Miha Dvojmoč

Korporativna obveščevalna dejavnost

Praktikum

Univerzitetna založba
Univerze v Mariboru

Univerza v Mariboru

Fakulteta za varnostne vede

Korporativna obveščevalna dejavnost

Praktikum

Avtor

Miha Dvojmoč

Februar 2026

Naslov *Title*
Korporativna obveščevalna dejavnost
Corporate Intelligence

Podnaslov *Subtitle*
Praktikum
Practicum

Avtor *Author*
Miha Dvojmoč
(Univerza v Mariboru, Fakulteta za varnostne vede)

Recenzija *Review*
Branko Lobnikar
(Univerza v Mariboru, Fakulteta za varnostne vede)

Jaroš Britovšek
(Ministrstvo za obrambo Republike Slovenije)

Lektoriranje *Language editing*
Andreja Breznik
(Virtual IN d.o.o.)

Tehnični urednik *Technical editor*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka *Cover designer*
Jan Perša
(Univerza v Mariboru, Univerzitetna založba)

Grafike na ovitku *Cover graphics*
A red and yellow background with lines of light, foto: Adrien, unsplash.com, 2023; Grayscale photo of person standing on train station, foto: Adid Sinclair, unsplash.com, 2018

Grafične priloge *Graphic material*
Vsi viri so lastni, če ni navedeno drugače.
Dvojmoč (avtor), 2026

Založnik *Published by*
Univerza v Mariboru
Univerzitetna založba
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj *Issued by*
Univerza v Mariboru
Fakulteta za varnostne vede
Kotnikova ulica 8, 1000 Ljubljana, Slovenija
https://fvv.um.si, fvv@um.si

Izdaja *Edition*
Prva izdaja

Vrsta publiakcije *Publication type*
E-knjiga

Izdano *Published at*
Maribor, Slovenija, februar 2026

Dostopno na *Available at*
https://press.um.si/index.php/ump/catalog/book/1099

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

005.934(0.034.2)

DVOJMOČ, Miha
Korporativna obveščevalna dejavnost [Elektronski vir] : praktikum / avtor Miha Dvojmoč. - 1. izd. - E-publikacija. - Maribor : Univerza v Mariboru, Univerzitetna založba, 2026

Način dostopa (URL): https://press.um.si/index.php/ump/catalog/book/1099

ISBN 978-961-299-113-5 (PDF)
doi: 10.18690/um.fvv.2.2026
COBISS.SI-ID 267931651

ISBN 978-961-299-113-5 (pdf)

DOI https://doi.org/10.18690/um.fvv.2.2026

Cena *Price* Brezplačni izvod

Odgovorna oseba založnika *For publisher* prof. dr. Zdravko Kačič, rektor Univerze v Mariboru

Citiranje *Attribution* Dvojmoč, M. (2025). *Korporativna obveščevalna dejavnost: Praktikum.* Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.fvv.2.2026

Univerzitetna založba
Univerze v Mariboru

Kazalo

Univerzitetna založba
Univerze v Mariboru

1 Predgovor

Praktikum je nastal kot rezultat nenehnega znanstvenega preučevanja in raziskovanja ter poučevanja in izvajanja vaj na Fakulteti za varnostne vede Univerze v Mariboru pri predmetu Korporativna obveščevalna dejavnost. Predmet je del izbirnega študijskega programa v 2. letniku magistrskega študija. Praktikum predstavlja zbirko vsebinsko zaokroženih poglavij in vprašanj, na podlagi katerih lahko študent preveri svoje znanje in poglobi razmišljanje. Vprašanja so teoretske narave in se razlikujejo po zahtevnosti.

Celoten praktikum je razdeljen na sedem tematskih sklopov, na koncu vsakega pa so teoretska vprašanja za ponovitev. Vprašanja so zastavljena z namenom, da študent osvežI pridobljeno znanje, hkrati pa spodbudijo poglobljeno in logično razmišljanje. Vsako poglavje je zasnovano tako, da študentu predstavi poglobljeno tematiko ter da pridobi znanje, potrebno za uspešno zaključitev predmeta, opravo izpita in vaj. Pomembno je, da to znanje ostane tudi po končanem študiju.

Cilj praktikuma je, kot že omenjeno, predvsem to, da študenti pridobijo znanje o korporativni obveščevalni dejavnosti ter da se preveri, kako dobro poznajo, razumejo in obvladajo to področje.

Univerzitetna založba
Univerze v Mariboru

2 Koncept korporativne obveščevalne dejavnosti

2.1 Obveščevalna dejavnost

Šaponja (1999, str. 9) je razložil potrebo po obveščevalni dejavnosti. Zapisal je: "Človek se sprva ni ukvarjal z definicijami. V vsakdanjem življenju, že v praskupnosti, je zelo hitro spoznal prednosti dobre obveščenosti in predvidevanja. To mu je prinašalo večji uspeh pri lovu, zmage v bojih in vojnah z drugimi plemeni. Sposobnost predvidevanja in dobra obveščenost sta mu omogočali lažje in boljše prilagajanje novemu okolju, večjo uspešnost in preživetje."

Obveščevalna dejavnost uporabniku prinaša različne prednosti. V preteklosti je bil to uspeh pri lovu, v današnjem času pa prednosti pri nacionalni varnosti ali gospodarskem uspehu. Šaponja (1999, str. 9–10) razjasni tudi, zakaj se je dejavnost materializirala v institucionalnem smislu. "Da bi človek svojo prednost pred drugimi in svojo varnost še povečal, je organiziral obveščevalno dejavnost v urejen sistem zbiranja, hranjenja in obdelave podatkov. Za to dejavnost je zadolžil ljudi, ki so se ukvarjali samo s tem – začel je organizirati obveščevalno in varnostno službo."

Ta zgodovinska izkušnja je privedla do formalne organizacije obveščevalnih struktur, kar danes predstavlja osnovo tako državne kot korporativne obveščevalne dejavnosti.

Obveščevalna dejavnost človeštvo spremlja že od samih začetkov civilizacije. Že v starodavnih državah, kot so Egipt, Babilon in Kitajska, so vladarji sistematično uporabljali zbiranje informacij za ohranjanje moči, nadzor nad prebivalstvom in predvidevanje nevarnosti (Dvornik, 1974). Kljub svoji dolgoletni vlogi v zgodovini, je bila obveščevalna dejavnost pogosto obravnavana z moralno zadržanostjo. Že antični misleci so jo dojemali kot dvorezen meč – po eni strani nujno orodje za ohranjanje varnosti države, po drugi pa kot dejavnost, ki vključuje prevaro, manipulacijo in izdajo (Warner, 2014). Takšna percepcija se ohranja tudi v sodobnem času, kjer se obveščevalno delo pogosto znajede na presečišču med nacionalno varnostjo in etičnimi vprašanji (Johnson, 2007). Različni avtorji in strokovnjaki, kot so na primer Andrew (2018), Podbregar (2008), Dvornik (1974) navajajo tudi ogromno različnih primerov uporabe obveščevalne dejavnosti v zgodovini. To pomeni, da je obveščevalna dejavnost prisotna že od nekdaj, njena percepcija v očeh javnosti pa je pretežno negativna. "Obveščevalna dejavnost v ljudeh vzbuja različna čustva. Takšna, kot so izkušnje in vedenja posameznika o njej. Večkrat je mistificirana, mnogi se je izogibajo, včasih tudi ignorirajo. Nekaterim se zdi, da je obveščevalno-varnostna dejavnost daleč stran od njih, druge pa večkrat zajame celo paranoja, da so zlorabljeni v te namene" (Podbregar, 2008, str. 13).

Razumevanje javne percepcije obveščevalne dejavnosti je ključnega pomena za razumevanje sprememb, ki so sledile v sodobni zgodovini, zlasti med hladno vojno in po 11. septembru leta 2001. "Sedanje obdobje lahko označimo kot obdobje konca »hladne vojne«, s tem pa je na nek način tudi konec obdobja ekspanzije obveščevalne dejavnosti, ki je svojo vlogo opravljala v procesu odkrite dominacije velesil. V ospredju so drugi problemi, ki terjajo drugačen pristop, kar se odraža tudi pri vsebini dela obveščevalnih služb. To se je pokazalo tudi po 11. 9. 2001, ko je bilo jasno, da sta se pomembno spremenila oziroma okrepila vloga in pomen obveščevalnih služb, saj si učinkovitega boja proti mednarodnemu terorizmu ter proti drugim oblikam ogrožanja varnosti v sodobnem svetu ni mogoče predstavljati brez ustrezne podpore teh služb, poleg tega pa je jasno, da so obveščevalne službe pomembna in obvezna sestavina sodobne ter prihodnje varnostne arhitekture" (Purg, 2002, str. 7-8).

»Po 11. septembru 2001 se je tudi trend v obveščevalni dejavnosti, ki je potekal od konca hladne vojne, k ekonomsko konkurenčni dejavnosti spremenil in se je spet povečala klasična – državna obveščevalna dejavnost … Trend sprememb obveščevalnih dejavnosti za potrebe podjetij in gospodarstva se je upočasnil.« (Raščan, 2005, str. 47)

Za nadaljnje razumevanje korporativne obveščevalne dejavnosti je najprej treba razjasniti in opredeliti osnovne pojme in definicije obveščevalne dejavnosti.

Sama definicija obveščevalne dejavnosti se razlikuje med različnimi avtorji.

Šaponja (1999, str. 10–12) o obveščevalni dejavnosti govori v širšem in ožjem smislu. »V širšem smislu jo lahko opredelimo kot organizirano pridobivanje novega znanja in informacij o dogodkih, pojavih in procesih v bivalnem ali poslovnem okolju, v naravi, družbi, skratka o vsem, kar se dogaja okrog nas. O obveščevalni dejavnosti govorimo v širšem smislu takrat, kadar obveščevalne organizacije za potrebe odločanja na organiziran in institucionaliziran način zbirajo, analizirajo in posredujejo končne izdelke. Delujejo samo pod pogoji in na načine, ki so dovoljeni vsem državljanom. Govorimo o običajnih načinih zbiranja podatkov, ki vključujejo podatke, ki so javno dostopni. Kadar pa obravnavamo obveščevalno dejavnost, ki jo izvajajo državne institucije, ki imajo zakonska pooblastila, da zbirajo tudi tajne podatke na posebne načine, govorimo o obveščevalni dejavnosti v ožjem smislu.«

Britovšek (2025) je v svojem prispevku razvijal opredelitev pojma obveščevalne dejavnosti. Čeprav je obveščevalni cikel uveljavljen model, ne odraža vedno realnih procesov, saj so ti kompleksni in se težko neposredno prenašajo v prakso. Obveščevalno dejavnost od drugih oblik zbiranja podatkov ločuje predvsem tekmovalno okolje. Cilj je doseči konkurenčno prednost pri odločanju. Protiobveščevalna dejavnost pa nasprotno zmanjšuje zmogljivost tekmecev.

Za lažje razumevanje mednarodne literature in terminologije je koristno poznati tudi angleške izraze in njihovo uporabo v različnih kontekstih. V angleškem jeziku se za obveščevalno dejavnost uporablja izraz "*intelligence*", ki pa v strokovni in znanstveni literaturi nima enoznačnega pomena. Avtorji s področja obveščevalnih študij (*intelligence studies*) poudarjajo, da gre za večpomenski pojem, ki se v praksi in teoriji najpogosteje uporablja v treh med seboj povezanih, vendar vsebinsko ločljivih pomenih (Warner, 2002; Lowenthal, 2019).

Prvič, izraz *intelligence* se nanaša na produkt obveščevalne dejavnosti, torej na najvišjo raven obdelanih informacij v okviru informacijske oziroma obveščevalne piramide. V tem pomenu označuje analitično ovrednotene, interpretirane in kontekstualizirane informacije, ki omogočajo sprejemanje utemeljenih ocen ter prilagajanje odločanja spremenjenim okoliščinam. Takšno razumevanje obveščevalne dejavnosti kot znanja za podporo odločanju je značilno za klasične teoretične pristope k obveščevalni dejavnosti (Lowenthal, 2019).

Drugič, pojem se uporablja za označevanje dejavnosti oziroma procesa, povezanega z načrtovanim in sistematičnim zbiranjem, analiziranjem ter interpretiranjem podatkov. V tem kontekstu obveščevalna dejavnost zajema celoten obveščevalni cikel, ki se praviloma povezuje z delovanjem nacionalnih obveščevalnih in varnostnih struktur, vendar se kot metodološki pristop uporablja tudi zunaj državnega sektorja (Johnson, 2024).

Tretjič, izraz *intelligence* se lahko nanaša na institucionalni oziroma organizacijski vidik, torej na obveščevalno službo ali obveščevalni sistem kot organizirano strukturo. V tem pomenu izraz ne označuje zgolj informacije ali dejavnosti, temveč institucijo, ki je pristojna za izvajanje obveščevalne dejavnosti. Takšna raba pojma je uveljavljena tako v anglo-ameriškem kot tudi v širšem evropskem prostoru in se uporablja za poimenovanje državnih obveščevalnih služb ter njihovih organizacijskih enot (Warner, 2002; Gill in Phythian, 2018). Na to večpomenskost pojma opozarja tudi Britovšek (2025), saj mora definicija obveščevalne dejavnosti upoštevati dejstvo, da jo izvajajo tudi nedržavne organizacije.

2.2 Korporativna obveščevalna dejavnost

Iz splošnega pogleda na obveščevalno dejavnost se je z razvojem gospodarstva in globalizacije izoblikovala tudi njena korporativna oblika, ki se osredotoča na pridobivanje in uporabo informacij za poslovne namene. Korporativna ne pomeni le velikih korporacij, temveč vključuje tudi manjša podjetja, nevladne organizacije in druge institucije, ki želijo izboljšati konkurenčnost in varovati poslovne procese. Korporativna varnost je del celovite varnosti v organizaciji ali podjetju, ki se vrti okoli različnih področij in vidikov delovanja. Eden izmed pomembnih vidikov korporativne varnosti je tudi učinkovito upravljanje informacij, kar se uresničuje skozi korporativno obveščevalno dejavnost. Sem uvrščamo tudi korporativno obveščanje, pri katerem prevladujeta ekonomsko oziroma poslovno obveščanje in konkurenčno obveščanje. Korporativno obveščanje bi lahko predstavljalo orodje povečanega ozaveščanja sodobnih organizacij, ki želijo poslovati varno, predvsem z vidika globalnega poslovanja, ob upoštevanju tveganj na trgu, pa tudi priložnosti lastnega konkurenčnega razvoja. Kot orodje za obvladovanje izzivov in nadgradnjo poslovanja z vidika konkurenčnosti in varnosti na trgu predstavlja samo zavedanje o nujnosti korporativne varnosti v sodobnem globalnem poslovanju neizogiben korak h konkurenčnemu in varnemu globalnemu poslovanju, z zavedanjem zunanjih tveganj, izkoriščanjem lastnih prednosti in poznavanju značilnosti trga (Dvojmoč, 2021).

