Poslovno-obavještajna djelatnost

Markanović, Toni

Master's thesis / Specijalistički diplomski stručni

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:929391

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Toni Markanović

POSLOVNO-OBAVJEŠTAJNA DJELATNOST

ZAVRŠNI RAD

Karlovac, 2018.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Toni Markanović

Business Intelligence

Final paper

Karlovac, 2018.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Toni Markanović

POSLOVNO OBAVJEŠTAJNA DJELATNOST

ZAVRŠNI RAD

Mentor:

Davor Kalem, struč. spec. crim.

Karlovac, 2018.

VELEUČILIŠTE U KARLOVCU
KARLOVAC UNIVERSITY OF APPLIED SCIENCES
Trg J.J.Strossmayera 9
HR-47000, Karlovac, Croatia
Tel. +385 - (0)47 - 843 - 510
Fax. +385 - (0)47 - 843 – 579

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Stručni / specijalistički studij: Specijalistički studij

Usmjerenje: Sigurnost i zaštita

Karlovac, 18.10.18

ZADATAK ZAVRŠNOG RADA

Student: Toni Markanović

Matični broj: 0420415040

Naslov: Poslovno-obavještajna djelatnost

.....

Opis zadatka:

1. Opisati razvoj i ulogu poslovno obavještajne djelatnosti
2. Pojasniti pojam poslovno obavještajne djelatnosti
3. Navesti zakonski temelj za provođenje poslovno obavještajne djelatnosti
4. Pojasniti faze i modele u poslovno obavještajnoj djelatnosti
5. Analiza podataka
6. Poslovno obavještajna djelatnost i informacijska sigurnost
7. Poslovno obavještajna djelatnost u Republici Hrvatskoj i rezultati istraživanja

Zadatak zadan:	Rok predaje rada:	Predviđeni datum obrane:
26 . 6. 2018.	9. 10. 2018.	18. 10. 2018.

Mentor:
Davor Kalem, struč. spec. crim.

Predsjednik ispitnog povjerenstva:
dr. sc. Nikola Trbojević, prof. V. škole

PREDGOVOR

U stvaranju završnog rada, svojim znanjem i iskustvom, uvelike mi je pomogao mentor Davor Kalem, struč. spec. crim, kojem iskreno zahvaljujem na uloženom trudu, prenesenom znanju i iskustvu.

Također se želim zahvaliti kolegama studentima i profesorima specijalističkog studija sigurnosti i zaštite, koji su mi svojim znanjem, podrškom i stručnošću olakšali studij te pružili motivaciju za daljnje usavršavanje i napredovanje.

Posebno se zahvaljujem obitelji na strpljenju, povjerenju i potpori pruženoj tijekom školovanja na Veleučilištu u Karlovcu.

SAŽETAK

U ovom završnom radu definirat će se što je poslovno-obavještajna djelatnost, njezinu podjelu, analize, metode kojima se koristi te razvoj poslovno-obavještajne djelatnosti u Republici Hrvatskoj.

Također će biti opisano koliko je razvijena poslovno-obavještajna djelatnost u Republici Hrvatskoj.

Ključne riječi: poslovno-obavještajna djelatnost, protuobavještajno djelovanje, informacijska sigurnost

ABSTRACT

In this final paper, it will be defined what business intelligence is, its distribution, analyses, and methodes that it uses and it will be described the development of business intelligence in the Republic of Croatia.

It will also be described how much the business intelligence activity has been developed in the Republic of Croatia

Key words: business intelligence, business counterintelligence, information security

SADRŽAJ:

1. UVOD

1.1. Definiranje predmeta istraživanja

U uvjetima otvorenog i integriranog svjetskog gospodarstva, pod utjecajem globalizacijskih procesa, pravodobne, kvalitetne i točne poslovne informacije predstavljaju temelj uspješnih i kvalitetnih poslovnih odluka i kreiranog poslovnog znanja koje su donositelju navedenih odluka oduvijek bile konkurentska prednost. U uvjetima krize, kojih smo svjedoci u današnje vrijeme, poslovno-obavještajno djelovanje predstavlja skup instrumenata i metoda koji su od presudne važnosti u sprječavanju donošenja loših poslovnih odluka koje u uvjetima krize zasigurno imaju teže posljedice, nego u normalnim poslovnim uvjetima. Strateški plan poduzeća izražava filozofiju i strategiju poslovnog subjekta te sadrži ciljeve poslovnog sustava, mehanizme i načine ostvarenja zacrtanih ciljeva. Iako podložan izmjenama, kvalitetno formiranje strateškog plana poduzeća i njegova implementacija su od presudne važnosti za uspješno poslovanje, rast i razvoj poduzeća. Upravo primjenom poslovno-obavještajnih metoda i analitičkih okvira poput analiza scenarija[1] i sustava ranog upozorenja[2], tvrtkama se omogućuje anticipiranje, detektiranje i sprječavanje negativnih poslovnih iznenađenja putem formulacije i implementacije prilagodljivih i na intelligenceu utemeljenih poslovnih strategija.

[1] Analiza scenarija je sredstvo predviđanja i upravljanja promjenama u općem i konkurentskom okruženju. Ono predstavlja most između razmišljanja o budućnosti i strategijske akcije.

[2] Zadatak sustava ranog upozorenja je prikazati moguće promjene u što ranijem stadiju kako bi uprava imala dovoljno prostora za manevar i što veći izbor mjera za savladavanje krizne situacije

1.2. Ciljevi rada

Glavni cilj ovog specijalističkog diplomskog rada je primjena metoda poslovno-obavještajnog djelovanja prilikom donošenja strateških poslovnih odluka i implementacije poslovne strategije.

Osnovni ciljevi istraživanja u okviru ovog specijalističkog diplomskog rada su:

- analizirati karakteristike i ciklus poslovno-obavještajnog djelovanja;
- razraditi koncept strategije i njegov značaj za ostvarivanje poslovne uspješnosti;
- analizirati upotrebu poslovno-obavještajnog djelovanja za donošenje strateških odluka;
- analizirati upotrebu i ulogu poslovno-obavještajnog djelovanja u hrvatskim poduzećima;
- provesti komparativnu analizu poslovnog-obavještavanja u Hrvatskoj naspram nekih zemalja Europe.

1.3. Metode istraživanja

Tema je obrađena teorijskim i empirijskim istraživanjima. U okviru istraživanja koristit će se brojne metode: metoda analize, metoda sinteze, metoda indukcije i dedukcije te metoda komparacije. Planirana istraživanja su provediva s obzirom na postojeću literaturu, znanstvene radove i rezultate istraživanja koja su se provodila od strane renomiranih organizacija i stručnjaka u Hrvatskoj i svijetu.

Empirijsko istraživanje je provedeno koristeći rezultate istraživanja iz 2011. na temu Business intelligencea u tvrtkama, koje posluju na teritoriju Republike Hrvatske. Navedeno istraživanje provedeno je u suradnji Odsjeka za sociologiju Filozofskog fakulteta Sveučilišta u Zagrebu i poslovnim tjednikom *Lider*. Istraživanje je podijeljeno u četiri skupine: opći podatci o veličini i položaju

poduzeća, primjene business intelligence aktivnosti u tvrtkama, primjene business intelligence aktivnosti u tvrtkama s obzirom na djelatnost tvrtke te primjene business intelligence aktivnosti u tvrtkama s obzirom na kretanje tržišnog udjela tvrtke.

1.4. Sadržaj rada

U uvodnom dijelu rada definirat će se predmet istraživanja te će se postaviti ciljevi rada. Također će se precizirati metode istraživanja, kao i koncept i sadržaj rada. U drugom dijelu rada pristupat će se predstavljanju poslovno-obavještajne djelatnosti. Pojam će biti definiran i razgraničen u odnosu na određene druge pojmove koji se koriste u praksi prilikom opisivanja sličnih aktivnosti. Nadalje, predstavit će se poslovno-obavještajni i protuobavještajni ciklus te upravljanje poslovnim informacijama. U trećem dijelu rada će se definirati i analizirati pojam strategija, i procesi strateškog planiranja i strateškog menadžmenta. Četvrti dio rada namijenjen je predstavljanju strateškog poslovno-obavještajnog djelovanja i njegovih principa. Također će se predstaviti uloga strateškog poslovno-obavještajnog djelovanja prilikom donošenja određenih strateških odluka. U petom dijelu će se predstaviti rezultati istraživanja provedenog za potrebe ovoga rada te temeljem njih izvršiti usporedba sa sličnim istraživanjima u svijetu. Završni dio rada rezerviran je za zaključna razmatranja i sažimanje spoznaja i rezultata istraživanja.

2. ZAKONSKI UVJETI ZA POSLOVNO-OBAVJEŠTAJNU DJELATNOST U REPUBLICI HRVATSKOJ

Poslovno-obavještajna djelatnost u Republici Hrvatskoj regulirana je nizom odredaba koje su propisane kako bi se djelatnost obavljala legalno, etički i bez povrede prava pojedinca. Neki od tih propisa jesu:

- UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), a stupa na snagu 25. svibnja 2018;
- PROVEDBENA UREDBA KOMISIJE (EU) br. 680/2014 od 16. travnja 2014. o utvrđivanju provedbenih tehničkih standarda o nadzornom izvješćivanju institucija u skladu s Uredbom (EU) br. 575/2013 Europskog parlamenta i Vijeća;
- Zakon o tajnosti podataka;
- Zakon o informacijskoj sigurnosti.

Zaštita pojedinca s obzirom na zaštitu osobnih podataka temeljno je pravo svake osobe te svatko ima pravo na zaštitu osobnih podataka. Obrada osobnih podataka osmišljena je tako da bude u službi čovječanstva. Iako je pravo za zaštitu podataka temeljno pravo svake osobe, ono nije apsolutno i stoga ga se mora razmatrati u vezi s njegovom funkcijom u društvu koje se ujednačava s drugim pravima prema načelu proporcionalnosti. Glavni temelji koji ne smiju biti ugroženi i moraju biti poštovani jesu privatni i obiteljski život, sloboda mišljenja i pravo na kulturnu, vjersku i jezičnu raznolikost. [14]

„Podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i

cjelovitosti za svoga vlasnik.“[3] Takvi dokumenti od strane nadležnog tijela mogu biti klasificirani[4] ili deklasificirani[5] te se utvrđuje stupanj tajnosti.

Postoje 4 stupnja tajnosti klasificiranih podataka:

a) vrlo tajno - klasificiraju se podaci čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske, a osobito sljedećim vrijednostima kao što su neovisnost RH, obrambena sposobnost i sigurnosno obavještajni sustav, sigurnost građana, itd.
b) tajno - klasificiraju se podaci čije bi neovlašteno otkrivanje teško naštetilo gore navedenim vrijednostima
c) povjerljivo - klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo gore navedenim vrijednostima
d) ograničeno - klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova

Pristup klasificiranim podacima imaju osobe kojima je to nužno za obavljanje poslova iz njihovog djelokruga te koje imaju izdan certifikat[6]. Način i provedba zaštite klasificiranih i neklasificiranih podataka propisat će se zakonom koji regulira područje informacijske sigurnosti. [11]

Pod informacijskom sigurnosti smatra se stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koji su propisani mjerama i standardima. Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti jesu:

[3] Zakon o tajnosti podataka, članak 2., NN 86/12
[4] Klasifikacija podatka je postupak utvrđivanja jednog od stupnjeva tajnosti podatka s obzirom na stupanj ugroze
[5] Deklasifikacija podatka je postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran
[6] Certifikat je Uvjerenje o obavljenoj sigurnosnoj provjeri koji izdaje Ured Vijeća za nacionalnu sigurnost

a) sigurnosna provjera – utvrđuju se mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima
b) fizička sigurnost – utvrđuju se mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci
c) sigurnost podatka – utvrđuju se mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka
d) sigurnost informacijskog sustava - utvrđuju se mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava
e) sigurnost poslovne suradnje – primjenjuju se propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe

Poslovi nadzora informacijske sigurnosti su poslovi nadzora organizacije, provedbe i učinkovitosti propisanih mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama. [12]

Zlouporaba podataka u bilo koje svrhe je kažnjiva te je podložna kaznenoj odgovornosti i sankcijama. Kako svaka pravna ili fizička osoba ima pravo na učinkoviti pravni lijek protiv pravno obvezujuće odluke nekog nadzornog tijela koja se na nju odnosi propisano Općom uredbom o zaštiti podataka, ima pravo na pritužbu i pravo na naknadu štete i odgovornosti. [14]

3. POSLOVNO-OBAVJEŠTAJNA DJELATNOST

Izvještajnom, odnosno obavještajnom djelatnošću su se ljudi zasigurno bavili od najranijih početaka organiziranja svojeg života, kao i života čitavog društva. Obavještajna djelatnost je tijekom svog povijesnog razvoja, posebice od razvitka gospodarstva, postala jednim od vitalnih područja ljudskog života i djelovanja. Ta vrsta obavještajne djelatnosti nije business intelligence u njegovom modernom značenju, zbog uključivanja drugih čimbenika poput špijunaže u business intelligence, no zasigurno predstavlja okvir iz kojeg sam pojam nastaje.

Poslovno-obavještajna djelatnost ima zadaću zaštiti se od mogućih subverzivnih postupaka strane države na čijem se teritoriju nalazi poslovni subjekt. U tom smislu poslovna obavještajna služba, u ime poslovne izvrsnosti, nije trošak, nego investicija.

Može se slobodno reći da je prvi teoretičar, na ovom planu, bio kineski filozof i ratnik Sun Tzu[7], koji je u svome djelu *„Umijeće ratovanja“* objasnio da je, zapravo, ono što suvremenim i dobrim generalima omogućuje da izvrše napad i osvajanje te postignu ciljeve jest prijašnje saznanje. Posebno je podvukao potrebu za „obavještajnom službom koja bi se bavila neprijateljem“. Spomenuto djelo se smatra Biblijom obavještajne službe.

