FBIM Transactions
DOI 10.12709/fbim.06.06.01.16

ZNAČAJ I VREDNOST POSLOVNIH INFORMACIJA I MERE ZAŠTITE U INDUSTRIJSKOJ ŠPIJUNAŽI

SIGNIFICANCE AND VALUE OF BUSINESS INFORMATION AND MEASURES OF PROTECTION IN THE INDUSTRIAL ESPIONAGE

Dragana Trnavac
Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta, Beograd, Srbija

Ljubomir Miljković
Poslovni i pravni fakultet „Union – Nikola Tesla“ Univerziteta, Beograd, Srbija

Ivica Petrović
Akademija za nacionalnu bezbednost, Beograd, Srbija

JEL Category:**D80, D82, D83, G32**

Apstrakt

Svet je prepun podataka i informacija, koje u poslovnom svetu imaju vrednost. Do informacija uvek želimo doći, ali ne možemo ih uvek imati u ključnom trenutku kada nam nužno trebaju. Od informacija može zavisiti poslovanje nekog preduzeća, iz tog razloga se informacije sve češće prodaju ili čak pokušavaju lažirati i ukrasti kako bi se sprečilo napredovanje konkurencije. Ovaj rad bavi se tematikom industrijske špijunaže koju rade obaveštajne službe u svrhu raznih interesa preduzeća iz neke države. U radu će biti objašnjeni pojmovi vezani za industrijsku špijunažu, važnost i vrednost poslovnih informacija i rasprostranjenost industrijske špijunaže. Isto tako, u radu će biti navedeni neki od motiva i razloga za postupak industrijske špijunaže, navešće se ciljevi kompanija koje plaćaju obaveštajnim službama da za njih rade, zatim strategije i metode koje koriste obaveštajne službe, tehnička podrška, legalnost postupaka i zaštita podataka. Informacije mogu biti podloga za razne aspekte poslovanja, poput lakšeg procesa odlučivanja, predviđanja, poslovnog delovanja, pružanja veće sigurnosti, olakšavanje pregovaranja. Tačnost i objektivnost procene koliko zapravo informacija vredi, zavisi od

Adresa autora zaduženog za korespodenciju:
Dragana Trnavac
draganatrnavac@gmail.com

više kriterijuma, poput vremena dobijanja informacije, ciljeva, korisnosti informacije, subjektivnom doživljaju važnosti informacije.

***Ključne reči**: industrijska špijunaža, poslovne informacije, zaštita podataka, vrednost informacije, legalnost i ilegalnost postupaka.*

Abstract

The world is full of data and information that has value in the business world. We always want to get information, but we cannot always have them at a crucial moment when we need them. The information can depend on the business of an enterprise, and therefore information is increasingly sold or even attempted to fake and steal to prevent the advance of the competition. This paper deals with the issue of industrial espionage operated by intelligence services for the purpose of various interests of a company from a country. The article will explain the concepts related to industrial espionage, the importance and value of business information and the spread of industrial espionage. Also, the paper will list some of the motives and reasons for the industrial espionage process, will indicate the goals of companies that pay intelligence services to work for them, then strategies and methods used by intelligence services, technical support, the legality of procedures and data protection. Then, the paper also provides a legal and illegal way of gathering information in order to benefit from competing companies. Information can be a basis for various aspects of business, such as easier decision-making, forecasting, business operations, providing greater security, facilitating bargaining. The accuracy and objectivity of assessing how much information really is worthy depend on several criteria, such as the time of obtaining information, goals, the usefulness of the information, the subjective perception of the importance of information.

***Keywords**: industrial spying, business information, data protection, information value, legality and illegality of procedures.*

1 UVOD

Industrijska špijunaža je korišćenje obaveštajnih službi u interesu kompanija iz vlastite države. Ciljevi i motivacija su jasni: sticanje većeg profita, bolja pozicioniranost na tržištu, pridobijanje potrošača, sticanje konkurentske prednosti itd. Međutim metode i strategije, posledice ili načini kako koristiti tehnologiju i zaštititi preduzeće od mogućih napada špijuna su manje poznati. Mnogi još smatraju da je obaveštajna služba isto što i industrijska špijunaža, tj. državna ili politička špijunaža, slični jesu sa malim razlikama.

Cilj i postojanje svakog preduzeća ogledaju se u sticanju profita i probijanju tj. prepoznatljivost na tržištu, s toga je sasvim jasno zašto industrijska špijunaža još uvek postoji. Čovek je od davnina težio istome – biti najbolji u nečemu, imati najviše, tako da se koristi svim mogućim sredstvima da bi ostvario svoj cilj i dokazao ko je najbolji. Važno je i pitanje etike industrijske špijunaže, koje je povezano s posledicama. Posledice koje čovek može prouzrokovati industrijskom špijunažom su velike. To mogu biti milionski gubici za konkurentsko preduzeće, gubitak ugleda preduzeća, isto tako i gubitak novca preduzeća ukoliko ga konkurent tuži i dokaže se krivica, preduzeće mora platiti kaznu. Prema Zakonu o zaštiti poslovne tajne Republike Srbije objavljene u Službenom glasniku broj 72/2011, novčane kazne kreću se od 20.000 do 3,000.000 dinara u zavisnosti od težine prekršaja koju nadoknađuje optuženi privredni subjekat. Gubitak novca preduzeću predstavlja i ako ulaže u špijunažu, a uloženo se ne vrati. Gubitak ugleda može značiti i gubitak saradnje i partnerstava s ostalim preduzećima, dok u obrnutom slučaju može značiti i velik napredak i nove saradnje.

