОБАЛИЗАЦИЈАТА НА КРИМИНАЛНИТЕ ПАЗАРИ

Повеќедимензионалната современа глобализација условила појава на глобализација на криминалот, а меѓународните криминални организации станале неформални центри на транснационална финансиска моќ. Капиталот што тие го поседуваат, често пати е

[403] Бошковиќ Миѓо, Бошковиќ Александар, op. cit. стр. 180.

[404] Види: Даниловиќ Нѣо, „Методологија прања новца код правних и физичких лица", *Зборник 2009*., Интернационална асоцијација криминалиста, Бања Лука-Сарајево 2009., стр. 92.

[405] Бошковиќ Миѓо, Бошковиќ Александар, op. cit. стр. 180.

поголем од бруто националниот приход на државите. Во ситуација кога дејствувањето на субјектите на националниот безбедносен систем е ограничен на својата територија, државните граници не претставуваат посебна пречка за интернационализација на злосторството. Од друга страна, меѓународната соработка на криминалните структури често е „поефикасна", отколку соработката на различните национални системи за безбедност, додека помеѓу некои држави од политички или од други причини, постои ограничена соработка. За разлика од нив криминалните организации немаат проблем да соработуваат, затоа што се поврзани со заеднички интереси и имаат далеку „поквалитетни координирани активности" водени од „тимско одлучување и дејствување".[406]

Во денешно време, криминалните пазари стануваат глобални, во опкружување кое дава можности за зголемување на стапката на криминален профит. Слободниот промет на стоки и услуги, луѓе, пари, современа технологија, рушење на традиционалните граници помеѓу државите, влијаат и на ширењето и на глобализацијата на криминалните пазари. Во врска со тоа, истражувањето кое е спроведено во рамките на Европол во 2006 година, укажува дека криминалните пазари се шират надвор од државните граници, бидејќи побарувачката е сè поголема, а понудата сè помала. Така, нелегалната трговија поминува низ Североисточна Европа, што е условено со високи стапки на данок во тие региони, особено во нордиските држави, додека во Југозападна Европа се поврзува со илегалната имиграција, со трговијата со кокаин и со канабис кои понатаму се дистрибуираат во државите од Европската унија. За Југоисточна Европа карактеристични се трговијата со наркотици, илегалната имиграција и трговијата со луѓе. Наведените активности од различни региони во сета ЕУ се пренесуваат.[407]

4.1. КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО ФУНКЦИЈА НА СПРЕЧУВАЊЕ НА ИНТЕРНАЦИОНАЛИЗАЦИЈА НА КРИМИНАЛНИ АКТИВНОСТИ

Организираниот криминал во последно време сè повеќе добива меѓународни димензии и однадвор влијае на безбедноста, а со тоа и на внатрешната стабилност на државите. Важните промени кои се

[406] Пошироко види: Мијалковић Саша, Бошковић Горан, „Безбедност у земљама Југоисточне Европе – нови домети полицијске сарадње", *Криминалистичке теме*, год. VIII, бр. 1-2, Сарајево 2008., стр. 29-30.

[407] Види: *OCTA - EU organized crime threat assessment 2006*, European Police Office, Europol, The Hague 2006, p. 26.

настанати на овој план доаѓаат на крајот на XX век и се поврзуваат со: организирањето на традиционалните криминални активности на широко/глобално ниво; зголемен степен на транснационални врски и облици на соработка помеѓу транснационалните криминални организации, како и повеќекратно зголемување на моќта на транснационалните криминални организации, кои влијаат на безбедноста на државата, ги поткопуваат демократските институци и го забавуваат економскиот раст и друго.[408]

Посебната општествена опасност од организираниот криминал е последица на неколку негови карактеристики по кои се разликува од традиционалниот криминал. Тие се: висок степен на организација на членството; војничка дисциплина и внатрешни хиерархиски односи; голема жед за пари, која тешко ја погодува материјалната егзистенција на жртвите и стабилноста на државниот буџет; тежнеење за власт, која им се заканува на опстанокот на државните институции; и транснационалност, поточно планетарната распространетост која не признава државни граници и национален суверенитет.[409] Почвата на Европа е многу погодна за развој на меѓународниот криминал, до чија експанзија доаѓа во почетокот на 80-тите години на XX век. Ваквата географската позиција на крајот на евроазискиот континент претставува крстосница на сите видови легален и илегален промет помеѓу Азија, Африка и Америка. Според ова, Европа претставува голем конзумент на многу предмети од илегално производство, набавка и трговија. Европа е лулка на демократијата, а развојот на правата и слободите придонесува за развојот на одредени видови криминал. Социјалните проблеми, етничкиот карактер, мултикултурализмот, но и други (пред сè криминогени) фактори, со развојот на сообраќајот и туризмот, доведуваат до интернационализација на криминалот.[410] На ова особено е чуствителна Југоисточна Европа во која повеќето држави доживеја промени во општествено-економските формации, структурно осиромашување, а некои од нив беа изложени на вооружени конфликти.

---

[408] Види во: Ивановски Зоран, „Глобални димензии на организираниот криминал и кризата во Република Македонија“, *Годишник на Факултет на безбедност*, Скопје 2002., стр. 127.

[409] Грубач Момчило, оп. цит. стр. 705.

[410] Види повеќе кај: Bossard André, „Police Cooperation in Europe“, *International Criminal Police Review*, No. 343, Paris 1980, pp. 282–289 (преведено у: *Izbor* broj 3, RSUP SR Hrvatske, Zagreb 1981, str. 275).

4.2. РАБОТЕЊЕ НА КОРПОРАЦИИТЕ ВО УСЛОВИ НА ЕКОНОМСКА ТРАНЗИЦИЈА

Условите на економската транзиција и масовниот прилив на странски инвестиции го потенцираат, според З. Кековиќ, значењето на однесувањето на општествено одговорните компании, а особено на корпорацискиот криминал, како облик на загрозување со потенцијално опасни последици, како поединците, така и општеството во целина. Во таа смисла, општествено одговорното однесување во тргувањето станува важен сегмент на корпорацискатa безбедност со посредство со кое се остварува (позитивно или негативно) влијание на поширок аспект на националната и на глобалната безбедност, на која, државите и меѓународните организации посветуваат сè поголемо влијание. За разлика од деловниот криминалитет, кој се извршува за лична корист, корпорацискиот криминалитет е наменет за остварување на деловните цели и добивки на самите компании. Помеѓу овие два вида криминал, не секогаш е можно да се повлече јасна граница, бидејќи криминалното работење на компаниите може да донесе многу голема корист и на поединци, особено на оние што се високопозиционирани.[411]

4.3. ОПШТЕСТВЕНО ОДГОВОРНО ОДНЕСУВАЊЕ НА КОМПАНИИТЕ

Филип Котлер и Ненси Ли го дефинираат однесувањето на општествено одговорните компании како „определување за унапредување на добросостојбата на заедницата преку дискрециони трговски практики и придонес на сметка на ресурсите на компаниите“, истакнувајќи дека клучен елемент на таа дефиниција е зборот (дискрециони). Според тоа, под корпорациска општествена одговорност не спаѓаат работните активности кои се пропишани со закон или пак кои по својата природа се морални или етички, а со тоа и очекувани, бидејќи тие се однесуваат на доброволно определување на одредени компании да изберат и да применуваат трговска практика и да ги постигнуваат споменатите придонеси. Ваквото определување на корпорациите мора да се демонстрира за да може една корпорација да се нарече општествено одговорна, а се извршува со усвојување трговски практики и/или друг вид придонес (парични и др.). Под добросостојба на заедницата, во овој случај се

[411] Види: Кековић Зоран, *Системи безбедности,* Факултет безбедности, Београд, 2009., стр. 220-221.

подразбираат условите во кои луѓето живеат, како и прашањата за заштитата на животната средина.[412]

Светскиот трговски совет за одржлив развој (World Business Council for Sustainable Development – WCSD), во согласност со фокусот и интерес на организацијата за економски развој, општествено одговорното однесување на корпорациите го дефинира како „определени компании да потпомагаат одржлив економски развој и во целта да го унапредуваат квалитетот на животот, да соработуваат со вработените, со нивните семејства, со локалните заедници и со општеството воопшто".[413] Според меѓународната организација „Бизнис за општествена одговорност" (Business for Social Responsibility – BSR), корпорациската општествена одговорност претставува „тргување кое одговара или ги надминува етичките, законските, пазарните и јавните очекувања, односно очекувања кои општеството ги има од деловните субјекти". Ваквото тргување подразбира „поврзување на трговските деловни одлуки со етичките вредности и со законските прописи, но и со почитување на луѓето, заедницата и животната средина".[414]

Иницијативите на корпорациите со општествена одговорност се поддржуваат во поширокаата општествена средина, и тоа на тие кои се насочени кон: здравјето на населението (спречување ширење сида, навремено вакцинирање, рано откривање на ракот на дојка и сл.), безбедноста на заедницата (спречување криминал, безбедност во училиштата, посебни програми за возачи и др.), образование (на пр. описменување, набавка на компјутери за училиштата, образување лица со посебни потреби), зачувување на животната средина (рециклирање, престанок на користење на штетни хемикалии, смалување непотребна амбалажа), развој на заедницата и економски развој (станбени кредити со ниска камата) и други основни потреби на луѓето (помош на гладните, бездомниците, сузбивање на дискриминацијата, заштита на животните и друго).[415]

---

[412] Kotler Ph., Lee N., *Korporativna društvena odgovornost: Učiniti najbolje za svoju kompaniju i za izabrani društveni cilj*, HESPERIAedu, Beograd 2009., str. 3.

[413] Според: „Corporate Social Responsibility", World Business Coucil for Sustainable Development (http: www.wbcsd.ch/templates/templateWBCSD1/layout.asp?type=p&MenuId=Mz13&d).

[414] Види: „Introduction", in: *White Paper*, Business for Social Responsibility (http: www.bsr.org/BSRResources/WhitePaperDetail.cfm?DocumentID=48809).

[415] Kotler Ph., Lee N., op. cit. str. 4.

Некои автори укажуваат дека корпорациската општествена одговорност може да се смета и како општествено средство кое треба да придонесе во развојот на општествената благосостојба преку: почитување на човековите права, културниот идентитет и автономијата, условите кои обезбеднуваат пристојна работа, чесна заработувачка, разумно работно време и добри услови за работа, одржлив развој и заштита на животната средина на локално, на национално, на регионално и на глобално ниво, поголема демократска одговорност кон луѓето од страна на јавните и на приватните актери на сите нивоа (во поглед на квалитет на производи и услуги, транспарентност, обезбедување одржлив стандард, разумни цени, правичност и почитување на правата на сопственост), придонес кон демократизацијата и ефикасноста на државата (уважување на владините побарувања во поглед на регулативата за транспарентност во тргувањето, заштита на интересите на животната околина, одржливоста во користењето на ресурсите), продлабочување партнерства и дијалог помеѓу субјектите кои се ангажирани во остварување на различни, но и на општи општествени и економски цели (акционерите очекуваат долгорочна стабилност на компаниите, лесен пристап до управата, локалната заедница очекува користење на безбедни процеси на производство и формирање, како и одржување на општествениот капитал), унапредување на родовата рамноправност во смисла на спречување на обиди за сексуално вознемирување и целосна дискриминација на работното место, придонес во одржлива рамнотежа меѓу работата и семејниот живот и отсуство на прекумерен стрес, поврзување на позитивните резултати кои глобалното деловно опкружување ги остварува преку истовремена солидарна одговорност кон луѓето кои глобализацијата ги исклучува или ги маргинализира, давање помош и надминување на нееднаквоста, како и елиминација на сиромаштијата (донаторство, спонзорство, филантропија).[416]

Според С. Клесенс, корпорациската општествена одговорност е концепт на управување на корпорацијата која оддржува баланс помеѓу економските и социјалните цели заради „воспоставување повисок стандард на живот преку одржувањето на профитабилноста на компаниите, за луѓето во тие компании и надвор од нив“, кои како такви претставуваат општествено одговорен и етички однос

[416] Според: Hopkins Michael, *The Planetary Bargain: Corporate Social Responsibility Matters,* Routledge, London 2003., pp. 17-20.

на компаниите кон заедницата во која остваруваат профит и кон сите општествени актери во заедницата и кон своите вработени.[417]

Во резултатите од истражувањето на работењето спроведено на 250 водечки светски корпорации, што во 2002 година го спровела американската агенција KPMG, присутен е тренд на постојано растење на бројот (американски) компании кои го имаат атрибутот за општествено одговорно работење. Според тоа, таа година дури 45% од споменатите корпорации објавиле извештај во врска со одредени активности за заштита на животната средина, поддршката на програми од пошироката општествена заедница, што е многу во однос на состојбата во 1999 година, кога истото го направиле 35% компании од САД.[418] На ваков тренд укажува и т.н. Кон-Роперовата извршна студија од 2000 година, која утврдила дека 69% од опфатените корпорации во истражувањето планираат во иднина да ја зголемат својата општествена одговорност,[419] како и податокот објавен во публикацијата Giving USA, според кој во периодот од 1999 година до 2002 година, добротворните прилози на корпорациите во САД пораснале од 9,6 на 12,2 милијарди долари.[420]

Треба да се земе предвид дека една од карактеристиките на современите светски процеси е делумниот пренос на економски и на политички инструменти од државните институции на деловните субјекти. Еден од показателите за овој тренд е и големината на капиталот кој се генерира во најголемите корпорации.[421] Во таа смисла, како пример се наведува податокот дека Microsoft остварува поголем годишен приход од 31 најнеразвиени земји заедно,[422] а на листата

---

[417] Види: Claesens Stijn, *Global Corporate Governance Forum*, The World Bank, Washington DC 2000., p. 23.

[418] Пошироко види: „KPMG Survey: More top U.S. Companies Reporting on Corporate Responsibility, in: *Corporate Social Responsibility Newswire Service press release*, KPMG LLP., Amstelveen NL, 10 June 2002 (http: www.csrwire.com. print.cgi/1153.html).

[419] Според: *2000 Cone/Roper Executive Study: Cause Initiatives from the Corporate Perspective*, Cone Commnunications, Boston, MA 2001., p. 26. (http: www. coneinc.com/pages/research.html).

[420] Повеќе види кај: „Giving USA", *Association of Fundraising Professionals*, Arlington VA 2003., pp. 5-6. (http: www.afpnet.org/tier3_print.cfm?folder_ id=2345&content_item_id=2286).

[421] Според: Weissbrodt David, Kruger Maria, „Businesses as Non-State Actors", in: Alston Philip, Robinson Mary (eds), *Non-State Actors and Human Rights*, Oxford University Press, Oxford 2005, p. 318.

[422] *Microsoft Corporation Business Report: Competitive Landscape*, Hoover's Company, Mountain View CA 2010., pp. 25-26.

на 100 најголеми светски економски субјекти, 51 место заземаат најголемите корпорации.[423] Концетрацијата на толкава економска моќ во рацете на корпорациите го наметнува и прашањето на „општествена одговорност на деловниот свет". Во врска со ова, во научната и во стручната јавност, мислењата се поделени. Еден од ставовите за прашањето на односот на човековите права, филантропијата и работењето е дека „човековите права и грижа за општествената заедница не се работа на бизнисот".[424] Како аргумент на овој став, се истакнува дека корпорациите имаат обврски само во однос на своите коминтенти и правното опкружување во кое работат, т.е. во спротивно би се појавил проблем на тн. „слободњаци". Како продолжение на ова се укажува дека што повеќе време и пари, етички определените корпорации инвестираат во почитувањето на човековите права и хуманитарни активности, повеќе ќе губат на конкурентност во однос на корпорациите кои за тоа не се грижат. Овој став по неколкуте различни случаи на кршење на човековите права и загрозување на средината од страна на одредени компании е ревидиран, првенствено поради зголемениот притисок на невладини организации и асоцијации на потрошувачи. Во врска со ова, бројни корпорации покренале и кампањи во кои се настојува да се претстават како одговорни членови на општеството, а и почнале да ги задоволуваат потребите и обврските кон „општествената одговорност во деловниот свет".[425]

Гледано од перспектива на деловните субјекти, изразот „општествена одговорност на деловниот свет" или „корпорациска одговорност", може според некои автори, да се толкува како стратегиски и долгорочен концепт во менаџментот, со кој треба да се реагира на конкретни проблеми во општеството со иницирање и со унапредување нови решенија.[426] Во теоријата не постои општо прифатена дефиниција на поимот општествено одговорно однесување на компаниите, но постои согласност дека заедничка цел на тој концепт е придонесот кон „одржлив развој".[427] Според тој пристап, се смета дека работните, економските и социјалните цели

[423] Пошироко види: Anderson Sarah, Cavanagh John, *The Top 200: The Rise of Global Corporate Power,* Institute for Policy studies, Washington DC 2000., pp. 6-8.

[424] Според: Muchlinski Peter, „Human rights and multinationals: is there a problem?", *International Affairs* No. 77, Chatam House UK 2001., p. 32.

[425] Ibid., p.4.

[426] Crowther David, *Social and Environmental Accounting*, Financial Times & Prentice Hall, London 2000., p. 20.

[427] Види: *European Commission - Green Paper on Alternative Dispute Resolution in Civil and Commercial law*, COM(2002)196 final, Brussels 19.04.2002., p. 22.

меѓусебно се надополнуваат, а дека не постојат спротивности меѓу нив.

Во извештаите кои се објавени од SustAinability[428] и Светската банка,[429] дадена е процена на нивоата на општествено одговорни деловни субјекти во светот, а во врска со тоа и двата извештаи носат слични заклучоци. Имено, сè е поголем бројот на компании кои следат правилна насока во оваа област, односно ги земаат предвид и интересите на заинтересираните страни надвор од своето работно опкружување, па се јавуваат и првите примери на добра практика, која вклучува и соработка со невладините организации и синдикатите. Од друга страна пак, најголем број мерки кои компаниите ги спроведуваат од сферата на општествената одговорност сепак се и понатаму изолирани примери, кои не допираат во основната дејност на корпорациите и не претставуваат дел од нивните долгорочни стратегии. Во практика дури и кај општествено одговорните компании се јавува конфликтно однесување, така што, на пример, се покренуваат активности во насока на недискриминаторска политика за вработување, а во исто време се врши лобирање со цел намалување на социјалните и на еколошките стандарди. Освен тоа, повеќето иницијативи на корпорациите од областа на општествената одговорност не се меѓусебно координирани, ниту пак се поврзани со глобалните иницијативи, па според тоа немаат некој значаен ефект. Во споменатите извештаи како посебен проблем во врска со концептот на општествено одговорно однесување на компаниите се истакнува спроведувањето на концептот на дело. Без разлика на вербалните залагања, многу е мал бројот на корпорации кои дозволуваат независна процена на активностите од областа на општествената одговорност, а обидите за воспоставување единствени стандарди за информирање за тие активности се наоѓаат на почетокот.

Светската економска криза по 2008 година наметна и други услови на работа и за мултинационалните корпорации. Во ситуација кога пазарниот натпревар не остава простор за понатамошен раст и

[428] Според: Beloe Seb, Elkington John, Prakash-Mani Kavita, Thorpe Jodie, Zollinger Peter (eds), *Gearing Up: From Corporate Responsibility to Good Governance and Scalable Solutions*, SustAinability & UN Global Compact Office, SustAinability Ltd, London 2004., pp. 12-13.

[429] *Company Codes of Conduct and International Standards: An Analytical Comparison*, *Part I - II*, World Bank, Washington DC 2003., p. 28.

развој на компаниите, само врз основа на цена и квалитет, до израз доаѓа корпорациската општествена одговорност кон вработените, клиентите, широката јавност, набавувачите или животната средина. Вложувајќи во едукација, култура и просперитет на локалната заедница, компаниите се во ситуација да не вложуваат само во својот добар имиџ, туку со тоа таа ја зајакнува и довербата и чувството на припадност на своите вработени, кои ја идентификуваат компанијата како свој работодавец, но и како добар сосед, а од друга страна, се создава стабилен и конкурентен пазар. Со тоа и локалната заедница добива свој покровител и поддршка за многу активности. Одговорните компании ги добиваат и ги задржуваат најдобри кадри, потрошувачите им се полојални, имаат полесен пристап до кредити и до финансии и на тој начин стануваат поконкурентни.[430] Корпорациите се сега принудени во своето дејствување да ѝ посветуваат сè поголемо внимание на јавноста, како и на екстерните фактори, односите со владата и поширокаta заедница финансиерите, новинарите, конкуренцијата, потрошувачите и политичарите), така и на интерните фактори (односите кон вработените и нивните семејства, акционерите, постојаните набавувачи, продажните агенти, агенции, постојаните консултанти и потенцијалните вработени). Притисокот на екстерната јавност, особено кон антиглобалистичките движења на транснационалните компании во услови на светска економска криза рапидно расте, а организираната јавност сè почесто и сè поуспешно ги принудува одговорните да работат на односот со локалната заедница и општеството во целина, поодговорно да се однесуваат кон природата, како и похумано и недискриминаторски да се однесуваат кон вработените.[431]

4.4. КРИМИНАЛ НА „БЕЛИТЕ ВРАТОВРСКИ“

Изразот „криминалот на белите вратоврски“ во стручната литература го вовел Едвин Сатерленд, кој со тоа име го означил криминалот сторен од страна на оние што им припаѓаат на богатите слоеви на општеството.[432] Овој вид криминал подразбира затајување данок, незаконска продажба, малверзации со хартии од вредност,

[430] Ђурић Кузмановић Татјана, Вуковић Марија, op. cit. стр. 34.

[431] Повеќе види: Ђурић Кузмановић Татјана, *Пословно окружење*, Алфа Граф, Нови Сад 2008., стр. 43-49.

[432] Види: Sutherland Edwin, *White Collar Crime*, Holt, Rinehart & Winston, New York 1949., pp. 11-17.

проневери, продажба на опасни производи и кражба. Според Сатерленд, не постои некоја суштинска разлика помеѓу „криминалот на белите вратоврски" и организираниот криминал. Истиот автор укажува и на тоа дека државните органи во многу земји од светот покажуваат висок степен на толеранција кон споменатиот вид криминал. Ставови слични на Сатерленд има и Лери Сигел кој двата вида криминал ги става во иста група, со таа разлика што кај „криминалот на белите вратоврски" се работи за противправна дејност на поединци и на институции кои влегле во бизнис со цел да стекнат профит преку легално работење, додека кај организираниот криминал подразбира нелегални активности на субјектите чија цел уште од самиот почеток била добивање придобивка на нелегален начин. Покрај другото, заедничка точка на овие два вида криминал е да ги нарушат принципите на слободното и легално пазарно работење.[433]

Марк Хелер ги подведува „криминалот на белите вратоврски" и организираниот криминал под категорија „илегални работни дејности", како заеднички назив за продажба на недозволени добра и услуги на купувачи кои знаат дека тие добра и услуги се илегални.[434] Мајкл Блок смета дека современите „организирани криминалци" често вршат дела кои спаѓаат (и) во криминалитетот на „белите вратоврски", додека „криминалците со бели јаки" често дејствуваат како рекетари.[435]

Во трудовите на оние автори што сметаат дека организираниот криминал и „криминалот на белите вратоврски" се два посебни вида криминалитет, основата за дистинкција ја наоѓаат во тоа што легитимните компании своите приходи најчесто ги стекнуваат при легална работа и не користат насилство за да го создадат и за да би го оддржале картелот.[436]

Овие критериуми, меѓутоа, не се толку очигледни како што изгледаат на прв поглед, бидејќи и површна анализа на работењето на повеќето компании покажува дека тоа е на граница на

[433] Повеќе види: Siegel Larry, *Criminology* (8th Edition), Wadsworth Publishing Company, Belmont CA 2008., p. 352.

[434] Haller H. Mark, „Illegal Enterprise: A Theoretical and Historical Interpretation", in: *Criminology*, Vol. 28, Issue 2, American Society of Criminology, Columbus OH, May 1990., pp. 217-221.

[435] Block K. Michael, „A Labor Theoretic Analysis of Criminal Choice", in: *The American Economic Review*, Vol. 65, No. 3, Princeton NJ 1975., p. 316.

[436] Livingston Jay, *Crime and Criminology*, Prentice Hall, Upper Saddle River NJ 1996., p. 225.

законитоста. Исто така, некои истражувања покажале дека како последица на недозволената дејност на корпорациите неретко доаѓа до нарушување на здравјето на луѓето, па и до смртни исходи.[437] Од друга страна пак, Хејзел Кроул смета дека организираниот криминал, за да опстои, мора да создаде еден вид параван за користење на легитимното работење, и тоа не само со цел перење пари. Заради тоа, во такви случаи, тешко е да се разликува што е (над) а што (под) земјата.[438] Во такви ситуации, многу криминолози, меѓу кои и врвните познавачи на оваа материја, како што се Никос Пасас и Дејвид Нелкен, тврдат дека и на теоретски и на емпириски план тешко е да се утврди јасна разлика меѓу организираниот криминал и криминалитетот на „белите вратоврски".[439]

Според некои други дефиниции, „криминалот на белите вратоврски" е криминал кој може да се изврши од страна на поединец или на група преку работа на одредено занимање, односно во врска со управувањето или раководењето со компанијата. Опасноста вработените, преку злоупотреба на положбата да бидат вклучени во „криминалот на белите вратоврски", може да се манифестира на неколку начина, и тоа: земање мито, замена на редоследот на услуги, вршење услуги на одредени лица, злоупотреба на системот со цел стекнување имотна корист, нерегуларен однос со купувачите. Во врска со тоа, како облик на „криминал на белите вратоврски" во корпорациите се вбројуваат и измамите во врска со осигурување, лажен стечај, измама на потрошувачите, компјутерски криминал, даночни измами, поткупување, корупција и политички измами, како и измами и кражби од страна на вработените.[440]

[437] Види: Schrager S. Laura, Short F. James, „Toward a Sociology of Organizational Crime", in: *Social Problems* 25, University of California Press, Berkeley CA 1978., pp. 411-414.

[438] Croall Hazel, *Understanding White Collar Crime*, Open University Press, Buckingham UK 1994., p. 16.

[439] Пошироко види: Passas Nikos, Nelken David, „The Thin Line Between Legitimate and Criminal Enterprises: Subsidy frauds in the European Community", *Crime, Law and Social Change*, No. 19, Springer-Verlag Gmbh, Heidelberg 1993., pp. 234-235.

[440] Бошковиќ Горан, op. cit. стр. 23.

4.5. МЕЃУНАРОДНИ ИНСТРУМЕНТИ ЗА СПРЕЧУВАЊЕ ТРАНСНАЦИОНАЛЕН ОРГАНИЗИРАН КРИМИНАЛ

Поаѓајќи од проблемот за поимно дефинирање на различни категории на современ криминал (конвенционален, професионален, организиран, политички, меѓународен, транснационален, итн.), некои автори под мултинационален криминал подразбираат: тероризам, шпионажа, трговија со дрога, трговија со оружје, перење пари, дестабилизација на странски влади и убиства на странски лидери. Од друга страна, во организираниот криминал спаѓаат: коцка, рекет, проституција, изнудување и слично.[441] Така, за транснационален организиран криминал се користат и термините мултинационален организиран криминал, прекугранично организиран криминал и меѓународен организиран криминал. Меѓутоа, без разлика на различните дефиниции, под транснационален организиран криминал се подразбира „активност на добро организирана криминална група, со строга хиерархија, дисциплина, одговорност, лојалност и поделба на задачите, чијашто цел е остварување поголем профит од криминална активност и легализација на нелегално стекнат имот, и чијашто дејност се одвива во меѓународни размери, која најчесто се остварува преку разновидни активности на транснационални криминални организации и групи".

Според конвенцијата на Обединетите нации против транснационалниот организиран криминал, усвоена во 2000 година во Палермо, организирана криминална група се дефинира како „група која се состои од три или повеќе лица, а егзистира извесен период и дејствува со цел извршување едно или повеќе тешки кривични дела заради посредно или непосредно остварување парична или друга материјална корист".[442] Тешките кривични дела се дефинирани како оние за кои е предвидена казна затвор над четири години. Деликтот е транснационален ако е извршен во две или во повеќе држави, исто ако е направен од една држава, но значајните елементи на неговата подготовка, планирање, насочување или контрола се изведени во друга држава, потоа ако е извршен во една држава, но е вклучена и криминална група која дејствува во повеќе држави и ако деликтот

[441] Според: Martin M. John, Romano T. Anne, *Multinational Crime: Terrorism, Espionage, Drug & Arms Trafficking*, Newbury Park, London 1992, p. 23.

[442] Конвенција на Обединетите нации против транснационалниот организиран криминал *„Службени лист СРЈ – меѓународни уговори"* бр. 6 од 27.06.2001.

е извршен во една држава, но има значајни последици на друга држава.[443] Врз основа на оваа конвенција, за кривични дела од областа на организираниот криминал, се смета учеството во групи кои во континуитет се занимаваат со криминал, корупција, перење пари, проституција, трговија со луѓе, дрога, царински измами и слично.

На состанокот на Европската комисија одржан на 19 септември 2001 година, донесени се препораки со кои се дефинирани принципите на борбата на ЕУ против организираниот криминалитет, а за таа цел дефинирани се и поимите „организирана криминална група“ и „тешко кривично дело“, во согласност со Конвенцијата на ООН против транснационалниот организиран криминал.[444]

Транснационалниот организиран криминал претставува закана за економските системи на националните држави, кои трпат штети поради илегалните економски активности и избегнување на плаќање на данок, првенствено на планот на намалување на прилив на средства во државниот буџет. Идиректните последици од таквото криминално дејствување се создавањето социјални тензии и незадоволство, како и поттикнување политичка нестабилност. Особено опасни облици на загрозување на безбедноста на економскиот систем се присутни во земјите на транзиција, во кои организираните криминални групи ги користат воспоставените врски со политичките структури, парите кои се добиени од криминални активности се вложуваат во процесот на приватизација со цел да се воспостави привилегирана положба на пазарот и воспоставување неформални центри на финансиска моќ, а многу често и изнесување на противправно стекнатиот капитал од земјата. Во ваков случај, покрај последиците кои настануваат врз економскиот систем, дејствувањето на транснационалниот организиран криминал ги загрозува и основните човекови права на вработените и на потрошувачите во дадената држава.[445]

[443] Член 3. став 2. Конвенција на ОН против транснационалниот организиран криминал.

[444] Според: *Organised Crime Situation Report* 2004, Council of Europe - Department of Crime Problems, Strasbourg 2004., p. 6.

[445] Савић Андреја, Стајић Љубомир, оп. цит. стр. 162.

V ГЛАВА

ВЛИЈАНИЕТО НА КОРПОРАЦИСКАТА ВРЗ НАЦИОНАЛНАТА БЕЗБЕДНОСТ ОД АСПЕКТ НА ИНФОРМАТИЧКАТА БЕЗБЕДНОСТ

1. НАЦИОНАЛНИ ИНФОРМАТИЧКИ РЕСУРСИ

Поради своето значење националните информатички ресурси во современата теорија на национална безбедност се сметаат за витални национални вредности, а нивното одржување и развој за примарни национални интереси.[446] Националните информатички ресурси опфаќаат: тоталитет на информатичките знаења (за современата информатичка технологија и нејзината употреба, како и дигитализирано знаење од други сфери на општествената дејност и свест), информатички материјално-технички капацитети и инфраструктура во посед на нацијата, како и нивно учество во глобални информатички процеси и односи.[447] Тие се клучен фактор на националната информатичка моќ, заснована на степен на технолошки развој (технолошка моќ), односно на стратегиската предност во однос на другите држави која субјектите на безбедност ја остваруваат со навремени и објективни разузнавачки информации и податоци (информатичка моќ во потесна смисла).[448]

Националните вредности и интереси во современиот свет можат да се остварат ако се засноваат на концепцијата на употребата на знаењето, која подразбира цели на кооперативна и динамична конкуренција на меѓународната сцена, контрола на мрежните јазли на меѓународните комуникации и организациска приспособливост, за што се неопходни ресурси во вид на вредни информации со подобрено искуство. Од тие причини и безбедноста и интегритетот на

[446] Мијалковић Саша, *Национална безбедност*, op.cit., стр.159-160.

[447] Националната информациска инфраструктура вклучува компјутерски мрежи, терминална опрема, софтверски услуги и апликации, бази на податоци, електронски записи, дигитални архиви и друго. Оваа инфраструктура овозможува брзо, едноставно и евтино складирање информации, враќање, пренос и обработка на дигитални податоци во форма на говор, податоци, видеа, анимации итн.

[448] Според: Мијалковић Саша, Арежина-Ђерић Вера, Бошковић Горан, „Корелација информационе и националне безбедности“, у: *Злоупотребе информационих технологија и заштита* (зборник радова ZITEH '10), ИТ Вештак, Београд 2010., стр. 65.

сајбер-просторот мора да се сметаат за важни, ако не се и единствени од виталните национални интереси. Тоа ги условува и измените на досегашното поимање на стратегијата за национална безбедност која би морала да ги уважи информатичките димензии на животот на општеството, државите и меѓународната зедница.[449]

Модерната концепција на безбедност бара избалансираност на целите, начините и средствата за концепциска употреба на дигитализираното знаење. Без разлика на тоа дали употребуваме политички, економски, воени или информатички елементи на националната моќ, државни или национални стратегиски цели најдобро се користат преку соработка во обликување на робусните информатички мрежи кои ја надминуваат динамичката конкуренција и го подобруваат заедничкото дејствување.[450] Со оглед на информатичката глобална меѓузависност, државите ќе тежнеат да бидат примарни архитекти и посредници во мрежните операции. Информатичките мрежи ќе бидат пожелна мета на напад на многу носители на загрозување на безбедноста, што ќе претставува истовремен напад на: поединецот, државата, меѓународната зедница, односно на другите (најнапред стопански) субјекти кои се распространети на овие нивоа. Урамнотежувањето на националните цели, начините и средствата за нивно достигнување, како и концепциската употреба на знаењето, се прв чекор кој води кон вистинските стратегиски одлуки во сферата на националната безбедност во новото информатичко време.[451]

1.1. ТРАНСФОРМАЦИЈА НА ИНДУСТРИСКОТО ВО ИНФОРМАТИЧКО ОПШТЕСТВО

Почетоците на информатичката технологија се врзуваат за 1858 година, кога Чарлс Бебик ја конструирал „диференцијалната машина“ врз основа на дупчени картички. Современиот развој на информатиката почнува во 1939 година, со компјутерскиот уред заснован на приципот на бинарна аритметика кој го патентирал Џон Винсент Атанасоф, како со појавата на електромеханичкиот бинарен сметач Конрад Зус во 1941 година. Нов замав следи во 1946 година,

[449] Види: Keohane O. Robert, Nye S. Joseph Jr, „Power, Interdependence and the Information Age“, in: Little Richard, Smith Michael (eds.), Perspectives on World Politics, Routledge, London-New York, 2006., pp. 187-190.

[450] Мијалковић Саша, Арежина-Ђерић Вера, Бошковић Горан, op. cit. стр. 66.

[451] Keohane O. Robert, Nye S. Joseph Jr, op. cit. p. 192.

кога на универзитетот Пенсилванија бил изработен прв електронски дигитален комјутер од општа намена (ENIAC), заснован на електронски цевки и тежок 30 тони. Оттогаш развојот на информатичката технологија се одвивал во неколку генерации. Во првата (1950-1958 година) компјутерите биле засновани на електронски цевки, и биле со голема димензија и мала меморија. Во втората генерација (1959-1964 година) воведени се транзистори, магнетини јадра, дупчени картички, програмски јазици ALGOL и COBOL. Третата генерација комјутери (1965-1972 година) донела внатрешно програмирање, помали димензии на компјутерот, надворешна меморија, можност за вмрежување на повеќе комјутери, престанок на употребата на дупчени картички. Во четвртата генерација (1972 година до крајот на XX век) се појавиле микропроцесори, високоинтегрирани кола, мултипрограмирање, голема брзина на комјутерот, пад на нивните цени, масовно производство и употреба, вмрежување. Петтата генерација компјутери, која почнува со преминот во XXI век, ги донесе чиповите, минијатуризацијата, интеграцијата на компјутерски, комуникациски и аудиовизуелни технологии со чипот како основа, големо зголемување на меморијата, преносни компјутери, создавање светски мрежи и податоци и друго.[452]

Како што истакнува К. Ома, до средината на 80-тите години на XX век поголемиот дел на луѓето на Запад веќе биле во допир со компјутери. Меѓутоа, тогашните големи компјутерски машини, кои прихранувале големи количини информации, а некои биле во состојба да играат шах, на многумина им дејствувале мистично, побудувајќи понекогаш и страв. Ентузијастите биле свртени кон персоналните компјутери (збир на различни слоеви во куќиштето, со придодаден екран и еден до два влезни уреди, како тастатура), кои им овозможувале едноставни видео игри и претставувале еден вид хоби. Потоа на пазарот дојдоа уште побрзи компјутери со поголеми можности за архивирање, додека апликациите стануваа сè пософистицирани. Постепено бројните компјутерски програми стануваа достапни, при што и бројните корисници на персоналните компјутери можеле да изработуваат едноставно програми кои, меѓутоа напишани на еден јазик, по правило не можат да функционираат во апликациите напишни на друг програмски јазик. Суштинската промена настапила со појавата на оперативните системи кои им овозможиле на различните апликации една покрај

[452] Javorović Božidar, Bilandžić Mirko, op. cit. str. 63.

друга да работат на ист уред. Исто така, благодарение на оперативните системи, веќе не била неопходна употребата на компјутерскиот код.

Револуционерниот пресврт во информатиката е врзан за 1985 година, кога незавршениот американски студент, Вилијам Гејтс и косопственикот до тогаш на јавноста непознатата компанија Microsoft ја лансирал првичната верзија на оперативниот систем Windows. Визијата која ја имал Гејтс не била создавање на уште еден од оперативните системи, туку создавање таков оперативен систем кој ќе може да се користи во сиот свет и со кој би се редефинирал односот на корисникот и на компјутерот, па и начинот на внесување на информации во компјутер. Наместо текстуални наредби преку тастатура, Windows овозможил избор на графички содржини презентирани на екранот со помош на уредот наречен маус. Секој чекор до кој било дојдено во развојот на персоналните комјутери кон крајот на XX век и почетокот на XXI век бил предвиден и подржуван со сè поновите Windows кои ги лансирал Microsoft. На тој начин, светот од индустриско преминал во информатичко општество.[453]

Соочувајќи ги поединици, општеството, нацијата, државата и меѓународната заедница со предизвиците на адаптирање, иновација и реагирање на приликите и можностите кои им се укажуваат, информатичката технологија врши трансформација од индустриско во информатичко општество, најавувајќи нова фаза на дигиталната ера. Улогата и значењето на информатичкиот систем во работата на современата државна управа (e-government), работењето, здравството, образованието, научната работа, системот на национална безбедност и одбраната, се неоспорни и клучни. Истовремено, зголемена е нивната ранливост од разни појави кои тежнеат кон нивната деструкција. Евидентно е дека националните информациски ресурси се во функција на другите општествени вредности, но и дека самите станале вредност на модерното општество.[454]

1.2. ОСНОВНИ ПРИНЦИПИ НА ИНФОРМАТИЧКОТО ОПШТЕСТВО

Во периодот од 1994 до 1995 година повеќе европски држави (Велика Британија, Франција, Холандија, Шведска, Данска, Норвешка, Финска) изработиле планови и политики за работа

[453] Според: Ohmae Kenichi, *Nova globalna pozornica: Izazovi i prilike u svijetu bez granica*, op. cit. стр. 35-36.

[454] Aas F. Katja, Gundhus O. Hellen, Lomell M. Heidi (eds), *Technologies of (In) Security – The Surveillance of Everyday Life*, Routledge, New York 2009., pp. 8-12.

и развој на електронската комуникација во своите општества. На трансевропското ниво во 1993 и во 1997 година се донесени документи на Европската унија за развој и т.н Бангеманов извештај (Bangemann Report).[455]

Европската унија во 2000 година за државите членки ги одреди развојните цели наречени „Лисабонска стратегија". Тој документ опфаќа цели и стратегии чија цел е „подготовка за транзиција во стопанството и во општеството кои се засновани на знаење, со подобра политика на работењето на информатичкото општество и истражување и развој". Изградбата на „информатичкото општество" за ЕУ е во директна врска со расположливоста и достапноста на информатичките технологии на граѓаните, организациите и сето општество. Европската унија дискусијата за информатичките општества ја прифати како една од политиките за проширување на инфраструктурата и зајакнување на единството на земјите членки. Е-Европа е лансирана во декември 1999 година, за да може ЕУ да ги загарантира сите користи од промените кои ги носи информатичкото општество. Главните цели на е-Европа се сите граѓани, секој дом и секое училиште, сите претпријатија и сета администрација да се доближат кон дигиталната ера и да им се овозможи пристап до интернет. Планот е да се создаде дигитално писмена Европа што ја поддржува претприемачката култура која е подготвена да финансира и да развива нови идеи. Е-Европа, исто така, сака да осигура дека целиот процес ќе биде општествено имплементиран, да се изгради доверба кај корисниците и да се придонесе кон општественото единство.[456]

Основните принципи на глобалното информатичко општество се дефинирани со Декларација за принципите, усвоени на Светскиот самит за информатичко општество (The World Summit od the Information Society), одржан во 2003 година во Женева, во организација на Меѓународната телекомуникациска унија (ITU). Во таа прилика претставниците на 175 земји, покрај Декларацијата со дванаесет принципи, го усвоиле и Акциониот план за нејзино спроведување. Во Декларацијата за принципите е истакнато дека информатичко-телекомуникациската технологија е есенцијална основа за сеопфатно информатичко општество и е поддржана идејата за

[455] Наречен по Мартин Бангеман, член на Европската комисија задолжена за информатички технологии и телекомуникации.

[456] Според: *Стратегија развоја информационог друштва у Републици Србији*, Влада Републике Србије, Београд, 8 јула 2010, године, стр. 1-2.

универзална, достапна, непристрасна, фер и финансиски прифатлива информатичко-телекомуникациска инфраструктура и сервис, со укажување на неопходност од спроведување информатичка и мрежна безбедност, автентификација, заштита на приватноста и заштита на корисниците. Нагласено е дека во изградбата на информатичкото општество, особено внимание ќе се обрне на потребите на маргинализираните и ранливите групи во општеството, вклучувајќи ги и емигрантите и бегалците, невработените и обесправени луѓе, малцинствата и номадските народи, како и на потребите на децата, на старите лица и на инвалидите.[457]

Со Акциониот план на Светскиот самит за информатичкото општество предложени се следните конкретни цели: сите села во светот да бидат комуникациски поврзани до 2010 година, а информатички вмрежени до 2015 година; сите универзитети да бидат поврзани до 2005 година, сите средни училишта до 2010 и сите основни училишта до 2015 година, сите болници до 2005 година и медицинските центри до 2010 година, потоа 90% од светската популација да биде покриена со безжични комуникации до 2010 година, а 100 % до 2015 година, сите централни служби на владите да имаат веб сајт и e-mail адреса до 2005 година, а сите органи на локалната власт до 2010 година.

1.3. НАЦИОНАЛНА ИНФОРМАТИЧКА МОЌ

Поседувањето важни податоци и информации отсекогаш претставувало еден од клучните фактори во остварување на општествената моќ. Тие општествени актери кои располагале со сигурни и пред сè навремени податоци, и кои на соодветен начин ги анализирале, можеле да ја спроведуваат својата моќ врз оние што таквите информации не ги имале или ги користеле во погрешен контекст. Заради тоа авторите коишто се занимаваат со општествените односи и влијанието врз нив, сè почесто зборуваат за моќ која се однесува на информации, медиумско влијание и контрола на комуникациите.[458] Ако поединецот, организацијата или државата сакаат да одговорат или да се приспособат на

[457] Види: Петковић Тодор, *Пословна шпијунажа и економско ратовање*, Protexi Group System, Нови Сад, 2009., стр. 288.

[458] Според: Rothkopf David, „Cyberpolitik: the Changing Nature of Power in the Information Age“, in: *Journal of International Affairs*, School of International and Public Affairs, Vol. 51, No. 2, Columbia University, New York 1998., pp. 325-326.

промените на опкружувањето, мора нужно да ја објективизираат реалната состојба во која се наоѓаат, за што им е потребен збир на најразлични информации. Поради растечката сознајна комплексност на современиот свет, утврдувањето на реалната состојба е поврзано со сè поголемото количество на информации, пред сè на оние специјализираните, кои ги обезбедуваат посебните служби. Тој што има контрола над таквите информации има општествена моќ и монопол. Во модерните општества особено е значаен надзор над протокот на информации, бидејќи тие се важни за давање одговор на барањата и предизвиците на опкружувањето. Ниту еден современ систем не може да ги пресече сите канали на комуникација, како што не е можна ниту целосната слобода на протокот на информации.[459]

Самата информатичка моќ е резултат на поседувањето знаења кои другите ги немаат, но им се потребни и ги сакаат. Информациите кои не му требаат на никого, се беспредметни и немаат никаква вредност, односно моќ. Информацискатa моќ се шири и на способноста за собирање информации, бидејќи за сите информации не важи слободен проток, со оглед дека често можат релативно лесно да се контролираат на национално ниво. Примерите за ограничување на протокот на информациите се однесуваат помеѓу другото, и на информациите од доменот на националната безбедност, податоци за лица, информации за влади или одделните нејзини сектори, деловни тајни, податоци од казнени евиденции за малолетници, податоци за бинарни компјутери, содржина на одделни телефонски разговори и друго.[460]

Информатичката моќ, која ја поседуваат земјите со развиена информатичката технологија ја унапредува технолошката моќ, го поттикнува развојот на стопанството и на економијата, придонесува за модернизација на вооружените сили, го унапредува животниот стандард на населението и обезбедува контрола на јазлите на транснационалните комуникации и електронскиот сообраќај, со што ја зголемува политичката моќ на државата.[461]

---

[459] Пошироко види кај: Keohane O. Robert, Nye S. Joseph, „Power and Interdependence in the Information Age“, *Foreign Affairs,* Vol. 77, No. 5, Council of Foreign Relations, New York 1998., pp. 82-83.

[460] Види: Svete Uroš, „Strateški značaj informacijsko-komunikacijske tehnologije u suvremenom međunarodnom okolišu“, *Polemos*, br. 18, Hrvatsko sociološko društvo & Naklada Jesenski i Turk, Zagreb 2006. str. 107

[461] Nye S. Joseph Jr, „Limits of American Power“, in: *Political Science*, Vol. 117, No. 4, The Academy of Political Science, New York 2002/2003., pp. 555-556.

1.4. НАЦИОНАЛНИ ИНФОРМАТИЧКИ РЕСУРСИ ВО ФУНКЦИЈА НА НАЦИОНАЛНАТА И НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ

Современите концепти на националната безбедност во својот фокус ги имаат идеите за реципроцитет, изградба на заеднички идентитет, како и заеднички интереси на државите и општествата. Во глобалниот свет, тие идеи најбрзо и најефикасно се шират и се реализираат со посредство на модерните информатички технологии. Електронските медиуми, сателитските комуникации и интернетот се најефикасните средства за создавање нови, глобални масовни култури, за изградба на нови регионални вредности и интереси и за конституирање на нови регионални идентитети. Исто така, секојдневната интерна и екстерна комуникација на меѓувладини организации-воени и цивилни, регионални и универзални, се базираат на информатичката технологија.[462] Современите војни се водат од страна на информатичко моќните држави, а против земјите кои не спаѓаат во лидери во тие области, но се наоѓаат на важни геостратегиски положби, располагаат со енергетски и индустриски ресурси и со евтина работна сила. Во таа смисла, државата која е информатички моќна, истовремено е и побезбедна. Колку е поголем бројот на таквите држави во одреден регион, толку ќе биде поголема и безбедноста на тие региони.[463]

Некои автори укажуваат дека пролиферацијата, односно ширењето на употребата на информатичките и на комуникациските технологии ширум светот, претставува еден од најзначајните фактори во сферата на билатералните односи помеѓу државите, а исто така и во односите помеѓу државите и другите учесници во современата безбедносна сфера, во која сè позначајна улога имаат и поединци, невладини организации, како и терористички и други бунтовнички групи и организации. Поради тоа улогата на информатичките ресурси во концептот на инструментална моќ е потребно да се разгледува и надвор од државните рамки, иако во начелата на државите и на мултинационалните организации е достапна информатичката структура и информациите воопшто.

[462] Пошироко во: Baylis John, „International and Global Security in the Post-Cold War Era“, in: Baylis John, Smith Steve, Owens Patricia (eds), *The Globalization of World Politics*, Oxford Press, New York 2001., pp. 263-266.

[463] Мијалковић Саша, Арежина-Ђерић Вера, Бошковић Горан, оп. цит. стр. 67.

Денешните хакери, терористи, но и држави кои спроведуваат офанзивна информатичка дејност, многу е тешко да се контролираат, поради употребата на информатички и комуникациски технологии, што од аспект на инструменталната моќ може да биде и позитивно и негативно.[464]

2. ФУНКЦИИ НА КОРПОРАЦИСКАТА БЕЗБЕДНОСТ ВО ОБЛАСТА НА ЗАШТИТАТА НА ТАЈНОСТА НА ПОДАТОЦИТЕ

Под поим податок се подразбира документ, односно секој напишан, умножен, нацртан, насликан, печатен, снимен, фотографиран, магнетен, оптички или кој било друг запис на податоци, сознание, мерка, постапка, предмет, усно соопштение или информација која, со оглед на својата содржина, има значење на тајност (доверливост) и целовитост за својот сопственик-субјект во чиишто рамки на дејствување настанал податокот.[465]

Податоците според отвореноста се делат на јавни и на тајни. Јавните податоци и информации се достапни за сите, слободно се објавуваат и секој може да ги користи, почитувајќи ги авторските права и другите со закон пропишани услови. Тајните податоци не ѝ се достапни на јавноста сè додека за доверливи ги смета оној што ги прогласил за такви. Станува збор за податоци и информации кои за некого претставуваат посебен интерес и со чие откривање или објавување би била нанесена штета, односно од кои на туѓа штета може да се оствари корист. Во прашање може да бидат личните податоци за граѓаните, особено важни деловни податоци на корпорацијата, воени, полициски или разузнавачки податоци, информации од највисоки државни тела и органи, како и доверливи информации на меѓународните организации. Тајните податоци се посебно заштитени и се достапни само за одредени лица и институции.[466]

Под поимот деловна тајна се подразбира збир на податоци и информации кои се користат во работењето, а кои му припаѓаат на

[464] Svete Uroš, op. cit. str. 109.

[465] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 198.

[466] Javorović Božidar, Bilandžić Mirko, op. cit. str. 37.

деловен субјект, носат економска корист и обезбедуваат одредена предност над конкуренцијата. Предмет на деловната тајна, која нејзиниот сопственик настојува да ја зачува во разумни рамки, може да бидат призводствена постапка, содржината на деловниот договор и друго.[467]

2.1. ИЗВОРИ НА ЗАГРОЗУВАЊЕ НА ТАЈНОСТА НА ПОДАТОЦИТЕ НА КОРПОРАЦИИТЕ

Загрозувањето на тајноста на податоците на корпорацијата преку дејствување на луѓето, без разлика дали е направено свесно или несвесно, во однос на средината од која потекнува може да се подели на: внатрешни извори на загрозување, надворешни извори на загрозување и комбинирани извори на загрозување. Внатрешните извори на загрозување ги претставуваат вработените во корпорацијата. Овој вид загрозување не може прецизно да се стави само во рамките на работното време, туку треба и надвор од него. Всушност, вработените по работното време, со недоволна безбедносна култура, свесно или несвесно можат да ја загрозат корпорацијата со изнесување податоци значајни за нејзиното работење. Во надворешните извори на загрозување спаѓаат лицата кои не се во работен однос во корпорацијата, а кои со своето штетно дејствување можат негативно да влијаат на нејзината безбедност. Комбинираните извори на загрозување опфаќаат заедничко штетно дејствување на лица кои се вработени и на лица кои не се во работен однос.[468]

Информатичките системи на корпорациите во денешно време се изложени на различни безбедносни закани кои го загрозуваат не само технолошкиот сегмент на деловниот субјект туку најчесто и неговата целокупна работа. Тие закани може да доаѓаат однадвор, но свој извор може да имаат и внатре во системот. Предмет на загрозување може да биде секоја вредност во информатички систем, како што се: информатичко-комуникациски систем на корпорацијата како целина; компјутери и податоци содржани во нив; податоци за деловните соработници, лични податоци за вработените, разни евиденции и бази на податоци, информатичко-комуникациска

[467] Види: Katulić Tihomir, *Uvod u zaštitu intelektualnog vlasništva u Republici Hrvatskoj*, CARNet – Hrvatska istraživačka i akademska mreža, Zagreb 2006., str. 50.

[468] Пошироко види кај: Мандиќ Горан, *Системи обезбедења и заштите*, Факултет цивилне одбране Универзитета у Београду, Београд 2004., стр. 33-40.

технологија, вклучувајќи ги и компјутерите и мобилните телефони, деловни и производни процеси; технологијата; вработени кои работат во организационите единици врзани за информатичко-комуникациски систем; техничко-безбедносните системи; интелектуалната сопственост и друго.[469]

Заштитата на тајноста на податоците во однос на внатрешните извори на загрозување можно е да се разгледуват низ организациски, персонален и правен аспект на заштита. Како што истакнува Х. Левит, „сите организации се хиерархиско уредени". Луѓето на секое ниво се потчинети на оние над нив. Оттаму, организацијата претставува структурирана институција. Ако не е структурирана, таа само претставува маса на луѓе. Таквата маса не може ништо да создаде; таа само уништува одредени работи. Важно е да се создаде организациска шема во која јасно ќе се видат задачите и одговорностите на поединецот.[470] Во таа смисла, организацискатa структура претставува формално утврден систем на односи меѓу поединецот и групата, во кој нивните меѓусебни врски се одредени со распоредот на задачите, одговорностите и авторитетот.[471] Формирањето на организацискатa структура подразбира поделба на работата, групирање и поврзување на одделни видови работа, делегирање на овластувања и одговорности во извршување на работите.[472] Изборот на внатрешната организациска структура зависи од конкретната ситуација, како што се бројот и структурата на извршители, расположливата техника, видот и карактерот на податоците кои треба да се штитат, бројот на корисници и друго, така што се можни различни пристапи.

Документацијата претставува најчест извор на откривање тајни податоци на корпорацијата. Документи се сите пишани, печатени, цртани или снимени материјали кои содржат одредени податоци. Во врска со тоа, задолжителните мерки на заштита на документите опфаќаат: проценување на значењето на документите, утврдување на видот и степенот на нивната тајност и утврдување на начинот на

[469] Javorović Božidar, Bilandžić Mirko, op. cit. str. 296.

[470] Според: Leavitt Harold, Dill William, Eyring Henry, *The Organizational World*, Harcourt Brace Jovanovich inc, New York 1973., p. 22.

[471] Види: Петковиќ Мирјана, Јаниќијевиќ Небојша, Богиќевиќ-Миликиќ Биљана, *Организација*, ЦИД Економски факултет, Београд 2006., стр.42.

[472] Види: Јовановиќ Петар, *Менаџмент – теорија и пракса*, Графослог, Београд 2004., стр. 79.

кој ќе се штитат, избор и одредување лица за работа со документите, како и лица кои можат да бидат запознати со тајните податоци (обем, услови и начин на запознавање), одредување просторија за обработка, користење и чување на документите, како и условите под кои овластените лица ќе можат да работат со тајните документи и службено да ги употребуваат; забрана за изнесување тајни документи надвор од одредени простории и одредување на услови под кои може да се изнесуваат; забрана за пристап на неповикани лица во просториите одредени за работа и за чување на тајните документи; забрана за снимање и за скицирање тајни документи и внесување апарати за снимање во одредени простории; одредување начин и средства со кои можат да се пренесуваат тајните податоци; одредување и подготовка на мерки за физичка и за техничка заштита; водење потребна евиденција за тајните документи; забрана за публикување на тајните податоци од документите без одобрение на овластеното лице и без контрола на пропишаните мерки за заштита.[473]

Во развиените земји вообичаено е склучување договор за тајност на деловните податоци меѓу компаниите кои меѓусебно соработуваат. Тие договори се познати како Non-Disclosure Agreement (NDA) и со него, меѓу другото, се предвидуваат високи парични казни за случаи на откривање тајни податоци. Вакви договори се ефикасно средство за пренесување на тајните знаења и другите доверливи податоци и информации за деловните партнери, на начин кој воспоставува и кој обезбедува контрола на нивното евентуално дистрибуирање.[474]

2.2. ПОСЕБНИ МЕРКИ ЗА ЗАШТИТА НА ТАЈНОСТА НА ПОДАТОЦИТЕ

Посебните мерки за заштита на тајноста на податоците опфаќаат: водење посебна евиденција за податоците, за лицата кои со тоа се запознаени и за лицата на кои податоците им се дадени на користење, земање писмени изјави, т.е чување на тајноста на нивната содржина од сите лица кои работат или кои ги употребуваат тие документи; одредување тајни називи на документите под кои ќе се водат работите и документацијата; одредување по број на примероци и лица на кои им се доставуваат и одредување

[473] Стајић Љубомир, *Основи безбедности*, Факултет цивилне одбране, Београд 2005, стр 324-325.

[474] Katulić Tihomir, op. cit. str. 51.

нанадлежно лице за одобрување, умножување или правење на изводи; чување на документите во метални каси и заштита на просторијата со мерки на физичка и техничка заштита; пренесување на документите со курир, под задолжителна придружба со оружје и соодветна техничка заштита на средствата за пренос на документите; писмено примопредавање на должноста меѓу лицата кои ракуваат со тие документи и лицата кои тие документи ги чуваат; комисиско уништување скици, концепти, матрици и други помошни материјали користени при изработката на тие документи.[475]

Правилното ракување со тајните податоци на корпорацијата се протега во текот на сиот животен циклус на тој податок или информација, вклучувајќи ги и оние аспекти што се однесуваат на повлекување и на уништување. На крајот на животниот циклус, се врши проверка дали тајниот податок или информацијата е за архивирање и трајно чување, или за симнување на степен на доверливост и јавно користење или уништување. Тајниот податок или информацијата која веќе не ѝ е потребна за работа на корпорацијата, заедно со дополнителниот материјал, се уништува така да не може да се изврши повторна реконструкција и неовластена употреба од страна на трети лица.[476]

С. Синковски и Б. Лучиќ укажуваат на два клучни проблема во обезбедување заштита на тајноста на податоците – високата цена и неефикасното користење. Во врска со тоа, тие се залагаат за воведување систем за управување со ресурсите за чување на податоците во корпорациите (Storage Resource Menagement-SRM). Овие автори ги дефинираат средствата на SRM како активни, интелектуални и централизирани решенија за водење на работите на ниво на корпорацијата од гледна точка на ресурсите за чување на податоци. За администраторот на заштитата, тие се средства на визуелна мрежа кои ги дефинираат правилата на управување и водат сметка за употребата на ресурсите за чување податоци. Storage Resource Menagement е компонента на целата инфраструктура за управување со корпорацијата, која го подобрува пристапот кон податоците.[477]

---

[475] Стајић Љубомир, op. cit. стр. 325.

[476] Види: Матић Горан, *Основи физичко-техничког обезбеђења*, Привредна комора Србије, Београд, 2006, стр.181.

[477] Според: Синковски Стеван, Лучић Бранислав, „Информациона безбедност – основа безбедног бизниса“, *Саветовање „Злоупотребе информационих технологија и заштита (Ziteh '06)“*, Удружење судских вештака за информационе технологије ИТ Вештак, Тара, 07. – 10.11.2006. године.

Функциите кои ги извршуваат средствата на Storage Resource Menagement опфаќаат: детекција, регистрација, дефинирање на видовите во мрежи (discovery), собирање податоци (data collection), прикажување (maping/visualization), формирање оперативни и ретроспективни извештаи (real-time and historical reporting), управување со настаните и предупредување (event logging and alerting), мониторинг и анализа на капацитетите (performance monitoring and analyzer), управување со содржините (content management), миграција на податоците (data migration), мониторинг на ресурсите на поединечниот сектор (quota monitoring), управување со капацитетите (capacity management), визуелизација, планирање на потребите за ресурси за чување податоци (provisioning), управување со магнетни ленти (media management), управување со промените и конфигурацијата на системот (configuration/change management), управување со правилата/политиката (policy management), управување со средствата од инвентарот (asset management) и друго.[478]

2.2.1. Рестрикции

Рестрикциите претставуваат спроведување на одредени непопуларни, но неизбежни постапки, како што се забрана за копирање на одредени документи, забрана за пристап кон одредени простории, примање приватни посети и сл. Во врска со тоа, потребно е да се обрне особено внимание на регулирање влез и движење во службените простории, режим на влез, движење и задржување, а правата врзани за тоа да се сведат на реалната потреба. Можно е да се користат следните видови на дозволи за влез: (пристап до сите простории во секое време, но само под надзор – пр. хигиеничарка); временска дозвола (пристап до сите простории, но само во одредено време – пр. ноќен чувар); просторна дозвола (пристап само до одредени простории во било кое време); просторно и временски ограничена дозвола (пристап само до одредени простории и само во одредено време – пр. кадри за внесување податоци или сервисери).[479]

Право на пристап во рестриктивен простор, до техниката, до податоците, до информациите и до документацијата треба да се дозволи и да се овозможи, според принципот на „минимум

[478] Според: Абалмазов И. Эдуард, „Концепция безопасности – математический анализ эффективности“, *Системы безопасности*, No. 1, Издателский дом „Гротек”, Москва 1995.

[479] Пошироко види: Петровиќ Слободан, *Полицијска информатика*, Криминалистичко-полицијска академија, Београд 2007., стр. 240-241.

овластувања", само на кадрите на кои тоа работно им е потребно и во одредена мера адекватно на потребите. Секој работник би требало да ги познава само оние елементи што се неопходни за извршување на неговите сопствени задачи.

2.2.2. Процедури

Процедурата е поединечен нормативен интерен акт со која се дефинира конкретно извршување и реализација на одредени работи и задачи.[480] Процедурите за работа утврдени со политиката за заштита треба да се документирани и да се одржуваат. Со работните процедури врзани за заштита на тајноста на податоците треба да се постапува како со официјални документи, а измените треба да ги одобри раководството. Процедурите треба да содржат детални упатства за извршување на секоја работа што опфаќа: обработка и постапување со информации; најмало време на отпочнување и најдоцно време на завршување на работата; упатство за постапување во случај на вонредни ситуации; контакт за поддршка во случај на неочекувани потешкотии при работењето.[481] Ако тајните податоци се наоѓаат на средствата за информатичка технологија (резидентни податоци) се дефинираат правилата: за кориснички пристап, за кориснички дозволи (read only, write, delete), за копирање на податоците, за архивирање, за пренесување по пошта, факс или e-mail, со директна телефонска комуникација, со мобилни телефони, телефонски секретарки, како и правилата за работење на мрежа.[482]

2.2.3. Контрола

Контролата како функција претставува активност на следење на однесувањето на организациските елементи и реализирање на поставените задачи во корпорацијата. Контролите овозможуваат недозволените активности да се откријат навремено, а можноста за извршување на криминалните активности значително да се редуцира. Контролата овозможува откривање на слабоста на заштитата и преземање соодветни акции со цел нивно елиминирање.[483]

---

[480] Види: Милошевиќ Милан, *Физичко-техничко обезбеђење и противпожарна заштита*, ИП Глосаријум, Београд 2006., стр. 18.

[481] *ИСО 17799: Информационе технологије – правила праксе за управљање сигурношћу информација*, Факултет безбедности Универзитета у Београду, Београд 2008., стр. 45-46.

[482] Според: Родиќ Бошко, Ѓорѓевиќ Горан, *Да ли сте сигурни да сте безбедни*, Продуктивност АД, Београд 2004., стр. 105.

[483] Види: Тамбуриќ Јован, „Контрола као функција управљања", *Војно дело*, Vol. 57, бр. 1, Министарство одбране СЦГ, Београд 2005., стр. 113-114.

Роберт Моклер контролата ја дефинирал како „системски обид да се постават стандарди по учинок со помош на планирани цели, да се проектира систем на информативна повратна спрега, да се споредат реалните резултати со однапред утврдени стандарди, да се утврди дали има отстапување, да се измери нивното значење и да се преземат мерки за сите системски ресурси да ги користат на најефикасен начин заради остварување на целите“.[484] Од оваа дефиниција произлегува дека контролата се состои од четири фази: утврдување стандарди и методи за мерење на резултатите, мерење на резултатите, споредување на резултатите со стандардите и преземање корективни акции (ако е потребно). Основната претпоставка за квалитетно спроведената заштита е можноста за контрола. Ако не постои контрола, заштитата со текот на времето ќе ослабне и нема да биде од корист.

Контролата има тројна функција: превентивна (избегнување несакани случувања); дедуктивна (откривање несакани случувања) и корективна (неутрализирање на негативните ефекти од несаканите случувања).[485] Меѓутоа, како што не е пожелно да се запостави контролата, исто така, не е пожелно да се претерува со неа, бидејќи на тој начин се намалуваат иницијативата и акциите и се предизвикува чувство на недоверба, а како краен резултат се јавува несамостојност во работата на вработените.

Во практика честопати се изедначуваат поимите контрола и надзор. Во врска со тоа, треба да се има предвид дека контролата и надзорот имаат заеднички елементи, пред сè во субординацијата на извршителите, односно влијанието на органите (телата) кои вршат надзор/контрола на оној над кој надзорот или контролата се извршуваат. Меѓутоа, ако како критериум се земе континуитет во извршувањето на надзорот/контролата, тогаш контролата може да се означи како еднократен или повеќекратен процес во рамките на надзорот и е негов составен дел. Надзорот без контрола е можен и остварлив, но во тој случај е недоволно ефикасен.[486]

---

[484] Според: Mockler J. Robert, *The Managagement Control Process*, Prentice Hall, Englewood Cliffs, New York 1984, p. 2.

[485] Петровиќ Слободан, оп. цит. стр. 242.

[486] Види пошироко кај: Томиќ Зоран, *Управно право-систем,* Службени лист СРЈ, Београд 2002., стр. 73-74.

2.2.4. Примена на криптографски техники

Посебна област на заштита на тајноста на податоците е примената на различните криптографски техники, кои треба да обезбедат реализација на следните безбедносни барања:

- тајност (confidentiality, secrecy) која обезбедува содржината на криптографски заштитениот податок да биде достапен само на овластените корисници;
- интегритет (data integrity) кој се однесува на можноста за откривање неовластена промена на информацискатa содржина на пораката;
- автентичност (authentication) која се однесува на можноста за утврдување на идентитетот на учесникот во комуникацијата;
- неодречливост (non-repudation) со која се спречува можноста за одречување на реализацијата на одредени активности на корисниците кои учествуваат во комуникацијата.[487]

Криптографските техники со кои се остваруваат споменатите барања, се реализираат со примената на соодветни криптографски алгоритми и протоколи. Тие техники се: преместување симболи на отворениот текст (транспозиција), замена на симболи на отворениот текст (супституција) и комбинација на системите за транспозиција и за супституција. Во таа смисла, транспозициските системи сочинуваат збир на шифрести системи кај кои симболите на отворениот текст се трансформираат во симболи на шифрата според однапред одредена шема на пермутација. При шифрирање симболите на отворениот текст ги менуваат местата, а создадената пермутација претставува клуч на преместувањето. Основната карактеристика на овие шифрести системи е пораката да може да се трансформира во толку различни шифри колку што изнесува вкупниот број на различни пермутации на симболите на отворениот текст.[488]

Супституциските ситеми формираат збир на шифрарски трансформации кај кои симболите на отворениот текст, според однапред утврдена постапка, се заменуваат со одредени симболи од просторот на шифрата. Современата трансформација на податоци и пораки може да се реализира и со погодна комбинација на транспозициските и суптитуциските системи, што создава

[487] Според: Scheiner Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Hoboken NJ 1996., pp. 18-19.

[488] Види пошироко: Denning Dorothy, *Cryptography and Data Security*, Addison-Wesley, Reading MA 1982., pp. 60-61.

комбиниран систем на шифрирање. Тој начин на трансформација на пораките во последно време главно се применува преку симетрични криптографски алгоритми, кај кои клучот за шифрирање е идентичен со клучот за дешифрирање, или со едноставна трансформација на клучот за шифрирање може да се изведе клуч за дешифрирање.[489]

2.3. ПЕРСОНАЛЕН АСПЕКТ НА ЗАШТИТА НА ТАЈНОСТА НА ПОДАТОЦИТЕ

Кога станува збор за персоналниот аспект на заштита на тајноста на податоците, треба да се има предвид, дека човекот од една страна, е носител на заштитата на податоци и информации, додека од друга страна, тој претставува потенцијална опасност. Заканата од „инсајдери“[490] е во сè поголем пораст, поради што човечките ресурси го претставуваат едното од клучните прашања на планот на заштитата. Под поимот „инсајдер“ не треба да се подразира само оној што е постојано вработен во корпорацијата, туку сите оние што имаат внатрешен пристап кон доверливи информации. Во врска со тоа, лицата со внатрешен пристап може да се распределат во следните категории: постојано вработен персонал, поранешни работници и вработени во кооперантски компании.[491]

Вработените, особено невнимателните и незадоволните работници, најверојатно претставуваат најголема закана. Тие имаат секојдневен пристап до чуствителни информации и за злоупотреба често им е потребно многу ниско ниво на образование. Голема закана претставуваат и поранешните работници во корпорацијата, без разлика дали се работи за отпуштени кадри или кадри кои преминале од една во друга компанија, особено конкурентска. Кооперантските компании можат да претставуваат голем проблем за безбедносните системи, бидејќи често имаат пристап до чуствителни податоци.

Во доменот на политиката на човечките ресурси неопходно е да се применат сите расположливи мерки со кои опасноста од „инсајдери“, ако не може целосно да се елиминира тогаш барем

[489] Исто., p.62.

[490] Термин изведен од англискиот збор „inside“ (внатре) - некој од внатре, кој има пристап до информациите, добро упатен; вработен во институција кој има пристап кон осетливи податоци.

[491] Според: Параушић Милан, „Инсајдери – највећа претња информационим системима“, *Безбедност* 5/05, Београд 2005., стр. 870.

да се доведе до прифатливи граници. Тие мерки се однесуваат на: планирање на човечките ресурси; избор на кадри; работна адаптација; безбедносно образование и стручно усовршување. Целите на тие мерки се следните: заштита на податоците и информациите со помош на кадри, што подразбира на клучни места да бидат поставени проверени, сигурни и стручни лица; заштита на податоци и информации од кадри, со оглед дека најголемата закана доаѓа од човекот, што подразбира секој вработен да биде предмет на постојано внимание од менаџментот, при што особено внимение треба да се посвети на индициите[492] кои би укажале на непочитување, склоност кон алкохол, коцка и дрога, финансиски и семејни проблеми и слично; заштита на самите кадри, односно заштита од сопствените ненамерни пропусти и грешки, што се спроведува преку нивното безбедносно образование и развивање безбедносна култура, како и создавање на таков систем на работа и работни услови во кој грешките ќе бидат сведени на минимум.[493]

2.4. БЕЗБЕДНОСНО ОБРАЗОВАНИЕ И ПОДИГНУВАЊЕ НА СВЕСТА НА ВРАБОТЕНИТЕ ВО КОРПОРАЦИИТЕ ЗА ВАЖНОСТА ЗА ЧУВАЊЕ ПОДАТОЦИ

Безбедносното образование треба да даде доволно знаење за потребите, причините и начините за заштита на тајноста на податоци, да ги објасни потребите и причините на почитување и придржување кон стандарните мерки и процедури за заштита, да ја развива безбедносната култура и да потсетува на обврските во однос на заштитата.[494]

Елементарните основи на заштитата на тајноста на податоците и информациите (безбедносни термини, концепти, чувствителни, закани, последици) се стекнуваат со подигање на свеста за потребите од заштита, а надоградувањето се реализира преку обука. Целта на свеста се презентира едноставно со фокусирање на вниманието на заштитата што им овозможува на поединците да ги препознаат

[492] Во криминалистичката терминологија индициите означуваат утврдени факти или околности кои посредно укажуваат на кривично дело, односно на неговиот сторител.

[493] Петровић Слободан, оп. цит. стр. 259-260.

[494] Според: Петровић Слободан, Ћирић Видојко, *Заштита података у аутоматизованим информационим системима*, Научна књига, Београд 1986., стр. 18.

и да ги разберат потенцијалните ризици, а со тоа и важноста на заштитата. Свеста ја креира чуствителноста на вработените на закани и спознанието дека треба да ги штитат податоците и информациите. Подигнувањето на свеста на вработените во корпорацијата за важноста на чување податоци и информации мора да биде секојдневна грижа. Релативно често со неофицијална комуникација или преку семинари на вработените им се укажува какви штети може да настанат со губење одредени информации и како тоа може да се одрази на нив. Една од превентивните мерки може да биде и периодично одржување информативни состаноци за заштита. Разгледуваните теми би требало да ги освежат и да ги надградат порано стекнатите знаења, но и да потсетат на обврската во однос на заштитата, особено затоа што со текот на времето слабее свеста за значењето на заштитата и се намалува вниманието и будноста кон недозволените активности.

2.5. ЗАШТИТА НА ТАЈНОСТА НА ПОДАТОЦИТЕ ВО ВОДЕЧКИТЕ СВЕТСКИ КОРПОРАЦИИ

Заедничка карактеристика на најзначајните корпорации во светот е заштитата на тајноста на податоците поврзани со нивното работење. Така Apple, една од водечките светски компании од областа на информатиката, не само што го крие дизајнот на своите производи, туку и датата на нивното појавување на пазарот, поради што појавата на нови модели на уредите од класата iPhone или iPod е предмет на постојано внимание од страна на медиумите, кои настојуваат да дојдат до „ексклузивни снимки“ на новата генерација мобилни телефони (smartphone) и до информации за карактеристиките на тие производи кои доаѓаат од „доверливи извори“. Вредноста на компанијата Google која е проценета на околу 45 милијарди УСД, исто така спаѓа во најмоќните корпорации од доменот на информатиката, во голема мера потекнува од пребарувачот и тајниот алгоритам кој овозможува на интернет за дел од секунда да се добијат саканите информации. Една од најпознатите светски деловни тајни е поврзана со рецептот на производство на напитокот кока кола. Кога во радиоемисијата „Тој американски живот“ емитувана на 11 февруари 2011 година преку Chicago Public Radio, е објавено дека е откриен тајниот рецепт на тој пијалок, портпаролот на корпорацијата Coca Cola тоа веднаш го демантирал, со напомена дека оригиналната кока-кола содржи една клучна состојка која се чува во тајност од јавноста и од конкуренцијата. Слично како и со кока-кола, една од

големите деловни тајни е поврзана за технологијата на изработка на кристалниот накит и украсите од марката Swarovski. Основачот на таа компанија Даниел Сваровски развил и патентирал посебен индустриски метод за преработка на кристали, со кој се запознати само одбрани работници на спомнатата австриска компанија.[495]

3. КОРПОРАЦИСКА БЕЗБЕДНОСТ ВО ОБЛАСТА НА ИНФОРМАТИЧКАТА ЗАШТИТА

3.1. ДЕФИНИРАЊЕ И ИСТОРИСКИ РАЗВОЈ НА ИНФОРМАТИЧКАТА ЗАШТИТА

Информатичката заштита, односно информатичката безбедност, е предмет на општ интерес како на државните институции така и на корпорациите и на другите стопански субјекти. Во таа смисла, како една од најважните задачи дефинирана е разработката и имплементацијата на прифатливите методи и средства за заштита на информациите, како и барање на системски решенија и средства за заштита со примена на најефективните алгоритми и методи на проектирање на средствата за заштита на информацијата – инструментите на информатичката безбедност. Историски гледано, информатичката заштита (информатичка безбедност) е дефинирана како: заштита на информатичките системи од неавторизиран пристап или модификација на информациите во складирањето, во обработката или во преносот како и од лишување на услугите на авторизираните корисници, вклучувјќи ги неопходните мерки на детекција, документирање и отстранување на таквите закани.[496]

Како што истакнува Д. Волф,[497] историски гледано, развојот на информатичката безбедност започнал во 60-тите години на XX век преку комуникациската безбедност (COMSEC – Communication Security). Со појавата на првите компјутери, на почетокот на 70-тите години, настанала компјутерската безбедност (COMPUSEC – Computer

[495] Види: „Строго чуване тајне успешних компанија“, *Блиц*, Београд 16.05.2011.

[496] Види: *National Information Systems Security Glossary*, NSTISSI No 4009, National Security Agency, Fort Meade MD, September 2000.

[497] Според: Wolf G. Daniel, „Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development“, *National Security Agency US*, Fort Meade MD, Juli 22, 2003.

Security). Кон крајот на 80-тите години на минатиот век COMSEC и COMPUSEC се обединети во информатичка безбедност (INFOSEC – Information Security), која се обидела да ги интегрира порано раздвоените дисциплини, како што се безбедност на персоналот, компјутерска безбедност, комуникациска безбедност и оперативна безбедност. Акцентот на INFOSEC во наредните години е ставен на спречување неавторизиран пристап кон инфоматичките системи, при што се разгледувани, пред сè доверливоста (confidentiality), интегритетот (integrity) и расположливоста (availability) на инфомациите.

За областа на информатичката заштита многу е значајно да бидат надминати ароганцијата и конзерватизмот кои можат да се јават во делот на менаџментот на корпорацијата, а кои можат да се исполнат преку потценување на заканите на интегритетот на информатичкиот систем, непознавање на основната структура ИС, како и избегнување комуникација со персонал кој работи на заштита на тој систем. Како образложенија и изговори за невложување во заштитните мерки често се споменуваат нивната висока цена и неисплатливост на краток рок.[498]

3.2. ТЕОРИЈА НА ИНФОРМАТИЧКО ВОЈУВАЊЕ (INFORMATION WARFARE-IW)

Спектарот на прашања за информатичката заштита е толку широк што ги допира и прашањата на националната безбедност. Како појдовна основа во дефинирање на основните поими од оваа област, се применува теоријата на информатичко војување (Information Warfare - IW). Примат во современата теорија и практика на информатичката заштита имаат Соединетите Американски Држави. Во Стратегијата на национална безбедност на САД од 2002 година,[499] наведено е дека четирите основни столба на меѓународната моќ на таа земја се дипломатската, воената, економската и информатичката моќ (DIME-Diplomatic/Political, Informational, Military, Economic).[500]

[498] Родиќ Бошко, Ђорђевиќ Горан, op. cit. стр. 11.

[499] Според: *The National Security Strategy of the United States of America*, President of the United States, Washington DC, September 2002., p. 14.

[500] Во последно време во западната воена теорија сè повеќе се зборува за седум елементи на националната моќ, во која покрај наведените четири, се воведуваат и три нови елементи: финансии, разузнавачка дејност и приврзаност кон закон (Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement-DIMEFIL).

Една од причините за масовно користење на информатичката сфера како оружје во современата ера е фактот дека модерните достигнувања во областа на техниката, медиумите и комуникациите станале достапни и за неразвиените земји. Тие нови околности придонесуваат кон можноста за изедначување на конкурентноста на појаки и на послаби земји во меѓусебното натпреварување, што може да доведе до „поништување“ на воениот принцип „решение на маса“, односно до тоа воената моќ повеќе да не е пресудна во одмерување на силите помеѓу две или повеќе држави. Оружјата на информатичката ера им помагаат на малите држави против големите и ги фаворизираат „слабите“ во однос на „силните“. На наведеното укажуваат и т.н. сајбер напади на неформални групи врз значајните воени и индустриски информатички системи на моќните држави како САД, Велика Британија и СР Германија. Од тие причини, на прагот во новата информатичка ера осмислувањето на правилната национална стратегија за безбедност може да има големо влијание за конечниот резултат на современите конфликти.[501]

Во доктринарниот документ на Министерството за одбрана на САД од 2003 година, под назив „Патоказ за информациони операции“ (Information Operations Roadmap),[502] изнесени се неколку насоки кои укажуваат на значењето на информатичката активност во рамките на идните воени операции кои ќе ги изведуваат вооружените сили на САД. Дадена е прогноза дека „информацијата“, која секогаш била од голема важност во воените вештини, денес и во иднина ќе има клучно значење за воен успех и нагласена потребата во идниот период при изведување на информациските операции на САД тие да бидат во надлежност на Министерството за одбрана, коешто истите ќе ги раководи централизирано. Основната цел на тие активности е остварување на американската доминација во глобалниот информатички спектар. Поради тоа потребно е да се изврши трансформација и сортирање на информациските операции на централни и главни по важност воени операции кои ги извршуваат вооружените сили на САД, заедно со копнените, со воздушните, со поморските и со специјалните операции. Исто така, според

[501] Види: Миљковић Милан, „Информационо ратовање у савременој теорији и пракси“, *Војно дело*, Министарство одбране Републике Србије, Београд, лето 2010., стр. 258-259.

[502] Пошироко види: *Information Operations Roadmap*, U.S. Department of Defense, Arlington County VA, 30 October 2003., pp. 6-9.

споменатиот документ, способност за брзо дистрибуирање „убедливи информации“, за противничкото јавно мислење, со кои директно се влијае на надлежните од противничката страна, претставува значајно зголемување на способноста за одвраќање од агресија.[503]

Институционализацијата на информатичкото војување првенствено била поврзана за воената сфера. Меѓутоа, стратегиското значење на информацијата условило проширување на Information Warfare и на други сфери на човековото дејствување, вклучувајќи го и раководењето со корпорациите. Од самата дефиниција за информатичкото војување произлегува дека се работи за акции што се преземаат за да се постигне информатичка супериорност, како и поддршка на деловните стратегии со што би се влијаело на информациите на конкурентите, со задржување на информатичката моќ, односно заштита на сопствените информации.[504] Анализата на оваа дефиниција укажува дека поимот информационо војување во сферата на корпорацискатa безбедност има три елементи, односно димензии: Офанзивна, која вклучува напад со информации поради откривање на негативните страни на противникот, негирање на спротивставените информации, нивно уништување, односно остварување на влијание на конкурентска перцепција; дефанзивна (IW hardening – непропуслива информациска заштита, внатре во информационото војување), која подразбира заштита на сопствените информации, но и заштита на информациите кои доаѓаат од страна на соработниците; експлоатациска, која настојува да ги искористи сопствените информации на вистински начин и во вистинско време како поддршка на одлучување и да го оневозможи конкурентот да ги искористи своите информации.[505]

Еден од примерите кои говорат за класична Information Warfare била тужбата која американската компанија Oracle – третиот производител на софтвери во светот ја поднела против германскиот конкурент – корпорацијата SAP, тврдејќи дека истата компанија ги крадела податоците и потоа неовластено продавала услуги на клиентите од Oracle по пониски цени. Калифорнискиот огранок на таа американска компанија во судот во Сан Франциско поднела тужба во

[503] Миљковић Милан, op. cit. стр. 259.

[504] Според: Boni William, Kovacich L. Gerald, *Netspionage: The Global Threat to Information*, Butterworth Heinemann, Boston/Oxford 2000., p. 223.

[505] Bilandžić Mirko, *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, op. cit. str. 53.

која во 11 точки се обвинува SAP за измама, нелојална конкуренција и неовластено копирање заштитен софтвер, со што направила кражба од големи размери. Во однос на овој спор се поставило прашањето поради што овие две моќни компании во информатичката сфера влегле во овој спор, ако се има предвид фактот дека за нивниот бизнис успех многу е значаен имиџот на компанијата и брендот што таа го направила. Одговорот на ова прашање е дека во заднината на судирот се нашла Information Warfare помеѓу Oracle и SAP околу превласта на глобалниот пазар на софтвер. Сличен судир истата година се појавил и меѓу американската компанија Hewlett-Packard (HP) и тајванската компанија Acer, која била обвинета дека неовластено користела пет патентирани технологии на HP за производство на персонални компјутери со барање да се забрани понатамошната продажба на производите на Ацер на пазарот на САД. И овој судир во заднина имал намера да ја спречи компанијата Acer да дојде на трето место на најголемите производители на комјутери во светот.[506]

Посебен случај во доменот на информатичкото војување претставува „аферата Викиликс", поврзана со дејствувањето на една меѓународна непрофитна медиумска организација со седиште во Шведска, која преку вебсајтот The Sunshine Press од 2006 година објавува на друг начин недостапни материјали, добиени од анонимни извори.[507] Споменатата организација тврди дека ја основале кинески дисиденти, како и новинари, математичари и информатички стручњаци од САД, Тајван, Европа, Австралија и Јужна Африка и таа има околу 1.2 милиони документи. Меѓу другото, во април 2010 година Викиликс објави снимка за инцидент кој се случил во 2007 година во која американските војници убиваат ирачки цивили. Во јули истата година Викиликис го објави „Авганистанскиот воен дневник" кој компилација на повеќе од 76.900 документи во врска со војната во Авганистан кои претходно не биле објавени во јавноста. Во октомври 2007 година преку споменатиот веб сајт се објавени речиси 400000 документи под името „Ирачки воени дневници". Исто така, во овој месец во 2010 година Викиликс проследил околу 250000 тајни документи на Стејт департменот во списанијата: The Guardian, New York Times, Le Monde, Der Spiegel. Откритијата на Викиликс

[506] Исто., стр.50-51.

[507] Според: Haddow Douglas, „Grim truths of Wikileaks Iraq video", *The Guardian*, London, 7 April 2010.

предизвикаа големо интересирање, а и контроверзи во светската јавност, додека самата веб страница во повеќе наврати била предмет на хакерски напади, за кои се обвинети некои разузнавачки и безбедносни служби на држави на кои објавените податоци не им биле во интерес. [508]

Има мислење дека евидентната непропорционалност во информатичкиот развој и употребата на информатичката технологија која е присутна меѓу различни современи компании и држави, претставува значаен технолошки фактор што придонесува технолошки инфериорните ентитети да работат на воспоставување рамнотежа за наоѓање слаби точки на противникот, односно кон конфликтите да приоѓаат на асиметричен начин. Притоа мора да се води сметка дека непропорционалноста во информатичкиот развој не се однесува само на можната употреба на информатичките и на комуникациските технологии за воени цели, кои во втората половина на XX век довеле до зголемување на конвенционалната моќ на силните светски држави, па дури и употребата на интернетот, односно глобално медиумско подрачје, во кои еден број помалку развиени држави и компании модерната употреба на информационата технологија ја доживуваат само како нов инструмент за спроведување на виртуелниот културен империјализам.[509]

3.3. ШТЕТНИ ВЛИЈАНИЈА НА ИНФОРМАТИЧКАТА ИНФРАСТРУКТУРА

Информатичката инфраструктура може да биде изложена на штетни влијанија од различна природа кои директно или индиректно можат да ја загрозат нејзината функционалност. Тие влијанија можат да се класификуваат на: дефекти, инциденти и напади.[510] Дефектите се потенцијално штетни настани, предизвикани од внатрешни дефекти на системот или дефекти на надворешните елементи неопходни за негово функционирање. Тие можат да бидат и како последици на грешки при самото проектирање на софтверот,

[508] Види: *„Развој система безбједности и заштите корпорација" (Зборник радова)*, Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука 2011., стр. 293.

[509] Svete Uroš, op. cit. str. 115.

[510] Според: Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R., *Survivable Network Systems: An Emerging Discipline*, Technical Report (CMU/SEI-97-TR-013.ESC-TR-97-013) CERT, Pittsburgh PA, November 1997.

дефекти на хардверот, човечки грешки и др. Категоријата на инциденти ги вклучува сите случајни настани како што се природните непогоди и катастрофи. За разлика од дефектите, инцидентите се настани чии причини се наоѓаат надвор од системот.[511]

Нападот на информатичкиот систем може да се дефинира како директна акција против мрежата или информатичкиот систем со цел неовластено да се пресретне или да се прекине некоја операција, да се преземе контрола и да се уништи, да се промени или да се корумпира податокот (со меморирање или обработка).[512] Според некои автори, можат да се разликуваат три видови напади на информатичкиот систем:

– физички напад, насочен кон расположливоста на нападнатиот систем (употреба на конвенционални оружја против инфраструктурата во која се наоѓаат информатичките системи или против линијата на преносот на информацијата);[513]
– електронски напад (користење енергетско оружје кое е во можност да емитува електромагнетна енергија концентрирана во снопови со автоматски или субавтоматски честички или оружје кое испушта електормагнетски импулси со цел да се преоптоварат или да се онеспособат електричните споеви на системот);
– сајбер напад (примена на т.н. злонамерни информатички програми чија задача е да го заразат информатичкиот систем на противникот со цел негово оштетување или крадење на различни доверливи или чуствителни податоци).[514]

Според Роберт Иген,[515] од безбедносните закани на информатичките системи кои се од внатрешно потекло, најзастапени се материјалните штети, оштетувања и дисфункција, што се појавуваат случајно поради лошото работење на вработените, на одговорните и на раководните лица. Во тој контекст, поопасни се оние загрозувања

[511] Петковић Тодор, op. cit. стр. 292.

[512] Види: Stallings William, *Network and Internetwork Security – Principles and Practice*, Prentice Hall, Englewood Cliffs, New Jersey 1995., pp. 29-30.

[513] Marlin Steve, Darvey Martin, „Disaster-Recovery Spending on the Rise", *Information Week*, Manhasset NY, Avgust 2004., p. 26.

[514] Петковић Тодор, оп. цит. стр. 293.

[515] Пошироко види: Eagan Robert „The Risks Assessment Methodology", in: Energy & Security: Global Challenges - Regional Perspecives (Conference Report), Program of Atlantic Security Studies & Prague Security Studies Institute, Prague 2005., pp. 42-44.

што се производ на свесно и намерно дејствување на човечкиот фактор, од разни видови имотен, економски, па сè до политички криминал. Надворешните загрозувања на информатичкиот систем можат да бидат од различна природа, од имотни, преку политички до компјутерски и други форми на високотехнолошки криминал (неовластени напади на информатичките системи од државни и од недржавни актери; копирање, преименување, кражба или уништување работни податоци; намерно предизвикување дисфункција на информатичкиот систем; електронска шпионажа; префрлање финансиски средства на приватни сметки; наведување одредени параметри за „самоуништување“ на информатичките системи; компјутерски саботажи, диверзии и терористички напади и др).

Б. Родиќ и Б. Ѓорѓевиќ укажуваат дека напаѓачите се појдовна точка за секој напад на компјутерските системи, иако се разликуваат по тоа кои се и од каде се, според своите способности и според тоа дали се внатре или се надвор од системот што го напаѓаат.[516] На тој начин, напаѓачите можат да се поделат на шест категории: хакери,[517] кои провалуваат во компјутерскиот систем главно заради предизвик кој претставува лажење на системот на заштита или заради желбата да добијат статус на приоритетен корисник на системот; шпиони, кои ги напаѓаат информатичките системи заради информации кои можат да бидат користени во политички, во воени или во економски цели; терористи, кои влегуваат во компјутерските системи за да предизвикаат страв кој им носи политичка корист или им овозможува собирање финансиски средства; организирани напаѓачи, кои за сметка на одредена компанија провалуваат во компутерските системи на конкурентските компании заради доаѓање до релевантни информации за својот наредбодавач; професионални криминалци, кои напаѓаат информатички системи заради финансиска корист, и вандали, кои напаѓаат компјутерски системи исклучиво да нанесат материјална штета.[518]

[516] Родиќ Бошко, Ђорђевиќ Горан, op. cit. стр. 21.

[517] Хакерите веќе подолго време се сметаат само како безопасни истражувачи на информациските системи. Во однос на нелегалност, нелегитимност, насилност и штетата што ја нанесуваат, нема големи разлики помеѓу нив и терористите.

[518] Родиќ Бошко, Ђорђевиќ Горан, op. cit. стр. 22.

Божидар Јаворовиќ укажува дека постојат следните извори и видови загрозувања на информатичките системи на корпорации:

- програмски (софтверски) извори на загрозување, кои можат да произлегуваат од грешки во програмите или од намерно со цел направени програми за нанесување штети во компјутерските системи (вируси, тројански коњи и спамови);
- хакерски напади, со намера за продор во компјутерските системи за со нив да се манипулира или да се дојде до заштитените податоци и информации на компаниите, до деловни тајни и други доверливи податоци и информации;
- пиратерија, односно бесправно умножување и продажба на пиратски софтвери и програми;
- физички напад на информатички и на комуникациски системи, вклучувајќи интерна и екстерна кражба на информации и податоци, кражба на информатичка опрема, онеспособување сервери, уништување информатичка опрема, намерно предизвикување пожари и терористички напади на информатичките системи;
- загрозување од околината (влага, бучава, прав, електрицитет, природни непогоди и катастрофи, прекин на електрична енергија и нагли промени во напонот);
- внатрешни организациски проблеми (несоодветна организација на информатичкиот систем, неизградена информациска и комуникациска мрежа, нестручен информатички кадар, лошо управување и недостаток на контрола, неодржување и лошо сервисирање на опремата, нередовно и нецелосно надополнување на базата со податоци, недоволна информатичка писменост и лоша обука на корисникот на системот, некомпатибилност на комјутерскиот систем);
- информатичка и деловна шпионажа (дејствување странски разузнавачки служби, шпионажа од страна на конкурентите, откривање и предавање тајни податоци);
- недолично и криминално однесување на корисниците на информациските системи и мрежи особено на интернетот;
- технички грешки во компонентите на информатичките и на комуникациските технологии.[519]

[519] Javorović Božidar, Bilandžić Mirko, op. cit. str. 297-306.

3.4. МЕТОДИ И СРЕДСТВА ЗА ЗАШТИТА НА ИНФОРМАЦИИТЕ

Под мерки за безбедност на информации се подразбира општи правила за заштита на податоци кои се реализираат на физичко, на техничко или на организациско ниво. Стандардите на информатичката безбедност се организациски и технички процедури и решенија наменети за систематско и унифицирано спроведување на пропишаните мерки на заштита. Со мерките и со стандардите на информатичката безбедност се утврдуваат минимални критериуми за заштита на доверливи податоци во деловните субјекти.[520]

Ефикасната примена на информатичката безбедност во деловните субјекти има потреба од систематско управување со различните аспекти на информатичката безбедност, а во согласност со стандардите што одговараат и со други нормативни рамки. Најзначајна меѓународна норма за управување со информатичка безбедност е стандард ISO/IEC 27001:2005, со кој се дефинираат потребите за воспоставување, одржување и континуирано подобрување на системот на управување со информатичка безбедност. Стандард ISO 27001 преку редица настани и правила пропишува начин на кој треба да биде организирана информатичката безбедност во која било организација без разлика на нејзината големина или дејност.[521] Специфичноста на оваа норма е во тоа што поимот информатичка безбедност не се гледа исклучиво од информатички аспект, туку се предвидува и примена на други елементи од корпорацискатa безбедност, како што се физичка и техничка безбедност, управување со човечки ресурси, правна заштита и др.[522]

Нормата ISO 27001 содржи правци и спецификации за помош на организациите кои се во развој на системите за управување на информатичката безбедност (ISMS – Information Security Menagement System). ISMS претставува систематски пристап во управување со безбедносни информации кои се наоѓаат во сопственост на орга-

[520] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 205.

[521] За Стандардот ISO/IEC 27001:2005 пошироко на http: www.iso-27001standard.com

[522] Стандардот ISO 27001 содржински се состои од 11 подрачја, 39 контролни цели и 133 контроли кои помагаат во идентификација, управувањето и намалувањето на различни закани за безбедносните информации, со што сеопфатно се покрива потребата од информатичка безбедност на деловните субјекти.

низацијата, а која вклучува извршители, процеси, информатички системи, политики и процедури.[523]

Според Б.Јаворовиќ, со цел заштита на информатичките системи на корпорациите потребно е спроведување мерки кои содржат различни подрачја, и тоа:

- нормативно-правни мерки кои значат, пред сè, донесување правилници за информатичка и комуникациска заштита со кои би се разработиле правата, обврските и одговорностите во сите структури во компанијата од управата, менаџментот и организациските единици па до секој вработен;
- организациски мерки, вклучувајќи воспоставување системи (организациони единици) за информатичка и комуникациска безбедност, организациски решенија за спроведување одредени заштитни мерки (ниво на пристап до информациските бази, процедури и постапки, безбедност на мрежата, организациски безбедносни зони и др.);
- програмски мерки (навремено програмирање одредени постапки за заштита во согласност со прашањата: кој, што, од што, каде, кога, како и со што, примена на антивирусна програма за заштита, заштита од пробив на хакери и други видови надворешно загрозување, поставување на т.н. firewall заштита, примена на „силни“ лозинки, програмски надградувања и др);
- техничко-технолошки мерки (искористување на заштитните можности на информатичко-комуникациската технологија, примена на технички средства, вклучување алармни системи, видео надзор, системи за ограничување пристап до просториите, серверите, базите и сл);
- кадровски мерки (безбедносни процедури при избор на работни менаџерски и водечки стручни кадри и прием на нови вработени, именување информатички менаџери, избор на способни системски и мрежни администратори и друго);
- образовни мерки (безбедносна обука на сите вработени и различни видови стручно усовршување во спроведување на безбедносните процедури и мерки на заштита, добивање соодветни сертификати и сл.);
- надзор и контрола, која вклучува проверка на рестриктивниот простор, преглед на софтвер и хардвер, вршење на тес-

[523] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 98.

тирање, следење одредени активности и безбедносни инциденти, постојана комуникација со одговорното раководство и стручните служби, увид во примената на меѓународните и на националните прописи и норми и др.);
- санкции, кои во зависност од нанесената штета можат да се движат од сослушување, опомена, намалување плата, материјална одговорност, промена на работното место, одземање овластувања до отказ и кривична одговорност;
- физички мерки, кои опфаќаат надзор на влезно-излезни места, идентификација на посетителите и на нивното доаѓање до одредени точки, спречување незаконско и неовластено движење во работниот простор, спречување кражби и провали, интервенција во случај на пожар и други загрозувања и слично;
- контраразузнавачки мерки, кои се преземаат на софтверско, на хардверско, на техничко и на физичко ниво, со цел спречување илегално и неовластено влегување во базата на тајни податоци, на конкурентски (домашни и странски) корпорации или странски разузнавачки служби.
- заштитно уредување на деловното опкружување (мерки за одржување на оптимална температура, намалување влага, бучава, прав) со цел за заштита и сигурна работа на информациските и комуникациските системи.[524]

3.5. СПРЕЧУВАЊЕ НЕАВТОРИЗИРАН ПРИСТАП ДО ИНФОРМАТИЧКИТЕ СИСТЕМИ НА КОРПОРАЦИИТЕ

Одредени автори укажуваат дека заштитата на информатичките системи на корпорациите од неавторизиран пристап опфаќа четири области од значење на информатичката безбедност: безбедносна проверка, физичка безбедност, безбедност на податоците и безбедност на информатичкиот систем. Во таа смисла, безбедносната проверка претставува област на информатичката безбедност во чии рамки се утврдуваат мерки и стандарди за информатичка безбедност и се применуваат на лица кои имаат пристап до заштитените податоци на корпорациите. Физичката безбедност е област на информатичката безбедност во чии рамки се утврдуваат мерки и безбедносни стандарди за заштита на објекти, простор и уреди во кои се наоѓаат податоци кои треба да се

[524] Javorović Božidar, Bilandžić Mirko, op. cit. str. 323-327.

заштитат. Безбедноста на податоците е област на информатичката безбедност за која се утврдуваат мерки и стандарди кои се применуваат како општи заштитни мерки за превенција, откривање и отстранување штети од загуби или неовластено откривање заштитени податоци. Во рамките на безбедносниот информациски систем се утврдуваат мерки и стандарди за заштита на податоци кои се обработуваат, се архивираат или се пренесуваат низ информатичкиот систем, и обезбедуваат заштита на интегритетот и расположливиот информатички систем во процесот на негово планирање, проектирање, инсталирање, користење, одржување и престанок на работа.[525]

Со авторизацијата на корисникот и по пристапот до информатичкиот систем се ограничуваат акциите и манипулациите со податоци и информации. Во таа насока, секоја спроведена акција над податоците или над информациите мора да биде регистрирана, особено промените, ако ги имало. Корисникот на податоците треба да се евидентира со време и видови проверки. Со тоа најчесто користено средство за идентификација на корисник е лозинка (password).[526]

3.6. АВТЕНТИЧНОСТ (AUTHENTICATION) И НЕПРОЦЕНЛИВОСТ (NON-REPUDIATION) НА ИНФОРМАЦИИТЕ

Со развојот во компјутерската технологија и појавата на мрежи (LAN и WAN и пред сè на интернетот) се проширила листата на видовите информации, пред кои се поставуваат безбедносни барања. Тоа се првенствено автентичноста и неодрекувањето. Врз основа на споменатите својства на информациите (или безбедносни сервиси на информации и информатички системи), во 90-тите години на XXI век е формулиран поимот информатичка сигурност (Information Assurance- IA). Важно да се воочи дека разликата не е само од терминолошка природа, туку се работи и за суштински промени.[527]

Утврдување на автентичноста значи докажување дека корисникот на информатичкиот систем е навистина тој за кој се претставува. Таков доказ обично се состои од комбинација на

[525] Ivandić Vidović Darija, Karlović Lidija, Ostojić Alen, op. cit. str. 206-207.

[526] Родић Бошко, Ђорђевић Горан, op. cit. стр. 22.

[527] Види: Stephenson Peter, „Authentication: A Pillar of Information Assurance", in: *SC Magazine*, Vol. 21, No. 1, New York, January 2010., p. 55.

податоци за следните карактеристики на корисникот: нешто што го знае само едно лице (лозинка), нешто што го има само едно лице (картичка), нешто што има само едно лице (отисок од прст), нешто што едноставно претставува однесување на некоја личност (ракопис, говор). Проверката на автентичноста е способност на системот да го верификува идентификаторот (или повеќе од нив) кој го предочува корисникот, односно утврдува дали кон системот пристапува оној корисник чиј идентификатор е предочен во системот.[528]

3.7. ДЕТЕКЦИЈА (DETECTION) И РЕАКЦИЈА (REACTION*)*

Важни карактеристики на информатичката безбедност се оперативност (operational in nature) и чувствителност на време (time-sensitive). Овие карактеристики ги изразуваат термините детекција и реакција. Во прашање се дефанзивни оперативни можности за кои заедно со традиционалните информатичко-заштитни активности, од доцните 90-тите години од минатиот век го користат терминот теорија на информатичко војување, односно одбранбени информациски операции. (Defensive Information Operations – DIO).[529] Поимот информатичка безбедност во САД официјално е воведен во 2002 година со директива на Министерството за одбрана. Според тој документ информатичката безбедност ја сочинуваат информациски операции за заштита и одбрана на информации и информациски системи, со кои се обезбедува нивната примена, интегритет, автентичност, доверливост и неодрекување, а што подразбира реставрација на информатичките системи и на инкорпорираните можности за заштита, детекција и реакција.[530]

3.8. ИНФОРМАТИЧКА БЕЗБЕДНОСТ ВО СОВРЕМЕНИОТ СВЕТ

За значењето на информатичката безбедност во САД сведочи структурата за управување на безбедносните информатички структури, во која освен државните институции важно место

[528] Родиќ Бошко, Ђорђевиќ Горан, op. cit. стр. 90.

[529] Според: „Field Manual No. 3-13, FM 3-13 (FM 100-6), in: *Information Operations: Doctrine, Tactics, Techniques and Procedures*, Department of the Army, Washington DC, November 2003.

[530] Според: *Department of Defense Directive No. 8500.1 Information Assurance*, U.S. Department of Defense, The Pentagon, Arlington County VA, October 24, 2002.

заземаат и научните установи.[531] Според нив, со информатичка безбедност во САД се занимаваат и други институции кои ги обединуваат теориските и практични истражувања, меѓу кои најпознати се координациски центри-тимови за одговор CERT/CC (Computer Emergency Response Team), CIAC (Computer Incident Advisory Capability) и FIRST (Forum of Incident Response and Security Teams). Овие установи собираат статистички податоци за нападите и ранливоста на хардвери и софтвери, при што наоѓаат ефикасни одговори за противдејства и ги објавуваат во билтени. Научно-истражувачката дејност во оваа област е дефинирана преку првите пет програми. Националниот план за заштита на информатичката инфраструктура на САД од 2000 година, како и петте национални приоритети во областа на заштитата на информатичките структури, дефинирани се во Националната стратегија за безбедност на сајбер просторот од 2003 година. Сите американски универзитети, почнувајќи од Универзитетот за национална одбрана (UND) во својот состав имаат факултети за информатичка безбедност.

Во САД постои тесна соработка помеѓу државниот и приватниот сектор на план на информатичката безбедност, што е дефинирано во сите доктринарни документи. Развиените европски земји во разбирањето на поимот информатичка безбедност со нагласен прагматичен пристап ги следат теоретските и практичните решенија кои се применуваат во САД.[532]

Воведувањето на поимот информатичка безбедност во Руската Федерација е од понов датум (од половина на 90-тите години на XX век). Според некои автори,[533] во поранешниот Советски Сојуз со децении на одредена листа на технолошки производи се забранувал извоз во земји од социјалистичката сфера. Советскиот Сојуз ја

[531] Национален институт за стандарди и технологија (NIST), Институт за заштита на информатичка инфраструктура (Institute of Information Infrastructure Protection-I^{3}P), Федерален центар за заштита на информатичка структура (FedCIRC), Национален центар за заштита на информатичка инфраструктура (NIPC), Национален центар за безбедност и реакција (NSIRC), Центар за анализа на информации (ISAC) и Центар за информатичка инфраструктура на федералните агенции и министерства.

[532] Види: Luiijf Eric, „Information Assurance and the Information Society“, in: Gattiker Urs, Pedersen Pia & Petersen Karsten (eds.)*, EICAR Proceedings*, Aalborg DK 1999., pp. 3-4.

[533] Панарин Н. Игор, *Проблемы обеспечения информационной безопасности*, Олма-Пресс, Москва 2003., стр. 11-12.

изгубил Студената војна поради занемарување на безбедноста во информатичката сфера, за што сведочи податокот дека во сиот Советски блок кон крајот на 70-тите години во употреба биле само 650 компјутери. Индикативно, во таа смисла, било анкетирањето на компетентни соговорници што го спровело реформски ориентираниот весник „Литературная газета" која ја спровела во 1988 година. (Каква е вашата оцена за овдешната ситуација со персоналните компјутери). Одговорите на прашањето биле слични: „Катастрофална... Нашето ниво на производство е од 100 до 1000 пати пониско од американското", „Ситуацијата е едноставно очајна", „Компјутерите кои ги произведуваме се грозни машини со кои ништо не може да се направи" итн. Инаку, информатичкото образование во Советскиот сојуз е воведено во 1985 година, а банкарските и другите трансакции и потоа се извршувале рачно, додека банкомати немало сè до распаѓањето на СССР.[534]

Во доктринарните документи на државите наследници на СССР, информатичката безбедност е дефинирана како состојба на заштита на животно важни личности, компании и држави во информатичката сфера од надворешни и од внатрешни опасности (ризици),[535] односно состојба на заштита на информатичката средина на компанијата која овозможува нејзино формирање, користење и развој во интерес на граѓаните, организацијата и државата. Може да се воочи дека во „Доктрината на информатичка безбедност во Руската Федерација" терминот информациската безбедност се користи во поширока смисла, додека во теоријата и практиката на западните земји тој поим се однесува само на информациите и информатичките системи. Исто така, според некои мислења, информатичката заштита, односно информатичката безбедност претставува дисциплина на информатичките технологии, бидејќи таа е нејзина основна компонента.

Во Руската Федерација во февруари 2003 година формиран е Координативен совет во Министерството за образование за прашањата околу подготовката на кадри од областа на заштита на државни тајни и информатичка безбедност, и е воведена група на специјалност наречена „Информатичка безбедност". Дефинирани се и федерални компоненти за информатичка безбедност, програми

[534] Според: Judy W. Richard, Clough L.Virginia, *The Information Age and Soviet Society*, Hudson Institute, Indianopolis IN 1989., pp. 23-25 & 35.

[535] Панарин Н. Игор, оп. цит. стр. 17.

за усовршување и последипломски студии (медоти и системи на заштита на информации, информациска безбедност). Во таа земја денес проблематиката поврзана за безбедност и заштита на информациите се изучува на 148 разни факултети. Покрај ова околу образованието кадри во областа на информатичката безбедност се занимаваат 12 министерства и канцеларии, многу научни организации и институции меѓу кои се и Московскиот државен институт Ломоносов и Академијата за криптографија на Руската Федерација.[536]

3.9. КОМПАРАТИВНА ПРАКТИКА НА БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ ВО НАЈВАЖНИТЕ СОВРЕМЕНИ КОРПОРАЦИИ

Според Здравко Баздан, информатичките системи на корпорациите можат да се поделат на: информатички системи за собирање и обработка на податоци; системи за информирање (внатрешно информирање менаџери и вработени, информирање на деловните партнери и слично); систем на информации кои се основа на сите информациони и деловни структури; интегрални информатички системи кој го сочинуваат изворите на податоци и информации, нивно собирање, селекција, проверка на обработените податоци, информатичка обработка, создавање, развој и одржување на информатичките бази, презентација на одредени сегменти или на целиот собран информатички материјал, пренос до корисникот, следење на успешноста и ефикасноста на работа на системот т.е. враќање на информациите во сопствената база на податоци и информации, со оптимален надзор и управување. Главен дел на тој систем-информатичко оперативна единица, често се нарекува и оперативно-информатички центар. На врвот на информатичкиот систем внатре во корпорацијата се наоѓа управа или информатички менаџмент под чија команда се и стручните служби за градење и развој на информатичкиот систем, истражување за информатички потреби, корисничка обработка и подготовка на информации, деловно-разузнавачка дејност и за информатички надзор и прашања за безбедноста. Според податоците на З. Бездан, од современите транснационални и мултинационални корпорации, со најсложени информатички системи располагаат: General Electric, Royal Dutch

[536] Петровић Лазар, „Информациона сигурност у савременом свету“, *Инфо М – Часопис за информационе технологије и мултимедијалне проблеме*, Vol. 6, бр. 24, Факултет организационих наука, Београд 2007., стр. 15-17.

Shell, General Motors, Toyota Motors, Exxon Mobil, British Petroleum, JP Morgan Chase, кои и според други параметри се меѓу најмоќните компании во светот.[537]

Како што истакнуваат Б. Родиќ и Г. Ѓорѓевиќ некои закани на информатичките системи во корпорациите никогаш не се откриваат, поради што често се ангажираат и посебни служби кои ги откриваат или ги проценуваат можностите за закана. Истовремено, ранливоста на системот е обратно пропорционална од степенот на неговата одбрана. Значењето на самиот информатички систем зависи од неговата финансиска, материјална или политичка вредност. Анализата на заканите, ранливоста и значењето на системот, расположливите противмерки и односот цена на ризик и цена на трошоци, помага во водење и одредување на потребните активности кои треба да ги преземат раководствата на компанијата и приоритетите на работата во согласност со ризиците во заштита на информациите, како и воведување одбранбена контрола за да се заштитат од самите ризици. Во некои ситуации потребно е постапката на оценување од ризици и изборот на контрола да мора да се повторат неколку пати за да се опфатат различни делови од корпорацијата или нејзини одделни информатички системи. Методите за оценување на ризици можат да се применат и на сета организација, или само на некои нејзини делови, како и на одделни информатички системи, специфични компоненти на системот или услуги, функции, каде што тоа е можно и е од корист.[538]

Божидар Јаворовиќ укажува дека информатичките системи за светот станале тоа што се и нервните системи и крвотокот во човечкиот организам, така што пропаѓањето на светскиот информатички систем би довел до распад на современата цивилизација и би го вратил животот на човекот на ниво од далечното минато. На макро ниво на корпорацијата, уништувањето на базата на податоци или на внатрешниот информациски систем би значело деловна катастрофа која многу компании не би ја преживеале. Според овој автор, проблем е што со сè поголемата сложеност, големина и важност на информатичките системи се зголемува нивната чувствителност на сите видови напади и загрозувања при што последицата од таа деструкција станува се потешка.[539]

[537] Bazdan Zdravko, op. cit. str. 66.

[538] Родић Бошко, Ђорђевић Горан, op. cit. стр. 189-190.

[539] Javorović Božidar, Bilandžić Mirko, op. cit. str. 100.

Современите светски корпорации сметаат дека информатичката безбедност е еден од најважните приоритети за водење на нивното работење. Во согласност со тоа евидентни се и радикалните промени во организацијата на службите за информатичка безбедност во тие компании, кои не само што се одвојуваат од службите за развој и за примена на информатичка технологија, туку често ја воведуваат и функцијата директор (CISI) и менаџер за информатичка безбедност (BISO). Тоа докажува дека прашањата за информатичка безбедност и проблемите за заштита на деловните информации Што до пред извесен период се сметаа за маргинални, успеаја да дојдат во позиција да бидат во делокруг на интересирање на самиот врвен менаџмент.[540]

3.10. СПРОТИВСТАВУВАЊЕ НА ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

Според Горан Бошковиќ, сајбер просторот е вештачка творба која бара висока техничка опременост и добра информатичка инфраструктура. Во неа паралелно постои виртуелна и реална, како и колективна комуникација. Како таков сајбер просторот претставува заедничка сопственост за доброто на целото човештво. Во тоа опкружување тешко е да се зборува за национални размери на криминалот и за неговата општествена опасност, барем во конвенционална смисла на зборот. Затоа високотехнолошкиот криминал се класификува во најизразен облик на прекугранично криминал, против кој борбата не може да биде конвенционална. Оттука, нивото на кое сторителите на дела во областа на високотехнолошкиот криминал и нивните организации се претворил во тоа што може да се нарече „информатичка војна“ е многу високо и е во константна нагорна линија.[541]

Високотехнолошкиот криминал опфаќа збир на кривични дела каде што како објект на извршување и како средство за извршување кривични дела се јавуваат, компјутери, компјутерски мрежи, компјутерски податоци, како и нивните продукти во материјален и во електронски облик. Оваа дефиниција вклучува голем број злоупотреби на информатичка технологија, како и злоупотребата во областа на радиодифузната технологија. Така,

[540] Според: Муравъева Ирина, „Новый взгляд на службу информационной безопасности компании“ (http: www.bre.ru/security/20033.html).

[541] Бошковић Горан, op. cit. стр. 106-107.

се разликуваат кривични дела во кои како средство и како објект за извршување се појавуваат компјутерите (Computer Crime), како и кривични дела во кои се појавуваат елементи на незаконско користење интернет. Бројот и видовите кривични дела од областа на високотехнолошкиот криминал, како и економската штета која настанува од извршување на овие кривични дела е многу тешко да се процени. Меѓутоа бројот на извршени кривични дела и на материјалната штета која е регистрирана од година во година е во постојан пораст. Начинот на извршување на кривичните дела заради самата природа на современи информатички технологии е многу различен и сè пософистициран.

Организирани криминални групи кои вршат кривични дела од високотехнолошки криминал можат да бидат концентрирани на одреден географски простор. Така, на просторот на Западна Африка функционираат голем број ораганизирани криминални групи, сцецијализирани за вршење измами, чие поле на дејствување е фокусирано на интернетот, како глобално средство за комуникација. Електронското банкарство и електронското работење, дополнително го олесниле извршувањето на кривичното дело „измама“ што се врши со злоупотреба на компјутерот. Услугата на електронскиот трансфер на пари преку системот за пренос на пари преку далечина (Western Union, Money Gram и други) во комбинација со лесно доверливите жртви и со значителна убедливост на сторителите, придонесува за придобивање противправна имотна корист од оштетени лица ширум светот, а што е најстрашно сите тие остануваат целосно неказнети.[542]

[542] Според: Урошевић Владимир, „«Нигеријска превара» у Републици Србији“, *Безбедност* бр. 3/2009, МУП Републике Србије, Београд 2009., стр. 145-146.

БИБЛИОГРАФИЈА

1. Aas F.K.; Gundhus O.H.; Lomell M.H. (eds), *Technologies of (In) Security – The Surveillance of Everyday Life*, Routledge, New York, 2009.
2. Avant D., *The Market for Force: The Consequences of Privatizing Security*, Cambridge University Press, New York, 2007.
3. Adamoli S.; Di Nicola A.; Savona U.E.; Zoffi P., *Organised Crime Around the World*, HEUNI, Helsinki, 1998.
4. Алексић Ж.; Миловановић, З.: *Лексикон криминалистике*, Глосаријум, Београд, 1995.
5. Anderson S.; Cavanagh J., *The Top 200: The Rise of Global Corporate Power,* Institute for Policy Studies, Washington DC, 2000.
6. Ansoff H.I., *Corporate Strategy,* Penguin Books, London, 1977.
7. Aron R., *Mir i rat među narodima*, Golden marketing, Zagreb, 2001.
8. Art J.R.; Waltz N.K. (eds.), *The Use of Force - Military Power and International Politics,* Rowman & Littlefield Publishers Inc., Oxford, 2004.
9. Архипова И.Н.; Кульба В.В., *Управление в чрезвычайных ситуациях*, РГГУ, Москва, 1998.
10. Ashvani K.; Messner D. (eds), *Power Shift and Global Governance: Challenges from South and North*, Anthem Press, London, 2011.
11. Ahić J., *Sistemi privatne sigurnosti*, Fakultet za kriminalistiku, kriminologiju i sigurnosne studije, Sarajevo, 2009.
12. Бабић В. (ур.).: *Корпоративно управљање у транзицији*, Економски факултет, Крагујевац, 2004.
13. Bailey H.D., *Patterns of Policing: A Comparative International Analysis*, Rutgers University Press, New Brunswick NJ, 1990.
14. Бакрески О. и Милошевиќ М., *Современи безбедносни системи*, Аутопринт Т.А., Скопје, 2010.
15. Бакрески О., *Контрола на безбедносниот сектор*, Филозофски факултет и Аутопринт, Скопје, 2012.
16. Бакрески О., *Основи на безбедносниот менаџмент*, Филозофски факултет, Скопје, 2011.
17. Banner K.D., *Designing Effective Organizations: Traditional & Transformational Views*, SAGE Publications, Thousand Oaks CA, 1995.

18. Barney J.; Hesterly S.W., *Strategic Management and Competitive Advantage*, Prentice Hall, London, 2005.

19. Baylis J.; Smith S.; Owens P. (eds), *The Globalization of World Politics*, Oxford Press, New York, 2001.

20. Беренд Т.И., *Економска историја Европе у XX веку*, Архипелаг, Београд, 2009.

21. Berle A.; Means G., *The Modern Corporation and Private Property*, Transaction Publishers, Piscataway NJ, 1932.

22. Beroggi E.G.G.; Wallace A.W. (eds.), *Computer Supported Risk Management*, Kluwer Academic Publishers, Norwell MA, 1995.

23. Бжежински З., *Велика шаховска табла*, ЦИД, Подгорица, 2001.

24. Bilandžić M., *Poslovno-obavještajno djelovanje: Business intelligence u praksi*, AGM, Zagreb, 2008.

25. Blair M.M., *Ownership and Control - Rethinking Corporate Governance for the Twenty-First Century*, The Brookings Institution Press, Washington DC, 1995.

26. Бодрожић Ђ., *Национална држава*, Српска књижевна задруга & Партенон, Београд, 2008.

27. Boni W.; Kovacich L.G., *Netspionage: The Global Threat to Information*, Butterworth Heinemann, Boston/Oxford, 2000.

28. Борн Х., *Парламентарни надзор безбедносног сектора: начела, механизми и пракса,* Приручник за посланике бр. 5/2003, Женевски центар за демократску контролу оружаних снага & Гораграф, Београд, 2003.

29. Бошковић Г., *Организовани криминал*, Криминалистичко-полицијска академија, Београд, 2011.

30. Бошковић М., *Систем обезбеђења,* Завод за уџбенике и наставна средства, Београд, 1997.

31. Бошковић М., *Физичко обезбеђење и заштита објеката*, Bodex, Београд, 1995.

32. Бошковић М.; Кековић З., *Безбедност лица, имовине и пословања предузећа*, ВШУП, Београд, 2003.

33. Бошковић М,; Бошковић А., *Корупција – прање новца – финансирање тероризма*, Факултет за безбједност и заштиту, Бања Лука, 2011.

34. Brancato K.C.; Tonello M.; Hexter E., *The Role of U.S. Corporate Boards In Enterprise Risk Management (Project Report)*, McKinsey & Company, New York, 2006.

35. Braunig M.J., *The New Executive Protection Bible*, ESI Education Development Corporation, 225 Teal Court, Aspen CO, 2000.

36. Bruce G. and Button Mark, *Private Security*, Palgrave Macmillan, New York, 2004.

37. Briggs R.; Edwards C., *The Business of Resilience: Corporate Security for the 21st Century*, Demos, London, 2006.

38. Булат В., *Теорија организације*, Информатор, Загреб, 1977.

39. Ванковска Б., *Меѓународна безбедност*, Филозофски факултет, Скопје, 2011.

40. Vaughan J. E., *Risk Management*, John Wiley & Sons Inc, New York, 1996.

41. Veić P.; Nadj I., *Zakon o privatnoj zaštiti sa komentarom*, Naklada Žagar, Rijeka, 2005.

42. Вејновић Д.; Шикман М., *Дефендологија: друштвени аспекти безбједности модерне државе*, Висока школа унутрашњих послова, Бања Лука, 2007.

43. Viotti R.P., *International Relations and World Politics: Security, Economy, Identity*, Prentice Hall, Upper Saddle River NJ, 1997.

44. Волзер М., *Праведни и неправедни ратови*, Службени гласник, Београд, 2010.

45. Wolfers A., *National Security as an Ambiguous Symbol, Discord and Collaboration*, John Hopkins University Press, Baltimore, 1962.

46. Vrbanc D., *Osobna zaštita,* Zagreb štit-Vrbanc, Zagreb, 2002.

47. Вујашевић М., *Послови обезбеђења војне полиције,* Генералштаб Војске Србије и Црне Горе, Београд, 2004.

48. Vukadinović R., *Teorije o međunarodnim odnosima*, Zagreb, 1978.

49. Вуковић С., *Чему приватизација*, ИКСИ, Београд, 1996.

50. Гаћиновић Р., *Политичко насиље и глобализација*, Драслар партнер, Београд, 2009.

51. Gärtner H.; Hyde-Price A.; Reiter E. (eds), *Europe's New Security Challenges*, Lynne Reinner Publishers, London, 2001.

52. George B.; Button M.: *Private Security*, Perpetuity Press, Leicester, 2000.

53. Genser Michael., *A Structural Framework for the Pricing of Corporate Securities: Economic and Empirical Issues,* Springer-Verlag New York, LLC, 2005.

54. Георгиева Л., *Менаџирање на ризици*, Филозофски факултет, Скопје, 2006.

55. Giddens A., *Runaway World: How Globalization is Reshaping our Lives*, Routledge, New York, 2003.

56. Гилад Б., *Рано упозоравање: Пословне стратегије за контролу ризика*, ХЕСПЕРИАеду, Београд, 2009.

57. Goodspeed J.D., *The Conspirators: A Study of the Coup d'Etat*, MacMillan, London, 1962.

58. Greenspan M., *Modern Law of Land Warfare*, University of California Press, Berkeley CA, 1959.

59. Gruner S.R., *Corporate Criminal Liability and Prevention*, ALM Properties Inc., Law Journal Press, New York, 2005.

60. Група аутора, *Нема тајни – приручник за приватне агенте*, Досиер, Београд, 2000.

61. Gurr T.R., *Why Men Rebel*, Princeton University Press, Princeton NJ, 1970.

62. Gyarmati I.; Vesel S.(eds.), *Security Sector Governance in the Western Balkans 2004,* Nomos Verlagsgesellschaft, Baden-Baden, 2004.

63. Даничић М., *Безбједносни менаџмент*, Факултет за безбједност и заштиту, Бања Лука, 2010.

64. Даничић М.: *Обезбеђење лица и имовине предузећа у Републици Српској*, Висока школа унутрашњих послова, Бања Лука, 2006.

65. Даничић М. ; Стајић Љ., *Приватна безбједност*, ВШУП, Бања Лука, 2008.

66. Даничић М., *Специфичности менаџмента у области приватне безбједности у Републици Српској*, Интернационална Асоцијација криминалиста, Бања Лука, 2009.

67. Даневски З., *Обезбедување,* Практикум, Скопје, 2004.

68. Deitelhoff Nicole, and Klaus Dieter Wolf (Editor), *Corporate Security Responsibility?: Corporate Governance Contributions to Peace and Security in Zones of Conflict*, Palgrave Macmillan, 2010.

69. Divjak B. (ur.), *Studija percepcije korupcije: Bosna i Hercegovina*, Transparency International BiH, Banja Luka – Sarajevo, 2002.

70. Димитријевић В., *Појам безбедности у међународним односима*, Савез удружења правника Југославије, Београд, 1973.

71. Димитријевић В.; Лазин Ђ. (ур.), *Људска права – међународни документи*, Центар маркетинг, Београд, 1993.

72. Димитријевић В.; Стојановић Р., *Међународни односи*, НИУ Службени лист СРЈ, Београд, 1996.

73. Драгаш О., *Савремена обавештајно-безбедносна заједница,* ИП „Рад“, Београд, 2009.

74. Драгишић З., *Безбедносни менаџмент,* ЈП Службени гласник, Београд, 2007.

75. Draper H., *Private police*, Harvester Press & Humanities Press, London – Atlantic Highlands NJ, 1978.

76. Druga znanstveno-stručna konferencija s međunarodnim sudjelovanjem «Menadžment i sigurnost - M&S 2007» (zbornik radova), Hrvatsko društvo inženjera sigurnosti & Visoka škola za sigurnost, Zagreb, 2007.

77. Drucker P., *Managing for Results*, Harper & Row, New York, 1964.

78. Дулановић Ж., *Мрежни и виртуални модели организационе структуре*, ФОН, Београд, 2002.

79. Eliott A.M., *Crime in Modern Society*, Harper & Brothers, New York, 1952.

80. Зиндовић И.: *Мултинационалне компаније и економска шпијунажа*, Alisa press, Краљево, 2008.

81. Ivandić Vidović D.; Karlović L.; Ostojić A., *Korporativna sigurnost*, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb, 2011.

82. Извештај о стању у области организованог и привредног криминала у Југоисточној Европи, CARPO Регионални пројекат, Европска унија и Савет Европе, Стразбур, 2006.

83. Intelligence Threat Handbook, U.S. Interagency Operations Security Support Staff, Washington, 1996.

84. Javorović B.; Bilandžić M., *Poslovne informacije i business intelligence*, Golden marketing & Tehnička knjiga, Zagreb, 2007.

85. Jackson P.; Siegel J. (eds), *Intelligence and Statecraft: The Use and Limits of Intelligence in International Society*, Greenwood Publishing Group, Westport CT, 2005.

86. Jäger T.; Kümmel G. (eds.), *Private Military and Security Companies*, VS Verlag für Sozialwissenschaften, Wiesbaden, 2007.

87. Јелизаров А., *Контрашпијунажа,* Паидеиа, Београд, 2001.

88. Johnson K.L. (ed), *Strategic Intelligence (Volumes 1-5)*, Praeger Security International, Westport CT & London, 2007.

89. Judy W.R.; Clough L.V., *The Information Age and Soviet Society*, Hudson Institute, Indianopolis IN 1989.

90. Karlović L. ; Ostojić A., *Zbirka propisa o zaštitarskoj i detektivskoj djelatnosti*, LAS d.o.o, Zagreb, 2000.

91. Kahaner L., *Competitive Intelligence: How to Gather, Analyze and Use Information to Move Your Business to the Top*, Touchstone Books, New York, 1996.

92. Кегли В. Ч. Јр.; Виткоф Р. Ј., *Светска политика*, Факултет политичких наука & Дипломатска академија МСП, Београд, 2004.

93. Кековић З., *Системи безбедности,* Факултет безбедности, Београд, 2009.

94. Кековић З.; Савић С.; Комазец Н.; Милошевић М.; Јовановић Д., *Процена ризика у заштити лица, имовине и пословања*, Центар за анализу ризика и управљање кризама, Београд, 2011.

95. Кесић З., *Приватни сектор у контроли криминалитета,* Досије студио, Београд, 2009.

96. Кешетовић Ж.; Кековић З., *Системи кризног менаџмента*, Факултет за безбједност и заштиту, Бања Лука, 2008.

97. Klare M.; Chandrani Y. (eds), *World Security – Challenges for a New Century*, Cengage Learning, South Melbourne AU, 1998.

98. Ковач М., *Стратегијска и доктринарна документа националне безбедности – Теоријске основе*, Свет књиге, Београд, 2003.

99. Kovacich L.G., *Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*, Butterworth Heinemann, Boston & Oxford, 1999.

100. Kovacich L.G.; Halibozek E.P., *The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program*, Butterworth Heinemann, Boston MA, 2002.

101. Kotler P.; Lee N., *Korporativna društvena odgovornost: Učiniti najbolje za svoju kompaniju i za izabrani društveni cilj*, HESPERIAedu, Beograd, 2009.

102. Котовчевски М.: *Национална безбедност на Република Македонија*, Македонска цивилизација, Скопје, 2000.

103. Corporate Manager's Security Handbook, AuthorHouse, 2012.

104. Кривокапић В.; Крстић О., *Криминалистика-тактика 2,* Полицијска академија, Београд, 2001.

105. Krummenacher A., *Krisenmanagement: Leitfaden zum Verhindern und Bewaltigen von Unternehmungskrisen*, Verlag Industrielle Organisation, Zürich, 1981.

106. Кривокапић В., *Основи полицијске криминалистике,* Публикум, Београд, 1995.

107. Christopher J. Cubbage and David J. Brooks, *Corporate Security in the Asia-Pacific Region: Crisis, Crime, Fraud, and Misconduct,* CRC Press, 2012.

108. Quade E.S, Boucher W.I. (eds): *Systems Analysis and Policy Planning: Application in Defense,* American Elsevier, New York, 1968.

109. Leavitt H., *Some Effects of Certain Communication Patterns on Group Performances,* Readings in Social Psychology, New York, 1952.

110. LeBeuf M.E., *Policing and Use of Information Technology: An Assessment*, Research Centre, Canadian Police College, Otawa, 2000.

111. Lipset S.M., *Political Man - The Social Bases of Politics*, Anchor Books, Garden City NY, 1960.

112. Loader Ian and Walker Neil, *Civilizing Security*, Cambridge: Cambridge University Press, 2007.

113. Luttwak E., *Coup d'Etat: A Practical Handbook*, Penguin Books, Harmondsworth UK, 1969.

114. Maddison A., *The World Economy – A Millennial Perspective*, OECD, Paris, 2001.

115. Мандић Г., *Систем обезбеђења и заштите,* ФЦО, Београд, 2004.

116. Mangold P., *National Security and International Relations*, Rotledge, London and New York, 1990.

117. Маринковић Д. (прир.), *Место и улога полиције у превенцији криминалитета – актуелно стање и могућности унапређења*, Криминалистичко-полицијска академија, Београд, 2007.

118. Марковић И.С., *Моћнији од ЦИА: Електронска шпијунажа у ери глобализације*, Институт за политичке студије, Београд, 2002.

119. Марковић С., *Основи корпоративне и индустријске безбедности,* Факултет за правне и пословне студије, Нови Сад, 2007.

120. Masleša R., *Teorije i sistemi sigurnosti*, Magistrat, Sarajevo, 2001.

121. Massie L.J., *Essential of Management,* Prentice Hall International, London, 1987.

122. Мастрюков Б.С., *Бесопасность в чрезвычайных ситуациях*, Издательский центр Академия, Москва, 2003.

123. Матић Г., *Основи физичко-техничког обезбеђења*, Привредна комора Србије, Београд, 2006.

124. Management of Defence, Democratic and Civilian Control, Including Integration of Security Sector, 2001.

125. Meadows H.D.; Meadows L.D.; Randers J.; Behrens W.W.III, *The Limits to Growth*, Universe Books, New York, 1972.

126. Metz S.; Millen R., *Insurgency and Counterinsurgency in the 21st Century: Reconceptualizing Threat and Response*, Diane Publishing, Darby PA, 2004.

127. Мијалковић С., *Национална безбедност,* КПА, Београд, 2009.

128. Мијалковић С.; Кесеровић Д., *Основи безбједности, са системом безбједности Босне и Херцеговине*, Факултет за безбједност и заштиту, Бања Лука, 2010.

129. Мијалковић С.; Милошевић М., *Обавјештајно-безбједносна дјелатност и службе*, Висока школа унутрашњих послова, Бања Лука, 2011.

130. Мијатовић Б., *Економија, политика и транзиција*, Фицом, Београд, 1998.

131. Miller P.J.; Leonard M.F., *Millenium Intelligence – Understanding and Conducting Competitive Intelligence in the Digital Era*, Information Today Inc., Medford NJ, 2000.

132. Милошевић М., *Обезбеђење имовине, лица и пословања,* Интермекс, Београд, 2004.

133. Милошевић М., *Физичко-техничко обезбеђење и противпожарна заштита*, ИП Глосаријум, Београд, 2006.

134. Милутиновић М., *Корпоративна безбедност*, Висока школа струковних студија за криминалистику и безбедност, Ниш, 2011.

135. Mintzberg H., *The Nature of Managerial Work,* Harper & Row, New York, 1973.

136. Mishan J.E., *The Costs of Economic Growth*, Stapples Press, London, 1967.

137. Mishkin S.F.; Eakins G.S., *Financijska tržišta i institucije*, Mate, Zagreb, 2005.

138. Млађан Д., *Последице пожара, хаварија и експлозија*, Криминалистичко-полицијска академија, Београд, 2009.

139. Мршевић З., *Организовани криминал*, Институт за криминолошка и социолошка истраживања, Београд, 1993.

140. Murray T.; McKim E., *The Policy Issues in Policing and Private Security*, Canadian Association of Ciefs of Police Publication, Ottawa, 2000.

141. McLuhan M., *Understanding Media: The Extensions of Man*, McGraw Hill, New York, 1964.

142. Nasheri H., *Economic Espionage and Industrial Spying*, Cambridge University Press, Cambridge UK, 2005.

143. Научни скуп «Дани безбједности» на тему: „Корпоративна безбједност – ризици, пријетње и мјере заштите“ (Зборник радова), Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука, 2010.

144. Научни скуп «Дани безбједности» на тему: „Развој система безбједности и заштите корпорација“ (Зборник радова), Факултет за безбједност и заштиту Универзитета Синергија, Бања Лука, 2011.

145. Научни скуп „Савремени облици угрожавања безбједности и стратегије супротстављања“ (Зборник радова), Универзитет Синергија, Бања Лука, 2009.

146. Nyamuya M., et.al. *Private Military Companies & International Law: Building New Leaders of Legal Accountability & Responsibility,* 2009.

147. Novak B., *Krizno komuniciranje*, Binoza press, Zagreb, 2001.

148. O'Brienand M.; Yar M., *Criminology – The Key Concepts*, Routledge, London & New York, 2008.

149. Ohmae K., *The End of the Nation-State: The Rise of Regional Economies*, Simon and Schuster Inc., New York, 1995.

150. Пајковић Д., *Обезбеђење одређених личности и објеката,* МУП Републике Србије, Београд, 2003.

151. Paoli L.; Fijnaut C. (eds.), *Organised Crime in Europe: Manifestations and Policies in the European Union Beyond*, Springer, Dordrecht NL, 2003.

152. Paul T.V.; Hall A.J, *International Order and the Future of World Politics*, Cambridge University Press, New York, 1999.

153. Петковић М.; Јанићијевић Н.; Богићевић-Миликић Б., *Организација*, ЦИД Економски факултет, Београд, 2006.

154. Петковић Т., *Пословна шпијунажа и економско ратовање*, Protexi Group System, Нови Сад, 2009.

155. Петровић Пироћанац З., *Економска шпијунажа*, Драслар Партнер & Центар Југоисток & Институт за политичке студије, Београд, 2005.

156. Петровић С., *Полицијска информатика*, Криминалистичко-полицијска академија, Београд, 2007.

157. Potter H.E. (ed.), *Economic Intelligence and National Security*, Carleton University Press & The Center for Trade Policy and Law, Ottawa, 1998.

158. Pfaltzgraff L.R.Jr.; Ra'anan U.; Milberg W. (eds), *Intelligence: Policy & National Security*, Archon Books, Hamden CT, 1981.

159. Радовановић Д., *Деликти насиља,* Институт за социолошка и криминолошка истраживања, Београд, 2002.

160. Радун В., *Конкуренција на нишану – Теоријски и практични аспекти истраживања конкуренције*, ХЕСПЕРИАеду, Београд, 2008.

161. Рађеновић Р., *Обезбеђење и безбедносна заштита одређених личности и објеката,* МУП Републике Србије – Институт безбедности, Београд, 1995.

162. Рађеновић Р., *Безбедност личности и објеката,* МДД Систем Београд, 2003.

163. Рајков М., *Теорија система*, ФОН, Београд, 1981.

164. Reid P., *How to Land a Top-Paying Corporate securities research analysts Job,* Emereo Pty Ltd, 2012.

165. Reiman J., *The Rich Get Richer and the Poor Get Prison: Ideology, Crime and Criminal Justice*, Allyn & Bacon, Boston, 1995.

166. Reich B.R., *Supercapitalism: The Transformation of Business, Democracy and Everyday Life*, Alfred A. Knopf, New York, 2007.

167. Richelson T.J., *The U.S. Intelligence Community*, Ballinger Publishing Company, Cambridge MA, 1985.

168. Родић Б.; Ђорђевић Г., *Да ли сте сигурни да сте безбедни*, Продуктивност АД, Београд, 2004.

169. *Руководство по обеспечению безопасности личности и предпринимателъства*, Институт безопасности предпринимательства при содействии Совета по безопасности предпринимательства России, Виком, Москва, 1996.

170. Rupert M., *Ideologies of Globalization – Contending Visions of a New World Order*, Routledge, London, 2000.

171. Савић А., *Национална безбедност,* КПА, Београд, 2007.

172. Савић А., *Начела оперативног рада државне безбедности,* Зборник радова наставника ВШУП, Бр. 1/1998.

173. Савић А., *Основи државне безбедности*, Образовно-истраживачки центар МУП-а Републике Србије, Београд, 1989.

174. Савић А., *Увод у државну безбедност,* ВШУП, Београд, 2000.

175. Савић А.; Стајић Љ., *Основи цивилне безбедности*, Факултет за правне и пословне студије, Нови Сад, 2006.

176. Sačić Ž., *Organizirani kriminalitet u Hrvatskoj*, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 1997.

177. See H.; Spoo E. (Hrsg.), *Wirtschaftskriminalität – kriminelle Wirtschaft*, Distel Verlag, Heilbronn, 1997.

178. Secret Service USA, *Курс заштитних операција,* Курс одржан у Београду, 2001.

179. *Security of Radioactive Sources,* TECDOC-1355, International Atomic Energy Agency, Austria, 2003.

180. *Security Sector Reform: Institutions, Society and Good Governance,* Bryden Alan and Fluri Philipp (eds.), Nomos Verlagsgesellschaft, Baden-Baden, 2003.

181. Симић Д., *Наука о безбедности*, Службени гласник, Београд, 2002.

182. Симић Р.; Бошковић М., *Физичко-техничка заштита објеката,* Институт безбедности, Београд, 1991.

183. Симовић-Хибер И., *Систем расправа о идеји владавине права, основама кривичног закона, појму злочиначке групе и интернационализацији кривичног права*, Институт за социолошка и криминолошка истраживања, Београд, 2007.

184. Simpson S., *Corporate Crime, Law and Social Control*, Cambridge University Press, Cambridge UK, 2002.

185. Sodaro J.M., *Comparative Politics: A Global Introduction*, McGraw-Hill, New York, 2004.

186. Славески С., *Безбедносен систем*, Европски универзитет, Скопје, 2009.

187. Ставрић Б.: *Корпоративни менаџмент*, Виша пословна школа, Београд, 1994.

188. Стајић Љ., *Основи система безбедности*, Правни факултет, Нови Сад, 2008.

189. Стајић Љ.; Гаћиновић Р., *Увод у студије безбедности*, Драслар, Београд, 2007.

190. Стратешко планирање – сагледавање екстерних фактора, МУП Републике Србије, Београд, 2003.

191. Small M., *Privatisation of Security and Military Functions and the Demise of the Modern Nationstate in Africa*. Durban, African Centre for the Constructive Resolution of Disputes, 2006.

192. Stiglitz E.J., *Globalization and its Discontents*, W.W.Norton, New York, 2002.

193. Sutherland E.,, *White Collar Crime*, Holt, Rinehart & Winston, New York, 1949.

194. Schneider G.: *Close Protection Operation in South Africa*, University of South Africa, March, 2005.

195. Schlegel K., *Just Deserts for Corporate Criminals*, Northeastern University Press, Lebanon NH, 1990.

196. Schwartau W., *Information Warfare: Chaos on the Electronic Superhighway*, Thunders Mountain Press, New York, 1994.

197. Schwartz M.; Dekeseredy W., *Contemporary Criminology*, Wadsworth Publishing Company, Belmont CA, 1996.

198. Schreier F. and Caparini M., *Privatising Security: Law, Practise and Governance of Private Military and Security Companies*, Geneva, DCAF, 2005.

199. Талијан М., *Руковођење унутрашњим пословима,* ВШУП, Београд, 2004.

200. Tatalović S., *Nacionalna i međunarodna sigurnost*, Politička kultura, Zagreb, 2006.

201. Tatalović S.; Bilandžić M., *Osnove nacionalne sigurnosti*, Policijska akademija, Zagreb, 2005.

202. Татомировић Д., *Практикум за обављање послова заштите имовине и лица са правилом вршења службе,* Ревија „Детектив“, Београд, 1997.

203. Tipurić D.; Hruška D.; Mešin M., *Promjene vrhovnog menadžmenta i korporativno upravljanje*, Sinergija, Zagreb, 2011.

204. Töpfer A., *Plötzliche Unternehmenskrisen: Gefahr Oder Chance?* Luchterhand Literaturverlag, München, 1999.

205. Фатић А.; Бановић Б. (ур.), *Друштвени аспекти организованог криминала*, Институт за међународну политику и привреду, Београд, 2011.

206. Fayol H., *Industrial and General Administration,* J.A.Coubrough, Geneva International Management Institute, 1930.

207. Fein A.R.; Vossekuil B., *Protective Intelligence and Threat Assessment Investigation,* U.S. Department of Justice, Washington, 1998.

208. Fehringer D.; Hohhof B. (eds.), *Competitive Intelligence Ethics: Navigating the Gray Zone,* Competitive Intelligence Foundation, Alexandria VA, 2006.

209. Fialka J.J., *War by Other Means: Economic Espionage in America*, W.W.Norton & Company, New York, 1997.

210. Fink S., *Sticky Fingers: Managing the Global Risk of Economic Espionage*, Dearborn Trade Publishing, Chicago, 2002.

211. Fischer, D., *Nonmilitary Aspects of Security: A Systems Approach*, Aldershot: United Nations Institute for Disarmament Research, 1993.

212. Freeman R.E.; Gilbert R.D., *Corporate Strategy and Search for Ethics*, Prentice Hall, Englewood Cliffs NJ, 1988.

213. Hammer M.; Champy J., *Reengineering the Corporation: A Manifesto for Business Revolution*, Nicholas Brealey Publishing, London, 1993.

214. Хаџић М.; Радоман Ј. (прир.), *Економија и безбедност*, Центар за цивилно-војне односе, Београд, 2009.

215. Hopkins M., *The Planetary Bargain: Corporate Social Responsibility Matters,* Routledge, London, 2003.

216. Hochstedler E. (ed.), *Corporations as Criminals*, Sage Publications, Beverly Hills CA, 1984.

217. Hubbard W. D., *The Failure of Risk Management: Why It's Broken and How to Fix It,* John Wiley & Sons Inc, Hoboken NJ, 2009.

218. Hufbauer G.C.; Schott J.J.; Elliott K.A., *Economic Sanctions in Support of Foreign Policy Goals*, Institute for International Economics, Washington DC, 1983.

219. CARPO Regional Project: Situation Report on Organised and Economic Crime in South-eastern Europe, Council of Europe & European Commission, Strasbourg, September, 2006.

220. Clinard M.; Yeager P., *Corporate Crime*, Transaction Publishers, New Brunswick NJ, 2006.

221. Chandler D.A.Jr, *Scale and Scope: The Dynamics of Industrial Capitalism*, The Belknap Press of Harvard University Press, Cambridge MA, 1994.

222. Combs E.R.; Moorhead D.J, *Competitive Intelligence Handbook*, Rowmann & Lttlefield, Lanham MD, 1993.

223. Consterdine P., *The Modern Bodyguard: The Complete Manual of Close Protection Training,* Summersdale, Chichester UK, 2006.

224. Coppola P. D., *Introduction to International Disaster Management*, Elsevier & Butterworth – Heinemann, Oxford UK, 2007.

225. Cordesman A.H.; Burke A.A., *Defending America: Asymmetric and Terrorist Attacks With Biological Wapons*, Center for Strategic and International Studies - CSIS, Washington DC, 2001.

226. Cortright D.; Lopez A.G., *The Sanctions Decade: Assessing UN Strategies in the 1990s*, Lynne Rienner, Boulder CO, 2000.

227. Cochrane A.; Talbot D., *Security: Welfare, Crime and Society,* McGraw Hill, Berkshire UK, 2008.

228. Croall H., *Understanding White Collar Crime*, Open University Press, Buckingham UK, 1994.

229. Цхадая Д.Н.; Подосенова С.Н., *Управление безопасностью труда*, ЦентрЛитНефтеГаз, Москва, 2008.

230. Чутурић С., *Организационе промене у предузећу,* Графика БОЈС, Београд, 2005.

231. Чутурић С., *Руковођење-чиниоци успеха у вођењу организације*, Графика БОЈС, Београд, 2005.

232. Ђурић Кузмановић Т., *Пословно окружење*, Алфа Граф, Нови Сад, 2008.

233. Шкулић М., *Организовани криминалитет*, Досије, Београд, 2003.

СПИСАНИЈА

1. *Administration and Society*, Vol. 25, No 1, SAGE Publications, Thousand Oaks CA, May, 1993.
2. *American Political Science Review* No. 55, Washington DC, 1961.
3. *Безбедност*, бр. 4/2008, МУП Републике Србије, Београд, 2008.
4. *Бизнис & финансије*, бр. 54, БИФ Пресс д.о.о., Београд, април, 2009.
5. VARSTVOSLOVJE, year 11, no. 2, 2009

6. *BoardRoom - Magazine for Corporate Governance, Leadership and Quality of Life*, No. 1, New York, 2002.
7. *British Journal of Criminology, 36, 2,* 1996
8. Business Week, No. 28, Bloomberg L.P., New York, 1985.
9. *Војно дело* бр. 2/2009, Министарство одбране Републике Србије, Београд, 2009.
10. *East European Constitutional Review*, Vol. 7, No. 2, New York University School of Law, New York, Spring, 1998.
11. *Економска мисао* бр. 3-4, Београд, 1994.
12. *Ekonomski pregled*, godina 53, br. 3–4, Hrvatsko društvo ekonomista & Ekonomski institut, Zagreb, 2002.
13. *European Journal of Operational Research*, Vol. 70, Issue 2, Elsevier, London, 1993.
14. *European Journal on Criminal Policy and Research*, Springer, Heidelberg 1999.Vol. 7, No. 2/ Vol. 9, No. 2, Springer, Heidelberg, 2001.
15. *Economic Survey of Europe 2000*, No. 2/3, United Nations, New York – Geneve, 2000.
16. *Криминалистичке теме*, год. VIII, бр. 1-2, Сарајево, 2008.
17. *Competitive Intelligence Magazine*, Vol. 10, No. 2, Issue 3, Alexandria VA, May-June, 2006.
18. *Criminology*, Vol. 28, Issue 2, American Society of Criminology, Columbus OH, May, 1990.
19. *Current Issue in Criminal Justice - Journal of the Institute of Criminology*, Vol. 11, No. 3, University of Sidney - Faculty of Law, Sydney, 2000.
20. *Crime, Law and Social Change*, No. 19, Springer-Verlag Gmbh, Heidelberg, 1993.
21. *Quarterly Journal of Economics*, Vol. 83, No. 1, Oxford University Press, Oxford UK, 1969.
22. *International Criminal Police Review*, No. 343, Paris, 1980.
23. *Schweizerische Zeitschrift fűr Strafrecht*, 1/2005, Stämpfli Verlag AG, Bern, 2005.
24. Leadership & Organization Development, Vol. 19, Issue 4, Emerald Group Publishing Limited, Bingley UK, 1998.
25. *Michigan Journal of International Law*, Vol. 29, No. 2, University of Michigan Law School, Ann Arbor MI, 2008.
26. *Међународни проблеми*, Вол. LXI, бр. 3, Институт за међународну политику и привреду, Београд, 2009.
27. Međunarodna politika, Institut za međunarodnu politiku i privredu (MPP), br. 1108, oktobar-decembar, 2002.

28. Međunarodne studije, Centar za međunarodne studije/hrvatske udruge za međunarodne studije, Zagreb, vol.V no.3, 2005.
29. National Intelligence Machinery, London: The Stationary Office, 2001.
30. *Наука, безбедност, полиција*, бр. 3, Београд, 2007.
31. *Nietherlands International Law Review*, Vol. 52, Issue 1, TMC Asser Institute, The Hague, April, 2005.
32. *Политика*, Београд, 06. јул., 2011.
33. *Policija i sigurnost*, br. 1-2, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, siječanj-travanj, 1997.
34. *Public Relation Review*, Vol. 35, Issue 1, Elsevier Inc, New York, March, 2009.
35. *Право и привреда*, бр. 9-12/06, Удружење правника у привреди Србије, Београд, 2006.
36. *Правни информатор* бр. 9, Београд, 2006.
37. *Polemos*, br. 18, Hrvatsko sociološko društvo & Naklada Jesenski i Turk, Zagreb, 2006.
38. *Public Personnel Management* Vol. 31, No. 2/2002, International Public Management Association for Human Resources, Alexandria VA, 2002.
39. *Ревија за безбедност* бр. 8/09, Београд август, 2009.
40. *Računovodstvo, Revizija i Financije*, br. 5-6, RriF Plus, Zagreb, 2007.
41. *Science, Security, Police (NBP)*, Vol. 8, No. 2, Belgrade, 2003.
42. *Српска политичка мисао*, Vol. 20, бр. 1-2, Београд, 2008.
43. Современа македонска одбрана, вол.XII, бр. 12, декември, 2005.
44. *Системы безопасности*, No. 1, Издателский дом „Гротек“, Москва, 1995.
45. The Review of Politics vol.48. No.4, Winter, 1986.
46. *The American Economic Review*, Vol. 65, No. 3, Princeton NJ, 1975.
47. *Transnational Organized Crime*, Vol. 2, No.1, Routledge, London, 1996.
48. *Financijska teorija i praksa*, Vol. 28, No. 2, Institut za javne financije, Zagreb 2004.
49. *Hrvatski vojnik,* broj 228 (podlistak), Zagreb, veljača, 2009.
50. *Harvard Business Review*, Vol. 79, No. 3, Harvard Business School Publishing, Cambridge MA, March, 2001.
51. *Foreign Policy*, Issue 110, Washington DC, Spring, 1998.
52. *Journal of Finance*, Vol. 51, No. 4, John Wiley & Sons Inc., Hoboken NJ, 1996.
53. *Journal of International Affairs*, School of International and Public Affairs, Vol. 51, No. 2, Columbia University, New York, 1998.

54. *Journal of Competitive Intelligence and Management*, Vol. 2, No. 1, Society of Competitive Intelligence Professionals (SCIP), Alexandria VA, Spring, 2004.
55. *Journal of Socio-Economics*, Vol. 38, Issue 1, Elsevier, Amsterdam NL, 2009.
56. *Journal of Risk and Insurance*, Vol. 57, No. 3, American Risk and Insurrance Association, Malvern PA, 1990.

МАТЕРИЈАЛИ ОД ИНТЕРНЕТ

http://www.academyci.com

http://www.basicint.org/ pubs/Papers/pmcs0603.pdf

http://www.bre.ru/security/20033.html

http://www.bsr.org/BSRResources/WhitePaperDetail.cfm?DocumentID=48809

http://www.businessintelligence.com

http://www.dataprotection2003.info

http://www.disasters.org/emgold/Library/GEMS.htm

http://www.disastercenter.com/

http://www.envsec.org/

http://www.ec.europa.eu/enlargement/how-does-it-work/progress_reports/index_en.htm

http://www.iac.wur.nl

http://www.iso.org/iso/iso_catalogue

http://www.iwar.org.uk/comsec/resources/sa-tools

http://www.knowledgepoint.com.au

http://www.kriminalpraevention.de

http://www.mchs.gov.ru/10759/

http://www.nappo.org

http://www.ncix.gov/publications/reports/fecie_all/fecie_2000.pdf

http://www.olapreport.com/fasmi.htm

http://www.preventionweb.net/globalplatform/

http://www.samvak.tripod.com/pp144.html

http://www.security-expert.org/shoplift.html
http://www.top100.seenews.com/companies
http://www.stabilitypact.org
http://www.scip.org/ci/
http://www.unep.org/
http://www.unicri.it/
http://www.fas.org/sgp/othergov/indust.html
http://www.cio-dpi.gc.ca/
http://www.coess.org/pdf/final_study_en.html
http:// www.coneinc.com/pages/research.html
http://www.worlddialogue.org/content.php?id=100