Četiri stoljeća prije nove ere Filip II. Makedonski temeljito je organizirao obavještajnu službu. Njegov sin Aleksandar III. Veliki, zvani Makedonski, nastavio je sa osvajanjima te je zahvaljujući obavještajnoj službi uspio gospodarski povezati područje od Gibraltara do Inda. U kratkim predasima između bitaka, nadahnjivao se Filipovim pismima u kojima je zabilježena nužnost pridavanja pozornosti obavještenjima o protivnicima. Na jednom mjestu njegov otac je zapisao: „Zlatom natovareni magarac, u stanju je osvojiti i najveću tvrđavu“. Ni otac, a ni sin nisu bili svjesni da će taj postulat vrijediti i na

[7] Sun Tzu, kineski general i vojni strateg, napisao knjigu „Umijeće ratovanja“ koja se smatra Biblijom obavještajne službe koja je nastala prije 2500. godina

početku 21. stoljeća, kada će ga, posebice, koristiti oni koji potkupljuju novcem kako bi došli u posjed poslovnih tajna. [8]

Pomorski gradovi-države poput Venecije i Dubrovnika iznimno su cijenili i razvijali gospodarsku obavještajnu djelatnost. Tako je Venecija bila bitno usmjerila svoje obavještajne resurse u proučavanje kineskog gospodarstva, dok je Dubrovnik postavio zadaću prikupljanja gospodarskih i političkih informacija o konkurentnim trgovačkim silama kao jedan od prioriteta svoje diplomatske službe. [1]

U znanstvenim krugovima 1959. godine pojavio se pojam *competitive intelligence* na čijim će se temeljima tridesetak godina poslije razvijati *business intelligence*. Tijekom 1970-ih godina William Rothschild[8] utemeljio je ozbiljnije znanstveno područje tog pojma, koje se dvadesetak godina kasnije počelo primjenjivati u organizaciji. [16] Općeprihvatljiva definicija pojma *competitive intelligence* ne postoji, odnosno teško ju je prevesti na hrvatski jezik, no može se reći da je to obavještajna djelatnost u odnosu prema ukupnoj konkurentnosti poslovnog subjekta.

Jednako kvalitetna je i definicija Larryja Kahanera[9], koji smatra da je *competitive intelligence* sustavan program za prikupljanje i analizu informacija o aktivnostima konkurenata i općim poslovima razvojnim smjerovima, koji se provodi da bi se ostvarili ciljevi vlastite kompanije. [2]

Bez obzira na različita tumačenja i shvaćanja definicije *competitive intelligence* , analiza definicija pokazuje da se različiti autori slažu o temeljima koji nesporno imaj četiri temeljna načela:

- otkriti prijetnje koje određenom poslovnom subjektu dolaze od njihovih konkurenata,
- eliminirati ili ublažiti utjecaj mogućih iznenađenja,

[8] William E. Rothschild (1933-danas) bivši je izvršni direktor tvrtke General Electric koji je započeo s vlastitom tvrtkom za poslovno savjetovanje, Rothschild Strategies Unlimited, te objavio knjige, posebice The Secret To GE's Success i Risk Taker, Caretaker, Surgeon i Undertaker: The Four Faces of Strategic Leadership, od kojih svi raspravljaju o uspješnim poslovnim strategijama na kojima je Rothschild bilo sudionik ili promatrač

[9] Larry Kahaner (1949-danas) je američki novinar, autor, ghostwriter i bivši licencirani privatni istražitelj. Napisao je knjigu Competitive Intelligence: How to Gather, Analyze and Use Information to Move Your Business to the Top koja je izdana 1996. godine

- povećati vlastitu konkurentsku prednost skraćujući vrijeme potrebno za reakciju te
- pronaći nove prigode za vlastitu poslovnu organizaciju. [3]

3.1. Defriniranje poslovno-obavještajne djelatnosti

Pojam *business intellignece* prvi put se pojavio 1989. godine kada je Howard Dresnera[10] shvatio da vođe poslovnih subjekata više ne mogu donositi odluke na temelju intuicije, već se čitav proces odlučivanja treba temeljiti na činjenicama. Korištenje činjenica umjesto intuicije je bit obavještajnih djelovanja, a time i glavni čimbenik koncepcije *business intelligence*a. [4]

S obzirom na značenje koje je dobio u suvremenim uvjetima, potrebno je odgovoriti na pitanje: što je zapravo business intelligence?

The Free Encyclopedia[11] navodi da je business intelligence proces prikupljanja informacija u poslovnom svijetu s ciljem stjecanja prednosti u odnosu prema konkurenciji. Bussines intelligence nije nelegalna aktivnost niti špijunaža. To je legalna aktivnost u poslovnom svijetu koju planiraju, organiziraju i provode poslovni objekti, koja podrazumijeva prikupljanje i analiziranje javnih i svima dostupnih podataka iz otvorenih izvora. [17]

3.1.1. Model obavještajnog djelovanja - business intelligence

Obavještajna djelatnost se ne događa stihijski, već je pažljivo pripremana i planiranana te sustavno provedena djelatnost. Njezin konačni rezultat jesu poslovno-obavještajna izvješća koja se u primjeni, zajedno s misaonom

[10] Howard Dresner je glavni istraživač tvrtke Dresner Advisory Services, ima preko 30 godina iskustva u IT industriji s 25 godina iskustva u Business Intelligece-u. Proveo je 13 godina u Gartneru, gdje je bio istraživač i glavni analitičar za BI. Objavio je nekoliko značajnih istraživanja poslovne inteligencije u industriji pod brandom Wisdom of Crowds.

[11] Free Encyclopedia je višejezični enciklopedijski sadržaj na internetu slobodnog sadržaja kojeg podržava Wikimedia Fundation i temelji se na modelu otvorenog sadžaja koji se može uređivati

aktivnošću, pretvaraju u poslovno znanje. Takvo poslovno znanje omogućuje poslovnom subjektu donošenje kvalitetnijih poslovnih planova i konkretnih poslovnih odluka, a naposljetku i provođenje poslovnih akcija.

Business intelligence je ciklična (kružna) aktivnost koja ima nekoliko temeljnih faza:

a) planiranje i upravljanje ciklusom business intelligencea – *planning and direction;*
b) prikupljenje podataka – *collection;*
c) obrada i analiza podataka i izrada obavještajnih analiza – *processing and analysis;*
d) distribucija gotovih obavještajnih proizvoda i njihova obrada – *dissemination.*

Slika 1. Model business intelligencea [1]

Kako bi proces business intelligencea bio uspješan, mora proći kroz razne faze, pri čemu je važno biti uspješan u svakoj od faza. Da bi prelazak na sljedeću fazu bio uspješan, potrebno je u potpunosti završiti prethodnu. Iako imaju zajedničku karakteristiku da se ne događaju same od sebe i da

zahtijevaju brižljivo planiranje i sustavnu provedbu, svaka od tih faza je različita. (slika 1).

a) Planiranje i upravljanje (planning and direction):
   Da bi sustav business intelligencea uspješno funkcionirao, potrebno je imati predodžbu o tome kakve podatke je potrebno prikupljati, odnosno, potrebno je odrediti ciljeve. Nakon što se odredi interes krajnjeg korisnika obavještajnog proizvoda, unutar poslovnog objekta izrađuju se planovi za ostvarivanje tog cilja.

b) Prikupljanje podataka (collection):
   Kada se radi o prikupljanju podataka i informacija, ono se provodi prema unaprijed utvrđenim okvirima koji ne dopuštaju improvizaciju. Razlika između pristupa jedino je u tome što opća razina, kao okvir, ima opća usmjerenja, dok konkretna zahtijeva razradu konkretnih planova za prikupljanje podataka i informacija. Iako postoje razne kategorizacije podataka, ne postoji niti jedna kategorizacija na koju je usmjeren business intelligence. Unatoč tome, sa stajališta business intelligencea, podatke je moguće logički strukturirati u tri opće kategorije:
   - javni, otvoreni i svima dostupni podatci,
   - privatni podatci koje posjeduju pojedinci te
   - tajni podatci.

   Kada se govori o business intelligenceu, prikupljanje podataka se odnosi samo na javne i svima dostupne podatke te na prikupljanje podataka u kontaktima s pojedincima koji posjeduju određeno znanje.

   Unutar business intelligencea postoje tri zone prikupljanja sredstava, odnosno podataka. Prva je *bijela zona*[12] *– etičnost i legalna sredstva*, koja podrazumijeva uporabu zakonitih i etičnih

[12] Primjer bijele zone: prikupljanje podataka iz medija, statističkih podataka, podataka o poslovanju i sličnih javnih izvora koji su legalni i etični

sredstava. Zatim slijedi *siva zona*[13] *– neetična, ali legalna sredstva*, te *crna zona*[14] *– neetična i nelegalna sredstva.* Business intelligence je dominantno usmjerena prema bijeloj zoni, iako u nekim slučajevima djelovanje upućuje na korištenje sive zone. Crna zona prelazi djelovanje business intelligencea i prelazi u špijunažu.

c) Analiza podataka (processing and analysis): Tijekom faze prikupljanja podataka pribavlja se velik broj različitih podataka koji su sirovog karaktera. Njih je potrebno raščlaniti, odvojiti važne od nevažnih, sistematizirati i kategorizirati ih, odnosno interpretirati. Prikupljenim informacijama treba provjeriti izvor i točnost te pouzdanost izvora. Sve to čini analizu podataka koji prolaze kroz razne metode obrade. Analiza[15], sinteza[16], indukcija[17] i dedukcija[18] su jedne od najčešćih metoda kojima bi se od niza obrađenih podataka i informacija stvorila jasna slika. To je temelj za primjerenu interpretaciju informacija i donošenje zaključaka. Gotova obavještajna informacija zapravo je odgovor na potrebe krajnjih korisnika. Njezina kvaliteta se može vrednovati kroz tri elementa:
    - točnost koja se utvrđuje nakon događaja,
    - relevantnost u odnosu prema izvorima zahtjeva te
    - pravodobnost dostavljanja.

[13] Primjer sive zone: prikupljanje podataka pomoću detektivskih agencija, posjedovanje kompromitirajućih podataka i sličnim načinima koji su neetični, ali legalni
[14] Primjer crne zone: prikupljanje podataka hakiranjem informacijskih sustava, ucjenom ili potkupljivanjem konkurencije i sličnim načinima koji su ilegalni i neetični
[15] Metoda analize je postupak znanstvenog istraživanja raščlanjivanjem složenih pojmova, sudova i zaključaka na njihove jednostavnije sastavne dijelove i elemente.
[16] Metoda sinteze je postupak znanstvenog istraživanja i objašnjavanja stvarnosti putem sinteze jednostavnih sudova u složenije.
[17] Induktivna metoda je sustavna primjena induktivnog na čina zaključivanja kojim se na temelju analize pojedina čnih činjenica dolazi do zaključka o općem sudu, od zapažanja konkretnih pojedinačnih slučajeva dolazi do općih zaključaka.
[18] Deduktivna metoda je sustavna primjena deduktivnog načina zaključivanja u kojemu se iz općih sudova izvode posebni i pojedinačni zaključci.

Ovisno o zahtjevu krajnjih korisnika te vremenskom determinantom, analize se mogu kategorizirati na različite načine. Mogu se izraziti u pisanom ili govornom obliku, mogu imati karakter tekućih, predviđajućih ili istraživačkih projekata ili predstavljati analitičke prikaze s područja *ranog upozorenja*[19] (early warning), mogu se prikazati u numeričkom, statističkom, grafičkom ili sličnom obliku.

d) Distribucija analiza (dissemination): Posljednja faza poslovno-obavještajnog ciklusa business intelligencea jest predstavljanje obavještajnog proizvoda krajnjem korisniku, voditeljima poslovnih subjekata, te korištenje tog proizvoda od strane menadžera u procesu odlučivanja. Distribucija ne predstavlja kraj ciklusa jer, ukoliko analiza utvrdi nedostatke ili kontradikcije, postavlja se zahtjev za novim analizama, čime se pokreće novi obavještajni ciklus. Neka poslovno-obavještajna studija, proizašla kao rezultat business intelligencea, može sadržavati i zaključak, ali taj zaključak nije „zaključnog karaktera“ jer se poslovno-obavještajni proces nastavlja. Zato nije nevažno da autor poslovnih intelligence studija od krajnjih korisnika dobije i osvrt na precizne studije (feedback). To je najbolji pokazatelj korisnosti i važnosti poslovno-obavještajnog ciklusa. [1]

3.1.2. Model protuobavještajnog djelovanja - business counterintelligence

Prethodno je istaknuto da business intelligence ima dvije dimenzije, dva aspekta djelovanja. Uz gore prikazan ofenzivni aspekt, business intelligence ima i defenzivnu, protuobavještajnu dimenziju (*counterintelligence*). Business counterintelligence podrazumijeva protuobavještajno djelovanje u poslovnom svijetu koji prvenstveno jamči sigurnost poslovnog subjekta i uspostavlja mehanizam za njegovu zaštitu. Time je business counterintelligence dio

[19] Sustav ranog upozorenja je sustav za upravljanje rizicima kako bi se izbjegla iznenađenja i identificirale poslovne prilike, koji omogućuje top-menadžerima osposobljavanje za djelovanje u krizama prije nego se dogode.

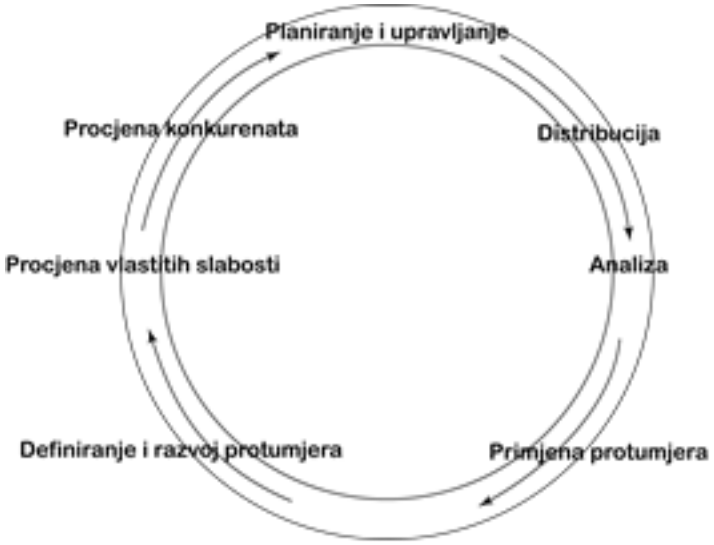
integralne poslovne sigurnosti. Ono podrazumijeva aktivnosti usmjerene na eliminaciju i reduciranje učinka intelligence aktivnosti suparnika te zaštitu informacija poslovnog subjekta od gospodarske i industrijske špijunaže.