Informacije imaju teško procenljivu vrednost, neki su autori pokušali postaviti formulu za izračunavanje, ali sasvim tačno izračunavanje nije moguće dobiti pošto se vrednost informacije posmatra sa različitih aspekata u zavisnosti od situacija.

Važno je razlikovati pojam obaveštajne službe od industrijske špijunaže. Obaveštajne službe rade većinom legalne radnje obaveštavanja, ali mogu se baviti i industrijskom špijunažom, koja je uglavnom kažnjiva. Mnogi autori slažu se kako je industrijska

špijunaža, kao obaveštajna delatnost, proces davanja pristupa informacijama nekome izvan preduzeća, otkrivanje poslovnih informacija, poput informacija o proizvodnji i proizvodima, poslovnih planova, informacija o klijentima i slično. Dakle, radi se o prikupljanju zaštićenih podataka nekog preduzeća. Čest je slučaj da se otkrivaju poslovne tajne tako da se zaposleni zbog dodatnih zarada ili ucena često upliću u takve postupke davanja podataka drugima, koji su kažnjivi. Moglo bi se reći da je industrijska špijunaža korišćenje usluga obaveštajnih službi u interesu preduzeća iz neke države, i pritom se koriste legalni i ilegalni postupci prikupljanja podataka, s ciljem onemogućavanja konkurentske firme da obavi svoj posao kako je planirano ili da se nabave informacije pre konkurentskog preduzeća, kako bi se preteklo, ili uklonilo s tržišta.

Isto tako, uz pojam obaveštajnih delatnosti, često se pojavljuje pojam poslovna inteligencija (engl. Business intelligence), koji je u prvobitnom konceptu označavao razne načine istraživanja, prikupljanje i analizu informacija. U modernom značenju, poslovna inteligencija označava legalnu aktivnost prikupljanja javnih podataka, koji su svima dostupni, a ti podaci mogu biti objavljeni i neobjavljeni, a sve s ciljem sticanje konkurentske prednosti. Prema Javoroviću i Bilandžiću, poslovna inteligencija (engl. Business inteligence) kao obaveštajna delatnost ima tri značaja, a to su:

- Proces prikupljanja podataka i informacija, zatim njihova obrada i analiza nakon koje postaju „znanje“
- Usmerenost na informacije iz kojih se mogu predvideti budući procesi, događaji, akcije ili kretanja
- Potporna uloga u procesu odlučivanja

Postoji mnogo poslovno inteligentnih alata koji se danas koriste, postaju sve popularniji jer olakšavaju poslovanje.(Javorović & Bilandžić, 2007, str. 201).

2 VAŽNOST I VREDNOST POSLOVNIH INFORMACIJA

Gledajući iz aspekta poslovnog sveta, sve informacije su važne, čak i one beskorisne mogu drugima biti korisne. Informacije mogu biti podloga za razne aspekte poslovanja, poput lakšeg procesa odlučivanja, predviđanja, poslovnog delovanja, pružaju veću sigurnost, olakšavaju pregovaranje itd. Zbog toga je vrlo teško tačno i objektivno proceniti koliko zapravo informacija vredi. To zavisi od više kriterijuma, poput vremena dobijanja informacije, ciljeva, korisnosti informacije, subjektivnom doživljaju važnosti informacije, i slično. Panian i Klepac (2003, str. 39-40) navode tri pristupa vrednovanja informacija, a to su:

1. Shannonov kvantitativni pristup
2. Hammingov vremenski pristup
3. Liautaudov poslovno-pragmatički pristup

2.1 Shannonov kvantitativni pristup

Claude Elwood Shannon (Panian & Klepac, 2003, str. 39-40) došao je do saznanja da se količina informacija zapravo može nazvati entropijom polja slučajnih događaja koje stvara informaciju, pa je postavio formulu za izračunavanje entropije koja glasi:

$$H(X) = -\sum_{i=1}^{n} p_i ldp_i i = 1, n$$

H(X) označava entropiju polja slučajnih događaja X, p_i označava verovatnoću i-tog događaja iz polja X, dok je ldp_i dualni logaritam vrednosti verovatnoće i-tog događaja iz polja X.