Korporativna obveščevalna dejavnost se je prilagodila spremembam na trgu in razvoju novih tehnologij, kar se odraža v pojavu novih trendov na tem področju (Lobnikar in Dvojmoč, 2017). Vse več organizacij in podjetij več pozornosti posvečajo varovanju dobrega imena ter odziva javnosti na oglaševanje. Prav tako so se orodja KOD pričela uporabljati tudi za analizo lojalnosti, kar pomeni, da organizacije oziroma podjetja pred samim sodelovanjem s poslovnim partnerjem preverijo njegovo ozadje, prejšnja sodelovanja in odnos s konkurenco.

Korporativna obveščevalna dejavnost spada na področje korporativne varnosti, njeni dve prevladujoči obliki pa sta poslovna inteligenca in konkurenčna obveščevalna dejavnost (Dvojmoč, 2019), pri čemer je konkurenčna obveščevalna dejavnost v literaturi včasih uporabljena kot širši pojem, včasih pa kot podkategorija KOD. Prednosti korporativne obveščevalne dejavnosti so:

- splošno izboljšanje delovanja organizacije;
- pridobitev konkurenčne prednosti;
- obvladovanje tveganj;
- zaščita celotne organizacije, zaposlenih, znanja, interesov, skrivnosti in poslovnih procesov pred različnimi varnostnimi tveganji;
- hitrejše in celovitejše odločitve;
- trajnosten razvoj organizacije;
- KOD postaja vse bolj potrebna, pomembna in stroškovno učinkovita.

2.3 Konkurenčna obveščevalna dejavnost

V času globalizacije se je namen obveščevalne dejavnosti razširil na različna področja. Ta premik ni bil le posledica tehnološkega napredka, temveč tudi potrebe organizacij po strateških informacijah, ki omogočajo boljše odločanje v konkurenčnem okolju. Tako je začela nastajati posebna veja obveščevalne dejavnosti – konkurenčna obveščevalna dejavnost. Predvsem na področju podjetništva in globalnega marketinga so ljudje začeli posegati po metodah dela obveščevalnih služb, ki so prinesle tudi pozitivne rezultate. Podobne metode dela so postale tudi stalnica pri pridobivanju podatkov o konkurenčnih podjetjih in inovacijah na svetovnih trgih. Kmalu zatem se je začela razvijati nova podvrsta obveščevalne dejavnosti. Njeni taktika in strategija sta vezani predvsem na podjetniško okolje. Teoretiki (npr. Kahaner, 1997; Fuld, 1995; Porter, 1980) so jo poimenovali konkurenčna obveščevalna dejavnost (angl. *competitive intelligence*). Kahaner (1997) poudarja, da se je konkurenčna obveščevalna dejavnost razvila kot odgovor na globalno tekmovanje

med podjetji, kjer informacije predstavljajo ključno orožje konkurenčne prednosti. Po njegovem mnenju podjetja, ki sistematično zbirajo in analizirajo tržne informacije, ne le zmanjšujejo tveganja, ampak oblikujejo proaktivne strategije za prihodnost. Pojem se je prvič pojavil v osemdesetih letih 20. stoletja (Lobnikar in Dvojmoč, 2017).

Etimološko beseda *intelligence* izhaja iz latinskega intelligere (intellego, intellegis, intellegere, intellexi, intellectum), kar lahko pomeni zaznati, opaziti, spoznati, razumeti, biti spreten, misliti, upoštevati, predstavljati.

Korporativna obveščevalna dejavnost, zlasti v obliki konkurenčne obveščevalne dejavnosti, ima kljub priljubljenosti v poslovni in marketinški sferi negativno konotacijo, saj jo večina povezuje z vojaško-varnostno obveščevalno dejavnostjo. O razvoju KOD se je pojavilo tudi več teorij, kaj naj bi konkurenčna obveščevalna dejavnost pomenila ter kakšni so njeni glavni cilji (Lobnikar in Dvojmoč, 2017). Za bolj natančno razumevanje vsebine in obsega te dejavnosti sta Vedder in Guynes (2001) dejavnost opredelila tako, da je konkurenčna obveščevalna dejavnost skupek zakonitih in etičnih metod zbiranja informacij o aktivnostih konkurentov.

Pirttimäki in Lönnqvist (2006) sta mnenja, da se z združitvijo več mnenj različnih teoretikov določi širok pojem, ki izpostavlja pomen upravljanja in preoblikovanja poslovnih informacij, iz katerih dobimo obveščevalni produkt, ki vpliva na končno odločanje pri sprejemanju različnih ciljev in vizij neke organizacije. Naslednjo teorijo so razvili člani SCIP (angl. *Society of Competitive Intelligence Professionals*). Tudi oni so mnenja, da nam konkurenčna obveščevalna dejavnost pomaga pri sprejemanju ključnih odločitev. Ta teorija zagovarja spremljanje splošnega konkurenčnega okolja in analizo dejanj znotraj organizacije. Tretja teorija pa se od prejšnjih dveh razlikuje po postopku, saj se konkurenčna obveščevalna dejavnost uvršča med mednarodno poznano orodje, izredno pomembno pri sprejemanju ključnih odločitev v organizaciji (Havenga in Botha, 2003). Čeprav se pristopi med seboj razlikujejo, pa vse teorije poudarjajo, da konkurenčna obveščevalna dejavnost ni zgolj zbiranje informacij, temveč gre predvsem za proces, ki omogoča strateško prednost. Skupni imenovalec vseh teorij je poudarek na preoblikovanju informacij v znanje, ki neposredno vpliva na kakovost odločanja v organizacijah.

Vse tri teorije, katerih avtorji so Pirttimäki in Lönnqvist (2006); SCIP in Havenga in Botha (2003) poudarjajo, da konkurenčna obveščevalna dejavnost vpliva predvsem na končne odločitve, preko katerih dobimo dober pogled na konkurenčno okolje, znotraj katerega lahko analiziramo spremembe, inovacije, obnašanje konkurence in podobno. Vseeno pa področje KOD obsega veliko širše področje, ki obsega tudi analizo organizacije s pomočjo

različnih orodij. S pomočjo KOD lahko gradimo tudi na defenzivnih tehnikah, s pomočjo katerih lahko vplivamo na manjše odtekanje informacij, poizvedovanje o orodjih in podobno.

Konkurenčna obveščevalna dejavnost je umetnost zakonitega in etičnega zbiranja, obdelovanja ter hranjenja informacij z namenom prispevanja k prihodnosti organizacije in njeno obvarovanje pred grožnjami konkurentov (Rouach in Santi, 2001). Je proces ali praksa, ki ustvarja in razširja uporabne obveščevalne informacije na podlagi načrtovanja, etičnega in zakonitega zbiranja, obdelovanja in analize informacij iz in o notranjem in zunanjem ali konkurenčnem okolju (Pellissier in Nenzhelele, 2013). Madureire idr. (2021) konkurenčno obveščevalno dejavnost opredeljujejo kot proces in v prihodnost usmerjene dejavnosti, ki se uporabljajo pri pridobivanju znanja o konkurenčnem okolju za izboljšanje uspešnosti organizacije. Zajema namensko in koordinirano spremljanje konkurentov ter tako predstavlja sistematičen program za zakonito zbiranje in analizo informacij o aktivnostih konkurentov ter poslovnih trendih (Diyaolu, 2019). Je analitičen proces, pri katerem se zbirajo javno dostopne informacije, ki nato z analizo omogočajo boljši vpogled v različne lastnosti konkurentov (Isson in Harriott, 2013).

Avtorji se strinjajo, da je bistvo konkurenčne obveščevalne dejavnosti v etičnem in zakonitem delovanju. Čeprav se razlikujejo v poudarkih, vsi potrjujejo, da mora biti zbiranje informacij izvedeno na zakonit in odgovoren način, kar konkurenčno obveščanje ločuje od industrijskega vohunstva (Fuld, 1995; Fleisher in Bensoussan, 2007; Podbregar, 2008; Pellissier in Nenzhelele, 2013).

Bernhardt (2003) meni, da je etika sestavni del konkurenčnega obveščanja, saj odgovorno ravnanje z informacijami gradi zaupanje znotraj organizacije in v njenem poslovnem okolju. Pravilno vzpostavljena kultura tako krepi strateško vodenje in dolgoročno konkurenčnost podjetja.

Konkurenčna obveščevalna dejavnost je usmerjena v zbiranje, analiziranje in interpretacijo informacij, ki podjetjem omogočajo razumevanje svojih konkurentov, tržnih trendov ter strateških priložnosti. Namen je podpora strateškega odločanja in omogočanje proaktivnega odzivanja na spremembe v poslovnem okolju (Fuld, 1995). Porter (1980) poudarja, da razumevanje industrijskih sil in konkurenčnih struktur podjetjem ter organizacijam omogoča oblikovanje učinkovitih strategij. Konkurenčna obveščevalna dejavnost je v tem kontekstu ključno orodje za identifikacijo groženj in priložnosti, saj podjetjem omogoča, da sprejemajo odločitve na podlagi sistematičnih ter relevantnih informacij. Porterjev model petih sil je eden izmed temeljnih pristopov, ki ga podjetja

uporabljajo v okviru konkurenčnega obveščanja. Analiza sil (konkurentov, dobaviteljev, kupcev, nadomestkov in novih vstopnikov) podjetju omogoča, da na podlagi zbranih informacij razume svojo pozicijo v industriji ter sprejema premišljene strateške odločitve.

Nameni in cilji konkurenčne obveščevalne dejavnosti so:

- pomoč odločevalcem pri sprejemanju odločitev;
- zagotovitev konkurenčne prednosti podjetja;
- spremljanje, razumevanje in predvidevanje dejanj konkurentov, strank in vlad ter sprememb na trgu in v zakonodaji;
- zagotovitev konteksta in pomena navidezno različnim dejstvom in domnevam;
- pridobitev strateške prednosti;
- izogibanje presenečenjem;
- prepoznavanje priložnosti;
- identificiranje groženj in razumevanje ranljivosti lastne organizacije;
- zmanjšanje reakcijskega časa;
- zaščita intelektualnega kapitala;
- predvidevanje in zgodnje prepoznavanje trendov;
- upravljanje in ustvarjanje baze znanja;
- oblikovanje, spodbujanje in izboljšanje strateškega načrtovanja;
- vzpostavitev sistematičnega pridobivanja in uporabe obveščevalnih informacij;
- ocenjevanje potencialnih partnerjev (Maune, 2014; Mohd Asri in Abdul Mohsin, 2020).

Ti cilji tvorijo osnovo za vzpostavitev učinkovitega sistema konkurenčnega obveščanja v organizaciji. V praksi to pomeni, da podjetje razvije procese za stalno spremljanje trga, prepoznavanje tveganj in priložnosti ter prilagajanje svojih strategij v realnem času.

Na konkurenčnost vpliva okolje organizacije, kamor uvrščamo trg, konkurenčna podjetja, stranke, industrijo in poslovne partnerje. Ti vplivajo na možnost širitve trgov, prihod akterjev na trge, možnost potencialnih novih virov za pridobivanje surovin, nove priložnosti za izboljšavo produktov in storitev, tehnološke spremembe, spremembe v potrebah na trgu ter sklepanje novih partnerstev. Na primer, tehnološko podjetje lahko s spremljanjem patentnih prijav konkurentov zazna razvoj novih tehnologij, kar mu omogoča pravočasno prilagoditev lastnega razvojnega načrta. Takšni primeri kažejo, kako lahko KOD neposredno vpliva na inovacijske procese in konkurenčno prednost.

Cilj oblikovanja uspešne strategije v organizaciji je predvsem ustvarjanje in ohranjanje konkurenčne prednosti pred konkurenco. Na ta način konkurenčna obveščevalna dejavnost predstavlja vir trajnejše konkurenčne prednosti. Poskrbeti je potrebno tudi, da prispeva hitre, relevantne in analizirane izdelke, ki skupaj z znanjem strokovnjakov s področja konkurenčnega obveščanja pomagajo oblikovati ter upravljati strategijo organizacije (Hughes idr., 2013).

Podjetja so si lahko med seboj konkurenčna na različnih področjih. To so lahko izdelki oziroma storitve (npr. kakovost proizvodov in zadovoljstvo kupcev), financiranje (npr. investicije, visoke cene, nizki stroški in kapital), tehnologija (npr. zaščita patentov), organizacija in kadri, strateška zavezništva (npr. z drugimi dobavitelji, distributerji in proizvajalci), proizvodnja (npr. večje proizvodne kapacitete in delovna sila), marketing ter oglaševanje in ugled.

Sam proces konkurenčnega obveščanja v organizacijah mora vključevati ne le zbiranje notranjih in zunanjih informacij od konkurentov, temveč tudi od strank, dobaviteljev, tehnologije, okolja in potencialnih poslovnih odnosov. V takih primerih proces konkurenčnega obveščanja zagotavlja sistem zgodnjega opozarjanja in pomaga predvideti dejavnost konkurentov, strank in vlad (Calof in Wright, 2008).

2.4 Poslovna inteligenca

Poslovna inteligenca se v določenih teoretskih in nacionalnih kontekstih povezuje z gospodarsko oziroma ekonomsko obveščevalno dejavnostjo, vendar pojmi niso sinonimni. Angleški izraz je *business intelligence* in tudi *economic intelligence*. Izraz *Economic intelligence* se v evropski literaturi pogosto razume kot širša, strateška dejavnost, ki vključuje zbiranje in analizo informacij za podporo strateškim odločitvam organizacij ter držav (Martre, 1994; Harbulot in Baumart, 1996). Nasprotno pa se izraz *business intelligence* pogosto razume predvsem kot IT-podprte metode zbiranja, shranjevanja in analize podatkov[1], ki služijo predvsem podpori poslovnim odločitvam na operativni ter taktični ravni, medtem ko je strateška raven bolj povezana s prognozami in simulacijami (Olszak & Ziemba, 2007). Poslovna inteligenca je tesno povezana s korporativno in konkurenčno obveščevalno dejavnostjo, pri čemer konkurenčna obveščevalna dejavnost analizira predvsem zunanje dejavnike ter konkurenco, medtem ko se poslovna inteligenca

[1] Npr. ETL-postopki (angl. *Extraction, Transformation, Load*) omogočajo izvleček podatkov iz različnih virov, njihovo čiščenje in preoblikovanje ter nalaganje v centralno shrambo; podatkovno skladišče (angl. *data warehouse*) predstavlja integrirano, tematsko organizirano zbirko zgodovinskih in agregiranih podatkov, optimizirano za analizo ter poročanje; OLAP-tehnologija (angl. *On-Line Analytical Processing*) omogoča hitro interaktivno večdimenzionalno analizo; rudarjenje podatkov (angl. *data mining*) pa avtomatizirano odkriva skrite vzorce, pravila in napovedi v velikih količinah podatkov z uporabo algoritmov (Olszak in Ziemba, 2007).

osredotoča tudi na notranje procese in strateško uporabo podatkov (Fuld, 1995; Porter, 1980).