U današnje vrijeme informacija je moć, do te mjere da može značiti uspjeh, ali i potpunu propast tvrtke. Čuvanjem ključnih informacija tvrtka ostvaruje svoju konkurentnost, a pojedinac štiti svoju ideju koju planira iskoristiti za dobivanje patenta. Kako bi se vlasnici povjerljivih informacija ipak zaštitili, koriste se NDA ugovori (eng. Non-disclosure agreement). Pomoću njih vlasnici informacija mogu odati svoje tajne drugoj strani, ali ostaju zaštićeni ukoliko druga strana odluči tu informaciju širiti dalje.

Analiza pokazuje da business counterintelligence ima tri temeljna cilja:

a) zadržavanje *statusa quo* vezano za položaj poslovnog subjekta u poslovnom okruženju,
b) procjenu mogućih opasnosti i prijetnji te
c) zaštita poslovnog subjekta od nelegalnih i neetičnih napada drugih subjekata.

Business counterintelligence ciklus započinje planiranjem, odnosno određivanjem zadataka na najvišim razinama odlučivanja. Ti zadatci moraju biti brižljivo planirani i postavljeni. U sljedećoj fazi treba odrediti izvore opasnosti, to jest potrebno je odrediti koji konkurenti mogu ugroziti poslovni subjekt. Nakon toga, nužno je analizirati vlastite slabosti koje uključuju određivanje „loših točaka“ putem kojih bi konkurent koji prikuplja podatke mogao doći do onih koji ga zanimaju. Pretposljednja faza uključuje razvoj i primjenu protumjera, odnosno sigurnosnih mehanizama koji trebaju zaštititi poslovni subjekt od ofenzivnih nasrtaja. U posljednjoj fazi ciklusa rezultati poduzetih aktivnosti se predstavljaju te se na temelju njih planira i određuje zadatak. [5]



Slika 2. Model bussiness counterintelligencea [2]

Sigurnost u suvremenim uvjetima ima sve veće značenje, ne samo kao preduvjet opstanka bilo kojeg entiteta, nego i za svakodnevno djelovanje na svim područjima ljudske djelatnosti pa i u poslovnom svijetu. Izloženost poslovnih subjekata raznim vrstama ugrožavanja i mnogim rizicima dovela je toga da je korporativna sigurnost postala nužna za opstanak poslovnih kompanija. Sigurnost poslovnih sustava u suvremenim uvjetima postala je njihova strateška funkcija. Karakteristika suvremenog poslovnog svijeta jest da su pojave novih vrsta ugrožavanja, proširenje njihova opsega i intenziteta te krajnjih učinaka, omogućili svojevrsnu simbiozu napora na razini nacionalne države i poslovnih subjekata.

Bez obzira na sve veće djelovanje državnih institucija u ostvarenju sigurnosti poslovnih subjekata, nepobitno je da su za sigurnost primarno odgovori oni sami. U suvremenim uvjetima djelovanje je, između ostalog, presudno vezano za informacije, bilo da je riječ o poslovnim planovima ili financijskom stanju. Gubitkom bilo koje kategorije informacija ugrožava se učinkovitost i sposobnost poslovnog subjekta.

Suvremena koncepcija informacijske sigurnosti polazi od dvije temeljne činjenice:

1. Nedostatak svijesti o ugroženosti poslovnih subjekta i potrebi da se uspostave odgovarajući sigurnosni mehanizmi.
2. Dosadašnja koncepcija sigurnosti poslovnih subjekata bila je usmjerena na uspostavu mehanizma informatičke sigurnosti. Takvo koncentriranje sigurnosnih mehanizama informatičke sigurnosti pokazalo se pogrešnim. Naime, suvremene studije pokazuju da su za 70% slučajeva gubitaka informacija unutar poslovnih subjekata odgovorni zaposlenici, što znači da su oni „ukrali“ informacije o poslovanju kompanije te ih predali drugima.[20]

Uz nastojanje da se poveća i poboljša stupanj sigurnosti, na mnogim područjima sigurnosti se primjenjuju razne mjere. Business intelligence uključuje primjenu niza mjera u četiri aspekta:

- **Tehnički aspekt:** Sigurnosne mjere s tog područja imaju zadaću reducirati sve ranjivosti i slabe točke unutar komunikacijskih sustava. Takve mjere trebaju osigurati povjerljivost, raspoloživost uporabe i integritet informatičkih sustava, ali i ostalih komunikacijskih sustava u poslovnom subjekt.[21]
- **Bihevioristički aspekt:** Usmjeren je na gubitak informacija „neetičkih“ sredstava. Potrebno je podizati svijest unutar poslovnog subjekta da može biti ugrožen i da je stoga potrebno uspostaviti mehanizme i oblike ponašanja za zaštitu informacija.[22]

[20] Primjer za „krađu“ informacija o poslovanju kompanije: Ako u mail postavkama zaposlenik na računalu na radnom mjestu omogući slanje mailova na njegovu privatnu mail poštu, u svrhu odgovaranja ili obavljanja posla izvan radnog mjesta (npr. na putu kući, na godišnjem odmoru, vikendom. Itd.) spada u kritičnu masu koju bi poslodavac mogao opisati kao lopova zbog iznošenja podataka izvan tvrtke.

[21] Primjer tehničkog aspekta: Ograničavanje uporabe informacija i podataka izvan tvrtke, koji mogu tvrtku dovesti u opasnost; korištenje jedinstvenog internog informatičkog sustava; zaštita dokumenata lozinkom

[22] Primjer biheviorističkog aspekta: Potpisivanje Ugovora o povjerljivosti podataka između poslodavca i zaposlenika koji raspolaže tajnim podatcima koji mogu ugroziti sigurnost tvrtke

- **Fizički apsekt:** Mnogi gubici informacija unutar poslovnih subjekata događaju se jednostavno zbog krađa koje omogućuje fizički ulazak neovlaštenih osoba u različite prostore poslovnog subjekta. Stoga, mjere vezane za ovaj aspekt imaju cilj regulirati i kontrolirati pristup ljudi u objekte, kao i njihovo ponašanje u tim prostorima. Bitno je uspostaviti kontrolu ulaska u takve objekte koji nikako ne smiju biti slobodni i neovlašteni.[23]
- **Personalno-kadrovski (osobni) aspekt:** Taj je aspekt usmjeren na uspostavu sigurnosnih mehanizama pri kadrovskom ulasku i izlasku zaposlenika iz poslovnih organizacija. Što se tiče zapošljavanja u poslovni subjekt, nužno je uspostaviti sigurnosne mehanizme, odnosno sigurnosne provjere za sve osobe koje će imati pristup osjetljivim informacijama. Svrha tih provjera jest osigurati u prihvatljivu razinu sigurnosti da osobe koje će imati pristup informacijama to neće zloupotrijebiti.[24] [1]

3.2. Poslovno-obavještajni ciklus

Obavještajna djelatnost je pažljivo pripremana i planirana te sustavno provedena aktivnost. Njezin konačni rezultat su gotove poslovno-obavještajne analize koje olakšavaju donošenje odluka. Uporaba konačnih rezultata business intelligencea poslovnom subjektu omogućuje određivanje kvalitetnijih poslovnih strategija i poslovnih odluka te provedbu poslovnih akcija.

Business intelligence je, kako je već navedeno, ciklička aktivnost, te se jednako kao i na razini nacionalnih obavještajnih sustava ostvaruje prema određenim pravilima. Ta su pravila strukturirana unutar tzv. poslovno-obavještajnog ciklusa, koji se analogijom prema obavještajnim institucijama

[23] Primjer fizičkog aspekta: Pristupne kartice na ulaznim i izlaznim vratima tvrtke, koja omogućuju ulazak samo ovlaštenim osobama
[24] Primjer za personalno-kadrovski aspekta: Potvrda o nekažnjavanju suda kojom se dokazuje da zaposlenik nema podnešenih prijava zlouporabe važnih podataka

određuje kao proces kojim se prikupljene informacije pretvaraju u gotove obavještajne proizvode i postaju dostupne kreatorima politike.

Njegove središnje faze su:

- prikupljanje i
- obrada i analiza podataka.

Proces prikupljanja podataka business intelligencea vrši se prema unaprijed utvrđenom planu te ne dopušta improvizaciju. To jasno određeno nastojanje jedna je od najvitalnijih funkcija tog procesa. Business intelligence je djelotvoran samo ako se ostvaruje prema strogo utvrđenim načelima kada su uzroci i posljedice povezani do krajnjih pojedinosti.

Kako bi proces prikupljanja podataka bio učinkovit, u njegovoj početnoj fazi nužno je imati jasnu spoznaju o vlastitom poslovnom subjektu i njegovim ciljevima. To je temelj za standardni upitnik (*intelligence profile* – obavještajni profil). Temeljno pitanje standardnog upitnika odgovara na osnovno pitanje: što poslovni sustav mora znati da bi ostvario uspjeh, odnosno svoje ciljeve. Svaki poslovni subjekt ima svoj standardni upitnik koji se ne može primjenjivati na drugi poslovni subjekt, što ga čini jedinstvenim. Izrada takvog upitnika zapravo je poveznica i za određivanje okvira „ključnih obavještajnih točaka“ (key intelligence topics – KIT-s). One predstavljaju mehanizam putem kojeg se definiraju i određuju zahtjevi na koje business intelligence sustav mora dati odgovor.

Znanstvenici i stručnjaci-praktičari na tom području uglavnom se slažu da postoje četiri kategorije „ključnih obavještajnih točaka“ koje su temeljni okvir za određivanje obavještajnih prioriteta. To su:

a) strategijsko poslovno odlučivanje (decision topics);
b) ključni konkurenti, dobavljači i klijenti (key player topics);
c) rano upozorenje vezano za moguće prijetnje i rano uočafvanje poslovnih prilika (early warning):
d) poslovno-protuobavještajne točke (counterintelligence topics).

Kategoriziranje podataka nije nimalo jednostavan proces. Prvenstveno treba prikupiti podatke koji trebaju biti određenog tipa. Primjerice, komercijalni odjeli unutar poslovnog subjekta trebaju podatke tog tipa, odjel financija trebaju podatke vezane uz financije, dok odjel marketinga treba podatke koji se odnose na poslodavce, a proizvodnji trebaju podatke vezane uz proizvodnju, itd.

Tri najznačajnije opće kategorije podataka koji predstavljaju interes business intelligencea, a zapravo su pokušaj da se odgovori na pitanje o tome što poslovni subjekt treba znati da bi uspješno poslovao, odnosno da bi ostvario svoje ciljeve jesu:

1. Podatci o okruženju u kojem djeluje poslovni subjekt:

   U tu kategoriju spadaju podatci koji se odnose na globalno okruženje u kojem djeluje poslovni subjekt. Takvi su podatci bitni jer gotovo svi događaji, procesi i pojave u današnjem globalnom okruženju mogu bitno utjecati na njegovo poslovanje.

2. Podatci koji se odnose na tržište:
   Ostvarenje dobiti prvenstvena je zadaća poslovnih subjekata, a taj cilj ostvaruje na tržištu. Stoga je prikupljanje podataka o tržištu itekako važno za poslovni subjekt. To podrazumijeva prikupljanje podataka o kretanjima na domaćem tržištu, ali i na regionalnom, pa i globalnom tržištu.

3. Podaci koji se odnose na konkurenciju:
   Tržišna utakmica se odvija među konkurentima. Stoga je potrebno prikupljati i podatke o konkurenciji. To uključuje podatke o izravnim konkurentima, točnije podatke o njihovoj poslovnoj strategiji, o financijskim uvjetima, o novim proizvodima i uslugama koje namjeravaju plasirati na tržište.

Podatci se mogu prikupljati posredstvom tehničkih sredstava i posredstvom „ljudskog izvora“. Prikupljanje podataka tehničkim putem odnosi se na uporabu nepresušnog globalnog izvora informacija – interneta. Ljudski izvori su resursi koji se nalaze unutar ili izvan poslovnog subjekta, a posjeduju informacije koje su predmet interesa. Time se na primjer bave detektivske agencije koje istražuju niz kadrovskih i tehničko-tehnoloških, izuzetno zahtjevnih, usluga koje se ne mogu samostalno riješiti. [4]

3.3. Analiza podataka

Tijekom faze prikupljanja podataka pribavi se golem broj različitih podataka. Prikupljeni podatci su „sirovi“ te ih je potrebno raščlaniti, odvojiti važne od nevažnih, kategorizirati, itd. To se ostvaruje kroz obradu koja vodi u sljedeću fazu – analizu podataka. Analiza podataka zapravo je slaganje mozaika od niza fragmenata, odnosno ostvarenje krajnjeg cilja analitičkog djelovanja – proizvodnja poslovno-obavještajnih informacija. Proizvodnja poslovno-obavještajnih analiza nastaje kao krajnji rezultat dviju djelotvornih faza djelovanja vezanih za obrađene podatke te ima dva integrirana elementa.

Prvi se odnosi na interpretaciju prikupljenih podataka, dok se drugi podrazumijeva da zbog dinamike i složenosti, krajnji analitički proizvod uz informacije mora ponuditi i odgovarajuće prosudbe, zaključke i projekcije budućih kretanja.

Tehnološka dostignuća su zasigurno jedan od razloga da se obavještajni mehanizam u potpunosti počeo primjenjivati u poslovnom svijetu. Obavještajni mehanizam, uz tehnološka dostignuća, postale su bitno sredstvo u poslovnom upravljanju i odlučivanju.

Informatička tehnologija, analitičke informatičke aplikacije i odgovarajući alati igraju važnu ulogu u izradi konačnih poslovno-obavještajnih analiza, koji su vrlo bitni za donošenje i realizaciju poslovnih odluka. Neke od njih je vrlo bitno istaknuti, a to su:

- skladištenje podataka;
- on – line analitičko obrađivanje – OLAP;
- rudarenje podataka;
- strateški sustav ranog upozoravanja;
- geografski informacijski sustavi;
- SWOT analiza. [5]

3.1. Skladištenje podataka (Data warehousing)

Pojam „skladište podataka" (engl. *Data Warehouse*) podrazumijeva zbirku podataka izoliranih iz operativnih baza i spremljenih u posebne baze, odnosno skladišta podataka. Ralph Kimball[25] definira skladište podataka kao kopiju transakcijskih podataka specifično strukturiranih za upite i analize. Glavna karakteristika koja određuje skladište podataka odnosi se na njegovu svrhu. U skladištu podataka podatci se skupljaju i organiziraju na način da budu lako dostupni da bi ih menadžment mogao na brz i jednostavan način koristiti za potrebe analize svog poslovanja. Postupak skladištenja podataka predstavlja kontinuirani proces planiranja, građenja, i prikupljanja podataka iz različitih izvora te njegovog korištenja, održavanja upravljanja i stalnog unaprjeđenja. Među mnogim koracima u tom kompleksnom kontinuiranom procesu bitno je naglasiti važnost posjedovanja vizije o tome što se želi postići kreiranjem skladišta podataka. Jedna od uloga skladišta je, primjerice, razvijanje i korištenje znanja zasnovanog na podatcima (engl. data-based knowledge). Iz prethodno navedenih definicija, jednostavno rečeno, glavni cilj skladišta podataka je osloboditi informacije koje su "zaključane" u bazama podataka i "pomiješati" ih s informacijama iz ostalih, u pravilu vanjskih izvora podataka. Velike organizacije danas sve više traže dodatne podatke iz vanjskih izvora,

[25] Ralph Kimball (1944.-danas) autor je knjige na temu skladištenja podataka i poslovne inteligencije. On je jedan od izvornih arhitekata skladištenja podataka i poznat je po dugoročnim uvjerenjima da skladišta podataka moraju biti osmišljeni tako da budu razumljiva. Njegova je metodologija, također poznata kao dimenzionalno modeliranje ili Kimballova metodologija, koja je postala standard na području odlučivanja.

kao što su npr. podaci o konkurenciji, demografski trendovi, prodajni trendovi i sl. [6]

3.2. On-line analitičko obrađivanje – OLAP

Baze podataka mrežne analitičke obrade (OLAP) obuhvaćaju upite vezane uz podršku poslovnom odlučivanju. OLAP je tehnologija baze podataka optimizirana za postavljanje upita i izvještavanje, umjesto za transakcije obrade. Izvorni podaci za OLAP su baze podataka Mrežne transakcijske obrade (OLTP) koje su obično spremljene u spremišta podataka. OLAP podaci se izvode iz ranijih podataka i sakupljaju se u strukture koje omogućavaju sofisticirane analize. OLAP podaci se također organiziraju hijerarhijski i spremaju u kocke, umjesto u tablice. To je sofisticirana tehnologija koja koristi višedimenzionalne strukture za omogućavanje brzog pristupa podatcima za analizu. Takva organizacija omogućuje jednostavno prikazivanje sažetaka visokih razina za izvješća zaokretnih tablica ili zaokretnih grafikona, poput ukupne prodaje za cijelo područje ili regiju te prikaz detalja za mjesta gdje je prodaja osobito dobra ili loša.

OLAP baze podataka dizajnirane su za ubrzavanje dohvaćanja podataka. Na taj se način omogućuje rad s većom količinom izvorišnih podataka nego što bi se moglo kad bi podatci bili organizirani u tradicionalnoj bazi podataka, u kojoj Excel mora dohvatiti sve pojedinačne zapise i zatim računati zbirne vrijednosti. OLAP baze podataka sadrže dvije osnovne vrste podataka: mjere, koje su brojčani podaci, količine i prosjeci koji se koriste za donošenje kvalitetnih poslovnih odluka i dimenzije, koje su kategorije koje se koriste za organiziranje tih mjera. OLAP baze podataka pomažu u organiziranju podataka u mnogo razina detalja, korištenjem istih poznatih kategorija za analizu podataka. [18]

3.3. Rudarenje podataka (Data mining)

Rudarenje podataka (eng. data mining) moglo bi se definirati kao pronalaženje zakonitosti u podacima. Ti podatci mogu biti organizirani u baze podataka, ali isto tako to mogu biti i tekstualni podatci, nestrukturirani podatci proizašli iz Web-a ili pak podatci organizirani u vremenske serije. Zakonitosti se pronalaze primjenom metoda koje svoje korijene vuku iz različitih područja kao što su, primjerice, statistika, matematika, baze podataka, teorija informacija, teorija vjerojatnosti i umjetna inteligencija. Ovo je vrlo mlado područje te postoji niz metodoloških pristupa problematici, kao i preferencije primjena metoda koje naginju ka određenom području ovisno o autorima koji obrađuju tu problematiku. S jedne strane, istraživanja u ovom području usmjerena su ka traženju metoda za rješavanje specifičnih problema, a s druge strane, kao rezultati istraživanja nude se nova metodološka rješenja poboljšanja postojećih metoda. S obzirom na interdisciplinarnost ovog područja, vrlo je teško povući jasnu granicu i deklarirati pojedine metode kao isključive metode rudarenja podataka. Vrlo velik broj korištenih metoda nedvojbeno pripadaju u područje statistike poput, primjerice, metoda uzorkovanja, ali u lancu rudarenja podataka mogu biti vrlo značajna karika prilikom analize podataka.

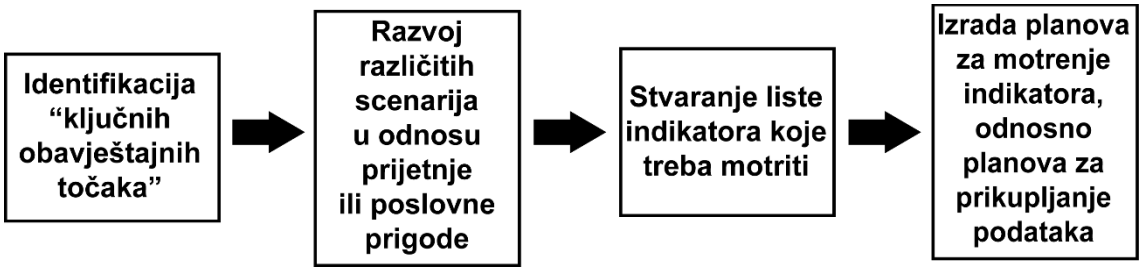
Izvori podataka mogu biti klasične tradicionalne baze podataka te primjena metoda rudarenja podataka nad tako formatiranim podacima spada u područje tradicionalnog rudarenja podataka. U novije vrijeme izdvajaju se područja s obzirom na izvore podataka kao što je to rudarenje Weba, rudarenje teksta te analiza vremenskih serija. Osnovni razlog izdvajanja ovih područja proizlazi iz činjenice što podaci nisu strukturirani u relacijske tablice[26], već su nestrukturirani ili pak strukturirani na temelju specifičnog formata.

[26] Redak tablice se naziva Relacija (engl. Relation), pojmovno je podudaran sa slogom podataka i predstavlja informaciju o jednom subjektu, dakle relacije su pohranjene kao tablice.

3.4. Strateški sustav ranog upozoravanja (Strategic early warning system)

Svrha sustava je što je prije moguće identificirati dinamičke ili sadržajne značajke pojava i situacija koje mogu utjecati na interese poduzeća. To je mehanizam posredstvom kojeg poslovni subjekti anticipiraju, detektiraju i, kada je to moguće, sprječavaju strateška iznenađenja. Sustav ranog upozorenja je sustav za upravljanje rizicima kako bi se izbjegla iznenađenja i identificirale poslovne prilike, koji omogućuje top-menadžerima osposobljavanje za djelovanje u krizama prije nego se dogode. Analitički okvir strateškog ranog upozorenja prije svega je orijentiran na strateške interese poslovnog subjekta. Temelji se na nadziranju i analizi prethodno definiranih indikatora koji ukazuju na promjene postojećeg stanja u poslovnom okruženju, a koji u konačnici mogu značiti prijetnju ili poslovni priliku. Temelji se na podacima koji govore o razmišljanjima i namjerama drugih aktera u poslovnom okruženju.

Poslovno-obavještajni proces, kada je u pitanju strateški sustav ranog upozorenja, odvija se unutar okvira koji se sastoji od nekoliko faza. Grafički model navedenog procesa je predstavljen u sljedećim fazama:



Slika 3: Okvir sustava ranog upozorenja [3]

Prva faza podrazumijeva identifikaciju ključnih obavještajnih točaka (key intelligence topics) koji su ranije predstavljeni.

Druga podrazumijeva razvoj analiza scenarija u odnosu na prijetnje ili poslovne prilike.

Treća podrazumijeva stvaranje liste indikatora koje treba motriti, dok četvrta uključuje izradu planova za motrenje indikatora tj. planova za prikupljanje podataka na temelju kojih će se izraditi analize upozorenja.

3.5. Geografski informacijski sustavi (GIS sustavi)

Ovi programski sustavi analiziraju informacije s geografskog aspekta. Informacije se prikazuju i analiziraju u grafičkom obliku. GIS sustavi pružaju geografsku, demografsku i socioekonomsku sliku stanovništva. Vizualizacijom podataka GIS sustavi prikazuju sliku o teritorijalnoj raspršenosti promatranih subjekata čime daju osnovne smjernice za donošenje daljnjih poslovnih odluka. Osnovni element GIS sustava je tzv. geokod koji predstavlja dvodimenzionalnu matricu gdje svaka točka reprezentira mjesto u prostoru.
Kod primjene u trgovačkim lancima GIS sustavi funkcioniraju na slijedeći način: prikupljanjem podataka o adresama svojih potrošača te uporabom GIS sustava trgovački lanci mogu dobiti točnu sliku o razmještaju stanovništva, kako na mikro tako i na makrolokaciji. Analizom se utvrđuju geografska područja na kojima je prodaja visoka, što olakšava donošenje odluka o alokaciji marketinških resursa prema onim područjima gdje prodajni rezultati nisu na takvoj razini. [7]

3.6. SWOT analiza (Strengths, Weaknesses, Opportunities, Threats analysis)

SWOT analiza je analitički okvir menadžmenta za dobivanje relevantnih informacija organizacije o samoj sebi i okolini u kojoj djeluje sada i u budućnosti

sa svrhom utvrđivanja strategijskih prilika i prijetnji u okolini i vlastitih strategijskih snaga i slabosti. Ona omogućava menadžmentu da razvije strategiju na temelju relevantnih informacija o organizaciji i okolini. Temelji se na pretpostavci da će organizacija postići najveći strategijski uspjeh maksimiziranjem vlastitih snaga i prilika u okolini uz istodobno minimiziranje prijetnji i slabosti, odnosno najboljom upotrebom unutarnjih snaga u korištenju prilika u okolini. Bitna je pretpostavka analiza suglasja unutarnjih i vanjskih faktora te utvrđivanje njihovih implikacija za strategiju. Zapravo, unutarnje snage i slabosti treba promatrati u kontekstu vanjskih prilika i prijetnji i obrnuto.

Prednosti su pozitivne unutarnje okolnosti i distinktivna svojstva organizacije koja joj osiguravaju ili mogu osigurati konkurentsku prednost. To je sve ono što organizacija radi posebno dobro i u čemu je bolja ili može postati bolja od konkurenta.

To može biti jako kvalitetan menadžment, motivirano i sposobno osoblje, specifičan proizvodni ili tehnološki *know-how*, ekskluzivno vlasništvo patenata, jak *image* i reputacija, dobri distribucijski kanali, poseban marketing i jake marketinške sposobnosti, posebna organizacijska kultura i odnos prema promjenama, kvalitetni materijali i proizvodi, posebni, partnerski odnosi s dobavljačima ili kupcima, optimalna uporaba resursa, niski troškovi itd. Sve to uz mnoštvo drugih činitelja može voditi i držati organizaciju ispred konkurenata, odnosno osiguravati joj konkurentsku prednost.

Nedostatci, slabosti su unutarnja svojstva organizacije koja smanjuju njezinu uspješnost i šanse u konkurentskoj utakmici. To mogu biti loši menadžeri, nedostatak vizije i okrenutost prema unutra te bavljenje aktualnim problemima, negativan odnos prema promjenama, birokratska kultura, nedostatak potrebnih znanja, kvalitetnih ljudi ili drugih resursa, zastarjela tehnologija, slab *image* i čitav niz drugih činitelja. Ukratko, nepostojanje svega onoga navedenog kao potencijalna prednost.

Slika 4. Prednosti i nedostatci SWOT analize [4]

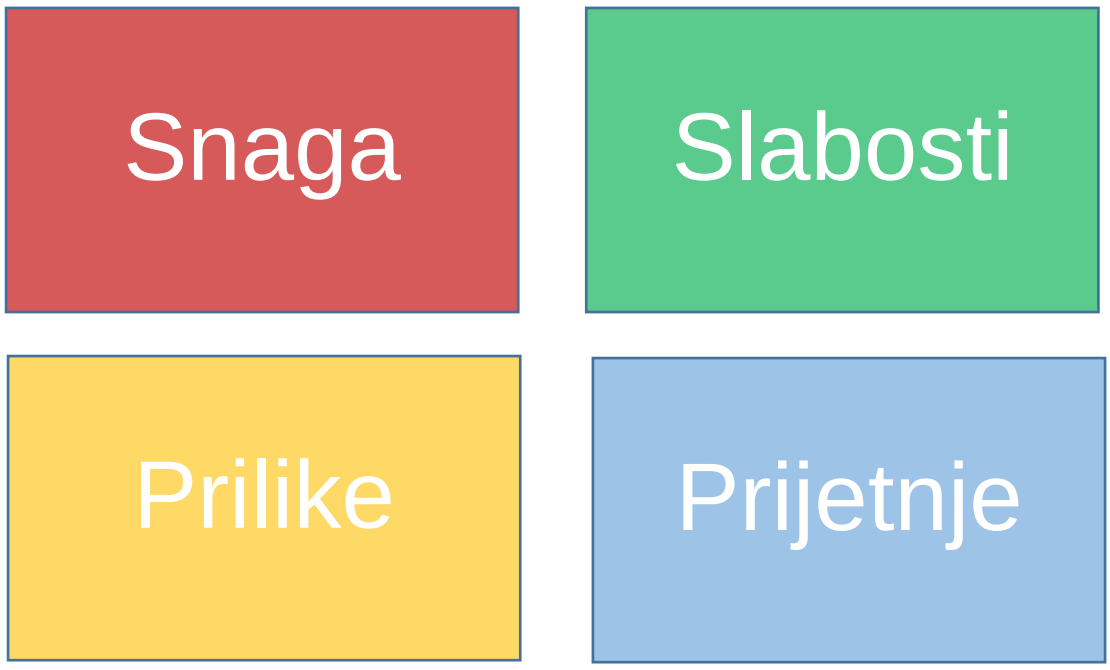
SWOT analiza je zbog svoje jednostavnosti i preglednosti najčešće korištena metoda analize elemenata vanjske i unutarnje okoline poduzeća. SWOT je engleski akronim za snagu (Strength), slabosti (Weaknesses), prilike (Opportunities) i prijetnje (Threats), pri čemu se snaga i slabosti odnose na unutarnje elemente okruženja poduzeća, a prilike i prijetnje na vanjske elemente okruženja.

Najvažniji vanjski i unutarnji čimbenici za budućnost poduzeća nazivaju se strateškim čimbenicima i oni se sumiraju u SWOT analizi. U konačnici bi SWOT analiza trebala identificirati prilike koje se trenutno ne mogu iskoristiti zbog nedostatka potrebnih resursa i jedinstvene kompetencije koje poduzeće posjeduje i superiornog načina na koji ih koristi. SWOT analiza ima vremensku dimenziju, odnosno kad god je to moguće, korisno je uspoređivati i pratiti SWOT analize napravljene za poduzeće u različitim vremenskim periodima te promatrati promjene stanja, odnosno kretanje poduzeća kroz ovu analizu. Unutarnje snage i slabosti uvelike se razlikuju za različite subjekte, a mogu se kategorizirati u menadžment i organizaciju, operacije, financije i ostale

čimbenike. Kod kategorizacije unutarnjih čimbenika za potrebe SWOT analize čini se opravdanim koristiti se najvažnijim unutarnjim čimbenicima organizacije: ciljevi i strategije, tehnologija i zadaci, veličina, kadrovi, životni ciklus poduzeća, proizvodi i lokacija, a pri određivanju snage i slabosti treba pristupiti što je više moguće pragmatično. U analizi vanjskog okruženja moraju se uzeti u obzir mnogi različiti čimbenici koji mogu biti ili prijetnje ili prilike, te se kategorizirati u sljedeće kategorije:

- ekonomski,
- društveni,
- političko-pravni,
- tehnološki,
- ekološki te
- etički.

Najvažniji dio vanjskog okruženja je industrijsko okruženje (kupci, dobavljači, konkurencija). [9]



Slika 5. Shema SWOT analize [5]

4. INFORMACIJSKA SIGURNOST

Razvoj informacijskih sustava i informatizacija, stvaranje i povezivanje informacijskih mreža u globalni internetski sustav te sve veća važnost podataka i informacija na svim područjima ljudskog života, ističe pitanje sigurnosti na informacijskim području. Uvođenjem informacijsko-komunikacijske tehnologije te informatizacijom svih poslovnih funkcija i procesa, društveni, a i gospodarski sustavi postaju funkcijski i poslovno ovisni o informacijsko-komunikacijskim sustavima.

Rušenjem jednog o tih sustava dolazi do poslovnih problema, ne samo u djelatnosti koju neposredno opslužuje, već u onima s kojima je funkcionalno povezan. Razvoj informacijskog društva zahtijeva istodobno razvoj informacijske sigurnosti.

Važnost poslovnih i drugih podataka i informacija za pojedinca te za sve ljudske oblike organiziranja izazov je svima koji žele poboljšati svoj rad i uvijete života, ali i za sve koji se protive promjenama. Prvi su usmjereni na razvoj informacijskih sustava, na informatizaciju društva, dok drugi djeluju protiv tog procesa s ciljem da razore informacijske sustave i preko njih ostvare svoje parcijalne, sebične interese kojima će se probiti ili napraviti štetu drugima. [19]

4.1. Ugroženost poslovnih informacija i informacijsko-komunikacijskog sustava

Predmet informacijsko-komunikacijske ugroženosti su sve vrijednosti na tom području, kao i na područjima koja su s njima povezana.

„Razvoj informacijskih i komunikacijskih tehnologija omogućio je procese koji povezuju svijet i olakšavaju život, ali je stvorio i nove prijetnje i rizike. Ovisnost društava i pojedinaca o internetu i informacijskoj tehnologiji predstavljaju posebnu osjetljivost. Napadi u kibernetičkom prostoru, bez obzira na motive, sve više ugrožavaju pojedince, organizacije i države. Istodobno,

organizacijska fluidnost, geografska rasprostranjenost, tehnološka difuznost i neograničena mogućnost komunikacije otežavaju identifikaciju napadača, njihovih namjera i sposobnosti. Kibernetički kriminal je u porastu, a kibernetički prostor sve se više koristi za nezakonito djelovanje. Osim moguće povrede sigurnosti klasificiranih, osobnih i osjetljivih podataka, prijetnju predstavlja i korištenje kibernetičkog prostora za izazivanje žrtava i šteta u materijalnom svijetu. Radikalne ideje i pokreti, koji prerastaju u ekstremizam i terorizam, multipliciraju se i šire na internetu i društvenim mrežama, čime poprimaju doseg i utjecaj kakav ranije nisu imali.“ [15]

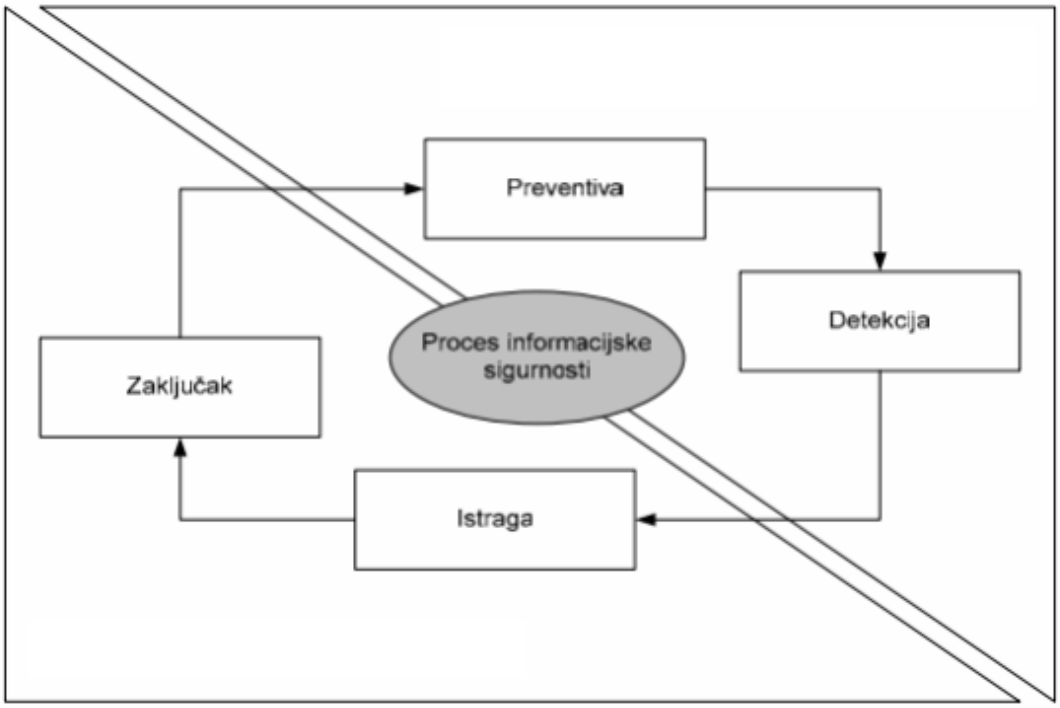
4.2. Informacijska sigurnost i sigurnost informacijskih sustava

Sigurnost je stanje i stupanj otpornosti i zaštićenosti od svih ugroženosti i opasnosti u kojemu se ne narušavaju normalni uvjeti, kako bi se omogućilo da se sve životne i radne funkcije odvijaju redovito.

„Informacijska sigurnost je stanje povjerljivosti, cjelovitosti i raspoloživosti podatka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda.“ [13]

Informacijska sigurnost definira se kao očuvanje:

- povjerljivosti – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj,
- integriteta – zaštita postojanja, točnosti i kompletnosti informacije kao i procesnih metoda,
- raspoloživosti – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva.



Slika 6. Proces procesnog pogleda na informacijsku sigurnost

Proces upravljanja informacijskom sigurnošću odgovoran je za trajno usavršavanje zakonskog okvira počevši od sigurnosne politike, preko provedbenih uredbi, pravilnika i smjernica, do detaljnih procedura postupanja pojedinih tijela državne uprave. Upravljanje informacijskom sigurnošću obuhvaća postupke kao što su identifikacija resursa, klasifikacija podataka, upravljanje rizikom, planiranje i implementacija mjera, postupci certifikacije osoblja i uređaja, postupci akreditacije sustava za rad, nadzor implementacije i učinkovitosti mjera i postupaka, praćenje informacijskih sustava tijekom životnog ciklusa te sustavnu edukaciju.

Na slici 6. prikazan je procesni pogled na informacijsku sigurnost, prema kojem je vidljiv gornji desni dio koji karakteriziraju preventivne mjere informacijske sigurnosti. Proaktivne su one mjere koje se primjenjuju prije nego se dogode sigurnosni incidenti i cilj im je spriječiti njihovu pojavu. Ova skupina mjera predstavlja suštinu sustava informacijske sigurnosti, a sastoji se od sigurnosne politike i provedbenih akata, organizacijskih i tehničkih normi, procjene i upravljanja rizikom te periodičnih revizijskih procesa.

U donjem lijevom dijelu slike 6. prikazane su reaktivne mjere. Reaktivne mjere su one koje se primjenjuju nakon što se dogode sigurnosni incidenti te im je cilj izvršiti procjenu i oporavak od štete uzrokovane tim incidentima, revidirati organizacijske i tehničke dijelove sustava u svrhu budućeg sprječavanja sličnih incidenata te provesti prikupljanje dokaznog materijala za otkrivanje i zakonsko procesuiranje počinitelja određenog sigurnosnog incidenta.

Dobro organiziran sustav upravljanja informacijskom sigurnošću jedne zemlje ima neposredno preventivni utjecaj na ukupno stanje sigurnosti zemlje te čini temelj za razvoj učinkovitih represivnih postupaka suvremenog informacijskog društva. [20]

4.3. Pristup zaštiti i sigurnosti

Informacijsko-komunikacijska sigurnost je jedan od najvažnijih uvjeta za opću sigurnost u društvu i osobnu sigurnost građana te za sigurnost poslovanja. S jedne strane je u pitanju funkcioniranje svih struktura države i društva koja je važna za sigurnost svakog građana, dok se s druge strane radi o ostvarivanju slobode i prava građana i njihovu statusu u društvu i položaju prema državnoj i poslovnoj strukturi.

Polazište za ostvarivanje informacijske sigurnosti može se naći u međunarodnim i nacionalnim propisima. Osnovno je da su informacije u službi čovjeka, njegove slobode, sigurnosti i napretka te da ostvarivanje informacijske sigurnosti znači i stvaranje uvjeta sigurnosti čovjeka i građana.

Informacijski sustavi se grade da bi djelovali u skladu s jednom od temeljnih postavki Ustava RH, koja glasi: „Čovjekova je sloboda i osobnost nepovrediva.“[27] [13]. „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te

[27] Ustav RH, članak 22., NN 05/14

nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovog prikupljanja.“[28] [10]

Uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca, voditelj obrade i izvršitelj obrade provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uključujući prema potrebi:

a) pseudonimizaciju[29] i enkripciju[30] osobnih podataka
b) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade
c) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta
d) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade. [14]

Pristup informacijsko-komunikacijskoj sigurnosti u Hrvatskoj i izgradnja sustava informacijske sigurnosti usklađuje se s pristupom i standardima Europske unije i NATO-a, pa se u skladu s time daje i polazna definicija prema kojoj „sustav informacijske sigurnosti obuhvaća ljude, procese, organizaciju i tehnologiju.“

[28] Ustav RH, članak 37. (NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14)

[29] Pseudonimizacija znači obrada osobnih podataka na način da se osobni podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se takve dodatne informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi

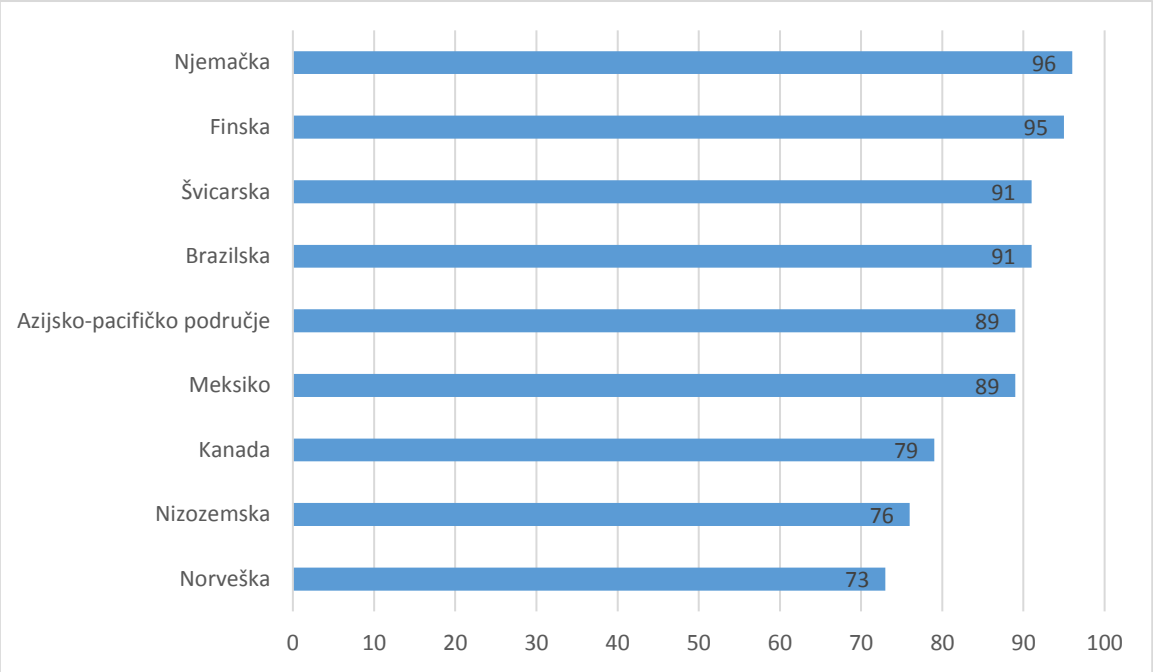
[30] Enkripcija ili šifriranje je proces u kriptografiji kojim se vrši izmjena podataka tako da se poruka, odnosno informacije, učine nečitljivim za osobe koje ne posjeduju određeno znanje

5. DOSADAŠNJA ISTRAŽIVANJA PRIMJENE BUSINESS INTELLIGENCEA U SVIJETU I U HRVATSKOJ

Istraživanja o primjeni business intelligencea prisutna su u svijetu godinama i u literaturi temeljito i opsežno prikazana. Uvid u rezultate istraživanja pruža jasnu sliku o primjeni business intelligencea u svijetu. Journal of Competitive Intelligence and Management, posvetio je, primjerice, 2004. niz posebnih brojeva (special issue) „studijama država“ (country studies) u kojima je istražena geneza business intelligencea u pojedinim državama te navedeni rezultati primjene u nacionalnim gospodarstvima. Sveobuhvatno istraživanje na svjetskoj razini provedeno je godinu kasnije. Već navedeni „Globalni obavještajni savez,“ 2005. proveo je istraživanje u 18 država diljem svijeta na uzorku od 287 kompanija. Rezultati istraživanja su pokazali da se business intelligence u svijetu primjenjuje u rasponu od 73% kompanija, što je slučaj u Norveškoj, do 96% u Saveznoj Republici Njemačkoj. Na svjetskoj razini prosjek je 87% kompanija koje primjenjuju business intelligence (vidi grafikon 2.)