Shannon je kasnije još dorađivao svoj prethodni zaključak, tako da dok je pokušavao izvesti vrednost informacije iz njene količine polazi od pretpostavke da polje X pre i-tog događaja karakteriše vrednost prethodne entropije, to jest H(X, 1), a nakon što se dogodi i-ti događaj, polje X ima vrednost entropije H(X, 2). Razlika entropija I(X)pre i posle i-tog događaja je količina informacija koja se generira tim događajem, odnosno:

$$I(X) = H(X, 1) - H(X, 2)$$

Rangovi koje Shannon postavlja kao vezu između količine informacija i vrednosti informacija su sledeći:

Ako je $H(X, 1) > 0$ $iH(X, 2) = 0$, tada je generisana potpuna, savršena informacija

Ako je $H(X,1) > 0\ iH(X,2) > 0, tako\ da\ jeH(X,1) > H(X,2)$, tada je generisana nepotpuna informacija

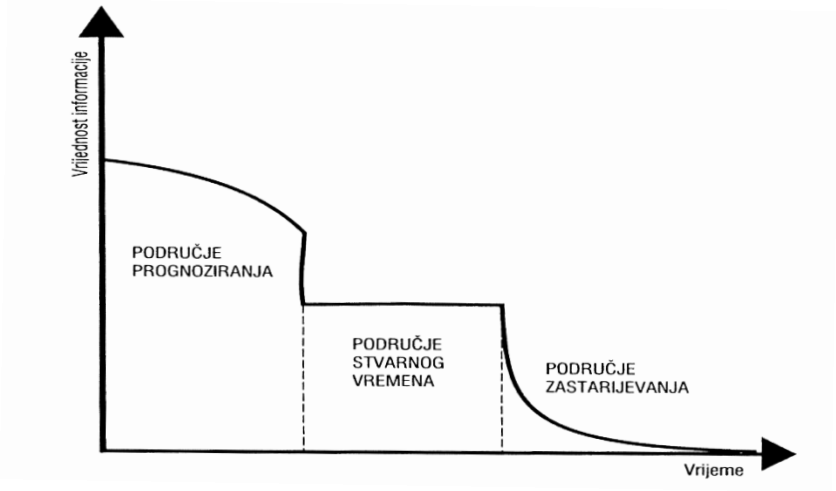
Ako je $H(X,1) = H(X,2) > 0$, tada je generisana nulta informacija

Ako je $0 < H(X,1) < H(X,2)$, tada je generisana negativna informacija, to jest dezinformacija

Shannon je delimično uspeo u povezivanju količine informacija s njihovom vrednošću, jer je postavio samo četiri ranga, ali je time dao velik doprinos razvoju naučnih otkrića u području vrednovanja informacija.

2.2 Hammingov vremenski pristup

Richard Hamming (Panian & Klepac, 2003, str. 42-43) postavio je koncept životnog ciklusa informacije, koji govori da svaka informacija ima trenutak nastajanja, vreme trajanja zatim vreme isteka nakon kojeg nestaje, to jest postaje irelevantna i nebitna. Vrednost informacije je funkcija vremena. Grafički Hamming to prikazuje kao što je prikazano na slici1.



Slika 1. Vrednost informacije u vremenu
Izvor:(Panian&Klepac, 2003, str. 42)

Na grafikonu prikazanog na slici 1 vidljivo je kako informacija ima tri karakteristična razdoblja, to jest područja – područje prognoziranja, područje stvarnog vremena i područje zastarevanja. Karakteristika područja prognoziranja je to što se informacija dobija i pre nego je nužno potrebna, na primer za donošenje odluke. U toj fazi informacija ima najveću vrednost tako da s vremenom pada nelinearno. Karakteristika područja stvarnog vremena je ta što se informacija pojavljuje upravo onda kada je zaista potrebna, i vrednost informacije ostaje konstantna sve do područja zastarevanja, za koje je karakteristično da se informacija dobija prekasno, informacija nije relevantna ili postojeća koja se prenosi iz prošlog područja takođe nije relevantna ili potrebna. U tom poslednjem području vrednost informacije naglo eksponencijalno pada.

Hammingova istraživanja dala su više rezultata i imala su jači odjek nego Shannonova, najviše u području menadžmenta, pošto savremeni menadžment zahteva informaciju u pravo vreme ili nešto ranije. Pokazalo se da treba dati dozu opreza području prognoziranja, jer se još uvek ne poznaju dobro prognostičke metode, savet je težiti tome da se informacija poseduje u području stvarnog vremena, pošto se tada omogućuje pravovremeno donošenje kvalitetnih odluka.

2.3 Liautaudov poslovno-pragmatički pristup

Bernard Liautaud (Panian&Klepac, 2003, str. 42) postavlja polazište za vrednovanje informacija na činjenicu da se vrednost neke informacije proteže u kontinuitetu. Celo preduzeće ili veći deo preduzeća koristi istu informaciju za različite odluke, ali isto tako upotreba neke informacije može se širiti i prema klijentima i partnerima. Prema tom polazištu, Liautaud zaključuje da se vrednost informacija može

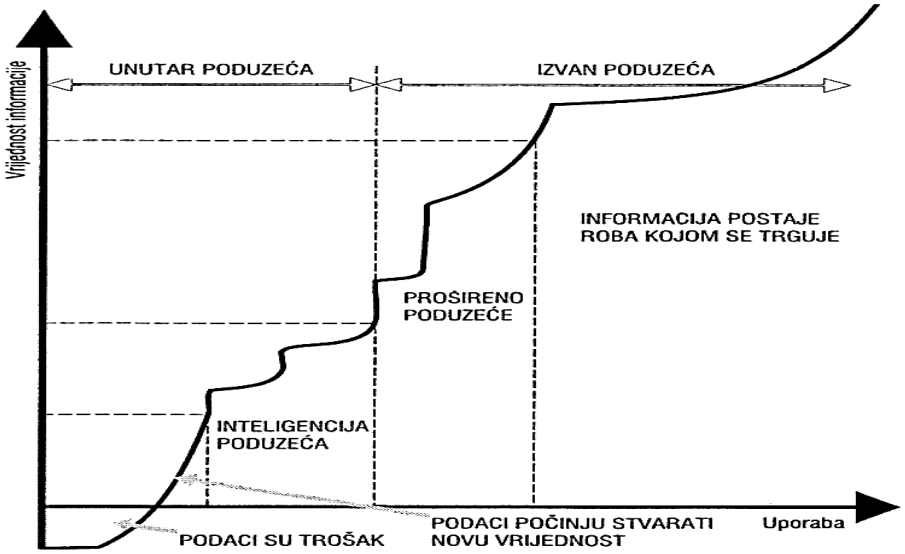
dovoljno precizno definisati, da bi bilo zadovoljavajuće, kao funkcija broja korisnika te informacije i broja poslovnih područja kojima korisnici pripadaju. Njegov zaključak može se iskazati sledećim izrazom:

$$Vrednost\ (informacija) \sim korisnici^2 \times poslovna\ područja$$

Izraz prikazuje kako vrednost posmatrane informacije raste srazmerno kvadratu broja korisnika koji mogu imati pristup informaciji pomnoženim sa brojem poslovnih područja u kojima se ti korisnici kreću, to jest rade. Liautaud je inspiraciju za kvadrirani broj korisnika uzeo iz „mrežnog rezultata“ jer smatra da je dobro da što više ljudi deli istu informaciju jer se lakše razumeju, lakše komuniciraju, bolje sarađuju i donose bolje odluke. Takođe, Liautaud tvrdi da se u kontinuitetu vrednosti određene informacije može uočiti pet zona:

- Zona u kojoj podaci predstavljaju trošak
- Zona u kojoj podaci počinju stvarati novu vrednost
- Zona inteligencije preduzeća
- Zona proširenog preduzeća
- Zona u kojoj informacija postaje roba kojom se trguje

Slika 2. prikazuje grafički kontinuitet vrednosti informacija, s označenim zonama.



Slika 2. Kontinuitet vrednosti informacije

Izvor:(Panian, Klepac, 2003, str. 45)

Zona u kojoj podaci predstavljaju trošak odnosi se na podatke koji su samo sačuvani na računaru, s njima se ništa ne radi, zauzimaju memorijsko mesto na računaru, a neko se mora i brinuti o tome da podaci ne nestanu ili ih treba održavati. Za rešavanje takvih situacija, potrebno je čuvati samo informacije koje će se moći ponovo koristiti u nekim analizama, ili za koje se zna da su potrebne u budućnosti.

Zona u kojoj podaci počinju stvarati novu vrednost je upravo korišćenje informacija koje preduzeće poseduje. Najlakše je preduzeće umrežiti i omogućiti onima koji trebaju koristiti informacije lak i jednostavan pristup svim važnim informacijama. Isto tako,kod novih informacija potrebno je olakšati razmenu sa svima koji ih trebaju znati.

Zona inteligencije preduzeća odnosi se na razmenu informacija unutar preduzeća, tako da svi korisnici informacija tu informaciju mogu razmotriti iz drugačijeg aspekta, vezanog uz svoju funkciju, i time postići sinergiju funkcija i bolje poslovanje.

Zona proširenog područja dozvoljava kontrolisano širenje informacija izvan preduzeća, na primer s poslovnim partnerom ili klijentom, čime se postiže rast poslovne inteligencije preduzeća.

Zona u kojoj je informacija roba kojom se trguje nadilazi prethodnu zonu, jer se u prethodnoj zoni radi isključivo o poslovnim saradnicima, dok se u ovoj zoni misli na prodaju, to jest deljenje informacija koje su u određenom preduzeću već sazrele s konkurentima.

3 LEGALNOST POSTUPAKA U INDUSTRIJSKOJ ŠPIJUNAŽI

Većina postupaka u industrijskoj špijunaži smatra se ilegalnim, ali ipak postoje neki legalni načini dobijanja informacija.

