Pregledni članak

POSLOVNO-KONTRAOBAVEŠTAJNI RAD KAO DETERMINANTA KORPORATIVNE SIGURNOSTI
(Uvodni referat)

Atanas Kozarev, PhD; email: kozarev.atanas@yahoo.com
Fakultet za pravne nauke, međunarodne odnose i diplomatiju u Skoplju
Srđan Vujinović, MA; email: svujin93@gmail.com
Student specijalističkih akademskih studija kriminalistike na Kriminalističko - policijskoj akademiji u Beogradu

Sažetak: U ovom radu će se analizirati poslovno-kontraobaveštajni rad kao determinanta korporativne sigurnosti. Tradicionalni pristupi u zaštiti resursa, koji se mogu zapaziti kod različitih korporacija, postaju sve manje efikasni. Njihovu efikasnost dovodi u pitanje sve brža evolucija pretnji koje otežajavaju dostizanje zamišljenih poslovnih ciljeva. U takvom neizvesnom okruženju koje karakteriše stalna promena pojavnih oblika, neophodno je implementirati niz mera koje bi proaktivno sprečile potencijalne napade na korporaciju. Većina napada na korporaciju, bez obzira na njihov cilj moraju ispuniti važan preduslov kako bi bili adekvatno organizovani. Preduslov je posedovanje poslovnih informacija o različitim oblastima korporativnog poslovanja, odnosno mera zaštite koje su implementirane u poslovnim objektima. Pretpostavka ovog rada je da je poslovno-kontraobaveštajni rad kao skup različitih mera i radnji osnova zaštite korporacije i faktor koji proaktivno može onemogućiti štetne događaje.
Ključne reči: korporativna sigurnost, poslovno-kontraobaveštajni rad, poslovna tajna, korporacija, sigurnosni menadžment

BUSINESS COUNTERINTELLIGENCE AS A DETERMINANT OF CORPORATE SECURITY
(Keynote paper)

Abstract: This paper will analyze business counterintelligence as a determinant of corporate security. Traditional approaches to protecting resources, which can be seen in various corporations, are becoming less and less effective. Their effectiveness is called into question by the increasingly rapid evolution of threats that make it difficult to achieve imagined business goals. In such an uncertain environment characterized by a constant change in appearance, it is necessary to implement a series of measures that would proactively prevent potential attacks on the corporation. Most corporate attacks, regardless of their goal, must meet an important prerequisite in order to be adequately organized. A prerequisite is the possession of business information on various areas of corporate business, i.e. protection measures implemented in corporate facilities. The premise of this paper is that business counterintelligence as a set of various measures and actions is the basis of corporate protection and a factor that can proactively disable harmful events.
Key words: corporate security, business counterintelligence, trade secret, corporation, security management

1. UVOD

Različitost tržišnih uslova i težnja za ostvarivanjem poslovnih ciljeva, u velikoj meri i na različite načine testiraju sposobnosti rukovodstva korporacija da stvore i održe konkurentnu prednost. Danas, teško je pričati o poslovanju koje se odvija na različitim tržištima, jer se sve više uočava tendencija sjedinjavanja tržišta, ta tendencija je posledica globalizacije kao sveprisutnog procesa u kome države učestvuju. Globalizacija je pored velikih poslovnih šansi

za korporacije donela i novu opasnost na tržištu koja se naziva konkurencija. Težnja da se pobedi u konkurentskoj utakmici proizvodi različite ideje kod rukovodstva određenih korporacija, od kojih neke nisu ni zakonite ni moralne. Blagovremeno posedovanje poslovnih informacija postaje značajna vrednost koja može uticati na stvaranje konkurentsku prednosti i samim tim primata na tržištu. Kako bi se razumelo ponašanje konkurenta na tržištu potrebno je prikupiti veliku količinu informacija, od kojih neke nisu javno dostupne. Nemogućnost neposrednog pristupa poslovnim informacijama o planovima konkurenta uz postojanje potrebe da se taj plan što pre sazna, može da racionalizuje aktivnosti korporacije i da ih odvede van okvira zakona. U takvim situacijama govori se o industrijskoj špijunaži.

Industrijska špijunaža je delatnost kojom se nastoje prikupiti poverljive poslovne informacije upotrebom različitih metoda koje su nelegalne, ali i neetičke ukoliko se uzme u obzir poslovna etika. Kao što se može naslutiti iz dosad pomenutog, poslovna informacija je ključni činilac uspešnog poslovanja u vremenu koga smo deo. Shvatajući to, opravdano se može postaviti pitanje kako poslovnu informaciju zaštititi od narastajuće konkurencije na sve povezanijem tržištu? Upravo odgovor na to pitanje je predmet ovog rada. Koncept koji je relativno skoro krenuo da dobija značaj, ali koji kao aktivnost nesumnjivo odavno postoji naziva se poslovno-kontraobaveštajni rad.

2. POJAM POSLOVNO-KONTRAOBAVEŠTAJNOG RADA

Korporativna sigurnost predstavlja složen pojam. Složenost ovog pojma proističe iz činjenice da se korporacije sve češće susreću sa novim pretnjama koje su posledica čovekovog tehnološkog napretka. Povremeno, pretnje su poznate, ali im je evoluirao pojavni oblik. Što je slučaj sa i industrijskom špijunažom, koja se sve češće može primetiti u različitim industrijama širom sveta. Naime, devedesetih godina dvadesetog veka, dominantan modus operandi industrijskih špijuna je bio fizička krađa poverljive dokumentacije. Danas, sajber prostor je mesto na kome se se najčešće odvijaju aktivnosti čiji je cilj krađa poslovnih tajni. Shodno tome, različitost pretnji i njihovih pojavnih oblika uslovljava formiranje sveobuhvatne strategije korporativne sigurnosti, čiji sadržaj mora konsolidovati korporativne resurse.

Sprečavanje nanošenja štete korporativnom poslovanju jedan je od zadataka sektora korporativne sigurnosti. Takav zadatak nije uvek lako realizovati, jer postoji mnoštvo faktora koji mogu predstavljati prepreku. Bez obzira na tu činjenicu, u korporativnom poslovanju se može primetiti jedna konstanta. Utisak koji će pažljiv posmatrač neminovno steći je da se adekvatnom zaštitom poverljivih poslovnih informacija nesumnjivo doprinosi sprečavanju štetnih događaja. Nevezano od prirode štetnog događaja, zaštitom poverljivih poslovnih informacija se onemogućava upoznavanja izvršioca sa specifičnostima poslovanja korporacije.

Slikovit primer možemo naći u krivičnom delu razbojništva. Nemogućnost razbojnika da sazna sve posebnosti zaštite banke na primer, povećava rizik da se napravi greška prilikom izvršenja dela. Poslovno-kontraobaveštajni rad kao zasebna aktivnost sektora korporativne sigurnosti doprinosi da se poslovne informacije dodatno zaštite. U razmatranju pojma poslovno-kontraobaveštajnog rada, neophodno je krenuti od opštijeg pojma koji je poznatiji kao kontraobaveštajni rad. Ovaj termin neposredno asocira na aktivnosti koje sprovode državne službe sa ciljem zaštite državne sigurnosti. Neki autori smatraju da je kontraobaveštajni rad

analitički i operativni proces kojim se nastoje identifikovati i neutralizovati aktivnosti stranih obaveštajnih službi koje su usmerene ka Sjedinjenim Američkim Državama.[11]

Goldman napominje da kontraobaveštajni rad uključuje aktivnosti čiji je cilj zaštita, prilikom sprovođenja aktivnosti teži se identifikaciji i sprečavanju delovanja stranih država, različitih tipova organizacija ili čak zlonamernih pojedinaca. Stav ovog autora je da se kontraobaveštajni rad može podeliti na: pasivni – koji je po prirodi defanzivan, i podrazumeva sve one radnje kojima se štite objekti i personal. Sa druge strane imamo aktivni (ofanzivni) kontraobaveštajni rad, on se sastoji od aktivnosti kojima se nastoji obmanuti neprijatelj, odnosno izvršiti penetracija u njegove rade sa ciljem zaštite interesa sopstvene države.[12]. Prema Golovinu, sintagma kontraobaveštajni rad podrazumeva sprovođenje različitih aktivnosti u cilju prikupljanja informacija kako bi se država zaštitila od špijunaže, sabotaža i atentata koje mogu realizovati različite organizacije i/ili pojedinci.[13]

Uzevši u obzir pomenuta pojmovna određenja kontraobaveštajnog rada, postavlja se pitanje šta je poslovno-kontraobaveštajni rad? Koje su njegove karakteristike i zbog čega je značajan za korporativnu sigurnost? Kako bismo dali odgovor na ova pitanja, neophodno je prvenstveno razumeti odnos koji postoji između privatnog i državnog sektora. Za takvu analizu najadekvatnije su Sjedinjene Američke Države. Sjedinjene Američke Države mnogo ulažu u svoj obaveštajno-sigurnosni sistem. Interesantna je i činjenica da je korporativni sektor ove države u tesnoj vezi sa državnom administracijom, bez obzira koja politička partija vodi administraciju. Ova povezanost je velika ističe Peri i dodaje da američke sigurnosne službe direktno savetuju korporacije koje potiču iz ove zemlje i sprovode raznovrsne kontraobaveštajne edukacije, sa ciljem sprečavanja krađe intelektualne svojine.[14] Takva bliska saradnja je pogotovo izražena kada korporacije posluju u takozvanim „kriznim područjima“. Područja ovog tipa može da karakteriše velika nestabilnost, nepostojanje pravne države i suštinski neprijateljsko okruženje koje nastoji da nanese štetu poslovanju korporacije. Odsustvo pravne zaštite i neprijateljsko okruženje u kojem se posluje, nesumnjivo opravdava postojanje sektora korporativne sigurnosti. Ova organizaciona jedinica mora da pronađe najadekvatnije načine na apsorbuje negativne uticaje okruženja u kom se korporacija nalazi, i da kreira strategije koje će imati pozitivne efekte na poslovanje. Jedna od aktivnosti kojom se korporacije mogu zaštititi u ovakvom okruženju je poslovno-kontraoobaveštajni rad.Pod pojam poslovno-kontraobaveštajni rad podvodi se sveobuhvatan napor korporacije, koji je zamišljen tako da spreči neovlašćen pristup osetljivim poslovnim informacijama. Dakle, može se reći da poslovno-kontraobaveštajni rad predstavlja sve radnje koje imaju za cilj ograničavanje pristupa važnim korporativnim informacijama, čije bi saznavanje moglo ugroziti poslovanje.[15]

3. CIKLUS POSLOVNO-KONTRAOBAVEŠTAJNOG RADA

Poslovno-kontraobaveštajni rad je proces, odnosno on je niz međusobno povezanih faza, čijom se realizacijom teži ostvarenju unapred planiranog cilja. Cilj je uopšteno govoreći proaktivno

[11] Turner, H., Historical Dictionary of United States Intelligence, Scarecrow Press, United States of America, 2006, str. 41.
[12] Goldman, J., Words of Intelligence – A Dictionary, Scarecrow Press, United States of America, 2006, str. 29.
[13] Golovin, A., Fundamental Elements of the Counterintelligence Discipline. Nova Science Publishers Inc, New York, 2009, str. 6.
[14] Perry, D., „Repugnant Philosophy“ – Ethics, Espionage and Covert Action. U: Ethics of Spying – A Reader for the Intelligence Professional, Scarecrow Press, United States of America, 2006, str. 236.
[15] Botos, H., Radu, G., Business counterintelligence practice. U: Romanian Intelligence Studies Review. National Institute for Intelligence Studies, Bucharest, 2018 str. 167

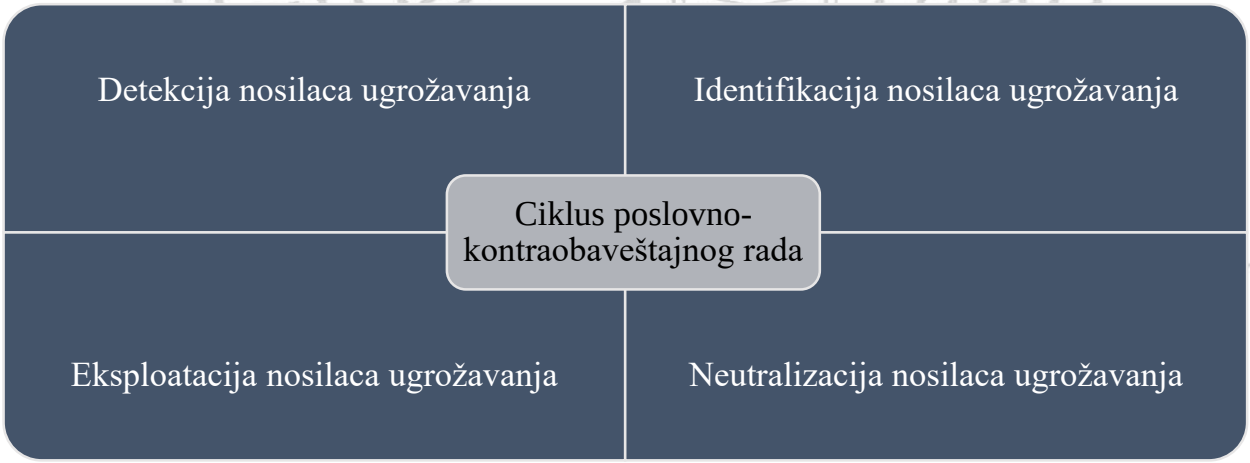
sprečavanje aktivnosti kojima se mogu neovlašćeno prikupiti poverljive poslovne informacije. U načelu, faze poslovno-kontraobaveštajnog rada možemo svrstati u četiri kategorije:

- Detekcija nosilaca ugrožavanja[16] vrednosti[17] korporacije;
- Identifikacija nosilaca ugrožavanja vrednosti korporacije;
- Eksploatacija nosilaca ugrožavanja nosilaca vrednosti korporacije;
- Neutralizacija nosilaca ugrožavanja vrednosti korporacije.[18]

Potrebno je napomenuti da nosioci poslovno-kontraobaveštajnog rada nisu samo članovi sektora korporativne sigurnosti. Vrlo čest slučaj je da sektor korporativne sigurnosti u korporaciji ne poseduje kadrovske kapacitete da bi realizovao poslovno-kontraobaveštajni rad.

Rešenje za ovakav problem se nalazi u angažovanju onih zaposlenih koji izvorno rade na drugim poslovnim funkcijama. Zaposleni koji nisu direktno vezani za sektor korporativne bezbednosti, mogu neposredno (opservacijom) ili posredno (po čuvenju) da dođu do informacija o pretnjama usmerenim ka korporativnim resursima.

Preduslov njihovog doprinosa poslovno-kontraobaveštajnom radu je prethodna sigurnosna edukacija. Ovaj tip edukacije je relevantan zato što omogućava zaposlenima da potpunije upoznaju oblast zaštite poslovnih informacija i metoda njihovog neovlašćenog prikupljanja. Vrsta sigurnosne edukacije koja će se sprovoditi zavisi od nekoliko faktora, neki od tih faktora su: tip korporacije i specifičnost delatnosti, veličina korporacije, broj lokacija na kojima se odvija poslovanje i broj zaposlenih na lokacijama, naposletku imamo i sigurnosnu procenu kao važan faktor. Uzevši u obzir pomenute faktore i mnoge druge, kreira se program sigurnosne edukacije za različite kategorije zaposlenih. Na taj način se i određuje ko može biti uvršten u aktivnosti poslovno-kontraobaveštajne zaštite korporacije. Detaljnije razmatranje faza poslovno kontraobaveštajnog rada će stvoriti jasniju sliku o važnosti svakog pomenutog koraka.



Izvor: (Vujinović, 2021)

[16] Pod terminom **nosilac ugrožavanja** podrazumeva se pojedinac ili grupa koja primenjuje različite metode kako bi neovlašćeno prikupila poverljive poslovne informacije.
[17] **Vrednosti** u ovom kontekstu su poverljive poslovne informacije. One mogu biti različitog sadržaja i uslovljene su delatnošću korporacije. U poslovno-kontraobaveštajnom radu, one su predmet zaštite.
[18] Vujinović, S. Uloga poslovno-kontraobaveštajnog rada u sprečavanju industrijske špijunaže, Master rad, Fakultet bezbednosti, Beograd, 2021, str. 49.

Detekcija nosilaca ugrožavanja – je prva faza poslovno-kontraobaveštajnog rada. Njen cilj je da se kroz kontinuirano praćenje internog i eksternog okruženja korporacije, uoče promene koje bi mogle da ukažu na aktivnosti neovlašćenog prikupljanja poverljivih poslovnih informacija. Kao što smo pomenuli, preporučljivo je da se oformi sistem u kom će i zaposleni na drugim poslovnim funkcijama biti osposobljeni za detektovanje sumnjivih radnji. Potrebno je reći da u fazi detekcije nije važna lokacija, jer se može desiti da napad na korporaciju otpočne van radnog vremena i prostora. Shodno tome, neposredno je uočljiva važnost sigurnosne edukacije zaposlenih, jer njihovo osposobljavanje da pravovremeno detektuju napad predstavlja važan faktor u zaštiti poverljivih poslovnih informacija.

Identifikacija nosilaca ugrožavanja – Nakon što se detektuju aktivnosti koje su usmerene ka poverljivim poslovnim informacijama korporacije, nastupa faza identifikacije. U ovoj fazi je poznato da neki entitet pokušava prodor sa ciljem razotkrivanja poslovnih tajni, međutim ne poseduju se jasne informacije o metodici i profilu napadača. Identifikacijom se nastoji odgovoriti na nekolicinu pitanja, koja se tiču identiteta pojedinca/grupa koja je organizovala napad. Pored toga, relevantna pitanja se tiču metoda koje se koriste. U ovoj fazi je vrlo značajno da se analiziraju sve informacije koje bi ukazale na dominante načine kojima napadač nastoji da dođe do poverljivih poslovnih informacija. Metodika napada može biti raznovrsna, u praksi često jeste, i suštinski je uslovljena kompetencijama koju nosilac ugrožavanja ima. Naravno, finansijski i kadrovski resursi su takođe važan faktor, i predstavljaju uvek važnu podlogu za kvalitetnu organizaciju napada na korporaciju. Faza identifikacije se privodi kraju kada sektor korporativne sigurnosti prikupi odgovarajuću količinu informacija o nosiocu ugrožavanja. Smatra da se da je količina informacija zadovoljavajuća ukoliko se stvori jasna slika o profilu i metodici rada napadača (nosioca ugrožavanja)

Eksploatacija nosilaca ugrožavanja – Eksploatacija je reč francuskog porekla, ova reč se najčešće koristi kada se misli na iskorišćavanje nekoga ili nečega. U kontekstu poslovno-kontraobaveštajnog rada eksploatacija stupa na scenu kada se u dovoljnoj meri razumeju postupci nosioca ugrožavanja. Obeležje faze eksploatacije je težnja da se slabosti nosioca ugrožavanja protiv njega iskoriste. S obzirom da su ljudi nosioci napada na korporacije, bez obzira na njegovu prirodu i nameru, razumno je očekivati da će se praviti greške. Sektor korporativne sigurnosti te greške mora da iskoristi, i uz njihovu pomoć stvori priliku za neutralizacijom daljeg delovanja nosioca ugrožavanja. Greške nosioca ugrožavanja mogu biti različite vrste, počevši od manjka sigurnosne kulture i otkrivanja svojih namera pa do netaktičnog ponašanja u toku napada. Bez obzira na tip greške, za sektor korporativne sigurnosti je važno da greške budu iskorištene kako bi mogli sprečiti dalje delovanje napadača.

Neutralizacija nosilaca ugrožavanja – Neutralizacijom se teži uticati na nosioca ugrožavanja da odustane od ideje napada na korporaciju. Uticanjem na određene aspekte njegovog delovanja ili celokupnu aktivnost nosilac ugrožavanja se stavlja u bezizlaznu poziciju, u kojoj njegovo dalje delovanje može biti potpuno stopirano.[19] Cilj sektora korporativne sigurnosti je da poslovno-kontraobaveštajnim radom odvrati i obeshrabri planove nosioca ugrožavanja.

[19] Prunckun, H., Counterintelligence – Theory and Practice. Roman & Littlefield Publishing Group Inc, Maryland 2019, str. 216.

4. UTICAJ POSLOVNO-KONTRAOBAVEŠTAJNOG RADA NA KORPORATIVNU SIGURNOST

Uticaj poslovno-kontraobaveštajnog rada mora da se reflektuje na sve korporativne resurse. Suština realizacije ove aktivnosti je da se kroz potpuno obuhvatanje korporativnih resursa (zaposlenih, poslovnih objekata i poslovnih informacija), u celosti umanje šanse uspeha nosilaca ugrožavanja. Čest problem koji se u korporativnoj praksi uviđa je da se aktivnosti koje sprovodi sektor korporativne sigurnosti tumače kao „preterane“.

Naime, neretko rukovodstvo korporacije svesno sprečava da se sugestije sektora korporativne sigurnosti primene, razlog je u tome što se te sugestije često doživljavaju kao nepotrebne. Takav stav je svakako proizvod neznanja i nepotpunog razumevanja značaja korporativne sigurnosti za poslovanje. Posledica ovakve pogrešne percepcije rukovodstva korporacije je primenjivanje reaktivne sigurnosne strategije, koja se sprovodi tek nakon što dođe do štetnog događaja. Takav pristup je pogrešan, jer samo proaktivnim radom i blagovremenim sprečavanjem neovlašćenog prikupljanja poverljivih poslovnih informacija je moguće efektivno sprečiti poslovne pretnje.

5. DOPRINOS KORPORATIVNE SIGURNOSTI U ZAŠTITI OD INDUSTRIJSKE ŠPIJUNAŽE

Industrijska špijunaža je realnost u savremenom poslovnom svijetu. Korporacije ulažu ogromna sredstva u inkluziju mehanizama ovog oblika špijunaže s ciljem da ostvare konkurentnu prednost u odnosu na svoje konkurente. Poznato je da ekonomski ratovi, koji danas zamjenjuju klasične, kontinuirano koriste aktuelna "oružja" industrijske špijunaže. Na udaru industrijske špijunaže nalazi se celokupna arhitektura jednog poslovnog, korporativnog entiteta, počevši od poslovne tajne, ljudskog kapitala, osnovnih biznis planova i interesa itd. Pri tome, ne postoji država u svetu koja je imuna na ovu savremenu poslovnu bezbednosnu pretnju. "Prema procenama FBI-a, Sjedinjene Države trpe godišnje između 130 i 330 milijardi dolara štete zbog industrijske špijunaže. Isti izvor tvrdi da oko 15 zemalja ima prilično agresivne programe industrijske špijunaže, koji su usmereni na Sjedinjene Države, a među njima su najagresivnije Kina i Rusija."[20]

Poslednjih nekoliko godina američko društvo je bilo ozbiljno potreseno kradjom personalnih informacija od nekoliko kompanija. Ulazak u bazu podataka jedne od tri kreditne agencije u SAD, Equifax, u periodu od maja do jula 2017 godine, rezultirao je kradjom osetljivih ličnih podataka od više od 143 miliona Amerikanaca, što je nešto manje od polovine gradjana SAD. Hakeri su ukrali podatke o adresama, datumima i mestima rodjenja, matičnim brojevima za socijalnu sigurnost (Social Security numbers), što je ekvivalent matičnom broju u Makedoniji, a u nekim slučajevima i brojevima vozačkih dozvola. Imajući u vidu kako funkcioniše američko društvo, intenzitet transakcija koje se odvijaju preko interneta, postoji opasnost od

[20] https://www.securitysee.com/2016/06/industrijska-spijunaza-kontra-mere/, 07.12.2022 година.(Industrijska špijunaža često obuhvata tehnologiju ili robu koja ima i civilnu i vojnu primenu. Zbog bezbednosnih razloga, američke obaveštajne službe kontrolišu izvoz osetljive tehnologije pojedinim zemljama.. Zbog toga mnoge američke kompanije moraju biti vrlo pažljive i štititi se od špijunaže, dok pokušavaju plasirati svoju robu i probiti se na nova tržišta. Između ostalog, posebna opasnost vreba od insajdera, koji su spremni da prodaju poslovne tajne kompanije drugima. Takođe veliku opasnost predstavlja internet i njegova upotreba bez adekvatnih zaštitnih softvera u okviru preduzeća.).

nanošenja velike materijalne i finansijske štete licima čiji su podaci ukradeni. Lice koje neovlašćeno raspolaže ovakvim podacima može neovlašćeno napraviti transfer sredstava, naneti štetu kreditnom rejtingu lica i još puno drugih stvari. Ovo je uticalo na reputaciju kompanije, što je rezultiralo ostavkama u Upravnom odboru.[21]

Za razliku od odavanja državnih tajni, što se sankcioniše krivičnim zakonima i što predstavlja krivično delo, korporacije veoma teško mogu koristiti zakonske mere protiv neovlašćenog odavanja poslovnih tajni. Ovo pravi zaštitu od poslovne špijunaže još složenijom i težom. Potreba za kvalitetnom zaštitom kod poslovne špijunaže postaje sve veća. Zbog ovoga kompanije su primorane da pronalaze i da implementiraju nove kreativne solucije koje će obezbijediti njihovu zaštitu od takozvane industrijske špijunaže. Najranjivije za ovakva dejstva su istraživačke jedinice korporacija.[22]

Korporativna sigurnost je često korišćen koncept u savremenoj poslovnoj praksi, obzirom na to da kompanije u značajnoj mjeri snose odgovornost u svom poslovanju za dešavanja i aktivnosti iz oblasti korporativne sigurnosti. U cilju da doprinesu rešavanju problema korupcije preduzeća, društvene zajednice u kojoj kompanije obavljaju svoju poslovnu aktivnost sprovode različite oblike bezbednosti iz oblasti zaštite svoje imovine, poslovnih procesa, informacione bezbednosti, pa sve do sigurnosti svojih kupaca, dobavljača i zaposlenih. Kako bi što uspešnije koristile mnogobrojne prednosti negovanja društveno odgovornog ponašanja, kompanije moraju da afirmišu svoje ideje i osećanja, brige za svoje probleme. Izuzetno je važno da obezbede potpunu transparentnost i posvećenost društvenim interesima.[23]

Korporativna sigurnost za kompanije podrazumeva obezbedjivanje njihove zaštite u odnosu na poslovni rad, bezbednost ljudskih resursa koji sačinjavaju jezgro jednog poslovnog subjekta, uspostavljanje sistema korporativne zaštite u ciljnoj (partnerskoj) kompaniji sa sledećim sadržajima:

- bezbednosna procena rizika
- projektovanje optimalne organizacije korporativne zaštite,
- projektovanje optimalnih potreba za adekvatnom strukturom stručnih bezbednosnih kadrova, normativnim uredjivanjem korporativne zaštite, uspostavljanjem funkcionalnih informacijskih sistema i uspostavljanjem sistema za fizičko-tehničko i inženjersko obezbedjenje.”[24]

Naime, putem ostvarivanja misije korporativne bezbednosti u suštini se ostvaruje ekonomska bezbednost poslovnog rada što podrazumeva i efikasnu prevenciju protiv korporativnih krivičnih djela. To se postiže preko realizacije nadležnosti menadžera korporativne bezbednosti koji su budno oko u jednoj kompaniji i daju bezbednosne usluge na različitim nivoima. Korporativne usluge su raznolike i u njih spadaju sledeći zasebni bezbednosni zadaci:

---

[21] Jolevski Z., Korporativna bezbednost u savremenoj uslužnoj ekonomiji i industriji 4.0., Zbornik radova Medjunarodne naučne i stručne konferencije: Integrisana korporativna bezbednost i digitalne transformacije: izazov za akademsku zajednicu i savremene korporacije, Asocijacija za korporativnu bezbednost, Skopje, 2018 godina,str. 17-19.

[22] Ibid.

[23] Jusufranić I., Značaj i uloga korporativne sigurnosti u poslovanju preduzeća, Зборник на трудови од Меѓународна научна и стручна конференција: Интегрирана корпоративна безбедност и дигиталните трансформации: предизвик за академската заедница и современие корпорации, Асоцијација за корпоративна безбедност, Скопје, 2018 година, стр. 27.

[24] Stojanović M., Pavlović D., Ekonomska bezbednost poslovanja, Beograd, 2014 godina, str. 207.

- bezbednost ljudskog kapitala u poslovnom subjektu i vezanog uz njega tržišnog kapitala,
- bezbednost menadžmenta poslovnog subjekta, vlasničkog kapitala,
- bezbednost poslovnih informacija, poslovnih strategija,
- informatička i industrijska bezbednost.

Uz ovaj katalog bezbednosnih korporativnih nadležnosti mogu se nabrojati i druge koje proizilaze iz svakodnevnog funkcionisanja kompanija i bezbednosnih rizika sa kojima se iste suočavaju u svom radu.[25]

„Korporativna bezbednost je permanentno uključena u mehanizme poslovnog rada na taj način što štiti normalno odvijanje poslovnih procesa, odstranjuje aktuelne bezbednosne probleme i zaposlenima stvara bezbedne uslove za rad. Konkretno posmatrano, korporativna bezbednost se aktivira u stvaranju planova i sprovodjenju mjera čiji je cilj: zaštita korisnika usluga, zaštita zaposlenih u poslovnoj organizaciji, zaštita imovine u vlasništvu poslovne organizacije, zaštita informacija i reputacije poslovne organizacije od materijalnih šteta, kriminalnih aktivnosti itd. Na ovaj način korporativna bezbednost predstavlja sastavni deo procesa koji upravljaju poslovnim rizicima iznutra u privrednom subjektu.”[26]

Praktično fokus korporativne bezbednosti u odnosu na zaštitu kompanija od industrijske špijunaže usmeren je ka:

- kvalitetnoj proceni rizika u radu preko detektiranja postojećih problema,
- predvidjanju njihovog razvoja i
- blagovremenom preduzimanju mjera i aktivnosti za njihovo odstranjivanje. To podrazumijeva detaljno istraživanje izvora ugrožavanja, kriminogenih, viktimogenih i patogenih žarišta koji mogu destabilisati radni proces u cjelini. Aktivnosti kojima se vrši bezbednosna procena uslovno se mogu podijeliti na sledeći način:
  1) Procena mogućih izvora (nosioca) ugrožavanja bezbednosti u korporacijama;
  2) Procena mogućih oblika (načina) ugrožavanja bezbednosti u korporacijama;
  3) Procena mogućih ugrožavanja bezbednosti u korporacijama i
  4) Analiza rizika.[27]

Korporativna bezbednost kao model zaštite funkcionisanja savremenih poslovnih subjekata ima svoje nadležnosti u prevenciji industrijske špijunaže zato što kao posebna grupacija bezbednosnih pretnji ima implikaciju i na ekonomsku bezbednost u celini. Tačke povezivanja izmedju potrebe za reduciranjem štetnih posledica industrijske špijinaže i menadžera za korporativnu bezbednost su vidljive i realne. Naime, industrijska špijunaža pretpostavlja i ulaganje finansija od strane top menadžera i vlasnika kompanija u oba smera: u jačanju korporativne bezbednosne svesti, prije svega kod zaposlenih i u vlastitoj svesti o kontinuiranom modernizovanju radnih i proizvodnih procesa. Bezbednosne procene rizika koje se mogu javiti u slučaju kada se ova ulaganja postave na margine strateških ciljeva kompanije, a koje se pripremaju od strane menadžera za korporativnu bezbednost, su prva stepenica signaliziranja

[25] Kozarev A. i dr., Ekološki kriminalitet i korporativna bezbednost u Republici Makedoniji, Zbornik radova Medjunarodne naučne i stručne konferencije : Integrisana korporativna bezbednost i digitalne transformacije: izazov za akademsku zajednicu i savremene korporacije, Asocijacija za korporativnu bezbednost, Skopje, 2018 godina, str. 13.
[26] Trivan D., Korporativna bezbednost, Dosije studio, Beograd, 2012, str. 84.
[27] Dragišić Z., Bezbednosni menadžment, Službeni glasnik, Beograd, 2007, str.47-52.

od strane sistema korporativne bezbednosti. Dalje, ovdje se nadovezuju korporativni indikatori u oblasti ljudskih resursa, zaštite informacija, poslovnih tajni, konkurentske prednosti itd. Na taj način, može se zaključiti da korporativna bezbjednost kao koncept, model, vizija, ima poseban značaj u povećanju ekonomske bezbednosti koja je prema prirodi industrijske špijunaže (sa ekonomskim predznakom) od ključnog značaja za jačanje poslovnog integriteta i povjerenja.

ZAKLJUČAK

Primena različitih zaštitnih mera čiji je cilj sprečavanje neovlašćenog prikupljanja poverljivih poslovnih informacija, predstavlja osnovu za dostizanje poslovnih ciljeva. Neadekvatna zaštita poslovne tajne, može naneti štetu koja ima potencijal da u potpunosti ugasi korporativno poslovanje. Nažalost takvih primera nije malo u zemljama na zapadu. U ovom radu smo fenomenološki obradili koncept poslovno-kontraobaveštajnog rada, koji suštinski predstavlja sastavni deo programa korporativne zaštite korporacije. Njegova svrsishodnost je neupitna, a on je funkcionalno i organizaciono najšešće zastupljen u velikim transnacionalnim korporacijama. Korporacija koja je nadaleko poznata po svom korporativno-kontraobaveštajnom programu, i koja predvodni američku vojno-namensku industriju je Lokhid Martin. Nakon nje slične korporativno-kontraobaveštajne programe su uvrstile i korporacije iz farmaceutske industrije poput Fajzera. Suštinski, stvara se impresija da onaj sektor korporativne sigurnosti koji ne uzima u obzir principe kontraobaveštajne zaštite, blago rečeno neadekvatno organizovan i osmišljen. Naravno, principi se moraju prilagoditi konkretnoj korporaciji u smislu njene organizacione strukture i ostalih specifičnosti. Zaključak koji se može izneti je da korporativna sigurnost kao stanje koje karakteriše odsustvo ugrožavanja korporativnih resursa umnogome zavisi od kvalitetnih proaktivnih aktivnosti koje se sprovode. Jedna od relevantnih aktivnosti koja ima zasluženo mesto u svakom zaštitnom programu korporacije je poslovno-kontraobaveštajni rad.

LITERATURA

[1] Botos, H., Radu, G., Business counterintelligence practice. U: Romanian Intelligence Studies Review. National Institute for Intelligence Studies, Bucharest, 2018, str. 165-175.
[2] Dragišić Z., Bezbednosni menadžment, Službeni glasnik, Beograd, 2007.
[3] Goldman, J., Words of Intelligence – A Dictionary.. Scarecrow Press, United States of America, 2006.
[4] Golovin, A., Fundamental Elements of the Counterintelligence Discipline, Nova Science Publishers Inc, New York, 2009.
[5] https://www.securitysee.com/2016/06/industrijska-spijunaza-kontra-mere/, pristupljeno 07.12.2022.
[6] Jolevski Z., Korporativna bezbednost u savremenoj uslužnoj ekonomiji i industriji 4.0., Zbornik radova Medjunarodne naučne i stručne konferencije: Integrisana korporativna bezbednost i digitalne transformacije: izazov za akademsku zajednicu i savremene korporacije, Asocijacija za korporativnu bezbednost, Skopje, 2018.
[7] Jusufranić I., Značaj i uloga korporativne sigurnosti u poslovanju preduzeća, Зборник на трудови од Меѓународна научна и стручна конференција: Интегрирана корпоративна безбедност и дигиталните трансфорации: предизвик за академската заедница и современие корпорации, Асоцијација за корпоративна безбедност, Скопје, 2018.

[8] Kozarev A. i dr., Ekološki kriminalitet i korporativna bezbednost u Republici Makedoniji, Zbornik radova Medjunarodne naučne i stručne konferencije : Integrisana korporativna bezbednost i digitalne transformacije: izazov za akademsku zajednicu i savremene korporacije, Asocijacija za korporativnu bezbednost, Skopje, 2018.
[9] Perry, D., „Repugnant Philosophy“ – Ethics, Espionage and Covert Action. U: Ethics of Spying – A Reader for the Intelligence Professional. United States of America: Scarecrow Press, 2006, str. 221-247.
[10] Prunckun, H.,. Counterintelligence – Theory and Practice, Roman & Littlefield Publishing Group Inc, Maryland, 2019.
[11] Stojanović M., Pavlović D., Ekonomska bezbednost poslovanja, Beograd, 2014.
[12] Trivan D., Korporativna bezbednost, Dosije studio, Beograd, 2012.
[13] Turner, H., Historical Dictionary of United States Intelligence, Scarecrow Press, United States of America:, 2006.
[14] Vujinović, S., Uloga poslovno-kontraobaveštajnog rada u sprečavanju industrijske špijunaže, Master rad, Fakultet bezbednosti, Beograd, 2021.