Pionirsko istraživanje o primjeni business intelligencea u hrvatskom gospodarstvu 2005. proveli su Darko Ivančević i Mislav Jurišić (Ivančević i Jurišić, 2005.; Jurišić, 2005.). Istraživanje je provedeno na uzorku od 85 tvrtki uporabom online ankete. Na upitnik je odgovorilo 23 tvrtke. Rezultati istraživanja su pokazali da 9% tvrtki ima zaseban business intelligence odjel (2 tvrtke), dok se 44% tvrtki povremeno unutar ostalih poslovnih aktivnosti bavi business intelligence područjem. Preostalih 47% tvrtki ni na koji način se nije bavilo business intelligenceom. U sklopu izrade završnog rada na specijalističkom poslijediplomskom studiju „Poslovno upravljanje - MBA“ na zagrebačkom Ekonomskom fakultetu, istraživanje o primjeni business intelligencea 2010. proveo je i Ognjen Zebić (Zebić, 2010.). Istraživanje je provedeno uporabom strukturiranog anketnog upitnika na uzorku od 84 hrvatska poduzeća. Odziv na anketu je bio 50%. Prema rezultatima istraživanja, 50% hrvatskih tvrtki ima odjel zadužen za business intelligence, odnosno prikupljanje i analizu poslovnih informacija. [10]

Graf 2. Primjena „business intelligencea“ u kompanijama u svijetu (2012.)



Na grafikonu 2. može se primijetiti da su na vodećim mjestima razvijene zemlje svijeta koje govore kolika je zapravo važnost primjena BI u tvrtkama. U Hrvatskoj je primjena BI u tvrtkama oko 24% što jako zaostaje za svijetom. Svakako bi se trebala probuditi svijest vezana uz važnost BI odjela koja na mikro razini olakšava posao tvrtkama i donosi im uspjeh, dok na makro razini unaprjeđuje gospodarstvo.

6. PRIMJENA BUSINESS INTELLIGENCEA U HRVATSKOM GOSPODARSTVU: REZULTATI ISTRAŽIVANJA U 2011. GODINI

6.1. Metodologija rada

Empirijsko istraživanje na temu business intelligencea u tvrtkama, koje posluju na teritoriju Republike Hrvatske, provedeno je u suradnji Odsjeka za sociologiju Filozofskog fakulteta Sveučilišta u Zagrebu i poslovnim tjednikom Lider. S namjerom detektiranja upoznatosti sa sustavom business intelligencea, primjenom sustava te planovima vezanim za budućnost primjene business intelligencea, pozivi za ispunjavanje online upitnika s popratnim pismom te izjavom o suglasnosti za sudjelovanje u istraživanju, poslani su elektroničkom poštom na adrese 1.000 najvećih tvrtki koje posluju u Republici Hrvatskoj. Baza 1.000 najvećih tvrtki, koja ujedno čini i populaciju istraživanja, objavljena je u lipnju 2010. u posebnom prilogu „1000 najvećih“ koji je publiciran uz 247. broj poslovnog tjednika Lider.

Osnovni kriterij po kojemu su rangirane tvrtke bio je ukupan prihod tvrtke ostvaren u 2009. S namjerom prikupljanja što većeg broja odgovora i postizanja reprezentativnosti uzorka, pozivi za sudjelovanje u istraživanju i ispunjavanje online upitnika te naknadni podsjetnici na poziv, slani su u nekoliko navrata. Istraživanje je započelo u mjesecu listopadu 2010. kada su prvi put poslani pozivi za sudjelovanje. Upravo u prvom ciklusu provedbe istraživanja, koji je završen u prvoj polovini studenoga 2010, pristigla je glavnina odgovora, njih 170. Nakon završetka prvog ciklusa istraživanja napravljene su projekcije kojima su utvrđene potrebne proporcije za regiju u kojoj je sjedište tvrtke (sjeverozapadna Hrvatska, središnja i panonska i Jadranska Hrvatska) i veličinu tvrtke (broj zaposlenih), a koje bi zadovoljavale stanje na populaciji 1.000 najvećih tvrtki koje posluju na teritoriju RH. Drugi ciklus istraživanja započeo je pri kraju veljače 2011. i zaključen je u prvoj polovini travnja 2011. godine čime je završen proces prikupljanja podataka. Prikupljena su ukupno 233 odgovora,

što označava povrat od 23,30%. Struktura odaziva aproksimativna je prethodno izvršenim projekcijama, ali su rezultati dodatno ponderirani kako bi bili zadovoljeni parametri populacije, a s namjerom donošenja pouzdanijih zaključaka o populaciji 1.000 najvećih tvrtki koje posluju na području Republike Hrvatske. Od 233 tvrtke koje su sudjelovale u istraživanju njih 168 posluje u sjeverozapadnoj Hrvatskoj, 30 u istočnoj, a 35 u južnoj Hrvatskoj. Prema veličini tvrtke u uzorku najviše su zastupljene tvrtke srednje veličine - 101, potom velike - 83, a malih tvrtki koje su se odazvale istraživanju je ukupno 49.

Tablica 1: Struktura odaziva tvrtki (neponderirani podatci)

	Veličina tvrtke (neponderirani podatci)						Ukupno	
	Mala		Srednja		Velika			
Sjedište tvrtke	n	(%)	n	(%)	n	(%)	n	(%)
Sjeverozapadna Hrvatska	39	23%	68	41%	61	36%	168	100%
Središnja i Panonska Hrvatska	4	13%	13	43%	13	43%	30	100%
Jadranska Hrvatska	6	17%	20	57%	9	26%	35	100%

Napomena: Podatci prikupljeni empirijskim istraživanjem.

Tablica 2: Struktura odaziva tvrtki (ponderirani podatci)[31]

	Veličina tvrtke (ponderirani podatci)						Ukupno	
	Mala		Srednja		Velika			
Sjedište tvrtke	n	(%)	n	(%)	n	(%)	n	(%)
Sjeverozapadna Hrvatska	34	22%	61	40%	58	38%	153	100%
Središnja i Panonska Hrvatska	4	13%	14	44%	14	44%	32	100%
Jadranska Hrvatska	8	17%	27	56%	13	27%	48	100%

Napomena: Podatci prikupljeni empirijskim istraživanjem.

Sa svrhom stjecanja što boljeg uvida u ovaj, kod nas prilično neistražen aspekt poslovanja koji postaje sve važnija karika u procesu donošenja poslovnih odluka, konstruiran je anketni upitnik s 27 pitanja. Upitnik je tematski podijeljen na tri dijela:

1. poznavanje i primjena business intelligence aktivnosti u praksi,

2. planovi tvrtke vezani uz business intelligence aktivnosti te mišljenje o planovima (implementacija, unapređenje, institucionalizacija, i sl.)

3. Opći podatci o tvrtki

Za potrebe ovog rada predstavljeni su oni podatci za koje se smatralo da su ključni za dobivanje realne slike stanja u 1.000 najvećih tvrtki koje posluju na području RH, a koje su u većoj ili manjoj mjeri upoznate s aktivnostima business intelligencea. Ističe se da su svi idući navedeni rezultati dobiveni statističkom obradom ponderiranih podataka te se u nastavku teksta podatci o regionalnoj zastupljenosti, kao i podatci o veličini tvrtke, razlikuju od onih iznesenih za strukturu odaziva (Tablica 1. i Tablica 2.). Statistička značajnost povezanosti dviju varijabli s više od dvije kategorije provjeravana je hi-kvadrat testom, uz koji je kao standardizirana mjera asocijacije (jačine povezanosti) navođen Cramerov V. Razina statističke značajnosti određena je na $p<0.05$. Svi rezultati dobiveni

[31] "ponderiranje“ ili vaganje, postupak kojim se određuje odgovarajuća vrijednost pojedinih veličina prilikom izračunavanja srednje vrijednosti.

su statističkim obradama u statističkom paketu SPSS (Statistical Package for the Social Science).

6.2. Rezultati istraživanja

Iako posljednjih nekoliko godina business intelligence postaje neizostavan mehanizam u poslovanju sve većeg broja tvrtki, način njegove primjene, doprinosi od primjene, mišljenja o business intelligenceu, planovi vezani uz budućnost business intelligencea i slično, i dalje su prilična nepoznanica, ne samo široj javnosti, nego i onim dijelovima društva koji su znatno više involvirani u gospodarska zbivanja u Hrvatskoj. Jedan od primarnih ciljeva istraživanja bio je saznati primjenjuju li se u hrvatskim tvrtkama aktivnosti business intelligencea. Nadalje, željelo se utvrditi koje poslovne informacije tvrtke prikupljaju i u kojoj mjeri to čine te u kojoj su regiji tvrtke najbolje upoznate s business intelligenceom, koje su veličine, kojeg tipa djelatnosti i kako one procjenjuju vlastitu konkurentnost i konkurentnost područja u kojem posluju.

Polazna, a ujedno i ključna hipoteza istraživanja, jest da većina tvrtki koje posluju na teritoriju RH, ne primjenjuje kontinuirano business intelligence kao institucionaliziranu sustavnu poslovnu funkciju.

Izvedene hipoteze su:

- primjena business intelligence aktivnosti nije jednako zastupljena u svim regijama;
- primjena business intelligence aktivnosti zastupljenija je u velikim tvrtkama;
- primjena business intelligence aktivnosti nije jednako zastupljena u svim djelatnostima;
- primjena business intelligence aktivnosti zastupljenija je u tvrtkama koje sebe smatraju konkurentnijima na tržištu.

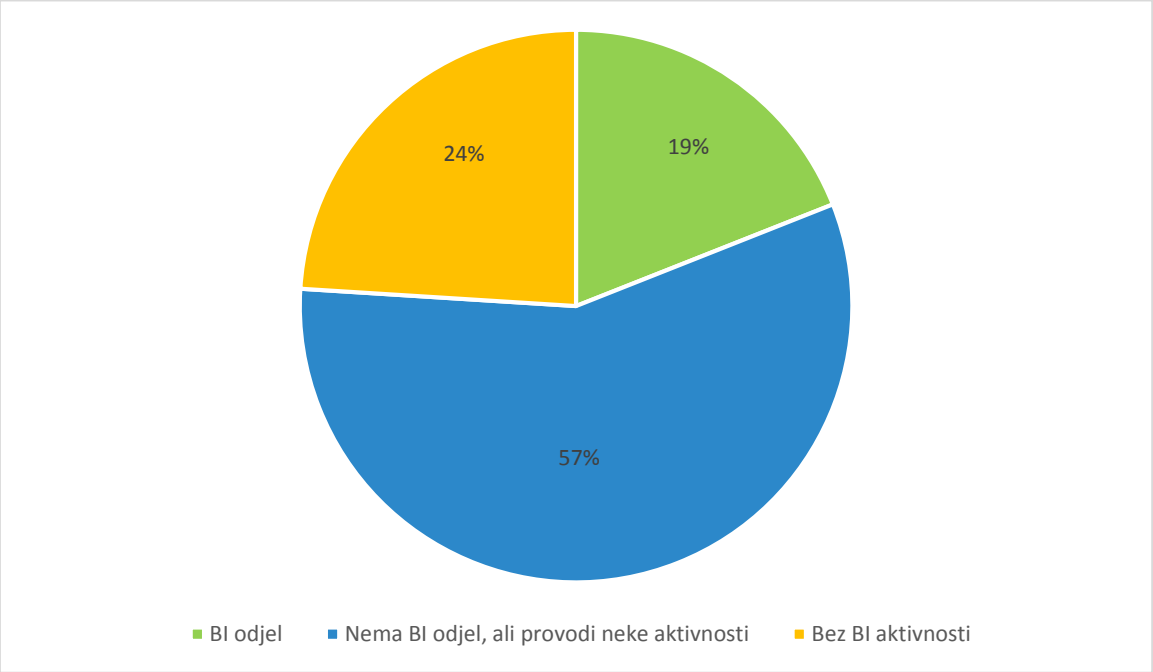
Na temelju dobivenih rezultata možemo zaključiti kako je polazna hipoteza o primjeni business intelligencea u tvrtkama koje posluju na teritoriju RH potvrđena. Premda većina tvrtki, njih 57%, primjenjuje neke od aktivnosti business intelligencea, institucionalizirani odjel koji se bavi business intelligence aktivnostima ima tek 19% tvrtki, što ide u prilog iznesenim pretpostavkama (vidjeti grafikon 3).