Jedna od legalnih metoda industrijske špijunaže je metoda „kopanja po đubretu“ (engl. *dumpster diving)*. Njena legalnost se ogleda u tome da preduzeća smeće izbacuju u kontejnere i kante na ulici, gde se smeće ostavlja kako bi ga odvezle i zbrinule firme koje se bave odvozom i zbrinjavanjem otpada, a kada se smeće ostavi na ulici, više se ne smatra privatnim vlasništvom (osim ako postoji znak poput zabranjenog pristupa ili ako je kontejner zaključan). (Robinson, 2003, str. 6)

Još jedna legalna metoda pribavljanja podataka je kupovina preduzeća ili proizvoda čije podatke želimo dobiti. Takođe, legalan način je i prisiljavanje preduzeća na to da se odreknu svojih tehnologija proizvodnje... Zapravo, to bi se moglo nazvati i ucenom. Kako je legalan način kupovine preduzeća, tako je legalno i partnerstvo s konkurentnim preduzećem, iako je sklopljeno i u svrhu dobijanja potrebnih informacija, ali to konkurent ne zna. Informacije otvorenog koda (engl. Open Source Information OSI) pruža velik izvor informacija, jer sadrži razne novinske članke, godišnje izveštaje preduzeća, prijave patenata, razne sudske papire i marketinške informacije. Još jedna legalna metoda prikupljanja informacija je zapošljavanje bivšeg radnika konkurentskog preduzeća, koji tada više nije obavezan da čuva poslovnu tajnu, ukoliko to nije drugačije regulisano njihovim prethodnim ugovorom, ili čak rado i deli informacije zbog nezadovoljstva starim preduzećem, iako je češći slučaj da takve osobe iz poštovanja ne žele otkriti informacije, ali u novo preduzeće donose svoje znanje i veštine, koje su verovatno stekli na starom radnom mestu. Još jedan od vrlo popularnih načina prikupljanja informacija je posećivanje sajmova preduzeća na kojima neko glumi zainteresovanu osobu za to preduzeće, kupca, istraživača ili slično. Te osobe su većinom vrlo dobro uvežbane da znaju tačno šta treba reći, i u kom trenutku, da bi izvukle informacije. Ako se radi o špijuniranju stranog preduzeća, često se kontaktiraju domaćini iz te zemlje koji rade u stranom konkurentskom preduzeću. Zbog privrženosti domovini, vrlo često i otkriju više nego što bi smeli. (Winkler, 2014, str. 2)

3.1 Ilegalni postupci

Ilegalnih postupaka je mnogo više nego legalnih, a i neki legalni su blizu granice do ilegalnih. Metoda *insajdera (doušnika)* zakonom je kažnjiva, to jest krađa informacija i odavanje nekome u zamenu za novac ili neku drugu uslugu. U velikim preduzećima najčešće se ljudi zapošljavaju dugoročno, što pridonosi pojavi *insajdera*, a i veličina preduzeća može im olakšati da što manje upadljivo kradu podatke, ako znaju kako se prikrivati. Provale u zgradu preduzeća su kažnjivi postupci, makar se radilo i o prolasku kroz otključana vrata zgrade pa tek potom pretraživanja ormara, fioka i krađi nekih dokumenata. Isto važi i za upadanje u računarski sistem. Metodu kopanja po đubretu *(engl. Dumpster diving)* ovaj autor navodi kao ilegalnu, ali to zavisi je li smeće izvan zgrade i ima li znaka privatnog poseda ukoliko je izvan, i kako je formulisan zakon u određenoj državi. Prisluškivanje, hakovanje i kriptoanaliza su takođe ilegalne metode špijuniranja.(Winkler, 2014, str. 3-4)

Zakon je drugačiji u svakoj državi, ali uglavnom su saglasni oko legalnosti špijunaže, zbog etičkih pitanja. Kaznena dela su primera radi hakovanje, kriptoanaliza, pristupanje računarima i sistemima za koje se nema ovlašćenje, onemogućavanje rada sistema, krivotvorenje podataka ili brisanje podataka, neovlašćeno presretanje računarskih podataka i tako dalje. Takođe, mogu se kažnjavati dela neovlašćenog zvučnog ili slikovnog snimanja, neovlašćeno otkrivanje poslovne tajne, krađa imovine (u ovom slučaju dokumenata s vrednim informacijama), prevare, primanje i davanje mita (primer kod *insajdera*), zloupotreba ovlašćenih informacija ili odavanje i neovlašćeno pribavljanje poslovne tajne.

4 ZAŠTITA PODATAKA

Preduzećima bi trebalo biti u interesu da podatke za koje znaju da su na meti konkurentima nekako zaštite. Zbog toga je dobro da se znaju slabosti metoda i tehničke podrške špijunaži. Od prisluškivanje telefonskih linija pomoću satelita se preduzeće može zaštititi tako da se telefonski aparati nalaze u prostoriji koja je Faradejev kavez, pri čemu je važno da su električni kablovi i spojevi kroz koje prolaze signali zakopani što dublje pod zemljom. Ovakva zaštita jedino ne pomaže ako špijuni imaju dogovor s telefonskim kompanijama da im ustupe sve što je potrebno. Što se tiče mobilne mreže, jedina zaštita je rastaviti mobilni telefon, izvaditi mu bateriju ili ga obložiti aluminijskom folijom. Vezano za zaštitu kompjutera, dobro je paziti kako su kancelarije uređene, može li neko gledati preko ramena osobi i tako dobiti lozinke, i takođe, nikakva zaštita ne vredi ako špijuni imaju dogovore s proizvođačima operacijskih sistema, jer tada špijuni mogu lako, samo sa spajanjem na Internet, preuzeti sve podatke koji im trebaju. Pomoću posebnog programa mogu i zaobići sve šifre koje i trebaju za pristup računarima. (Čuljak)

Poznati i jaki računarski virusi imali su i svrhu pouke – podigli su računarsku savest. Mnoge organizacije dobile su uvid u to kako što bolje zaštititi svoje informacijske sisteme. Primetilo se da je glavni razlog nezaštićenosti bio nedostatak osnovnih sigurnosnih principa. Veliki nedostatak našao se i u javnoj objavi programskog koda, jer je velika mogućnost da će se iskoristiti u takve kriminalne svrhe špijunaže i sabotaže.(Nacionalni CERT, 2012, str. 17)

Winkler(2014) navodi kako se svako preduzeće može zaštititi na četiri načina, i time čak učiniti prevenciju špijunaži, a to su:

- Tehnička zaštita
- Operativna sigurnost
- Fizička zaštita
- Zaštita osoblja

Za postizanje tehničke sigurnosti važno je imati razne protivmere. Zaštita tehničkih alata u preduzeću stvara poverljivost, integritet i dostupnost računarskih sistema i mreža. Uz malo truda može se postići zaštićenost komunikacijskih kanala, a time i informacija. Operativna sigurnost odnosi se na procese preduzeća, koji bi mogli ugroziti informacije u netehničkom smislu. Na primer, preduzeće može postaviti pravila o znanju informacija, odrediti ko sme koliko znati, ili pak se mogu ograničiti korišćenja komunikacijskih kanala. Takođe, operativna sigurnost uključuje i politiku sigurnosti vezanu za dobavljače ili spoljne saradnike, koji se dodatno proveravaju. Važno je i iskomunicirati sa svim zaposlenima o važnosti informacija i posledicama ako nekome nešto otkriju, objasniti kako se što bolje zaštiti i raditi na tome da zaštita informacija postane deo kulture preduzeća. Pošto se veliki broj krađa informacija događa i zbog fizičkih upada stranih osoba u preduzeće, treba raditi i na fizičkoj sigurnosti preduzeća. Prvenstveno treba postaviti dobar sistem kontrole ulaska u zgradu preduzeća i npr. neke od bitnih proizvodnih pogona i slično, ali treba i zaposlenima onemogućiti pristup nekim podacima. Savet je i da zaposleni nose oznake s imenom i pozicijom u preduzeću na majicama, košuljama ili radnoj odeći, a isto tako i spoljni saradnici, posetioci trebaju dobiti oznaku prilikom ulaska u zgradu. Te oznake imaju smisla kada zaposleni ponekad i pogledaju na tuđe oznake, pa vide nose li ispravnu, to jest svoju. Često se na takve oznake stavlja i slika osobe kako bi je bilo lakše povezati s imenom. Još jedan način fizičke zaštite je kontrola smeća, to jest trebalo bi važne dokumente ili spaliti ili uništiti na neki drugi način. Za vreme pauza, pametno je računar zaključati lozinkom, i paziti da se te lozinke ne nalaze na nekom papiriću u blizini računara. Korisno je takve lozinke s vremena na vreme i promeniti. Sve papire koji na sebi imaju poverljive informacije trebalo bi držati u zaključanim fiokama ili ormarima i negde dobro sakriti ključ od brave. Zaštita osoblja odnosi se na proveravanje ko od zaposlenih ima pristup kojim informacijama te postavljanje pravila kojim informacijama i na koji način bi smeo pristupiti. Mnoga preduzeća nisu svesna da podatke mogu krasti domari, čuvari ili čistačice. Administrativno osoblje moralo bi sarađivati sa službom za ljudske resurse kako bi saznali kada neko od zaposlenih dobije otkaz, da se njegov korisnički račun za korišćenje računara odmah obriše.(Winkler, 2014, str. 5-6)

4.1 Povezanost upravljanja znanjem sa industrijskom špijunažom

Upravljanje znanjem (engl. *knowledge management)* je sastavni deo svakog preduzeća. Kako navode Lee i Rosenbaum, upravljanje znanjem sadrži ključne informacije, ključne igrače, odnose, strateške ciljeve, operativne principe i mehanizme, itd, tako da misle kako je upravljanje znanjem zapravo alat kojim preduzeće špijunira samo sebe, u pozitivnom smislu. Može se videti ko je povezan i aktivan, koje su vrednosti preduzeća, ko doprinosi, ko sarađuje, ko ima informacije i slično, a to su sve vredna saznanja za preduzeća, ali i za njenog neprijatelja. Upravljanje znanjem preduzeće čini povezanijom, življom i efektivnijom. Obzirom da sadrže i podatke o klijentima, planove preduzeća, poslovne tajne, cenovnike i slično, često se takve platforme nalaze na metama špijuna i hakera. Lee i Rosenbaum takođe govore kako su upravljanje znanjem (*knowledge management)* delovi i neupravljanje znanjem (engl. *anti knowledge management)* delovi celine. To objašnjavaju time što se vide praznine i greške u znanju i razumevanju onih koji ih koriste, a to svakako dodatno koristi špijunima, pogotovo ako imaju informacije i znanja koji mogu nadomestiti te praznine. (Lee & Rosenbaum, 2003)

Colibasanu spominje pojam sposobnost analiziranja konkurentnosti preduzeća na tržištu, u daljem tekstu „*competitive intelligence“*, alat za proces donošenja odluka koji pomaže dajući odgovore na ključna pitanja. Taj alat je najviše vezan uz strateški menadžment, jer je usredsređen na postavljanje i rešavanje hipoteze, podržavajući održivi razvoj preduzeća u promenjivom i nestabilnom okruženju. *Competitive intelligence* je logičan proces testiranja, provera ispravnosti pretpostavke ili hipoteze, kao i rešavanja ključnih poslovnih problema. Proces se sastoji od ključnih koraka, a to su identifikovanje potreba za informacijama i znanjem u preduzeću, prikupljanje informacija, analiziranje zatim sinteza prikupljenih podataka, i na kraju objava rezultata. Ovaj alat pomaže preduzeću i time što prati šta se događa sa konkurentskim preduzećima, šta rade i kakva im je pozicija na tržištu, i prati promene poslovnog okruženja. Autorka špijunažu povezuje s pojmom *competitive intelligence* u jednoj zajedničkoj stvari, a to je sticanje i zadržavanje ili održavanje konkurentske prednosti. Razlika koju navodi je da *competitive intelligence* alat stvara stabilno okruženje za donošenje poslovnih odluka, dok se špijunažom samo postiže to da se pribave informacije, ali ne da se i od njih napravi znanje potrebno preduzeću. Isto tako, te informacije mogu biti korisne vrlo kratko, ukoliko ih špijunska strana ne obradi brzo i ne iskoristi pre onih kojima su ih uzeli. Može postojati mogućnost da i špijuni koriste *competitive intelligence* sisteme. Još jedna velika razlika koju navodi autorka je ta da je korišćenje *competitive intelligence* sistema etički ispravno, dok je špijunaža neetično ponašanje, i zakonski kažnjivo. (Colibasanu)

Korišćenje analize konkurentnosti preduzeća (eng *competitive intelligence)* sistema, poslovne inteligencije (engl. *business inteligence)* sistema ili upravljanje znanjem (engl. *knowledge managemen*t) sistema preduzeće dovodi na metu špijunima, tako da se preduzeća moraju na neki način zaštititi od mogućih napada. Alstete je u New Yorku 2002. godine proveo istraživanje u kojem je ispitao svest i percepciju zaposlenih o krađi i zaštiti informacija. Sproveo je to na način da ih je ispitivao o sigurnosti imovine znanja, to jest informacija, ne samo u okolnostima promena nakon napada 11.09.2001., nego u opštem smislu povećanja sigurnosti u preduzećima u kojima rade. Ispitanici su zaposlenici u srednjim i velikim preduzećima. Rezultat koji je dobijen ispitivanjem raspoređuje se u četiri kategorije percepcije zaposlenih:

1. zaposleni su svesni vrednosti upravljanja znanjem,
2. zaposleni nisu svesni vrednosti upravljanja znanjem,
3. nema povećanja sigurnosti,
4. sigurnost je povećana.

Ova studija je pokazala kako su mnogi menadžeri uvereni da njihova preduzeća imaju barem osnovno shvatanje o vrednosti upravljanja znanjem i da imaju neke mere zaštite, ali nedovoljno se bave planiranjem većih mera zaštite. Kako bi se što efektivnije zaštitile, preduzeća moraju biti svesna vrednosti svojih informacija i znanja, tek tada mogu planirati šta treba štititi i do koje mere sigurnosti treba postaviti zaštitu.(Alstete, 2003)

5 ZAKLJUČAK

Što se tiče metoda, zaključak je da su metode nastajale u skladu s vremenom i tehnologijama, mnogo se metoda promenilo i nestalo, nove nastaju, i kako tehnologija bude napredovala, čovek će uvek naći način da se prilagodi i iskoristi tehnologiju što je moguće više i bolje. Neke metode će verovatno teže zastareti, kao npr. metoda *insajdera*, koja je najčešće korišćena u današnje vreme, barem po onome što se u javnosti govori i piše. Dok traje finansijska kriza u svetu, ljudi će štošta učiniti ne bi li dobili novac, ali nisu svesni da oni daju pristup informacijama za malu svotu novca s obzirom koliku vrednost ta informacija predstavlja onome kojima je potrebna. Takođe, digitalne tehnologije učinile su to da ljudi lakše dođu do informacija, a da ne ostave trag jer digitalne dokumente samo trebaju iskopirati, ne moraju ih fizički ukrasti.

Brojni primeri postoje za industrijsku špijunažu, to je već svakodnevnica, i smatramo da industrijska špijunaža neće nestati, nego će se samo još više razvijati, pogotovo dok je društvo kapitalistički usmereno. Dok god traje borba za tržištem i novcem, ljudi će tražiti sve načine ne bi li došli do onog što najviše žele – informacije.

CITIRANI RADOVI

Alstete, J. (2003). *Trends In Corporate Knowledge Asset Protection.* Preuzeto 09 01, 2013 sa http://www.tlainc.com/articl47.htm

Colibasanu, A. O. (2003.). *Between Intelligence and Espionage in the Contemporary Business Environment.* Preuzeto 09 01, 2014 sa http://www.ekonomikaamanagement.cz/getFile.php?fileKey=CEJVB0NUCAdVCEZIU1VHB0MIUUMEBAVDVFVWQ1VUBAVGQ1VCXgQFBERIRENCZA==

Čuljak, T. (n.d.). *Obavještajno sigurnosne službe.* Preuzeto 04 15, 2014 sa http://bs.scribd.com/doc/147948442/obavje%C5%A1tajno-sigurnosne-slu%C5%BEbe

Javorović, B., & Bilandžić, M. (2007). *Poslovne informacije i business intelligence.* Zagreb: Golden marketing – Tehnička knjiga.

Lee , J., & Rosenbaum, A. (2003). *Knowledge management: Portal for corporate espionage? Part 1.* Preuzeto 09 01, 2014 sa 2003: http://www.kmworld.com/Articles/Editorial/Features/Knowledge-management-Portal-for-corporate-espionage-Part-1--9508.aspx

Nacionalni CERT. (2012). *Zlonamjerni programi u službi država, dostupno na linku.* Preuzeto 074 05, 2014 sa http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2012-10-338.pdf

Panian, Ž., & Klepac, G. (2003). *Poslovna inteligencija.* Zagreb: MASMEDIA.

Robinson, W. S. (2003). *(2003), Corporate Espionage 101, SANS Institute, .* Preuzeto 02. 07 2014 iz http://faculty.usfsp.edu/gkearns/Articles_Fraud/corporate%20espionage.pdf

Winkler, I. (2014). *Case study of industrial espionage through social engineering, National Computer Security Association.* Preuzeto 06. 07 2014 iz http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.115&rep=rep1&type=pdf

Datum prve prijave: 08.02.2018.
Datum prijema korigovanog članka: 09.03.2018.
Datum prihvatanja članka: 15.03.2018.

Kako citiratiovaj rad? / How to citethisarticle?

*Style – **APA** SixthEdition:*

Trnavac, D., Miljković, L., & Petrović, I. (2018, Apr 15). Značaj i vrednost poslovnih informacija i mere zaštite u industrijskoj špijunaži. (Z. Čekerevac, Ed.) *FBIM Transactions, 6*(1), 160-169. doi:10.12709/fbim.06.06.01.16

*Style – **Chicago**SixteenthEdition:*

Trnavac, Dragana, Ljubomir Miljković, and Ivica Petrović. 2018. "Značaj i vrednost poslovnih informacija i mere zaštite u industrijskoj špijunaži." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 6 (1): 160-169. doi:10.12709/fbim.06.06.01.16.

*Style – **GOST** Name Sort:*

Trnavac Dragana, Miljković Ljubomir and Petrović Ivica Značaj i vrednost poslovnih informacija i mere zaštite u industrijskoj špijunaži [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Toronto - Beograd : MESTE, Apr 15, 2018. - 1 : Vol. 6. - pp. 160-169.

*Style – **Harvard**Anglia:*

Trnavac, D., Miljković, L. & Petrović, I., 2018. Značaj i vrednost poslovnih informacija i mere zaštite u industrijskoj špijunaži. *FBIM Transactions,* 15 Apr, 6(1), pp. 160-169.

Style – **ISO 690**Numerical Reference:

Značaj i vrednost poslovnih informacija i mere zaštite u industrijskoj špijunaži. **Trnavac, Dragana, Miljković, Ljubomir and Petrović, Ivica.** [ed.] Zoran Čekerevac. 1, Toronto - Beograd : MESTE, Apr 15, 2018, FBIM Transactions, Vol. 6, pp. 160-169.