Je skupek konceptov, metod in procesov za izboljšanje poslovnih odločitev z uporabo informacij iz različnih virov, izkušenj ter dodajanjem predpostavk za oblikovanje natančnega razumevanja poslovne dinamike (Brackett, 2001). Je tudi proces zbiranja, analiziranja in vizualizacije podatkov, pri čemer rezultati testa služijo kot podlaga za poslovne odločitve (Cekuls, 2023). Predstavlja zbiranje, upravljanje in analizo večjih količin podatkov o strankah oziroma uporabnikih, produktih, storitvah, nalogah, podpori, partnerjih ter vseh transakcijah v organizaciji (Hao idr., 2000).

Nameni in cilji poslovne inteligence so:

- preučevanje hitrosti, obsega in smeri gospodarskih reform ter spremljanje izvajanja gospodarskih politik;
- razumevanje vzorcev strank;
- identifikacija priložnosti za rast prodaje in dobička;
- pomoč pri sprejemanju strateških odločitev;
- prilagajanje spremembam v poslovnem okolju;
- sprejemanje hitrejših in celovitejših odločitev;
- večja uspešnost organizacije;
- izogibanje presenečenjem in podpora pri ukrepanju v primeru neugodnih situacij.

Ti cilji so bistveni tudi za širše razumevanje korporativne obveščevalne dejavnosti, saj poslovna inteligenca predstavlja notranji steber. Omogoča učinkovito odločanje, upravljanje z znanjem in dolgoročno konkurenčno prednost (Bernhardt, 2003).
Poznamo tudi nekaj izzivov poslovne inteligence, na primer:

- hitre spremembe na trgu in v okolju informacijskih tehnologij;
- preobremenjenost z informacijami oziroma velike količine podatkov;
- pomanjkljiva kakovost virov in podatkov (pomanjkanje zanesljivosti, natančnosti in ažurnosti);
- integracija in nekompatibilnost različnih sistemov;
- varnost podatkov;
- težave pri zajemu, dostopu in razumevanju podatkov;
- pomanjkanje strokovnega znanja in veščin za analizo večjih količin podatkov.

To področje je dobro obravnavati z angleškim prevodom (angl. *Business Intelligence*), saj ga v slovenščino prevajamo kot poslovno inteligenco ali kot poslovno obveščanje. Ulcej idr. (2010) definirajo poslovno inteligenco kot menedžerski pristop, ki podatke, pridobljene s pomočjo informacijsko-komunikacijske opreme pretvarja v obveščevalni izdelek. S tem pa vpliva tudi na ključne odločitve in postavljanje ciljev znotraj organizacije. Lönnqvista in Pirttimäkia v poslovno inteligenco poleg pridobivanja ter pretvarjanja informacij vključujeta tudi samo upravljanje in ravnanje z informacijami (Ulcej idr., 2010).

Poslovna inteligenca, znana tudi kot gospodarska ali ekonomska obveščevalna dejavnost (angl. *economic intelligence*), v strokovni literaturi pogosto nosi več poimenovanj. Medtem ko jo nekateri avtorji ločujejo, del literature obravnava gospodarsko oziroma ekonomsko obveščevalno dejavnost in poslovno inteligenco kot sorodna koncepta, vendar sodobni pristopi opozarjajo na pomembne konceptualne ter funkcionalne razlike med njima (Zemmouchi-Ghmori, 2013; Hromozdova idr., 2021). V okviru te dejavnosti naj bi bili ključni operativni izvajalci pogosto člani državnih varnostnih obveščevalnih služb, saj naj bi šlo za dejavnost, ki presega zgolj komercialno analizo in vključuje elemente strateške zbirke informacij za nacionalno ali mednarodno politično-ekonomsko delovanje (Popovici, 2014). V praksi to pomeni, da gospodarska oziroma ekonomska obveščevalna dejavnost združuje sistematično spremljanje gospodarskega okolja, analizo informacij iz javnih in zaupnih virov ter njihovo uporabo za podporo odločitvam in zaščito strateških gospodarskih interesov (Ahdil, 2024).

Ne glede na različne terminološke pristope gre v vseh primerih za proces, katerega ključni cilj je pretvorba podatkov v znanje, ki podpira varno in konkurenčno poslovanje.

Odgovorite na vprašanja

Kaj je obveščevalna dejavnost?

Katera dva dogodka oziroma obdobji sta pomembna za obveščevalno dejavnost iz perspektive današnjega časa in zakaj?

Kako različni avtorji definirajo obveščevalno dejavnost?

Kako pojem obveščevalne dejavnosti razumemo v angleščini?

Kaj je korporativna varnost in kaj v organizaciji zagotavlja?

Kaj je korporativno obveščanje?

Katere so prednosti korporativne obveščevalne dejavnosti?

Katere teorije so se razvile o razvoju konkurenčne obveščevalne dejavnosti?

Kaj poudarjajo vse tri teorije o razvoju?

Kateri so nameni in cilji konkurenčne obveščevalne dejavnosti?

Kaj vpliva na konkurenčnost organizacije?

Na katerih področjih so si podjetja lahko konkurenčna?

Kaj je poslovna inteligenca?

Kateri so nameni in cilji poslovne inteligence?

Naštejte nekaj izzivov poslovne inteligence.

Kako je tudi poimenovana poslovna inteligenca ter kakšen je njen prevod v angleščino?

Preučite hipotetično situacijo, v kateri želi podjetje vzpostaviti korporativno obveščevalno enoto. Pripravite predlog organizacijske umestitve, glavnih nalog in ključnih ciljev korporativne obveščevalne enote.

Izberite podjetje po lastni izbiri in analizirajte njegove glavne konkurente. Opredelite, katere vrste informacij bi bile za podjetje najbolj uporabne za konkurenčno analizo in kako bi jih pridobili na zakonit način.

Univerzitetna založba
Univerze v Mariboru

3 Predmeti korporativne obveščevalne dejavnosti

Predmeti korporativne obveščevalne dejavnosti so podatki (angl. *data*), informacije (angl. *information*), znanje (angl. *knowledge*) in obveščevalne informacije oziroma obveščevalni podatek, izdelek ali produkt (angl. *intelligence*). Ti elementi so med seboj tesno povezani in predstavljajo zaporedne faze v procesu ustvarjanja obveščevalne vrednosti – od surovega podatka do končnega obveščevalnega izdelka, ki omogoča sprejemanje odločitev (Pellissier in Nenzhelele, 2013).

3.1 Podatek

Podatek je niz diskretnih in objektivnih dejstev o določenih dogodkih (Davenport in Prusak, 1998). »Podatki so prva postaja pri nastajajoči verigi informacija-znanje in so običajno v obliki črk, besed, številk ali katerih drugih simbolov. Njihovo dešifriranje temelji na predhodno usvojenih informacijah, ki pomagajo dati podatkom pomen (Haywood, 1997, str. 1). Podatek je torej neko nevtralno sporočilo, ki ga lahko opredelimo kot surovo dejstvo ali osnovni opis stvari, dogodkov in dejavnosti, ki so zabeleženi, shranjeni in urejeni, pri tem pa sami po sebi ne posredujejo nikakršnega konkretnega pomena.« (Potparič in Dvoršek, 2012, str. 42)

»Podatek je opredmeteno dejstvo o določeni stvari, s katero predstavimo informacijo; je formaliziran prikaz dejstev in spoznanj, primernih za interpretacijo in obdelavo.« (Priročnik za delo z izpisi klicev, 2010, str. 5)

Opažanja ali dejstva izven konteksta in kot taki nimajo vrednosti (Zack, 1999). Dejstvo je preverjen podatek. Po vrstah podatkov ločimo besedila (opisni podatki); števila; slike; zvoke in videje. Predstavimo jih lahko na dva načina, in sicer zvezno/analogno ali diskretno/digitalno. Po urejenosti pa jih ločimo na strukturirane: to so tisti, ki imajo vnaprej določeno strukturo (na primer tabele in grafi) ter nestrukturirane (na primer besedila v dokumentih).

Podatki sami po sebi še ne ustvarjajo vrednosti. Šele, ko jim dodamo pomen in kontekst, postanejo informacije, ki jih je mogoče uporabiti pri odločanju.

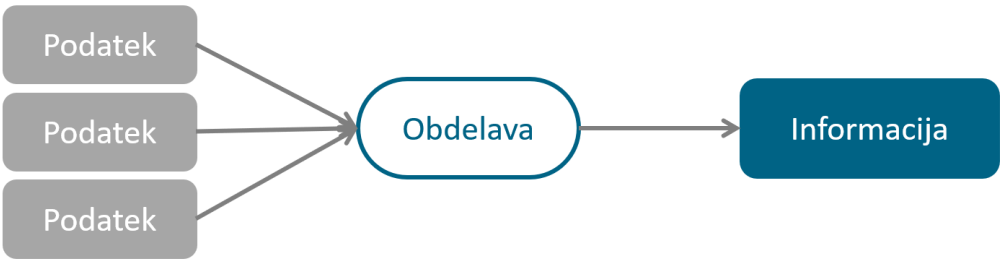
3.2 Informacija

Informacija je seštevek podatka in pripadajočih lastnosti, relevantnosti ter konteksta (Joia, 2000). Informacija predstavlja eno izmed najmočnejših in najbolj obetavnih "orožij" v organizaciji. Predstavlja pa lahko premoženje, vir ali sredstvo v poslovnih procesih.

»V nasprotju s podatkom je informacija zbirka podatkov, ki so organizirani tako, da so za uporabnika smiselni. Ključni dejavnik pri pretvorbi podatka v informacijo je človek. Proces pretvorbe podatka v informacijo temelji na procesu sprejemanja, prepoznavanja in konverzije, ki ga omogočata naša kognitivna zgodovina in sposobnost dešifriranja simbolov znotraj neke kulture. Do pretvorbe podatkov v informacije lahko pride le takrat, ko smo tem podatkom sposobni dodati vrednost iz 22 zalog informacij, do katerih imamo dostop in ki so lahko v obliki spomina, knjig ali v elektronski obliki.« (Potparič in Dvoršek, 2012).

Informacijo sestavlja posamezni podatek ali skupina podatkov, ki so iz več razlogov pridobljeni in zbrani s pomočjo različnih senzorjev. Informacija je ugotovitev stanja ali stvari, ki obstaja ali je obstajala v neki točki v času in prostoru. Opredeljena je kot »neobdelan« podatek različnih opisov, ki se lahko uporabi pri izdelavi obveščevalnih podatkov (AJP–2, 2003).

Ko se informacije združijo, analizirajo in povežejo s preteklimi izkušnjami in razumevanje okolja, prehajajo v višjo raven – znanje.



Slika 1: Informacija
Vir: lasten.

3.3 Znanje

Enotne definicije, kaj je znanje in katere so posamezne dimenzije znanja, ni. Znanje je pogosto definirano kot mešanica razumevanja, interpretacij in informacij (Gomezelj Omerzel, 2010). V Slovarju slovenskega knjižnega jezika (n. d.) je definirano kot »(1) celota podatkov, ki si jih nekdo vtisne v zavest z učenjem, študijem // celota znanih, ugotovljenih podatkov o stvarnosti; (2) z učenjem pridobljeno tako poznavanje besedila, da se to lahko pove, navede // izurjenost, usposobljenost za kako dejavnost; (3) poznavanje nečesa; (4) veščina, spretnost.«

Pri definiranju znanja se lahko opremo tudi na *know-that* in *know-how* ter razlike med njima. *Know-that* pomeni vedeti nekaj in predstavlja tradicionalni pogled na znanje. Mišljenje posameznika pa mora biti pri tem dokazljivo in resnično. *Know-how* pa pomeni bolj praktično opredelitev znanja. Pri tem je pomembno predvsem, kako primerno, učinkovito in uspešno se izvajajo nekatere dejavnosti (Gomezelj Omerzel, 2010).

V okviru organizacij pa ločimo tri dimenzije znanja. Prva predstavlja znanje na ravni posameznika, skupine ali celotne organizacije. Druga dimenzija ločuje znanje na eksplicitno in implicitno. Tretja pa zajema praktično znanje (Gomezelj Omerzel, 2010).

Znanje je torej višja oblika razumevanja informacij, vendar v obveščevalnem procesu še ni končni cilj. Šele, ko znanje uporabimo za napovedovanje, vrednotenje in odločanje, dobimo obveščevalno informacijo oziroma produkt.

3.4 Obveščevalna informacija

Šaponja (1999) končni izdelek obveščevalnega procesa imenuje obveščevalna informacija ali izdelek. Je vsak končni izdelek obdelave podatkov, v katerem je pridobljena določena uporabna vrednost za obveščevalno službo. Končni izdelki obveščevalne dejavnosti so

izdelki: obveščevalne informacije, analize, ocene, napovedi in druge oblike celovitih obveščevalnih izdelkov.

Obveščevalna informacija razlaga dejstva, združuje informacije, išče vlive na podjetje in njihove reakcije na morebitne vplive (Egan, 2001). Je informacija, ki je bila filtrirana, povzeta in analizirana (Kahaner, 1997). Poleg tega ponuja tudi odgovore na vprašanja, kot sta na primer:

- Kaj se lahko zgodi jutri?
- Kako naj se podjetje na to pripravi?

Slika 2: Obveščevalna informacija
Vir: lasten.

Vrednost obveščevalne informacije lahko merimo na podlagi različnih atributov. To so: točnost, objektivnost, uporabnost, relevantnost, primernost (pripravljenost na nadaljnjo analizo) in pravočasnost (na podlagi časovne komponente).

Imeti podatek, informacijo ali tudi znanje ni dovolj ali ni optimalno. Znanje je treba nadgraditi, priti do obveščevalnega produkta, ki vodi do specifičnih odločitev in delovanj. Le-te organizaciji omogočajo konkurenčno prednost. Podbregar (2008) poudarja, da pravočasne in dobre informacije pomenijo prednost, ne glede na področje. Vseeno pa je potrebno imeti sposobnost in zmogljivost, da te informacije analiziramo na pravi način ter jim dodamo zmožnost, da je na podlagi njih mogoče ukrepati. Fleisher in Bensoussan (2003) sta zapisala, da v današnjem svetu zbiranje podatkov in informacij ni ključna zadeva. Ključno za definiranje ustreznih strategij je raziskovanje in vrednotenje informacij z analizo.

Proces od podatka do obveščevalne informacije je temeljni mehanizem korporativne obveščevalne dejavnosti, saj omogoča prehod od surovih dejstev do strateškega znanja, ki podpira varno, premišljeno in konkurenčno delovanje organizacij ter podjetij.

Odgovorite na vprašanja

Kaj so predmeti korporativne obveščevalne dejavnosti?

Kaj je definicija podatka?

Kako ločimo podatke po vrstah?

Kaj je informacija?

Kakšna je povezava med podatkom in informacijo?

Kako bi opredelili oziroma definirali znanje?

Katere tri dimenzije znanja ločimo v okviru organizacij?

Kaj je obveščevalna informacija?

Na podlagi česa lahko merimo vrednost obveščevalne informacije?

Napišite po dva praktična primera pojmov podatek in informacija.

Predpostavite, da ste analitik v podjetju, ki se pripravlja na širitev na tuji trg. Opredelite, katere obveščevalne informacije bi potrebovali za sprejem odločitve, in jih razvrstite po pomembnosti.

Univerzitetna založba
Univerze v Mariboru

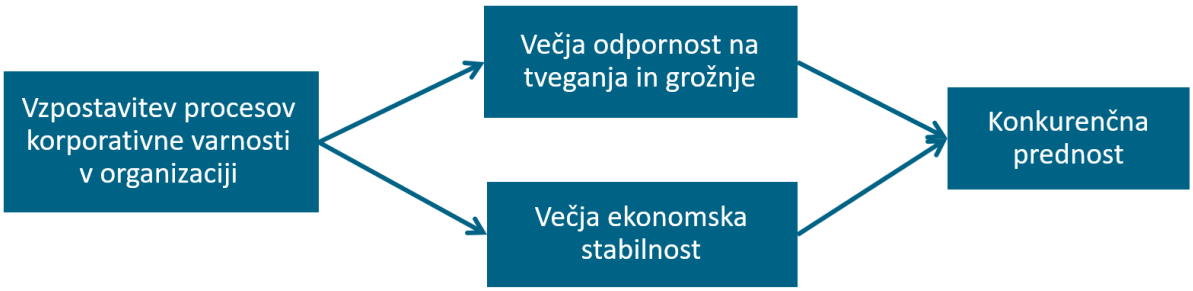
4 Varnost in korporativna obveščevalna dejavnost v organizacijah

Varnostna področja v organizacijah zajemajo:

- korporativno obveščevalno dejavnost;
- protiobveščevalno dejavnost;
- skladnost z zakonodajo;
- korporativno varnost;
- varnost podatkov;
- kibernetsko varnost;
- varnostno kulturo zaposlenih;
- informacijsko varnost;
- fizično in tehnično varovanje;
- zasebno varovanje;
- detektivsko dejavnost;
- poslovno preiskovanje in drugo.

Vsa ta področja so medsebojno povezana in tvorijo okvir za zanesljivo zaščito podjetja pred notranjimi in zunanjimi grožnjami, hkrati pa omogočajo učinkovito uporabo KOD kot strateškega orodja.

4.1 Korporativna varnost



Slika 3: Korporativna varnost
Vir: lasten.

Korporativna varnost je dejavnost, katere cilj je zagotoviti varnost v organizacijah (Dvojmoč, 2017). Vsaka organizacija mora sprejeti celosten pristop k zagotavljanju varnosti. Sem uvrščamo identifikacijo tveganj, uvedbo varnostnih ukrepov, različna usposabljanja zaposlenih, redna preverjanja in posodabljanja dokumentov, določanje ukrepov z namenom preprečevanja tveganj ter podobno (Mwakibete, 2019).

Shema 3 prikazuje, da vzpostavitev procesov korporativne varnosti neposredno prispeva k večji odpornosti organizacije na tveganja in grožnje ter k večji ekonomski stabilnosti. S tem se povečuje tudi konkurenčna prednost organizacije, kar kaže na tesno povezanost korporativne varnosti in konkurenčne obveščevalne dejavnosti. Zaradi naraščanja izzivov je vzpostavitev in zagotavljanje celovite varnosti zelo pomembno. Pri tem ima korporativna varnost izredno pomembno vlogo, celovita varnost pa je odvisna predvsem od dobrega varnostnega menedžmenta. Le-ta je odgovoren za to, da sprejema odločitve o varnosti (Prislan in Bernik, 2016). S samo vzpostavitvijo korporativne varnosti oziroma njenih procesov, se v organizaciji vzpostavi večja odpornost na tveganja in grožnje ter tudi večja ekonomska stabilnost. S tem je organizacija bolj konkurenčna in ima v primerjavi z ostalimi konkurenti prednost.

Podjetje, ki izvaja redne varnostne preglede in izobraževanja za zaposlene o prepoznavanju nevarnosti, zmanjšuje možnost izgube podatkov ter povečuje odpornost na konkurenčne pritiske. Takšna praksa neposredno podpira konkurenčno obveščevalno dejavnost (Fuld, 1995).

4.2 Etika v korporativni obveščevalni dejavnosti

Korporativna obveščevalna dejavnost spoštuje zakone, poslovne skrivnosti in zasebnost ter se izogiba prevaram, izsiljevanju, vdiranju v računalniške sisteme, prisluškovanju in podkupovanju. Državna obveščevalna dejavnost ima več pooblastil in lahko v določenih pogojih posega v nekatere človekove pravice (z razliko od zasebne obveščevalne dejavnosti).

4.2.1 Siva področja in neetična ravnanja

Področja, ki mejijo med zakonitim oziroma etičnim in nezakonitim oziroma neetičnim, imenujemo siva področja. V praksi točne ločnice med tem kaj je prav in kaj ni, ne obstajajo. Za neetična ravnanja gre takrat, ko je prisoten vsaj eden od naslednjih dejavnikov:

- Taktike, ki so uporabljene za zavarovanje informacij, so vprašljive in presegajo sprejemljivo, etično ali zakonito poslovno prakso.
- Narava pridobljenih informacij se šteje za interno ali tajno.
- Namen uporabe informacij je v nasprotju z javnim interesom.

Etično izvajanje KOD je ključno, saj nepravilno ali nezakonito zbiranje informacij ne samo ogroža ugled podjetja, ampak lahko privede tudi do pravnih posledic in izgube konkurenčne prednosti.

4.2.2 Krepitev etike v KOD

Etični kodeksi v organizacijah spodbujajo etično ravnanje, pošteno vedenje, profesionalizem, zaščito ugleda organizacije, zakonito delovanje, transparentnost, izogibanje navzkrižja interesov, pošteno in nezavajajoče delovanje, upoštevanje politik, ciljev in usmeritev organizacije. Pri etičnih kodeksih gre za napisana pravila vedenja in moralnih norm znotraj organizacije. Predstavljajo podlago za ukrepanje ob kršitvi dolžnega ravnanja posameznikov. Vsi zaposleni morajo biti z etičnimi kodeksi seznanjeni, vsi novo zaposleni pa etični kodeks prejmejo ob podpisu pogodbe, s čimer se strinjajo, da so ga prejeli in tudi prebrali (Mihelič in Culiberg, 2014).

V Slovarju slovenskega knjižnega jezika (n. d.) je kodeks opredeljen kot zakonik, zbirka zakonov, družbeno priznan in uveljavljen sistem načel, predpisov.

Tista podjetja, ki razvijajo etične kodekse se soočajo s problemom, kako te etične norme določiti in kako bodo sprejemljive za vse zaposlene. Etični kodeks mora biti jasen, natančen, vsebovati pa mora tudi jasne cilje (Kaptein in Schwartz, 2007). Kodeksi se med seboj razlikujejo v njihovem razumevanju odgovornosti, pravic in dolžnosti ter tudi v razumevanju etične odgovornosti.

Etični kodeks strokovnjakom pomaga pri poštenem poslovanju. Dokument etičnega kodeksa opisuje tudi, kako naj bi strokovnjaki pristopali k reševanju težav, ter temelji na temeljnih vrednotah organizacije, ki jih ti strokovnjaki upoštevajo (Hayes, 2023). Razvoj etičnega kodeksa je v največji meri odvisen od vodstva podjetja. Kršitev etičnega kodeksa lahko privede tudi do odpovedi delovnega razmerja, saj gre za pomemben dokument, ki jasno določa pravila vedenja in zagotavlja podlago za preventivno opozarjanje (Hayes, 2023).

Če podjetje razvija program etičnega izobraževanja za zaposlene in vključuje simulacije situacij, kjer bi se morali odločati med etično ter neetično uporabo obveščevalnih podatkov, se izboljša zavedanje tveganj in etičnih dilem, hkrati pa se krepi varnostna kultura ter konkurenčna odpornost.

Večina etičnih kodeksov zajema tri tipe vprašanj, in sicer:

- vprašanja glede zaupnih podatkov;
- vprašanja glede morebitne zaposlitve zunaj podjetja, ki lahko pripelje do konfliktnega stanja;
- vprašanja glede vprašanja podkupovanj (Hrastelj, 1995).

K še višji etičnosti lahko organizacija pripomore z izvajanjem različnih programov med svojimi zaposlenimi, z usposabljanjem o etiki in z etičnimi kodeksi. Tudi vodilni morajo biti dober zgled za vse zaposlene (Schermerhorn, 2002).

4.3 Varnostna kultura

Varnostno kulturo lahko opredelimo kot »skupek odgovornih in sprejetih vrednot, zavedanja in načinov vedenja vseh, ki sodelujejo v posameznem sistemu. V idealnem smislu je opredeljena kot odprta kultura, ki naj bi temeljila na zaupanju, poštenju, dobri komunikaciji, uspešnem sodelovanju, dobrem gospodarjenju, temelječ na spoštovanju osebne varnosti in varnosti celotne organizacije. Varnostna kultura naj bi bila integrirana

v vsako aktivnost organizacije, njen proces naj bi bil usklajen in voden, njeno učinkovitost pa je treba spremljati in dopolnjevati.« (Čaleta in Čaleta, 2012, str. 108-109)

Vršec (2003, str. 38) varnostno kulturo opisuje kot: »gre za zavest, da ima vsakdo pravico in dolžnost poskrbeti za svojo varnost in hkrati prispevati k varnosti bivalnega, delovnega, poslovnega in širšega okolja«. Vodstvo organizacije mora na individualni in kolektivni ravni vse zaposlene ozaveščati in s tem dvigniti varnostno kulturo na čim višjo raven (Whitman in Smith, 2005, str. 21).

Podjetje, ki redno izvaja treninge, simulacije incidentov in interno izobraževanje o poročanju nevarnosti, krepi varnostno kulturo ter hkrati povečuje učinkovitost korporativne obveščevalne dejavnosti, saj zaposleni zgodaj zaznajo nepravilnosti in potencialne grožnje.

Varnostna kultura se nanaša na skupne vrednote neke skupine oziroma zaposlenih v organizaciji. Ukvarja se s formalnimi varnostnimi zahtevami v organizacijah, povezana pa je z menedžerskim in nadzornim sistemom. Poudarja prispevek vsakega posameznika na vseh ravneh. Je relativno trajna, stabilna in odporna na spremembe, vpliva pa na vedenje zaposlenih pri njihovem delu ter se odraža v organizacijski pripravljenosti, da se razvije in uči iz napak, incidentov ter nezgod. Dimenzije oziroma vidike varnostne kulture delimo na:

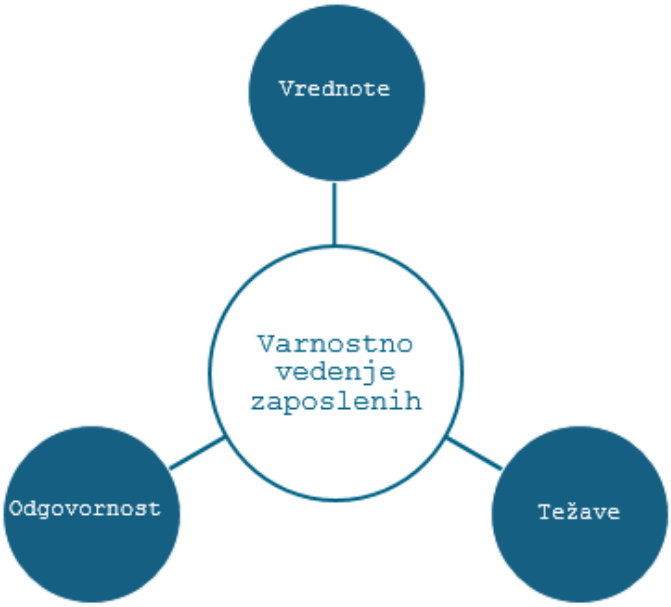
- situacijske: struktura organizacije (npr. politike, delovna pravila in sistemi upravljanja);
- vedenjske: strokovno opazovanje, samoporočanje in rezultati ukrepov;
- psihološke: vprašalniki, ki merijo dojemanje varnosti.

»Situacijske vidike varnostne kulture je mogoče opaziti v strukturi organizacije, ki zajema politike, delovna pravila, sisteme upravljanja, itd. Vedenjske vidike se meri s pomočjo strokovnega opazovanja, samo-poročanja in rezultatov ukrepov, medtem, ko je psihološka dimenzija najpogosteje proučevana s pomočjo vprašalnikov, ki merijo posameznikovo dojemanje varnosti.« (Choudhry idr., 2007)

Značilnosti dobre varnostne kulture so, da se varnost dojema kot sestavni del strategije obvladovanja tveganj ter da je pogled na nevarnosti objektiven. Prav tako se spodbuja nekaznovalno okolje in kultura zaupanja. Vzpostaviti je treba zavest o pomenu komuniciranja varnostnih informacij, kot so informacije o incidentih ali nezgodah ter poročanje o napakah. Določeni morajo biti realni in učinkoviti varnostni predpisi ter

zagotovljena ustrezna usposobljenost in razumevanje varnosti med zaposlenimi. Zelo pomembno je tudi, da je v organizaciji prisotna varnostna etika.

4.4 Varnostno vedenje zaposlenih



Slika 4: Varnostno vedenje zaposlenih
Vir: lasten.

- Osebne vrednote in način vedenja: večina posameznikov verjame v pomembnost skupnih vrednost in praviloma hitro prevzame organizacijski sistem vrednot, saj jim je lažje delati v skladu z dogovorjenimi pravili kot brez njih.
- Občutek odgovornosti do delodajalca: je posledica psihološkega pritiska, ki ga čutijo posamezniki in zajema prostovoljno upoštevanje pričakovanj organizacije.
- Težave pri upoštevanju predpisanih postopkov: pri nerazumljivih ali težko izvedljivih varnostnih mehanizmih, kjer njihovo upoštevanje nima vidnih učinkov, imajo zaposleni izredno nizko stopnjo tolerance za vedenje v skladu z njimi.

4.5 Protiobveščevalna dejavnost

Znotraj korporativne obveščevalne dejavnosti govorimo tudi o protiobveščevalni obveščevalni dejavnosti (POD). Oddelek POD mora v organizaciji delovati individualno in mora biti ločen od ostalih oddelkov. Njegova primarna naloga je predvsem analiza dejanj konkurence, ki bi lahko na kakršen koli način vplivala na organizacijo. Oddelek pa je odgovoren tudi za izvajanje internega nadzora. Pri tem je pozornost posvečena predvsem zaposlenim, strankam in dejanjem konkurence.

Korporativna protiobveščevalna dejavnost je nujen proces zavarovanja poslovnih skrivnosti, načrtov, programske opreme in dolgoročnih ciljev pred konkurenco. Za uspešno POD je potrebna zaščita in oprema (Ezendu, 2010).

Namen protiobveščevalne dejavnosti je zmanjšanje učinkovitosti obveščevalnih aktivnosti tujih oziroma nepartnerskih organizacij. Poleg tega pa tudi zaščita informacij in znanja pred ekonomskim oziroma industrijskim vohunjenjem ter zaščita ugleda organizacije.

Glavna tri vprašanja protiobveščevalne dejavnosti so naslednja.

- Kaj želijo tekmeci odkriti o nas in zakaj?
- Kako nameravajo to storiti?
- Kakšni protiukrepi so potrebni?

Protiobveščevalno dejavnost delimo na pasivno in aktivno. Pasivna PD vključuje preprečevanje nasprotnikove dejavnosti – obrambni in preventivni protiukrepi (na primer poročanje o grožnjah, tehnični protiukrepi in penetracijski testi). Aktivna PD pa vključuje preiskave in operacije za nevtralizacijo novih groženj.

4.5.1 Predmeti zaščite in varovanja

To so intelektualna lastnina, osebni in tajni podatki, poslovne skrivnosti, računalniška omrežja, poslovni ter informacijski sistemi, konkurenčna prednost, ugled in dobro ime gospodarske družbe.

Podjetje znotraj POD uporablja simulacije industrijskega vohunjenja in testiranje zaposlenih na področju zaupnih informacij, s čimer se zmanjšuje tveganje uhajanja podatkov.

4.6 Ukrepi za zagotavljanje varnosti podjetij

Za zagotavljanje varnosti podjetja se uporabljajo različni ukrepi:

- varnostna politika: skupek pravil, napotkov in postopkov, ki opredeljujejo, kako v organizaciji upravljati, ščititi in ravnati z določenimi viri z namenom doseganja konkretno zastavljenih varnostnih ciljev;
- izvajanje fizičnega in tehničnega varovanja;

- varnostno svetovanje: prenos znanja, izkušenj in raziskovalnih spoznanj od svetovalca na vodstvo in strokovnjake za varnost v organizaciji;
- razvijanje varnostne kulture: splet vrednot, prepričanj, simbolov in načinov za reševanje varnostnih problemov, ki so podlaga za odgovorno varovanje ljudi, poslovnih procesov in materialnih ter intelektualnih virov organizacije.

Praktični ukrepi omogočajo sistemski pristop k zaščiti poslovnih procesov in krepitev odpornosti organizacije na notranje ter zunanje grožnje.

4.7 Definicija vohunjenja

Korporativno vohunjenje je neetična ali nezakonita praksa, pri kateri organizacija ali njeni zaposleni izvajajo aktivnosti zbiranja informacij o drugih podjetjih ali konkurentih z namenom pridobitve konkurenčne prednosti. Vohunstvo pomeni prepovedano zbiranje tajnih, z zakoni zaščitenih podatkov, ali pa opravljanje z zakoni prepovedanih aktivnosti, povezanih z obveščevalno dejavnostjo. Šaponja (1999) definira tudi kot protipravne aktivnosti, za katere določa pravni red kazenskopravne sankcije.

V praksi so primeri vohunjenja na primer kraje dokumentov in poslovnih skrivnosti, podkupovanje zaposlenih, vdori v računalniške sisteme ter prisluškovanje ali prestrezanje komunikacij. Posledice vohunjenja so med drugim kazenska odgovornost, škoda ugledu in finančne izgube. Poznamo notranje (zaposleni) in zunanje vohune.

Med potencialnimi indikatorji, da je organizacija postala tarča gospodarskega vohunjenja, lahko prepoznamo več značilnih znakov. Do sumov o takšnih dejavnostih običajno pride, kadar konkurenčna podjetja predčasno razpolagajo z informacijami o novih projektih, zaupnih poslih, poslovnih strategijah in drugih poslovnih skrivnostih organizacije (Rothke, 2001). Pomemben opozorilni znak so tudi nenavadna poizvedovanja s strani neznanih posameznikov ali subjektov, ki se predstavljajo kot študenti, raziskovalci ali poslovni partnerji in izkazujejo nenavadno zanimanje za notranje procese ali razvojne projekte podjetja. Med indikativne situacije lahko štejemo tudi prihod tehničnih serviserjev in zunanjih izvajalcev, katerih storitev organizacija ni naročila, kar lahko nakazuje na možnost namestitve prisluškovalnih ali drugih nadzornih naprav (Phillips in Pohl, 2025). Sumljivo je tudi, kadar ista konkurenčna podjetja organizacijo redno prehitevajo pri pridobivanju pomembnih poslovnih pogodb ali pri lansiranju produktov, ki so nenavadno podobni izdelkom in storitvam, ki jih je organizacija načrtovala. To lahko nakazuje na nedovoljen dostop do zaupnih informacij. Med skrajne primere sodi tudi dejansko odkritje

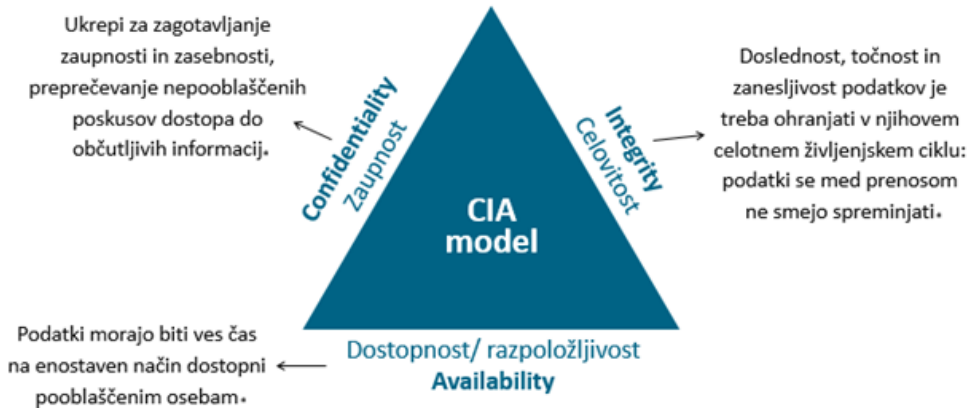
prisluškovalnih naprav, nepooblaščenih snemalnikov ali drugih tehničnih sredstev za nadzor in pridobivanje informacij v poslovnih prostorih organizacije. Prav tako lahko povečano zanimanje tujih podjetij ali posameznikov za obisk organizacije pomeni poskus zbiranja informacij pod krinko poslovnega sodelovanja. Dodaten pokazatelj možnega vohunjenja predstavljajo primeri tatvin zaupne dokumentacije, informacijskih sistemov, prenosnih računalnikov ali druge opreme, ki vsebuje občutljive podatke. Pomemben signal je tudi odhod ključnih zaposlenih v konkurenčna podjetja, še posebej če obstaja utemeljen sum, da bi lahko prenesli poslovno občutljive informacije in znanja. Nenazadnje velja omeniti, da nekatera konkurenčna podjetja ustanavljajo specializirane obveščevalne oddelke ali povečujejo število analitikov, ki se ukvarjajo s strateškim spremljanjem industrije, konkurenčne analize in poslovnega obveščanja, kar lahko pomeni izvajanje gospodarskega vohunjenja oziroma pripravo na takšne dejavnosti (Trim, 2002).

Pred vohunjenjem se podjetja lahko zaščitijo na različne načine. Z zaščito podatkov in informacij se ukvarja varnostni del korporativne obveščevalne dejavnosti, korporativna varnost oziroma protiobveščevalni sektor. Protiobveščevalna dejavnost v podjetju se nanaša na ukrepe, ki jih organizacija izvaja za zaščito svojih občutljivih informacij, poslovnih skrivnosti in sredstev pred zunanjimi grožnjami. Zunanje grožnje so na primer korporativno vohunjenje, konkurenčna obveščevalna dejavnost drugih podjetij in podobno. Glavni cilj je preprečevanje ali zmanjševanje tveganj, povezanih z izgubo podatkov, finančnimi izgubami ali škodo za ugled podjetja. Predvsem pa je v podjetju pomembno ozaveščanje zaposlenih in nadzor nad dostopi.

4.8 Zagotavljanje informacijske varnosti

Zagotavljanje informacijske varnosti je v organizaciji zahtevna naloga. Zagotoviti mora zaščito temeljnih poslovnih procesov in omogočiti njihovo nemoteno ter kredibilno delovanje. Sama učinkovitost informacijske varnosti je odvisna predvsem od pravilne izbire ukrepov, saj v nasprotnem primeru lahko pride do negativnih vplivov na neprekinjeno poslovanje, skladnost postopkov in podobno (Prislan in Bernik, 2013).

Zaščita podatkov in informacij je v organizaciji zelo pomembna. Vsaka organizacija, ki želi delovati učinkovito, mora zagotavljati varnost informacij. Zelo pomemben model varstva podatkov je triada CIA. Okrajšava imena predstavlja tri elemente in sicer: *Confidentiality* (zaupnost), *Integrity* (celovitost) in *Availability* (dostopnost oziroma razpoložljivost). Model CIA je bil razvit predvsem za pomoč posameznikom in organizacijam pri razvoju celovitega pristopa k varstvu podatkov (Infocenter, 2023).



Slika 5: CIA model
Vir: lasten.

4.9 Vpeljava korporativne obveščevalne dejavnosti v korporacijo

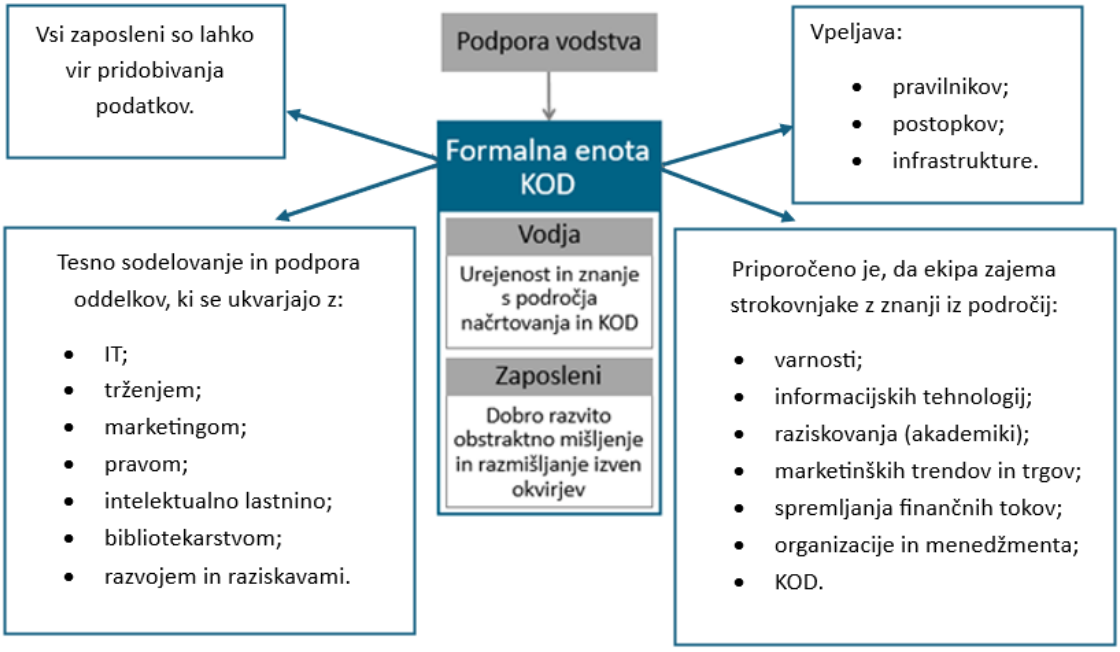
Korporativna obveščevalna dejavnost se je v korporacije vpeljala predvsem zaradi potrebe po formalni enoti, ki bi se sistematično ukvarjala s KOD. Prednost le-te je večja uspešnost organizacije, zaščita pred vohunjenjem in konkurenčna prednost. Pri vpeljavi takšne dejavnosti v organizacijo je potrebno:

- definirati prejemnike produktov;
- določiti način vpeljave;
- pripraviti sistemizacijo postopkov;
- seznaniti vodstvo z dejavnostjo;
- usposobiti zaposlene (predvsem na področju pridobivanja podatkov);
- pripraviti potrebne organizacijske ukrepe.

V multinacionalnem podjetju, ki je uvedlo KOD, analitiki redno pripravljajo poročila o konkurenci, tržnih trendih in možnih grožnjah, kar vodstvu omogoča hitrejše strateške odločanje.

4.10 Formalna enota korporativne obveščevalne dejavnosti

Formalna enota KOD predstavlja strukturiran pristop k zbiranju, analiziranju in uporabi informacij znotraj organizacije. Namen enote je zagotavljanje sistematičnega procesa KOD, ki omogoča boljše strateške odločitve, konkurenčno prednost in zaščito poslovnih skrivnosti.



Slika 6: Formalna enota KOD
Vir: lasten.

Vloga formalne enote je osrednji element organizacijske strukture za obveščevalno dejavnost. Njena vloga vključuje zbiranje podatkov, analizo in interpretacijo ter podporo odločanju. Za učinkovito delovanje deluje tesno v povezavi z drugimi ključnimi oddelki, kot so na primer IT, trženje, pravo, intelektualna lastnina, bibliotekarstvo ter razvoj in raziskave. Pri tem je podpora vodstva nujna, saj zagotavlja ustrezne vire, legitimnost in strateške usmeritve.

Odgovorite na vprašanja

Kaj je korporativna varnost v organizaciji?

Kaj so siva področja v korporativni obveščevalni dejavnosti?

Kateri dejavniki nakazujejo na neetična ravnanja?

Kaj spodbujajo etični kodeksi?

Kaj so etični kodeksi?

Katere tipe vprašanj zajema večina etičnih kodeksov?

Kaj predstavlja varnostna kultura v organizaciji?

Zakaj je varnostna kultura pomembna?

Katere so dimenzije varnostne kulture? Opišite jih.

Katere so značilnosti dobre varnostne kulture?

Kaj vključujemo v varnostno vedenje zaposlenih? Opišite.

Kaj je namen protiobveščevalne dejavnosti v zasebnem sektorju?

Katera so tri glavna vprašanja protiobveščevalne dejavnosti?

Kaj je pasivna protiobveščevalna dejavnost in kaj je aktivna?

Kateri so ukrepi za zagotavljanje varnosti podjetij?

Kaj je vohunjenje?

Kateri so znaki, ki kažejo na to, da je organizacija tarča vohunjenja?

Na kakšne načine se podjetja lahko zaščitijo pred vohunjenjem?

Kako se v organizaciji zagotavlja informacijska varnost?

Katera so tri ključna področja zagotavljanja informacijske varnosti?

Kaj je glavni razlog, da se je korporativna obveščevalna dejavnost sploh vpeljala v korporacijo?

Kaj je pri tem potrebno?

Na primeru večjega podjetja analizirajte, kako je korporativna varnost povezana z obveščevalnimi procesi. Ugotovite, katere informacije so ključne za preprečevanje notranjih in zunanjih groženj.

Predpostavite, da podjetje uvaja program ozaveščanja zaposlenih o varnostni kulturi. Pripravite predlog treh ukrepov za izboljšanje varnostnega vedenja zaposlenih z vidika zaščite informacij.

Univerzitetna založba
Univerze v Mariboru

5 Obveščevalni cikel

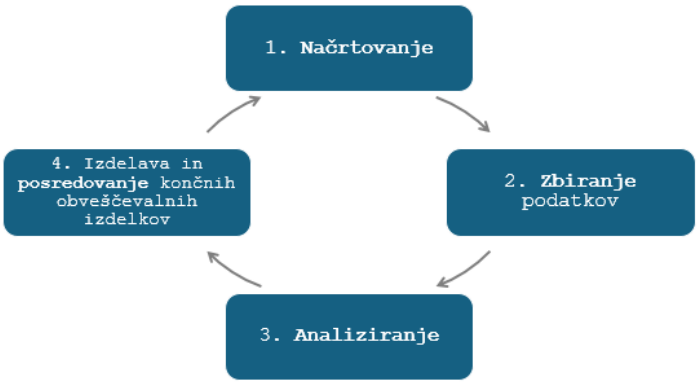
Obveščevalni cikel predstavlja jedro obveščevalne dejavnosti in ima ključno vlogo pri razumevanju tega področja. Obveščevalne dejavnosti potekajo po načelu obveščevalnega cikla, ki se izvaja v več zaporednih, ciklično povezanih korakih. Število teh korakov se od avtorja do avtorja razlikuje, prav tako pa se razlikujejo tudi poimenovanja posameznih stopenj oziroma korakov.

Do razlik med avtorji pride predvsem zato, ker nekateri avtorji posamezne stopnje oziroma korake razdeljujejo bolj podrobno. Na splošno ima krog štiri stopnje, in sicer so to:

1. načrtovanje – 1. stopnja;
2. zbiranje podatkov – 2. stopnja;
3. analiziranje (analitična obdelava podatkov in izdelava obveščevalnih izdelkov) – 3. stopnja;
4. izdelava in posredovanje končnih obveščevalnih izdelkov uporabnikom – 4. stopnja (Šaponja, 1999).

"Proces se začne z načrtovanjem, s katerim se določi kako, s kakšnimi sredstvi in katere podatke je treba zbrati. Naslednja stopnja je zbiranje podatkov. Zbrane podatke se posreduje analitičnim službam, ki podatke ovrednotijo in analizirajo, kar se odvija v tretji stopnji. Zbiralcem podatkov naložijo dodatno zbiranje podatkov, bodisi zato, ker jih imajo še vedno premalo, da bi lahko izdelali končni izdelek, bodisi zato, ker z analizo ugotovijo,

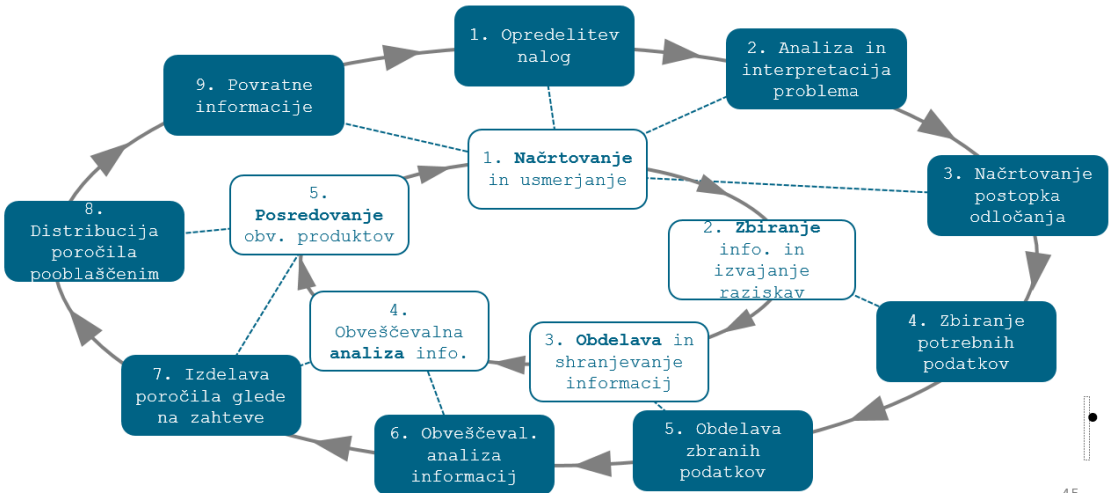
da jih je potrebno dodatno preveriti. Razlogov za dodatno zbiranje podatkov je poleg teh dveh osnovnih lahko še več. Četrta stopnja ciklusa je izdelava končnega izdelka kot rezultata celotnega obveščevalnega procesa, in sicer na podlagi analiz zbranih podatkov. Oblike končnih izdelkov so zelo različne in se prilagajajo namenu uporabe in uporabniku. Medsebojno se razlikujejo glede na to, ali gre za obveščevalne ali varnostne službe. Ciklus se lahko ponovno začne tudi takrat, kadar uporabnik z dobljenim odgovorom ni zadovoljen in želi še bolj poglobljeno analizo." (Šaponja 1999, str. 67)



Slika 7: Obveščevalni cikel
Vir: lasten.

V kontekstu korporativne obveščevalne dejavnosti obveščevalni cikel podjetjem omogoča sistematično zbiranje, analizo in uporabo informacij, ki zagotavljajo konkurenčno prednost.

Poznamo tudi petstopenjski in devetstopenjski obveščevalni cikel. Spodaj lahko vidimo primerjavo med njima.



Slika 8: 5-stopenjski obveščevalni cikel
Vir: lasten.

Richelson (1989 v Purg, 2002) pojasnjuje posamezne stopnje petstopenjskega obveščevalnega cikla. Pojem obveščevalnega ciklusa zajema zbiranje in obdelavo podatkov in njihovo posredovanje ustreznim organom.

Ta cikel je sestavljen iz petih stopenj:

1. Načrtovanje in usmerjanje – zajema menedžment celotnega postopka pridobivanja obveščevalnih podatkov, od identifikacije potrebe po podatkih do izročitve obveščevalnega izdelka naročniku. Opredeliti je treba tudi cilje in objekte obveščevalnega delovanja, z operativnim načrtom pa se določijo podrobnosti (kaj, zakaj, kako ipd.).
2. Zbiranje – zajema pridobivanje surovih podatkov, iz katerih se nato izdela končni obveščevalni izdelek. Podatki se lahko zbirajo preko javnih virov, elektronskih medijev, fotografiranja, človeških virov, posebnih metod zbiranja, nadzora telekomunikacijskih sredstev, nadzora poštnih pošiljk, prisluškovanja v prostoru, tajnega sledenja ipd.
3. Obdelava – nanaša se na spremembo ogromne količine podatkov v obliko, ki je primernejša za izdelavo obveščevalne informacije. Zajema prevajanje, dekodiranje in sortiranje podatkov po vsebini in količini.
4. Analiza – osnovna informacija se spremeni v končni obveščevalni podatek. Pri tem se integrirajo vsi razpoložljivi podatki, lahko pa se jih tudi interpretira in oceni.
5. Posredovanje – pomeni distribucijo in izročitev končnega obveščevalnega podatka uporabnikom in naročnikom (Richelson, 1989 v Purg, 2002).

Primer je, ko podjetje spremlja konkurenco. Strateško določi, katere trge in konkurente spremljati (načrtovanje), zbira podatke iz javnih baz ter medijev (zbiranje), analizira trende in primerja s svojimi produkti (analiza) ter nato pripravi poročilo za vodstvo (posredovanje).

Kot že omenjeno so stopnje štiristopenjskega cikla: načrtovanje, zbiranje podatkov, analiza in izdelovanje ter posredovanje končnih obveščevalnih izdelkov.

5.1 Načrtovanje

Šaponja (1999) stopnjo načrtovanja razdeli na strateški, operativni in taktični načrt. V strateškem načrtu obveščevalna služba opredeli način in postopke ter naloge, ki izhajajo iz delovnih usmeritev usmerjevalcev. Strateški načrt je pogosto razdeljen na dva dela, na splošni in na del, ki zajema organizacijske, kadrovske, materialne ter finančne zadeve. Sam strateški načrt je podlaga za oblikovanje operativnega načrta v ostalih stopnjah

obveščevalnega kroga. Operativni načrt se nanaša na izvajanje konkretnih nalog. Izhaja iz analize problema in načinov rešitev. Najožji vrhovi obveščevalnovarnostnih služb potrdijo in dovoljujejo operativne načrte. Taktični načrt pa pomeni načrtovanje konkretnega postopka in potrebnih finančnih, človeških ter drugih virov. Pri tem je potrebno upoštevati taktična načela in pravila. Pregledati je potrebno že obstoječe znanje, ki ga organizacija poseduje, načrtovati pa je potrebno zbiranje podatkov, kamor uvrščamo identifikacijo tipov podatkov oziroma informacij, ki jih bomo pridobili in identifikacijo virov.

5.2 Zbiranje podatkov

Zbiranje podatkov predstavlja drugo fazo obveščevalnega cikla, ki sledi določanju potreb in ciljev obveščevalne dejavnosti. Zbiranje podatkov je najbolj izpostavljen vidik obveščevalne dejavnosti. Ta stopnja pomeni pridobivanje neobdelanih surovih podatkov in informacij. Takšni podatki so osnovni, nepovezani in še niso umeščeni v celoto. Zbiranje le-teh mora biti sistematično organizirano in vodeno. Pri tem se uporabljajo notranji, zunanji in javno dostopni viri. Dodamo pa lahko tudi dodatno zbiranje nejavnih oziroma internih informacij s spraševanjem ljudi. Predvsem je pomembna varna hramba podatkov in virov, dostop do le-teh pa je omogočen le tistim, ki so upravičeni do seznanitve s temi podatki. Zbiranje podatkov mora vedno potekati zakonito in etično (Ajayi, 2023). Etika zbiranja podatkov zajema spoštovanje zasebnosti posameznikov, zaupnosti poslovnih informacij in skladnost z zakonodajo o varstvu osebnih podatkov ter poslovnih skrivnosti (Bartes, 2011).

Viri preko katerih se pridobivajo podatki morajo biti vredni zaupanja oziroma zanesljivi. Delimo jih na primarne in sekundarne vire. Pri vrednotenju virov je ključno upoštevati njihovo zanesljivost, objektivnost, dostopnost in preverljivost. Vsak vir mora biti analiziran glede na možnost pristranskosti in namen, s katerim je bil ustvarjen (Ajayi, 2023). *Primarni viri* so posamezniki, kot so na primer zaposleni v podjetju, strokovnjaki iz drugih organizacij in podobno. Vključujejo pridobivanje podatkov od človeških virov, osebno zaznavo, udeležbo na sejmih in podobno. Pridobivanje podatkov od takšnih virov zahteva znanje s področja intervjuvanja in mreženja. *Sekundarni viri* pa so javno dostopni (na primer baze, znanstvene revije, tržne publikacije, novice, mediji, spletne strani podjetij, letna poročila, televizijska poročanja in knjige) ter interni dokumenti (Bartes, 2011).

»Kjerkoli pridobivaš podatke, vedno si najuspešnejši, če jih pridobivaš po različnih kanalih, od katerih je kljub internetu in sodobni informacijski družbi človek (HUMINT) še vedno ključnega pomena, enako kot pred 2.500 leti v času kitajskega generala.« (Dvoršak, 2003, str. 2)

HUMINT metoda pridobivanja podatkov (angl. *Human Intelligence*) predstavlja pridobivanje podatkov z uporabo človeških virov. Predstavlja obveščevalne mreže ljudi (na primer kontakti s strankami, zaposlenimi, strokovnjaki, konkurenti, tržnimi analitiki, novinarji, univerzitetnimi profesorji, vladnimi predstavniki in dobavitelji), podatki pa se pridobivajo na javen ali tajen način. Človeški vir je oseba, od katere se podatki pridobivajo z razlogom, da se jih uporabi za zagotovitev obveščevalnih potreb. Te podatke zbira HUMINT- strokovnjak, ki je usposobljen za to zbiranje. Pri teh metodi je potrebno upoštevati tveganja, ki so povezana z varnostjo virov, možnostjo napačne interpretacije informacij in etičnimi dilemami pri pridobivanju podatkov (Henschke, 2024).

OSINT metoda pridobivanja podatkov (angl. *Open Source Intelligence*) predstavlja pridobivanje podatkov iz javno dostopnih virov. Velja za ključno metodo pridobivanja podatkov v zasebnem sektorju. Javno dostopni viri pa so na primer spletni viri, letna poročila, knjige in časopisi, revije, baze ter drugi mediji. Več o metodi OSINT pa bo predstavljeno v nadaljevanju.

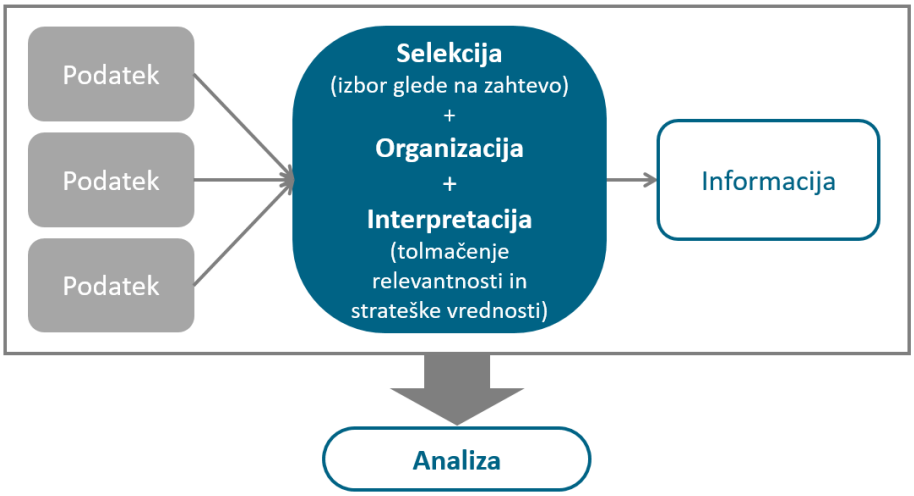
5.3 Analiza

Analiza predstavlja tretjo fazo obveščevalnega cikla, kjer se zbrani podatki pretvorijo v uporabne informacije, ki podpirajo odločanje v organizaciji. Z analizo se navidezno nepovezane in surove podatke pretvori v obveščevalne informacije. Predstavlja osrednji element obveščevalnega procesa in predstavlja največji izziv ter zahteva najvišjo usposobljenost tistih, ki se z njo ukvarjajo.

"Večplastno, multidisciplinarno kombinacijo znanstvenih in neznanstvenih procesov s katerimi posamezniki interpretirajo podatke ali informacije z namenom zagotovitve pomembnih spoznanj. Uporablja se za izpeljavo korelacij, ocenjevanje trendov in vzorcev, identificiranja vrzeli v zmogljivostih, in predvsem ugotavljanje ter ocenjevanje priložnosti, ki so na voljo organizaciji. Analiza odgovori na kritično »pa kaj?« (angl. *so what?*) vprašanje pri zbranih podatkih in omogoči vpogled, utemeljen na potrebah odločevalcev." (Fleisher in Bensoussan, 2003). Namen analize je torej ustvariti relevantno obveščevalno sliko, ki odločevalcem omogoča razumevanje okolja, konkurence in priložnosti za ukrepanje.

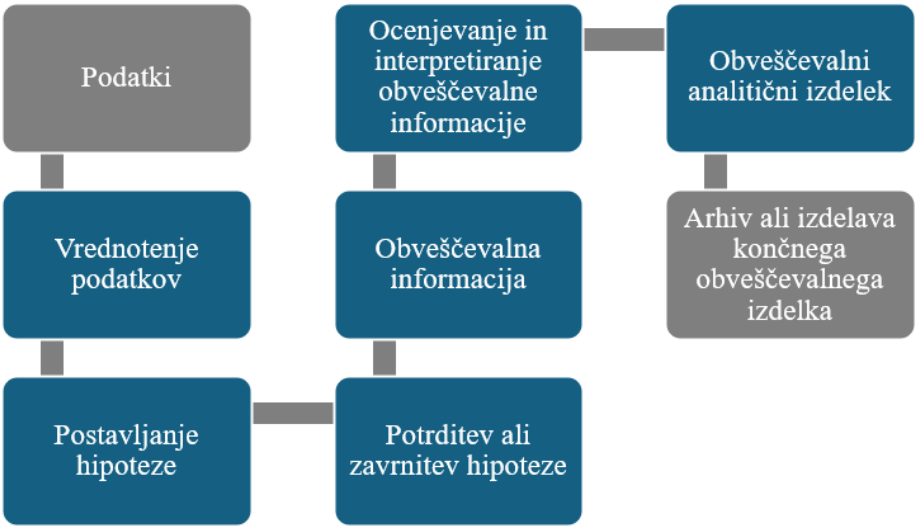
Podatke se najprej obdela tako, da se jih pretvori v obliko, primerno za analizo. To se naredi na primer z vrednotenjem podatkov, pisanjem povzetkov o ključnih dejstvih, prevajanjem, dešifriranjem, selekcijo in primerjavo. Preverja se zanesljivost, pravilnost oziroma točnost, aktualnost in celovitost teh virov ter informacij. Analiza mora temeljiti na potrebah naročnika oziroma uporabnika končnega izdelka.

Obdelava podatkov:



Slika 9: Obdelava podatkov
Vir: lasten.

Analitični proces:



Slika 10: Analitični proces
Vir: lasten.

Modeli in tehnike, ki se uporabljajo pri analizi, so:

- analiza SWOT;
- primerjalno ocenjevanje/analiza (angl. *Benchmarking*);
- analiza okolja (STEEP);
- načrtovanje oziroma analiza scenarijev;
- analiza PEST;
- Porterjev model petih sil (angl. *Porter's Five Forces*);
- profiliranje konkurentov;
- slepe točke (angl. *blind spots*);
- tehnika štirih kotov (angl. *Four Corner*).

5.3.1 SWOT analiza

Analiza SWOT je ena izmed osnovnih in najpogosteje uporabljenih metod v procesu konkurenčne obveščevalne analize.

	Pozitivni dejavniki	**Negativni dejavniki**
Notranji dejavniki Na njih lahko neposredno vplivamo sami. *Osebje, finance, proizvodne zmogljivosti, marketing, raziskave in razvoj, nabava, prodaja …*	**Strengths – prednosti** Značilnosti organizacije, ki predstavljajo prednosti pred drugimi. *V čem smo dobri oz. boljši od konkurence (npr. posedovanje veščin, tehničnega znanja, tehnologij in kakovost)?*	**Weaknesses – slabosti** Lastnosti, ki organizacijo postavijo v slabši položaj glede na druge. *Kje je treba izboljšati organizacijo (npr. pomanjanje veščin, ugleda, nestrokovni kadri, slaba lokacija, nelikvidnost in slaba kakovost)?*
Zunanji dejavniki Na njih ne moremo vplivati sami. *Makroekonomija, tehnološke spremembe, zakonodaja, družbeno-kulturne spremembe in spremembe na trgu (novi tržni trendi ipd.) …*	**Opportunities – priložnosti** Dejanski ali potencialni pogoji, ki (lahko) koristijo organizaciji oz. pozitivno vplivajo na njeno delovanje. *Npr. nižji davki, liberalizacija trgov, zvesti kupci, malo konkurentov in rastoči trg.*	**Threats – nevarnosti oz. grožnje** Dejanski ali potencialni pogoji, ki (lahko) negativno vplivajo na organizacijo. *Npr. povišanje davkov, vstop novega močnega konkurenta, negotove gospodarske razmere in neplačniki.*

Slika 11: SWOT analiza
Vir: lasten.

Analiza SWOT oceni prednosti, slabosti, priložnosti in nevarnosti oziroma grožnje, s katerimi se podjetje sooča. Z analizo se ugotavlja, kje je podjetje močna in kje šibka, kateri zunanji ter notranji dejavniki bi lahko pripomogli ali škodovali uspehu delovanja podjetja in na katerih področjih poslovanja je potrebne več pozornosti za rast. Predstavlja pomembno orodje za analizo varnosti in določitev načinov, za izboljšavo področja varnosti v prihodnosti (Thinkcurity, 2022).

Analiza se uporablja za oceno konkurenčnega položaja podjetja in za razvoj strateškega načrtovanja. Predstavlja tudi tehniko za oceno uspešnosti, tveganja, konkurenčnosti in potenciala podjetja, kamor spada tudi celotno delo podjetja (Kenton, 2023).

Na začetku je potrebno določiti prednosti in slabosti. Le-te predstavljajo notranje dejavnike, ki kot taki vplivajo na poslovanje podjetja. Po tem se določijo priložnosti in nevarnosti, ki pa predstavljajo zunanje dejavnike, ki vplivajo na podjetje ter njegovo uspešnost (Thinkcurity, 2022). Prednosti pri analizi SWOT so ugodne notranje dejavnosti procesi in vedenja podjetja. To so dejavniki, ki prispevajo k uspehu podjetja in njegove znamke. Slabosti pa so notranji dejavniki, ki zavirajo razvoj podjetja. Lahko so posledica kulture podjetja, pomanjkanja virov ali pomanjkanja procesov upravljanja. Prepoznava slabosti je bistvenega pomena za vsako analizo SWOT. S tem se omogoči, da se prepoznajo področja, na katerih so mogoče izboljšave (Thinkcurity, 2022). Priložnosti in nevarnosti oziroma grožnje so zunanji dejavniki, saj se nanašajo na dogajanje zunaj podjetja. Priložnosti predstavljajo možnosti, da se v prihodnosti zgodi nekaj pozitivnega, oziroma odgovor na vprašanje, kaj bi se lahko zgodilo. Grožnje oziroma nevarnosti pa so zunanji dejavniki, ki lahko negativno vplivajo na podjetje in nanje podjetje nima neposrednega vpliva (Parsons, 2025).

Da bi analiza SWOT bila uspešna, mora pri njej sodelovati skupina ljudi iz različnih oddelkov podjetja. Pri tem gre za tako imenovani "*brainstorming*", pri katerem vsak zaposleni poda svoje ideje in mnenja (Kenton, 2023).

V okviru korporativne obveščevalne dejavnosti se analiza SWOT uporablja za oceno notranje varnosti, prepoznavanje tržnih tveganj in razvoj konkurenčnih strategij.

Najboljši čas za izvedbo analize SWOT je:

- na začetku leta, saj je s tem podjetje pripravljeno na sprejemanje odločitev;
- enkrat na leto ali večkrat: priporočljivo je, da se analiza opravi vsaj enkrat letno, lahko pa tudi večkrat, saj v podjetjih pogosto prihaja do sprememb;
- ko v podjetju pride do sprememb;
- ob ustanovitvi podjetja: analiza je način za preverjanje sposobnosti idej posameznikov in strateškega načrta (Furgison, 2020).

5.3.2 BENCHMARKING – primerjalno vrednotenje

Benchmarking oz. primerjalno vrednotenje ima v obveščevalnem procesu pomembno vlogo pri primerjalni analizi uspešnosti in prepoznavanju najboljših praks konkurence.

Slika 12: Benchmarking – primerjalno vrednotenje
Vir: lasten.

Benchmarking se uporablja za več različnih namenov. Je orodje za merjenje, učenje in pripomore k izboljšavam. Je orodje, ki se uporablja za primerjavo podjetij, njihovih procesov, proizvodov, storitev in poslovanja z ostalimi podjetji. Osnovni namen *benchmarkinga* je nenehno izboljševanje najboljših rezultatov. Identificira se priložnosti za izboljšanje in implementacije najboljše prakse za višjo uspešnost. S pravilnim pristopom k *benchmarkingu* se izboljšuje delovanje, prispeva pa se tudi k rasti in inovacijam v celotni industriji (Todorović, 2023).

V okviru KOD je *benchmarking* ključen za spremljanje konkurenčnih trendov in prilagajanje poslovnih strategij spremembam v okolju.

5.3.3 STEEP – analiza okolja

Social Socialni oz. družbeni dejavniki	**Technological** Tehnološki dejavniki	**Economical** Ekonomski dejavniki	**Ecological** Ekološki oz. okoljski dejavniki	**Political** Politični dejavniki
Družbene spremembe: demografske spremembe, kultura, vedenje in življenjski slog ljudi.	Tehnološki napredek: inovacije in trendi razvoja produktov.	Ekonomsko okolje: ekonomska rast, obrestne mere, dohodek, trg in konkurenca.	Ekološki vpliv produktov in storitev.	Politične spremembe vključujejo zakonodajo in regulacije trga.

Slika 13: STEEP-analiza okolja
Vir: lasten.

Analiza STEEP podjetjem omogoča celovito razumevanje širšega konteksta okolja, v katerem delujejo, ter prepoznavanje ključnih makrotrendov, ki vplivajo na njihovo konkurenčnost.

Wheelen in Hunger (2012) navajata, da se analiza STEEP ukvarja z analiziranjem in spremljanjem razvojnih trendov v širšem ter naravnem okolju. Ime analize je sestavljeno iz začetnih črk posameznih dejavnikov. Duhova (2015) je ta področja poimenovala:

- družbeno-kulturna;
- tehnološka;
- gospodarska;
- ekološka;
- politično-pravna.

5.3.4 PEST analiza

Analiza PEST je tesno povezana z analizo STEEP in se pogosto uporablja v zgodnjih fazah strateškega načrtovanja.

Analiza zunanjih makro dejavnikov

Political factor Politični vpliv	**Economic factor** Ekonomski vpliv	**Social factor** Socialni oz. družbeni vpliv	**Technological factor** Tehnološki vpliv
Analiza pravnih, regulacijskih in drugih standardov ter politične stabilnosti in vladnega vpliva na ekonomijo. *Npr. davčna politika, delovno pravo, okoljska zakonodaja, trgovske omejitve, carinske dajatve, politična stabilnost, režim, zakonodajni trendi, stopnja korupcije.*	Analiza vpliva ekonomskih dejavnikov na finančno poslovanje podjetja. *Npr. ekonomska rast, obrestne mere, menjalni tečaji, stopnja inflacije, vpliv globalizacije, strošek delovne sile.*	Analiza socialnih, psiholoških in kulturnih faktorjev. *Npr. kulturni vidiki in ozaveščenost o skrbi za zdravje, demografska slika (npr. stopnja rasti populacije in razporeditev populacije po starosti), odnos do poklicnega napredovanja, izobrazbena sestava, življenjski slog prebivalstva, migracije, distribucija prihodkov.*	Analiza tehnološke razvitosti določenega okolja. *Npr. raziskave in razvoj, avtomatizacija, spodbujanje tehnologije in stopnja tehnoloških sprememb, vpliv tehnologije, dostop do interneta in mobilnih tehnologij.*

Slika 14: PEST analiza
Vir: lasten.

PEST analiza je eno izmed najbolj priljubljenih orodij, ki se uporablja pri poslovni analizi. Obsega okoliščine, v katerih se znajdejo posamezniki, izdelki ali podjetja, ter dejavnike, ki lahko pomagajo pri sprejemanju odločitev in razumevanju trenutnega ali prihodnjega položaja na trgu (Bush, 2016). Gre za analizo, ki je posebej primerna za proučevanje poslovnega okolja. Že iz imena PEST je razvidno, da vključuje štiri dejavnike, in sicer:

- P – pravno-politični dejavniki,
- E – ekonomski dejavniki,
- S – sociokulturni dejavniki
- T – tehnološki dejavniki (SPOT, 2023).

Na primer, politični dejavniki lahko vključujejo spremembe zakonodaje ali davčne politike, ekonomsko gospodarske cikle in tehnološki napredek, ki vpliva na digitalizacijo poslovanja.

5.4 Izdelava in posredovanje končnih obveščevalnih izdelkov

Zadnja stopnja obveščevalnega cikla, ki je zaradi njegove ciklične narave lahko hkrati tudi prva, je izdelava in posredovanje končnih obveščevalnih izdelkov. Kot navaja Šaponja (1999), je oblika obveščevalnega izdelka odvisna od potreb uporabnika in vrste organizacije: »V tej stopnji obveščevalnega delovnega procesa dobijo analitični izdelki obliko, ki je za uporabnika najbolj primerna, obliko, ki jo določa zakon. Glede na zahteve in vrsto naročnikov ter vrsto službe izbere vodstvo najprimernejši analitični izdelek ali več takih izdelkov skupaj. Poseben oddelek službe ali njegov del zadolži, da izdelek ustrezno oblikuje.« (Šaponja, 1999, str. 169)

Med izdelavo obveščevalnih izdelkov spada tudi povzetek ugotovitev v obliki poročila. Poročilo mora biti jasno, jedrnato in sistematično urejeno. Vsebuje opis in cilje naloge, opombe k poročilu, zaključke oziroma ugotovitve obveščevalne analize, predloge ukrepov, ki jih je treba sprejeti, ter priloge; lahko pa vključuje tudi predstavitve, dokumente, elektronske medije in podobno. Pri tem je treba paziti, da se v poročilu ali na kakršen koli drug način ne razkrijejo viri in uporabljeno znanje. Pri pripravi poročil je treba dosledno upoštevati načelo varovanja virov, kar pomeni, da se identiteta vira, način zbiranja podatkov in uporabljene metode zaščitijo pred razkritjem, saj bi njihova objava lahko ogrozila nadaljnje delovanje obveščevalnega sistema ali povzročila pravne posledice.

Posredovanje pomeni razširjanje oziroma predstavitev omenjenega poročila pooblaščenim prejemnikom. Omogočeno je zgolj tistim osebam, ki se morajo z vsebino seznaniti in na njeni podlagi ukrepati. Takšni obveščevalni izdelki so običajno namenjeni najvišjemu vodstvu organizacije. Prekomerna distribucija lahko povzroči zmanjšanje zaznane vrednosti teh izdelkov ter poveča tveganje za razkritje oziroma uhajanje informacij izven organizacije. Ob predstavitvi oziroma seznanitvi s končnimi izdelki se pogosto pojavijo nova vprašanja, ki zahtevajo ponoven začetek obveščevalnega cikla.

Odgovorite na vprašanja

Kaj je obveščevalni cikel?

Katere so štiri stopnje cikla?

Na kratko opišite proces cikla obveščanja.

Katere so stopnje 5-stopenjskega obveščevalnega cikla? Na kratko jih predstavite.

Kaj je SWOT analiza? Opišite jo.

Kdaj je najboljši čas za izvedbo SWOT analize?

Kaj je benchmarking?

Kaj je STEEP analiza okolja?

Kaj je PEST analiza?

Izberite podjetje in izvedite eno izmed analiz glede na aktualno poslovno okolje. Rezultate predstavite v kratkem obveščevalnem poročilu in interpretirajte glavne ugotovitve.

Univerzitetna založba
Univerze v Mariboru

6 Zakonodaja

Pravna ureditev predstavlja temeljno izhodišče za zakonito izvajanje korporativne obveščevalne dejavnosti, saj se ta pogosto dotika občutljivih osebnih, poslovnih in tajnih podatkov. Razumevanje veljavne zakonodaje je zato nujno za preprečevanje zlorab, varovanje zasebnosti ter zagotavljanje skladnosti z etičnimi in pravnimi normami.

Zakonodaja, ki se ukvarja s predmeti korporativne obveščevalne dejavnosti:

- *General data protection regulation* (GDPR) oziroma Splošna uredba o varstvu podatkov (SUVP);
- Zakon o varstvu osebnih podatkov (ZVOP-2);
- Zakon o delovnih razmerjih (ZDR): prepoved konkurence;
- Zakon o dostopu do informacij javnega značaja;
- Zakon o informacijski varnosti (ZinfV);
- Zakon o poslovni skrivnosti (ZposS);
- Zakon o tajnih podatkih (ZTP) itd.

6.1 General data protection regulation (GDPR) – Splošna uredba o varstvu podatkov (SUVP)

Določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o prostem pretoku osebnih podatkov. varuje temeljne pravice ter svoboščine posameznikovih in zlasti njihovo pravico do varstva osebnih podatkov.

V okviru korporativne obveščevalne dejavnosti se pogosto obdelujejo osebni podatki zaposlenih, poslovnih partnerjev ali strank. Zato morajo biti vsi postopki zbiranja, shranjevanja in analiziranja podatkov usklajeni z določbami GDPR.

Osebni podatek je katerakoli informacija v zvezi z določenim ali določljivim posameznikom.

Pravica do dostopa: posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca dobiti potrditev, ali se v zvezi z njim obdelujejo osebni podatki, in kadar je temu tako, dostop do osebnih podatkov ter drugih povezanih informacij.

Pravica do popravka: posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja popravi netočne osebne podatkov zvezi z njim.

Pravica do izbrisa oziroma pozabe: posameznik, na katerega se nanašajo osebni podatki, ima pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim, upravljavec pa ima obveznost osebne podatke brez nepotrebnega odlašanja izbrisati

Pomembna je tudi pooblaščena oseba za varstvo podatkov (DPO), ki organizaciji svetuje glede skladnosti z uredbo, spremlja izvajanje varnostnih ukrepov in deluje kot kontaktna točka z nadzornim organom (Informacijskim pooblaščencem).

Upravljavec mora v primeru kršitev, popravkov ali izbrisov osebnih podatkov ali omejitve obdelave obvestiti osebe. V vsaki organizaciji mora biti imenovana tudi pooblaščena oseba za varstvo podatkov.

6.2 Zakon o varstvu osebnih podatkov (ZVOP-2)

ZVOP-2 dopolnjuje in natančneje ureja izvajanje Splošne uredbe o varstvu podatkov v slovenskem pravnem prostoru.

Ureja uresničevanje človekove pravice do varstva osebnih podatkov. Obdelava osebnih podatkov je prepovedana, če se izvaja na način ali ima za posledico nedopustno diskriminacijo glede na:

- narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, invalidnost, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske predispozicije, druge osebne okoliščine posameznika itd.

Rok hrambe osebnih podatkov je omejen na najkrajše možno obdobje in le, dokler je hramba potrebna za dosego namena obdelave, zaradi katerega so se osebni podatki zbirali in nadalje obdelovali, razen če drug zakon za posamezne obdelave določa rok hrambe. Po izpolnitvi namena obdelave se osebni podatki izbrišejo, uničijo ali anonimizirajo oziroma se izvede drug postopek, ki onemogoča identifikacijo posameznika, na katerega se nanašajo osebni podatki, zlasti omejevanje dostopa do njih, njihovo blokiranje ali arhiviranje.

Pooblaščena oseba za varstvo osebnih podatkov: upravljavcu ali obdelovalcu na neodvisen način svetuje pri zagotavljanju skladnosti obdelave s Splošno uredbo in z zakonom. Obdelava osebnih podatkov za raziskovanje je dovoljena, če se upošteva etična načela in metodologijo ter pravila glede varstva osebnih podatkov.

Videonadzor predstavlja pomemben element pri varovanju premoženja in informacijskih sistemov, vendar mora biti vedno izveden v skladu z načelom sorazmernosti ter spoštovanjem zasebnosti posameznikov. Določbe o videonadzoru in varstvu osebnih podatkov:

- Odločitev o uvedbi videonadzora sprejme predstojnik, direktor ali drug pooblaščen posameznik.
- V pisni odločbi morajo biti obrazloženi razlogi za uvedbo videonadzora.
- Smiselno se na vidnem mestu objavi obvestilo, ki vsebuje: pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor; namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov; informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave; kontaktne podatke pooblaščene osebe (tel. številka ali naslov e-pošte); neobičajne nadaljnje obdelave (npr. prenosi subjektom v tretje države, spremljanje dogajanja v živo in možnost zvočne intervencije v primeru spremljanja dogajanja v živo).
- Zbirka posnetkov videonadzornega sistema vsebuje: posnetek posameznika (slika), podatek o lokaciji, datum in čas posnetka, izjemoma tudi zvok.

– Praviloma se posnetki videonadzora hranijo največ eno leto.

Videonadzor ni dovoljeno izvajati v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in podobno. Zagotovljen mora biti dnevnik vpogledov, obdelave in posredovanja posnetkov. Videonadzor dostopa v uradne službene oziroma poslovne prostore se lahko izvaja, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Znotraj delovnih prostorov se lahko izvaja le, kadar je to nujno potrebno za varnost ljudi ali premoženja ali preprečevanje ali varovanje tajnih podatkov ali poslovnih skrivnosti in podobno, teh namenov pa ni mogoče doseči z milejšimi sredstvi. Videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, se sme izvajati le v delih prevoznega sredstva, namenjenih potnikom, za namen varnosti potnikov in premoženja ter tega ni mogoče doseči z milejšimi ukrepi. Na javnih površinah je videonadzor dovoljen le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in tega ni mogoče doseči z milejšimi sredstvi. Obdelava biometričnih osebnih podatkov pa lahko poteka le, če je to nujno potrebno.

ZVOP-2 tako predstavlja nacionalni okvir za etično in zakonito uporabo osebnih podatkov, kar je ključno tudi v procesih korporativne obveščevalne dejavnosti, kjer so informacije pogosto občutljive narave.

6.3 Zakon o poslovni skrivnosti (ZposS)

Ureja področje poslovne skrivnosti, pravila določitve in varstva poslovne skrivnosti pred njeno protipravno pridobitvijo, uporabo ter razkritjem. Poslovna skrivnost zajema nerazkrito strokovno znanje, izkušnje in poslovne informacije, ki izpolnjujejo naslednje zahteve:

– je skrivnost, ki ni splošno znana ali lahko dosegljiva osebam v krogih, ki se običajno ukvarjajo s to vrsto informacij;
– ima tržno vrednost;
– imetnik poslovne skrivnosti je v danih okoliščinah razumno ukrepal, da jo ohrani kot skrivnost (na primer določil v pisni obliki ali seznanil uporabnike).

Pomen Zakona o poslovni skrivnosti presega zgolj pravno varstvo informacij. V kontekstu korporativne obveščevalne dejavnosti zakon določa meje med zakonito konkurenčno analizo in protipravnim pridobivanjem informacij. Kahaner (1997) poudarja, da poznavanje zakonodaje o poslovnih skrivnostih podjetjem omogoča etično izvajanje konkurenčne inteligence, kar zmanjšuje pravna tveganja in krepi ugled organizacije.
Za poslovno skrivnost se ne morejo določiti informacije, ki so po zakonu javne in informacije o kršitvi zakona ali poslovnih običajev. Pridobitev poslovne skrivnosti se šteje za zakonito, če se pridobi z:

- neodvisnim odkritjem ali stvaritvijo;
- opazovanjem, proučevanjem, razstavljanjem na sestavne dele ali preizkušanjem izdelka ali predmeta, ki je bil dan na voljo javnosti ali je v zakoniti posesti pridobitelja, katerega ne zavezuje nobena pravno veljavna dolžnost omejitve pridobitve poslovne skrivnosti;
- uresničevanjem pravice delavcev ali predstavnikov delavcev do obveščenosti in posvetovanja v skladu z veljavnimi predpisi, kadar je tako razkritje potrebno za ta namen;
- vsakim drugim ravnanjem, za katero se v danih okoliščinah šteje, da je v skladu s poštenimi poslovnimi praksami;
- uresničevanjem pravice dostopa do informacij javnega značaja ali v skladu z zakoni ipd.

Pridobitev poslovne skrivnosti je protipravna, če se izvede z neposrednim nedovoljenim dostopom, prisvojitvijo ali kopiranjem vsebin, ki vsebujejo poslovno skrivnost ali je iz njih mogoče dognati poslovno skrivnost, ali z drugim ravnanjem, za katero se šteje, da je v nasprotju s poštenimi poslovnimi praksami. Pridobi se od osebe, ki je poslovno skrivnost uporabljala ali razkrila protipravno, vendar je pridobitelj v času pridobitve za to vedel ali bi v danih okoliščinah to moral vedeti.

Uporaba ali razkritje poslovne skrivnosti sta protipravna, če jo uporabi ali razkrije oseba, ki izpolnjuje enega od teh pogojev:

- poslovno skrivnost je pridobila protipravno;
- krši sporazum o zaupnosti/drugo dolžnost molčečnosti v zvezi s poslovnimi skrivnostmi;
- krši pogodbeno/drugo dolžnost omejitve uporabe poslovne skrivnosti;
- je v času uporabe ali razkritja vedela ali bi morala vedeti, da je bila poslovna skrivnost, ki jo je pridobila od druge osebe uporabljena ali razkrita protipravno.

Za KOD to pomeni, da so metode, kot so analiza javno dostopnih virov, tržne raziskave ali analiza konkurentov na podlagi zakonitih virov, dopustne in priporočene.

6.3.1 Ostalo o poslovni skrivnosti

Poslovna skrivnost ščiti tudi podatke, znanje in vrednosti gospodarske družbe pred konkurenco. Z razkritjem nepooblaščeni osebi bi lahko nastala občutna škoda. Varuje znanje o:

- načinu in postopku organiziranja določenega delovnega procesa;
- tehnologiji;
- informacijah o poslovnih partnerjih;
- zaposlenih;
- finančnih podatkih;
- drugih vrstah pomembnih informacij (ki so se znotraj gospodarske družbe zbirale in razvijale več let).

Predmet poslovne skrivnosti je vedno dejstvo in ne domneva.
V kontekstu korporativne obveščevalne dejavnosti pomen varovanja poslovnih skrivnosti ni le v zaščiti informacij, temveč tudi v oblikovanju organizacijske kulture zaupnosti.

6.3.2 Varovanje poslovnih skrivnosti

Sistem varovanja poslovnih skrivnosti mora biti del celovite varnostne politike podjetja in temeljiti na oceni tveganj.

Celovit sistem varovanja poslovne skrivnosti mora vključevati:

- kadrovsko varnost: varnostno preverjanje zaposlenih; varnostno izobraževanje, usposabljanje in izpopolnjevanje zaposlenih; varovanje oseb na izpostavljenih delovnih mestih;
- fizično varnost: fizično in tehnično varovanje, določitev varnostnih območij, opredelitev načina vstopa ter izbor sistema varovanja;
- administrativno varnost: označevanje, obdelovanje, posredovanje, hranjenje in uničevanje medijev z zapisom podatkov, označenih kot poslovna skrivnost; določanje stopnje tajnosti poslovne skrivnosti; opredelitev nalog vseh oseb, ki se ukvarjajo z varovanjem poslovnih skrivnosti;

- informacijsko varnost: vzpostavitev in vzdrževanje učinkovitega sistema z zagotovljeno tajnostjo in dostopnostjo podatkov, ki so shranjeni, obdelovani ali poslani preko informacijskega omrežja; zasnova politike informacijske varnosti; odobritev ustreznega varnostnega organa pred uporabo informacijskega omrežja za shranjevanje, obdelovanje ali prenos tajnih podatkov; opredelitev pogojev za priključitev zunanjih informacijskih sistemov v informacijsko omrežje gospodarske družbe; določitev načinov sporočanja incidentov, povezanih z informacijsko varnostjo, ustreznemu varnostnemu organu gospodarske družbe;
- industrijsko varnost.

Pomembno je oblikovanje internih pravil, ki razvijajo čut za varovanje poslovnih skrivnosti in urejajo področje odnosa posameznikov, ki zapuščajo gospodarsko družbo, do poslovnih skrivnosti družbe. Varnostni ukrepi morajo temeljiti na oceni ogroženosti. Za vzpostavitev in izvajanje sistemov varovanja poslovne skrivnosti je odgovorno vodstvo in vsi zaposleni.

Interni dokument, ki bi jasno predstavljal pravilne načine obravnave poslovnih skrivnosti, naj bi vseboval naslednje sklope:

- splošne določbe;
- stopnje tajnosti poslovnih skrivnosti;
- pooblaščene osebe, odgovorne za določanje poslovnih skrivnosti;
- kriterije za določanje stopenj tajnosti;
- postopek označevanja poslovnih skrivnosti;
- postopke obdelovanja in dostopa do tajnih podatkov;
- hrambo poslovnih skrivnosti;
- razmnoževanje poslovnih skrivnosti;
- tiskanje poslovnih skrivnosti;
- postopek uničevanja poslovnih skrivnosti;
- predhodne in končne določbe.

V praksi so tovrstni interni akti ključni, ker vzpostavljajo formalni okvir za ločevanje med zakonitim pridobivanjem tržnih informacij in varovanjem lastnih podatkovnih virov.

6.4 Zakon o tajnih podatkih (ZTP)

S tem zakonom se določajo skupne osnove enotnega sistema določanja, varovanja in dostopa do tajnih podatkov z delovnega področja državnih organov RS, ki se nanašajo na javno varnost, obrambo, zunanje zadeve ali obveščevalno ter varnostno dejavnost države in prenehanje tajnosti takšnih podatkov. Po tem zakonu se morajo ravnati državni organi, organi lokalnih skupnosti, nosilci javnih pooblastil, drugi organi in gospodarske družbe. