METODI, TRENDOVI I ALATI U KORPORATIVNOJ SIGURNOSTI POSLOVNA ŠPIJUNAŽA-mit ili stvarnost

Doc.dr. Kemal Brkić, email: kemal.brkic@yahoo.com
Internacionalni univerzitet Travnik u Travniku
Univerzitet modernih znanosti, CKM Mostar
Sandi Dizdarević, mag., email: sandi_lps@hotmail.com
Univerzitet modernih znanosti, CKM Mostar

Sažetak: Ekonomski, pravni i socijalni ambijent unutar jedne zemlje, s posebnim akcentom na zemlje u tranziciji utiče na razvoj poslovnih sistema. Danas, kao dio korporativne strategije uveliko je prisutan niz alata pomoću kojih se nastoji diskreditovati konkurentno preduzeće, s ciljem opstanka a time i ekonomskog prosperiteta. Predmet ovog stručnog rada prožima se kroz prizmu deskripcije brojnih alata koji se koriste u okviru ekonomske špijunaže poslovnih preduzeća. Motiv autora je potreba da ukažemo savremenim menadžerima na neke od osnovnih mjera na koje trebaju računati u komunikaciji sa svojim poslovnim patrnerima, ali i vlastitim osobljem. Cilj rada ogleda se u činjenici da će rad pružiti skroman doprinos u razvoju svijesti menadžera i potrebi za jačanjem korporativnih sigurnosnih alata unutar njihovih preduzeća. Najmanja neopreznost srednjeg i top menadžmenta može imati nepopravljive poslijedice. S druge strane, danas na tržištu opstaju ona preduzeća koja imaju pravovremenu i kvalitetnu informaciju, jer ko raspolaže informacijom taj dominira situacijom.
Ključne riječi: Poslovna, špijunaža, ponašanja, mjere i radnje, informacija

METHOD, TRENDS AND TOOLS IN CORPORATE SECURITY BUSINESS INTELLIGENCE – Myth or Reality

Abstract: Economic, legal and social environment within the country, with particular focus on countries in transition, affect the development of business systems Today, as a part of corporate strategy companies use a set of tools to discredit competing company with aim to survive and thus the economic prosperity. Subject of this professional work permeates through the prism of description of number of tools that are used for economic espionage of business enterprises. Author's motive is need to point out to modern managers on some of the basic measures they should be aware in communication not only with business partners, but also with their own staff. Aim of this work reflects in fact that this professional work will provide modest contribution in development of manager awareness and need to strengthen the corporative security tools within their companies. Minimum lack of caution of middle and top management may have unrecoverable consequences. On the other side, companies that survive on market today are companies that have timely and quality information, because those with information dominate the situation.
Keywords: Business, espionage, behaviour, measures and actions, information

Uvodna razmatranja

Savremeni poslovni svijet temeljen na realnom konceptu funkcioniše po konkretnim matricama ponašanja. Matrice ponašanja poslovnog svjeta temelje se na principima integracija, dezintegracija, udruživanja i razdruživanja. Svi principi imaju jedinstveni cilj, koji možemo nazvati interesno povezivanje. Interesno povezivanje nije, niti može biti statička dimenzija korporacija i preduzeća. U dinamičkoj dimenziji interesnog povezivanja, s ciljem dobiti i opstanka veoma često dolazi do interesnog sukobljavanja. Poslovni procesi velikih i srednjih korporacija/preduzeća danas u realnom svijetu uveliko se temelje i ovise od stanja sigurnosti u državi. Međutim, ti procesi ne smiju se vezati samo za stanje sigurnosti države, već se trebaju fokusirati i na vlastitu unutrašnju i vanjsku sigurnost svog poslovanja.

Sigurnosni procesi korporacija, slični su procesima sigurnosti država. Prema Abazoviću: „bezbjednost, odnosno sigurnost svake države je nezaobilazan faktor njene opstojnosti, funkcioniranja, egzistiranja i koegzistiranja sa drugim državama, međunarodnim institucijama i bilateralnim, trilateralnim ili drugim povezivanjima na regionalnom, kontinentalnom ili globalnom svjetskom nivou".[122] Analagno zaključku kojeg je iznio Abazović možemo kazati da u svim poslovnim/korporativnim procesima sigurnost kako unutrašnja tako i vanjska ima ulogu koja može uticati na nivo i intezitet dobiti, te u krajnjoj instanci opstanak. Slično kreiranju ekonomskih obavještajnih službi država ili njihovih organizacionih jedinica, danas mnoge svjetske korporacije i preduzeća formiraju svoje obavještajne odjele (busines intelligence) u okviru odjela ili departmana za korporativnu sigurnost.

Danas je gotovo nezamislivo pozitivno poslovanje korporacija bez postojanja business intelligence u okviru odjela za korporativnu sigurnost. Kako ističu Vidović, Karlović i Ostojić: „Business intelligence" i poslovne informacije kao njegov središnji element, u današnjm uvjetima predstavljaju strateški menadžerski resurs.[123] Evidentno je da su poslovne informacije središnji element na temelju kojeg se kreiraju menadžerske odluke na osnovu kojih se implementiraju poslovni procesi. U današnjoj epohi razvoja nauke i tehnologije mnoge korporacije koriste se rezultatima takvih pronalazaka, između kojih su i tehnički elementi špijunaže. Takvi modeli rada koriste se isključivo za otkrivanje poslovnih tajni konkurentnih preduća s ciljem preduhitrenja, kompromitacije, sabotaže ili uništenja. Određen broj korporacija i preduzeća zanemarujući značaj korporativne sigurnosti propali su zbog nekvalitetnih i neblagovremenih odluka top menadžmenta. Dio tih odluka, svakako se treba pripisati ulozi i značaju specifičnih alata koje je suprotna strana poduzela, između kojih posebno dolazi do izražaja poslovna špijunaža. Da li je otkrivanje poslovnih tajni konkurentnih preduzeća dovelo do gubitka tržišta, prihoda i na kraju opstanka veoma teško je prepisati špijunaži, jer čak ni najveći i najkvalitetniji menadžeri nisu svjesni da su njihove korporacije bile meta. Zbog toga, ovaj rad ima za cilj da top menadžerima ukaže na samo neke od oblika poslovne špijunaže koje mogu imati dalekosežne posljedice.

1. ULOGA ODJELA ZA KORPORATIVNU SIGURNOST

Kakva će uloga, vrsta i veličina odjela za korporativnu sigurnost korporacije ili preduzeća biti ovisi od niza faktora. Prvi i osnovni faktor, na kojeg mnogi poslovni subjekti ukazuju su finansijske mogućnosti neophodne za finansiranje djelatnosti odjela. Međutim, iza termina finansijske mogućnosti jako često se krije neznanje top menadžmenta o ulozi odjela za korporativnu sigurnost. Danas, neke od korporacija ili preduzeća aktivno provode neke od mjera bussines intelligence, a da nisu ni svjesne. Problem nastaje upravo u nepotpunom ciklusu, koji na kraju rezultira nedovoljno kvalitetnim informacijama na temelju kojih se trebaju kreirati menadžerske odluke. Organizacijski proces odjela za korporativnu sigurnost prema Vidović i dr. (2011): „mora odražavati poslovnu strategiju poduzeća-analizirati situaciju, odlučivati šta raditi, a zatim organizirati obavljanje posla".[124]

Odjeli za korporativnu sigurnost prema stručnoj javnosti trebaju se obrazovati kao stručna tijela čiji rad će se temeljiti na ofanzivnoj i defanzivnoj djelatnosti. To znači da će se obje

[122] Abazović, M. (2002). Državna bezbjednost: Uvod i temeljni pojmovi, Sarajevo, str. 2.
[123] Vidović, D. Karlović, L. Ostojić, A. (2011). Korporativna sigurnost, Zagreb, str. 236.
[124] Ibid, str. 67.

djelatnosti temeljiti na ključnim poslovno obavještajnom djelatnostima. Pod obavještajnom djelatnosti, prema Abazoviću smatra se da se ista: „odvija kroz obavještajni postupak, obavještajni krug, ili obavještajni ciklus“.[125] Drugim riječima mogli bismo kazati da je poslovno obavještajna djelatnost jedna vrsta poslovno obavještajnog istraživanja s ciljem prikupljanja, sistematizacije, analize, dostavljanja i korištenja gotovog proizvoda, odnosno podatka. Na temelju takvih provjerenih podataka menadžment kompanije može donositi odgovorajuće odluke. Prema Đorđeviću (1985): „Nosilac preventivno-zaštitne funkcije ekonomskog sektora je ekonomska obavještajna služba koja prikuplja obavještajne podatke o ekonomskom stanju, resursima, potencijalima i planovima određene države“.[126] Po sličnom principu djeluju i savremeni odjeli korporativne sigurnosti korporacija i preduzeća. Podaci koje odjeli za korporativnu sigurnost prikupljaju u najvećoj mjeri dolaze iz otvorenih izvora, odnosno izvora dostupni široj javnosti. Međutim, dio tih podataka onih koji su najzačajniji prikupljaju se tajnim metodima. Prema Pajeviću: „Prodire se u institucije i objekte stranih država preko kojih se može doći do privrednih, naučnih, geografskih i drugih tajni“. [127] Uloga odjela za korporativnu sigurnost, ne ogleda se samo u značaju koji se temelji na prikupljanju poslovnih informacija. Iako je potreba za poslovnom tajnom najzačajniji element, izuzetna je i potreba za očuvanjem vlastitih poslovnih tajni. Očuvanje vlastite poslovne tajne predstavlja defanzivnu djelatnost korporacije, odnosno *bussines counterintelligence*. Cilj bussines counterintteligence ogleda se prevashodno u uvođenju takvih procedura kojim će se postići određeni nivo sigurnosti poslovnog subjekta i uspostaviti mehanizmi za zaštitu vlastite poslovne djelatnosti.

Centralni dio bussines intelligence i counterintteligence su prodiranje i zaštita poslovnih informacija. Iako su prisutne sličnosti između državne i poslovne obavještajne djelatnosti, između njih postoje naglašene različitosti. Prema Pajeviću (2013): „Te razlike temelje se u okviru obavještajnih objekata (ciljeva ili predmeta) adresirane na svaku od četiri discipline. Obavještajni predmeti su vlastiti resursi i pozicije, neutralan ambijent u kojem su svi učesnici u interakciji, potencijalne sigurnosne prijetnje orjentirane prema nacijama-državama i poslovnom sektoru“.[128]

2. INFORMACIJE

Informacije su kroz istoriju postojanja država, korporacija i preduzeća bile jedan od najvažnijih aspekata. Kako ističe Vidović i dr. (2011): „Upravo na temelju informacija i uz pomoć njih donose se odluke, obavljaju najrazličitiji zadaci, uspostavljaju odnosi, planiraju aktivnosti, stječu nova znanja i spoznaje“.[129] Međutim, nisu sve informacije od značaja za konkurentsko preduzeće ili drugo zainteresovano pravno i/ili fizičko lice. Zbog toga u teoriji i praksi postoji klasifikacija informacija. Informaciju možemo klasifikovati prema vrsti akta, odnosno sadržaja koji taj akt nosi, kao i po značaju za poslovni proces korporacije i preduzeća. Veoma često u praksi dolazi do nerazlikovanja između termina podatak i informacija, na šta ukazuju brojni stručnjaci. Vidović i dr. ukazuju da: „Informacije i podatak

[125] Abazović, M. (2002). Državna bezbjednost- Uvod i temeljni pojmovi, Sarajevo, str. 202.
[126] Pajević, M. (2013). Savremene obavještajne teorije, Mostar, str. 97. (citat Đorđevića preuzet iz knjige dr.sci Majida Pajevića)
[127] Ibid, str. 98
[128] Pajević, M. (2013). Savremene obavještajne teorije, Mostar, str. 141.
[129] Vidović, D. Karlović, L. Ostojić, A. (2011). Korporativna sigurnost, Zagreb, str. 93.

nisu sinonimi, iako se vrlo često poistovjećuju".[130] Mogli bismo kazati da u praktičnom smislu podatak ima veću snagu jer predstavlja već utvrđenu činjenicu. Informacija je dio činjenice, odnosno podatka koja je rezultat određene vrste saznanja. Informacije i podaci u državnom sektoru klasificiraju se po stepenu važnosti na „veoma tajno", „tajno", „povjerljivo" i „interno".[131] Međutim, za poslovanje korporacija i preduzeća značajne su poslovne informacije, koje se također mogu klasificirati prema stepenu važnosti. Poslovne informacije, odnosno poslovna tajna prema Krivičnom zakonu Federacije BiH je: „Podatak ili isprava koja je zakonom, drugim propisom ili općim aktom privrednog društva, ustanove ili druge pravne osobe određen poslovnom tajnom, a koji predstavlja proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada, te drugi podatak zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine privredne interese".[132] Zakonom je informacija vezana za tajnu čije otkrivanje bi bilo na štetu privrednog pravnog lica, i u krajnjoj instanci predstavljalo krivično djelo.

Međutim, puno širu definiciju poslovne informacije daje Trivan (2012), prema kojem pod pojmom poslovna informacija: „Podrazumijevaju se sva saznanja koja su u funkciji unutrašnjeg i spoljnog djelovanja korporacija, tj. sve informacije potrebne za poslovanje i obavljanje poslovnih interesa i ciljeva".[133] Ovakvo široko definisanje značilo bi da svaka poslovna informacija, pa čak i ona koja je beznačajna se ima posmatrati kao poslovna, čiji vlasnik je korporacija ili preduzeće. Iz različitih pristupa definisanju informacija i podataka možemo zaključiti da zakonsko riješenje više teži formalizaciji u smislu određivanja vrste tajnosti, i odgovornosti onog koji otkrije poslovnu tajnu, dok je u Trivanoj definiciji značaj na šteti. Puno objektivnije shvatanje, koje je materijalističko i praktično daje Trivan, jer je fokus pažnje usmjeren na zaštitnu poslovnih interesa. Ko će biti odgovoran za otkrivanje poslovne tajne važan je, ali on dolazi post deliktno. Puno važnije pitanje koje se postavlja jeste šta je sa korporacijom? Kada dođe do propasti i gašenja korporacije, pitanje odgovornosti po našem mišljenju je sporedna stvar. Država neće nadoknaditi štetu vlasniku korporacije ili preduzeća, već će tragati za krivcem i utvrđivati njegovu odgovornost. S toga, postavlja se pitanje na koji način zaštiti interese, odnosno poslovne informacije?

Odgovor je u teorijskom smislu jednostavno dati, prevencijom dok u praktičnom smislu podrazumijeva puni angažman stručnjaka za sigurnost kroz niz aktivnosti. Prvi, osnovni element u zaštiti je pravni okvir kojim se trebaju odrediti šta su to poslovne informacije, poslovne tajne, ko može i kada odrediti stepen tajnosti na poslovnu informaciju, obaveze i dužnosti onih koji saznaju za takvu informaciju i niz drugih bitnih predispozicija. Većina korporacija i preduzeća ima ispunjen prvi osnovni element. Međutim, postavlja se pitanje kako onda dolazi do prodiranja, odnosno curenja informacija i poslovnih tajni korporacija i preduzeća? Odgovor je jednostavan: nizom aktivnosti koje se nazivaju jedinstvenim imenom ŠPIJUNAŽA.

3. POSLOVNA ŠPIJUNAŽA-MIT ILI STVARNOST

Danas u literaturi ne postoji ujednačeno shvatanje pojma poslovna špijunaža. Prvobitni pojam špijunaže prema Abazoviću (2002) imala je: „uže značenje nego danas, jer su sredstva i načini

[130] Ibid, str. 93.
[131] Zakon o zaštiti tajnih podataka BiH, („Sl. novine", br. 54/05)
[132] Krivični zakon Federacije BiH, čl. 2. st. 24. („Sl. novine F BiH", broj: 09/03)
[133] Trivan, D. (2012). Korporativna sigurnost, Beograd, str. 111.

dolaženja do povjerljivih podataka bili uži, manji".[134] Isti autor ukazuje da špijunaža danas ima političko i krivično pravno značenje. U političkom značenju se prema Abazoviću pod špijunažom: „nastoji doći do podataka o činjenicama koje neko skriva (pojedinac, ustanova, organizacija, država), dok u krivično pravnom špijunažu čini samo djelatnost koja je međunarodnim ili domaćim pravom zabranjena, tj. određena kao krivično djelo špijunaže".[135] Evidentno je da Abazović ukazuje i na poslovnu špijunažu, ali da se ista poduzima isključivo od državnih organa.

Danas u poslovnom svijetu i stručnoj javnosti se govori o ekonomskoj, privrednoj i industrijskoj špijunaži. Bilandžić zastupa stav da ove termine treba svrstati pod jedan pojam, poslovna špijunaža.[136] Najednostavnije shvatanje poslovne špijunaže jeste da ista podrazumjeva različite djelatnosti, koje se uvijek provode tajno, od strane operativaca korporacije ili koji rade za korporaciju, koji primjenjuju različite dozvoljene i nedozvoljene metode i tehnike s ciljem dolaska do poslovnih tajne konkurentske korporacije ili preduzeća. Poslovnu špijunažu ne treba proistovjećivati sa poslovno obavještajnom djelatnosti. Poslovno obavještajna djelatnost daleko je šira aktivnost od poslovne špijunaže. Poslovna špijunaža je samo dio i krajnje sredstvo koje se primjenjuje u okvirima poslovno obavještajnog djelovanja. Prema Petkoviću (2008) samo „20% podataka-informacija se dobija kroz tajne operacije, tajne izvore i tajne agente (špijune)".[137] Poslovne informacije do kojih se nastoji doći poslovnom špijunažom mogu da budu potpune iz kojih se vidi cilj i svrha, operativna koje sadrže dio podatka, potvrđujuća pomoću koje potvrđujemo dio činjenica koje se znaju. Veoma često, pa čak i u stručnoj literaturi dolazi do izjednačavanja termina agent, i špijun.

Između ova dva pojma postoje jasne razlike. Pod pojmom agent Modly (1998) podrazumijeva: „jednu od metoda obavještajnih službi. To je osoba koja radi u objektu od interesa i stvarni je pribavljač informacija".[138] Pod agentom možemo smatrati i osobu koja iz različitih motiva, pripadniku službe ili korporacije stalno ili povremeno, ali uvijek tajno dostavlja podatke i/ili informacije o planovima ili poslovnim procesima koji imaju status povjerljivog. Veoma često špijunima nazivamo osobe koje rade profesionalno za neku službu, ili korporaciju. Time bismo pod pojmom špijuni mogli podrazumijevati osobe koje raspolažu sa specifičnim znanjima, i koji postupaju za interese države ili korporacije. Iako se mnogi poslovni subjekti danas deklariraju kao kategorički prijatelji sa poslovnim partnerima, praksa u pogledu dolaska do informacija govori suprotno. Zbog toga, kad god se govori o poslovnoj špijunaži, treba imati na umu da je to vrsta, odnosno oblik neprijateljskog postupanja.

4. IZVORI INFORMACIJA U POSLOVNIM KORPORACIJAMA ILI PREDUZEĆIMA

Prema Petkoviću (2008): „Povjerljiva ili tajna poslovna informacija se može dobiti iz različitih izvora koji, najčešće, neiskusnom čovjeku uopšte ne padaju na pamet".[139] Među najbitnije izvore ili nositelje informacija spadaju ljudi koji znaju za takvu informaciju. Prilikom pripreme za utvrđivanje osoba koje raspolažu sa povjerljivom poslovnom

[134] Abazović, M. (2002). Državna bezbjednost- Uvod i temeljni pojmovi, Sarajevo, str. 264.
[135] Ibid, str. 264.
[136] Preuzeto iz knjige Korporativna sigurnost, Trivan, D. str. 98.
[137] Petković, V.M. (2008), Špijunaža, priručnik za neupučene, Beograd, str. 9.
[138] Modly, D. (1998), Priručni kriminalistički leksikon, Sarajevo, str. 12.
[139] Petković, V.M. (2008), Špijunaža, priručnik za neupučene, Beograd, str. 16.

informacijom, potrebno je napraviti gradaciju svih osoba. Te osobe mogu biti tvorci informacije, top menadžeri koji trebaju osmisliti način sprovođenja nekog plana u djelo, niži nivoi menadžmenta, sekretarice ili stručnjaci koji rade za korporaciju ili kompaniju. Pored osoba kao izvora informacija, kao izvor se mogu javiti i elektronski uređaji poput telefona, računara, laptopa i sl. Kao veoma korisne informacije mogu biti i vlastite opservacije, čiji rezultati mogu biti od interesa za pridobijanje. Veoma često se i sami pitamo zašto bi neka osoba pristala da odaje poslovne tajne suprotnoj strani? Odgovora na ovo pitanje je jako puno. Neki to rade radi novca, drugi radi prevlasti, treći jer su infiltrirani, odnosno ubačeni i djeluju kao rezidentni operativci, neki zbog nezadovoljstva nadređenim, neki zbog seksualno patoloških poriva, a neki čisto iz hira. Međutim, veoma često neke osobe jednostavno ne žele raditi za suprotnu stranu, a neke nisu ni svjesne da čitavu svoju karijeru rade za konkurentsku firmu. Izvori informacija mogu biti različiti oblici seminara, sastanaci ili izvještaji koje korporacija podnosi. Naučna istraživanja i stručni radovi su svakako jedan od nezaobilaznih oblika saznanja koji mogu biti od interesa za korporaciju ili preduzeće. Iako fotografije kao takve ne predstavljaju dokaz u sudskim postupcima, iste se u sigurnosnoj praksi smatraju jednim od svojevrsnih oblika informacija. Fotografije se u obavještajnom radu mogu koristiti i kao oblik komunikacije između operativca, rezidentnog operativca ili agenta. Da bi se ista kao takva koristila neophodno je utvrđivanje unaprijed pisanih pravila sa kojim će biti upoznati samo operativci i agenti koji rade na konkrenom zadatku. Ono što svaki menadžer treba imati na umu jeste da početne informacije o namjerama konkurentske firme uvijek dolaze iz otvorenih izvora, bilo putem medija, putem pogovaranja, ili „šaputanjem među radnicima“. Kao izvor informacije veoma često se javljaju i elektronska sredstva veze. Danas u epohi razvoja tehnologije, jedan stručan rad nije dovoljan za opis elektronskih sredstava koja mogu poslužiti kao izvor. Međutim, i dalje su veoma atraktivni telefoni sa različitim aplikacijama, internet ali i drugi.

5. METODI RADA U OKVIRU POSLOVNE ŠPIJUNAŽE

Prikupljanje podataka i informacije predstavlja osnovnu djelatnost poslovno obavještajnog i kontraobavještajnog rada. Osnovna razlika između prikupljanja podataka i informacija u okviru obavještajnog rada i poslovne špijunaže ogleda se u načinu i sredstvima. Način rada u poslovnoj špijunaži uvijek je tajan, te time i sredstva koja se koriste predstavljaju svojevrsnu mističnost. Može se kazati da jedna od maksima poslovne špijunaže glasi: primijeniti samo ona nužna sredstva pomoću kojih je moguće ostvariti cilj. Jedan od ciljeva svakog oblika špijunaže, pa time i poslovne jeste očuvati konspirativnost, tj. tajnost. Jedan od mogućih i čini se najednostavnijih načina u okviru poslovne špijunaže je vrbovanje informatora ili osoba unutar konkurentske korporacije ili preduzeća. Sam čin vrbovanja predstavlja veoma složen proces terenskog rada. Sastoji se od proučavanja mete, osobe koja je najpogodnija za vrbovanje s ciljem detaljnog proučavanja života, poslovne karijere, odnosa sa drugim osobama, kontaktima, prijateljima, ljubavnicama. Treba imati na umu da se ovdje uvijek radi o ljudima iz rukovodnih struktura, odnosno najužeg rukovodstva institucije koja je konkurentska meta. Kako ističe Petković (2008): „Pravilo je da u vrbovanju učestvuje najmanje tri operativca, svaki u određenoj fazi vrbovanja: najprije u kontaktu sa odabranim licem dolazi tzv. nagovarač i pokušava da mu predoči šta se od njega očekuje uz nagovještaj mogućnosti davanja protivusluga raznih vrsta, u sljedećoj fazi radi vrbovščik kome je zadatak

da odabrano lice čvršće veže za sebe i na kraju dolazi do upoznavanja za voditeljem tima koji ujedno i rukovdi radom agenta na terenu i osmatra reagovanje sredine u kojoj agent radi".[140]

Drugi mogući metod je infiltracija osobe u konkurentsku firmu, s ciljem prikupljanja podataka. Ovaj metod predstavlja složeniji proces od prethodnog jer zahtijeva puno više vremena, resursa, pripreme i finansijskih troškova. S druge strane, savremene korporacije prilikom prijema osoba na značajne funkcije vrše detaljne sigurnosne provjere. Iako je bilo koji oblik poslovne špijunaže zakonom zabranjen, veoma često prilikom kontradiverzionih pregleda prostorija za sastanke, prostorija u kojem borave top menadžeri pronađu se tehnički podesne sprave za prisluškivanje. To znači da se u okviru poslovne špijunaže koriste tehnička pomagala za dolazak do informacija. Ovakvi uređaji veoma teško se otkrivaju, pa čak i po otkrivanju jako teško se ustanovljava od koga su postavljeni. Jedan od mogućih metoda poslovne špijunaže koji je zabilježen u praksama mnogih zemalja jesu ucjene. Operativci zaduženi za praćenje mete, veoma često dođu do kompromitirajućih materijala. Pomoću takvih materijala meta se ucjenjuje i veoma često takva osoba postaje vrhunski informator koji u kontinuitetu dostavlja veoma povjerljive podatke. Pored ovih postoje i brojni drugi metodi rada. Zapravo, metodi rada u okviru poslovne špijunaže dosežu vrhunac ljudske mašte.

ZAKLJUČNA RAZMATRANJA

U radu se nastojalo ukazati na mogućnosti koje danas u kapitalističkim društvima, uprkos brojnim zakonskim ograničenjima odvažni se mogu koristiti djelatnostima poslovne špijunaže. Osnovni cilj u radu nastojao se ostvariti kroz prikaz metoda rada poslovne špijunaže, kako bi čitatelju a posebno menadžerima stvorio predstavu o potrebi za maksimalnim nivoima zaštite. Jedan od preduvjeta za zaštitu je shvatanje sigurnosti kao procesa koji se ostvaruje ulaganjem u ljudske resurse. Menadžeri za sigurnost korporacija u vremenu jake konkurentnosti moraju biti vrhunski praktičari koje svoje znanje iz različitih oblasti kontinuirano nadopunjuju.

Primarna djelatnost savremenih manadžera treba se sastojati u edukativnim i preventivnim djelatnostima. Kroz edukativne djelatnosti cilj je razvijati sigurnosno kulturu svih uposlenih o značaju informacija. Poduzimanjem mjera provjera uposlenika, zaštitom elektronskih informacija, fizičko tehničkom zaštitom prostorija, kontradiverzionim kontinuiranim pregledima osiguravaju se najviši standardi sigurnosti. S druge strane, najvažnija zaštita je permanentna edukacija i interakcija sa rukovodiocima korporacija, jer samo vrhunski sigurnosni operativac određene situacije može prepoznati kao djelatnost poslovne špijunaže. Polje poslovne špijunaže proseže se u skoro sve sfere poslovnog svijeta. Mnogi upravni odbori i top menadžeri nakon velikih poslovnih gubitaka stiču dojam da su njihove djelatnosti postale metom osoba koje djeluju iz pozadine, osoba za koje se malo zna, i osoba o kojima će se teško nešto saznati. Osobe koje se bave poslovnom špijunažom zapravo predstavljaju vrhunske stručnjake koji se koriste znanjima o ljudskom ponašanju, motivima, sigurnosnim protokolima. Radi se o osobama koje svoje stručne djelatnosti sprovode bez puno spektakularnosti, u tišini svoje oštroumnosti. Nakon završenog posla veoma često nestaju na način kako su i došli, u tišini.

[140] Petković, M.V. (2008). Špijunaža priručnik za neupučene, Beograd, str. 50-51.

LITERATURA

[1] Abazović, M. (2002). *Državna bezbjednost: uvod i temeljni pojmovi,* Sarajevo: Fakultet kriminalističkih nauka,
[2] Vidović, D. Karlović, L. Ostojić, A. (2011). *Korporativna sigurnost,* Zagreb: Udruga hrvatskih menadžera sigurnosti,
[3] Modly, D. (1998). *Priručni kriminalistički leksikon,* Sarajevo: Univerzitet u Sarajevu Fakultet kriminalističkih nauka,
[4] Pajević, M. (2013). *Savremene obavještajne teorije,* Mostar: Visoka škola „Logos centar“ Mostar,
[5] Petković, M.V. (2008). *Špijunaža-Priručnik za neupućene,* Beograd: Knjiga komerc Beograd,
[6] Trivan, D. (2012). *Korporativna bezbjednost,* Beograd: Dosije studio,

Zakonski i podzakonski akti

[1] Krivični zakon Federacije BiH („Sl. novine“, br. 09/03),
[2] Zakon o zaštiti tajnih podataka BiH („Sl. novine“, br. 54/05).