Uzme li se u obzir važnost ovih aktivnosti za poslovanje tvrtke, ne ohrabruje činjenica kako se među 1.000 najvećih tvrtki, nalazo tako mali broj njih s institucionaliziranim odjelom. Za usporedbu, zastupljenost institucionaliziranih odjela u tvrtkama pojedinih zemlja, kao što je već ranije u tekstu istaknuto, kreće se od 96% u Njemačkoj, 95% u Finskoj, 91% u Švicarskoj i Brazilu, 89% u Meksiku, itd. Najviše od svega treba zabrinjavati činjenica kako gotovo jedna četvrtina (24%) od 1000 najvećih tvrtki, ne primjenjuje nikakve aktivnosti iz ovog sustava. Međutim, valja istaknuti postojanje velikog broja onih koje primjenjuju neke od aktivnosti business intelligencea.

Kako bi se ponudio bolji uvid u primjenu business intelligence aktivnosti unutar Hrvatske, istraženi su neki opći podatci o tvrtkama koje (ne)primjenjuju navedene aktivnosti. S obzirom na regiju u kojoj posluju tvrtke, nema statistički značajne razlike u primjeni business intelligence aktivnosti čime je opovrgnuta prethodno iznesena teza o regionalnim razlikama (Hi-kvadrat test, $x2 = 3.626$, $p=0.727$).

Ipak, iz postotaka se može vidjeti kako se najveći udio tvrtki s institucionaliziranim odjelom za business intelligence aktivnosti te tvrtki koje primjenjuju neke od aktivnosti ovog sustava nalazi u sjeverozapadnoj regiji (78%), što je posve razumljivo jer se u ovoj regiji nalazi glavni grad, kao i dvije od četiri najrazvijenije županije Republike Hrvatske. Nadalje, u ovoj regiji je najveći broj registriranih poslovnih subjekata, a od 1.000 najvećih iz populacije istraživanja ovdje ih je čak 655. U južnoj regiji se nalazi najveći broj tvrtki koje ne primjenjuju nikakve business intelligence aktivnosti (31%).

Grafkon 3: Prikaz primjene business intelligence aktivnosti u tvrtkama[32]

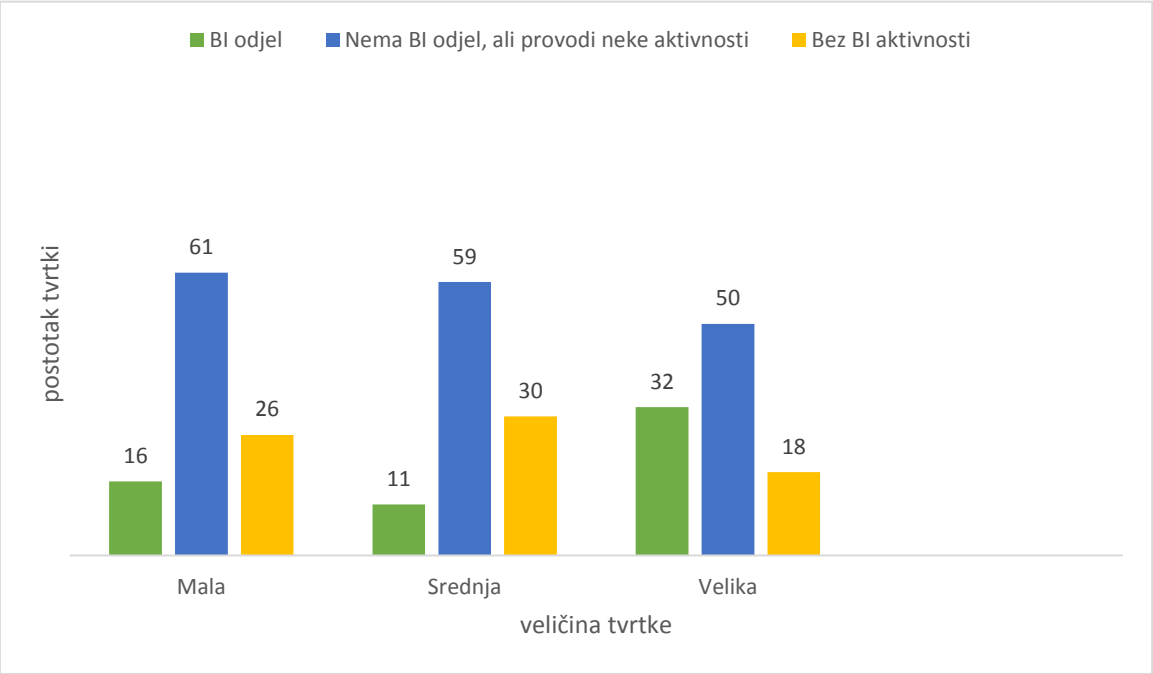


Izvor: Podatci prikupljeni istraživanjem

Između tvrtki postoji statistički značajna razlika s obzirom na veličinu tvrtke i primjenu business intelligence aktivnosti (Hi-kvadrat test, x2 =17.439, p=0.008). Očekivano, u velikim tvrtkama je najveći broj institucionaliziranih odjela za business intelligence aktivnosti (32%), čime je potvrđena hipoteza.

[32] U orginalnom obliku ova varijabla sastojala se od dvije odvojene varijable: a)„Primjenjuju li se u Vašoj tvrtki aktivnosti upravljanja poslovnim informacijama“: (1) da; (2) ne; (3) ne znam i b) „Postoji li unutar Vaše tvrtke institucionalizirani odjel za upravljanje poslovnim informacijama“: (1) da; (2) ne; (3) ne znam. Za potrebe ovog rada i preglednosti, dvije čestice su spojene u jednu.

Grafikon 4: Prikaz primjene business intelligence aktivnosti u tvrtkama s obzirom na veličinu tvrtke[33]



Izvor: Podatci prikupljeni istraživanjem

Iznenađuju dobiveni rezultati, da se u malim tvrtkama i tvrtkama srednje veličine podjednako primjenjuju neke aktivnosti business intelligencea.

[33] „Tip tvrtke prema veličini“: (1) mala-20%; (2) srednja-44%; (3) velika-46%.

Tablica 3: Prikaz primjene business intelligence aktivnosti u tvrtkama s obzirom na djelatnost tvrtke

	BI odjel		**Nema BI odjel, ali provodi neke aktivnosti**		**Bez BI aktivnosti**		**Ukupno**	
Djelatnost tvrtke	n	(%)	n	(%)	n	(%)	n	(%)
Graditeljstvo i komunalno gospodarstvo	2	11%	13	68%	4	21%	19	100%
Bankarstvo i financije	6	24%	15	60%	4	16%	25	100%
Industrija	6	14%	28	67%	8	19%	42	100%
Poljoprivreda, prehrambena industrija i šumarstvo	3	27%	3	27%	5	46%	11	100%
Promet i veze	2	13%	9	56%	5	31%	16	100%
Trgovina	11	20%	30	53%	15	27%	56	100%
Turizam	1	10%	5	50%	4	40%	10	100%
Informacije i komunikacije	11	27%	22	55%	7	18%	40	100%

Napomena: Podatci prikupljeni istraživanjem

Osnovna djelatnost najvećeg broja tvrtki nalazi se u sektoru trgovine, industrije te informacija i komunikacija. Najmanji broj tvrtki nalazi se u sektoru turizma te poljoprivrede, prehrambene industrije i šumarstva. Business intelligence aktivnostima najviše se služe tvrtke u sektoru bankarstva i financija (84%) te u sektoru informacija i komunikacija (82%). Budući da se radi o najbrže rastućim sektorima čije se poslovanje u velikoj mjeri temelji na informacijama, ovo je posve očekivan nalaz. U sektoru turizma i u sektoru poljoprivrede, prehrambene industrije i šumarstva najmanji broj tvrtki primjenjuje

business intelligence aktivnosti. Između tvrtki ne postoji statistički značajna razlika prema tipu djelatnosti i primjeni business intelligence aktivnosti (Hi-kvadrat test, x2 =17.007, p=0.711).

Tablica 4: Prikaz primjene business intelligence aktivnosti u tvrtkama s obzirom na procjenu konkurencije u području poslovanja

	BI odjel		**Nema BI odjel, ali provodi neke aktivnosti**		**Bez BI aktivnosti**		**Ukupno**	
Konkurencija u području poslovanja	n	(%)	n	(%)	n	(%)	n	(%)
Slaba	3	33%	2	22%	4	45%	9	100%
Srednja	6	20%	15	50%	9	30%	30	100%
Jaka	33	18%	111	60%	42	22%	186	100%
Ne mogu procijeniti	1	20%	2	40%	2	40%	5	100%

Napomena: Podatci prikupljeni empirijskim istraživanjem.

Između brojnih pitanja na koje je u istraživanju tražen odgovor bilo je i ono koje dovodi u odnos procjenu konkurencije i konkurentnosti pojedine tvrtke i razinu primjene business intelligence aktivnosti. Naime, konkurencija u onom području poslovanja u kojem tvrtka posluje generalno se percipira jakom, s time da statistički značajna razlika u primjeni business intelligence aktivnosti, s obzirom na procjenu konkurencije u području poslovanja, ne postoji (Hi-kvadrat test, x^2=6.387, p=0.381). Valja istaknuti kako najveći broj tvrtki, koje primjenjuju neke business intelligence aktivnosti, percipira konkurenciju u području poslovanja jakom, odnosno vrlo jakom.

Što se tiče same procjene konkurentnosti tvrtke, najveći broj tvrtki smatra kako je njihova konkurentnost jaka, odnosno vrlo jaka. Statistički značajna

razlika u primjeni business intelligence aktivnosti, s obzirom na procjenu konkurentnosti tvrtke. Važno je zamijetiti kako nema tvrtki s institucionaliziranim business intelligence odjelom, a koje konkurentnost svoje tvrtke percipiraju slabom. Najveći broj tvrtki, koje primjenjuju neke od business intelligence aktivnosti, smatra konkurentnost svoje tvrtke jakom, odnosno vrlo jakom. Svakako je zanimljiv nalaz kako postoji znatan broj tvrtki koje ne primjenjuju nikakve business intelligence aktivnosti, dok konkurentnost tvrtke percipiraju jakom. Među tvrtkama tog tipa nailazi se na najveći broj onih koje se bave trgovinom, industrijom te poljoprivredom, prehrambenom industrijom i šumarstvom.

Tablica 5: Prikaz primjene business intelligence aktivnosti u tvrtkama s obzirom na procjenu konkurentnosti tvrtke

	BI odjel		**Nema BI odjel, ali provodi neke aktivnosti**		**Bez BI aktivnosti**		**Ukupno**	
Konkurencija u području poslovanja	n	(%)	n	(%)	n	(%)	n	(%)
Slaba	0	0%	1	33%	2	67%	3	100%
Srednja	4	10%	25	59%	13	31%	42	100%
Jaka	35	21%	98	57%	39	22%	172	100%
Ne mogu procijeniti	3	18%	6	57%	2	24%	11	100%

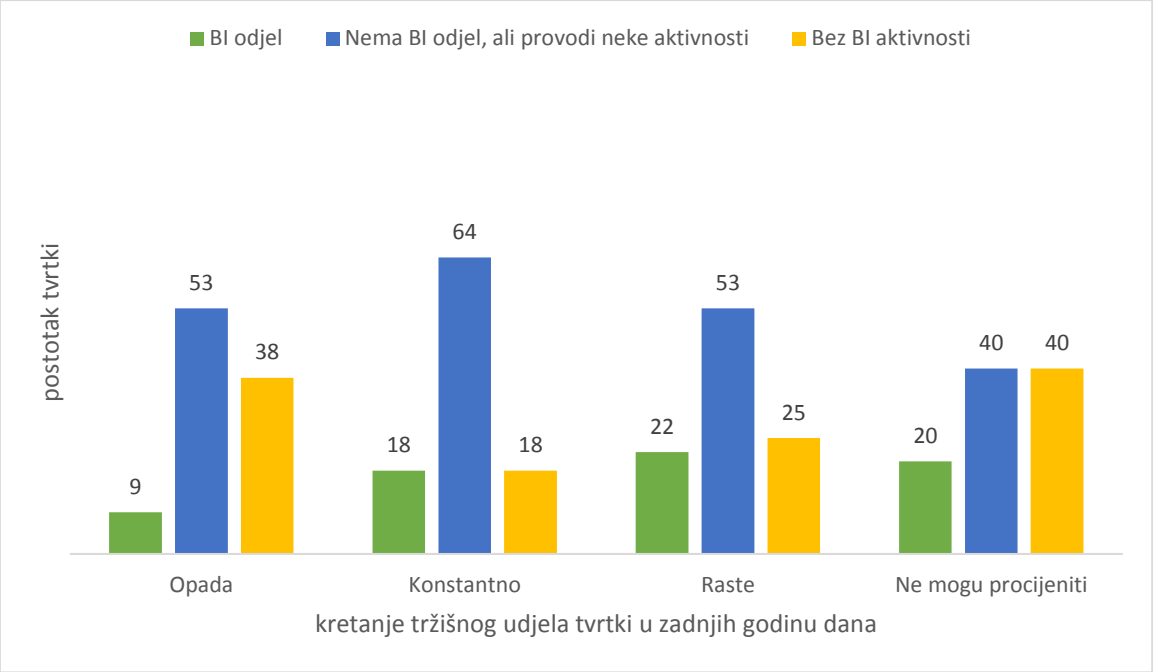
Napomena: Podatci prikupljeni empirijskim istraživanjem.

Statistički značajna razlika u primjeni business intelligence aktivnosti, s obzirom na kretanje tržišnog udjela tvrtke u posljednjih godinu dana, ne postoji (Hi-kvadrat test, $x^2=9.533$, $p=0.146$).

Uočljivo je kako tržišni udio u najmanjoj mjeri pada upravo u tvrtkama koje imaju institucionalizirani business intelligence odjel, dok u najvećoj mjeri

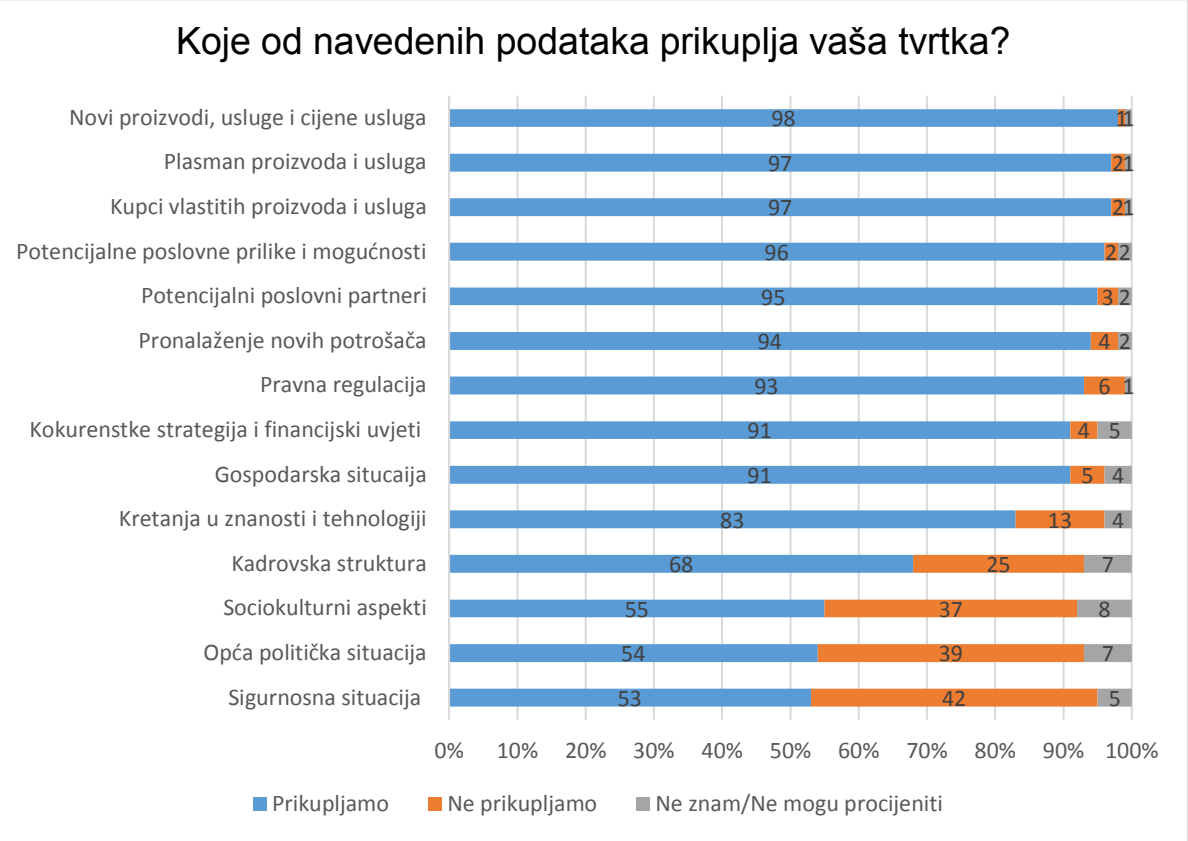
raste, odnosno ostaje konstantan u tvrtkama koje primjenjuju barem neke od business intelligence aktivnosti.

Grafikon 5: Prikaz primjene business intelligence aktivnosti u tvrtkama s obzirom na kretanje tržišnog udjela tvrtke u posljednjih godinu dana



Kada je riječ o business intelligence aktivnosti, odnosno podatcima koje tvrtke prikupljaju, evidentno je kako je većina tvrtki usmjerena ka prikupljanju podataka koji su povezani s konkurentima, potencijalnim poslovnim suradnicima te krajnjim potrošačima roba i usluga, kako postojećima tako i onima koje se nastoji pridobiti. Od 76% tvrtki koje primjenjuju neke business intelligence aktivnosti ili koje pak imaju institucionaliziran odjel, tim kategorijama podatka zaokupljeno je njih više od 90%. U osnovnoj kategorizaciji podatka koji su ključni za business intelligence uz podatke o tržištu i konkurenciji neizostavni su i podaci koji se odnose na okruženje u kojem djeluje poslovni subjekt (Bilandžić, 2008:92). Upravo u posljednjoj kategoriji najjasnije se uočava disparitet u prioritetima koje tvrtke daju određenim tipovima podataka. Tvrtke su najviše zaokupljene prikupljanjem podataka o gospodarskoj situaciji, pravnoj regulaciji, prvenstveno pravnoj regulaciji poslovanja, a velik značaj pridaju i kretanju na području tehnologije i znanosti.

Grafikon 6: Kategorije podataka koje prikupljaju tvrtke koje primjenjuju neke business intelligence aktivnosti ili imaju institucionalizirani business intelligence odjel



Zanimljivo je istaknuti kako u prosjeku tek polovina tvrtki, koje primjenjuju business intelligence, prikuplja podatke o općoj političkoj situaciji, sigurnosnoj situaciji i sociokulturnim aspektima okruženja u kojem posluju. U sklopu nacionalnog gospodarstva i poslovanja na relativno malom tržištu Republike Hrvatske, podaci o okruženju u kojem posluje tvrtke možda i nisu presudni za osvajanje većeg tržišnog udjela i postizanja konkurentske prednosti poslovnog subjekta, no s ulaskom na mnogo veće, sociokulturno raznolikije te konkurentnije tržište Europske unije, upravo ovi segmenti postaju jedni od ključnih za konkurentnije poslovanje pojedine tvrtke. Zanemariti sociokulturni aspekt, političku ili sigurnosnu situaciju u zemlji u kojoj se želi poslovati,

odnosno prodati neku robu ili usluge, značilo bi tržišnu pustolovinu s neizvjesnim rezultatima poslovanja. Za svaki poslovni uspjeh i stjecanje konkurentske prednosti potreban je stalni angažman na svim područjima koji utječu na poslovanje, to znači stalan monitoring tržišta, konkurencije i okruženja u kojem se posluje ili se želi poslovati.

Na kraju je bitno istaknuti da većina tvrtki, koje imaju institucionalizirani odjel za business intelligence aktivnosti ili primjenjuju neke aktivnosti iz ovog sustava, smatra kako taj sustav znatno pridonosi u predviđanju i upravljanju rizicima, prepoznavanju isplativih tržišnih niša, prepoznavanju snage i slabosti konkurenata, razvijanju novih profitabilnih proizvoda, praćenju vanjskih faktora koji utječu na poslovanje (politički, ekonomski, sociokulturni, tehnološki), povećanju produktivnosti, boljoj komunikaciji i suradnji unutar poduzeća, većoj sigurnosti vlastitih informacija, povećanju tržišnog udjela, ostvarenju većeg profita, uštedi vremena, razvitku, održavanju i upravljanju odnosa s krajnjim potrošačima, upravljanju ljudskim resursima, profiliranju poslovnih partnera. One tvrtke koje ne primjenjuju ni ma kakve aktivnosti iz sustava business intelligence, kao glavne razloge neprimjene navode prvenstveno nedovoljno poznavanje funkcioniranja ovog sustava. Bitan razlog je i nepostojanje kompetentnog kadra kao i nedostatna financijska sredstva.

Utjecaj stranog obavještajnog djelovanja na procese donošenja odluka u Republici Hrvatskoj uključuje i elemente hibridnog djelovanja u plasiranje tzv. „lažnih vijesti“ u javni prostor i pokušaje narušavanja međunarodnog ugleda. U sklopu hibridnog djelovanja u hrvatski medijski i informativni prostor nastoje se ubaciti lažne ili iskrivljene vijesti u kojima se Republiku Hrvatsku, EU i NATO prikazuje u negativnom svjetlu te se želi utjecati na stabilnost hrvatskih institucija, regionalnog okruženja i euroatlantskog i europskog zajedništva.

Sigurnosno-obavještajna agencija (SOA) ima jednu od zadaća zaštititi gospodarski sustav Republike Hrvatske prikupljanjem i analizom podataka iz područja gospodarstva o temama koje mogu utjecati na nacionalnu sigurnosti i gospodarske interese unutar države. SOA također prati sigurnosne, gospodarske i financijske procese koji mogu utjecati na hrvatska gospodarstva

u inozemstvu, kao i procese i aktivnosti koje bi mogli ugroziti sigurnost hrvatskih gospodarskih subjekata u nestabilnim područjima svijeta. Stoga, izvješća SOA-e o stanju sigurnosti su od velike koristi za hrvatsko gospodarstvo i za stabilnost poslovanja kako u inozemstvu, tako i unutra Republike Hrvatske.

7. ZAKLJUČAK

Poslovno-obavještajna djelatnost je sustavno i plansko djelovanje koje pomaže donošenju poslovnih odluka i procesa unutar poduzeća. Temelji se na etičnosti i djeluje u skladu sa zakonom te se zbog toga ne može staviti u kontekst špijunaže. Prikupljanje i analiza podataka prikupljen na etičan način glavna je zadaća poslovno-obavještajne djelatnosti te, bivajući takvom, opskrbljuje poduzeće njegovom najvećom imovinom, informacijama. Te informacije prikupljene iz različitih izvora analiziraju se na različite načine i daju rezultate koji su potrebni rukovodećim organima unutar poduzeća za donošenje poslovnih odluka.

Na današnjem tržištu prepunom novih ideja vrlo je teško opstati bez postavljanja ciljeva i planova, kao i razrade strategija napada i obrane. Za ostvarivanje postavljenih planova i ciljeva veliku ulogu ima analiziranje okoline poduzeća, formuliranje i implementiranje svoje strategije. Kontinuirano praćenje strateškog menadžmenta neophodno je za rano otkrivanje odstupanja od zadaća i planova te se sukladno tome poduzimaju korektivne mjere. Takav proces je dokazani ključ poslovne uspješnosti.

Poslovno-obavještajno djelovanje predstavlja ključan resurs svakom modernom, proaktivnom i uspješnom poduzeću na tržištu. Takvo djelovanje prisutno je i u hrvatskim poduzećima. Istraživanja su pokazala kako relativno velik broj srednjih i velikih poduzeća ima odjele poslovno-obavještajne djelatnosti te se njima koristi u svrhe savjetovanja menadžmenta i prepoznavanje ključnih informacijskih potreba kako bi se osigurala dodatna konkurentska prednost hrvatskih poduzeća.

Poslovno obavještavanje u Republici Hrvatskoj se, u odnosu na svijet, nalazi na stupnju razvoja koji zahtjeva dodatna ulaganja i interes kako bi se širilo i bilo zastupljenije u hrvatskom gospodarstvu.

Zaključno, poslovno-obavještajno djelovanje je od velikog značaja poduzećima u modernom poslovanju, koje se najviše ogleda prikupljanjem i

analizom informacija koje u konačnici utječu na donošenje strateških odluka te formulacije i provođenja strategije poduzeća. Hrvatska poduzeća su aktivni korisnici poslovno-obavještajnog djelovanja te se u određenim segmentima navedene discipline ravnopravno nose s velikim poslovno-obavještajnim silama. Kako bi se ono dalje razvijalo i omogućavalo dodatne konkurentske prednosti hrvatskim poduzećima zahtjeva podizanje razine svijesti i dodatna ulaganja.

LITERATURA

Knjige:

[1] Javorović Božidar, Bilandžić Mirko: „Poslovne informacije i business intelligence“, Golden marketing, Zagreb, ISBN: 978-953-212-295-4

[2] Kahaner Larry, Competitive Intelligence: How to Gather, Analyze and Use Information to Move Your Business to the Top, New York, 1996, ISBN: 978-068-484-404-6

[3] Combs Richard E., Moorhead, D. J. Competitive Intelligence Handbook, 1993, ISBN: 978-081-082-606-9

[4] Dedijer Stevan, Opening Plenary Lecture, Business intelligence, Zagreb, 1999., ISBN 978-085-496-520-5

[5] Bernhardt Douglas, Competitive Intelligence: How to acquire and use corporate intelligence and counter-intelligence, 2003, ISBN: 978-027-365-928-0

[6] Kimball Ralph, The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling, 2013., ISBN: 978-111-853-080-1

[7] Klepac Goran, Mršić Leo: Poslovna inteligencija kroz poslovne slučajeve, Liderpress/TimPress, Zagreb, 2006, ISBN: 953-95472-1-0

Stručni i znanstveni radovi i članci:

[8] Bazdan Zdravko, Menadžeri moraju znati: poslovno obavještajna djelatnost kreira najvažniji resurs upravljanja, 2009., JEL klasifikacija: L_{20}

[9] Gonan Božac, M. (2008). SWOT analiza monističkog i dualističkog sustava korporacijskog upravljanja i konvergencija, Ekonomski pregled, Vol.59, No.7-8, str. 376

[10] Čulig Benjamin, Bilandžić Mirko., Business intelligence u Hrvatskom gospodarstvu, JEL klasifikacija L20, M21, 2012.

Zakoni i propisi:

[11] Zakon o tajnosti podataka NN 86/12

[12] Zakon o informacijskoj sigurnosti NN 79/07

[13] Ustav RH, (NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14)

[14] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

[15] Strategija nacionalne sigurnosti RH, (NN 73/17)

Internetski izvori:

[16] Fuld and Company, Inc. The Global Leader in Competitive Intelligence, https://www.fuld.com/, pristupljeno 14.7.2018

[17] Society of Competitive Intelligence Professionals, http://www.scrip.com/, pristupljeno 14.7.2018

[18] Pregled mrežne analitičke obrade (OLAP) - https://support.office.com/hr-hr/article/pregled-mre%C5%BEne-analiti%C4%8Dke-obrade-olap-15d2cdde-f70b-4277-b009-ed732b75fdd6 – pristupljeno 16.7.2018

[19] Sigurnosno-obavještajna agrencija (SOA) - https://www.soa.hr/hr/podrucja-rada/informacijska-sigurnost/ - pristupljeno 20.7.2018

[20] Osnovni podatci vezani uz informatičku sigurnost - http://security.foi.hr/wiki/index.php/Zakoni_Republike_Hrvatske_vezani_uz_informacijsku_sigurnost_i_za%C5%A1titu_podataka – pristupljeno 22.7.2018

POPIS SLIKA, GRAFIKONA I TABLICA

Popis slika:

Popis grafikona:

Popis tablica: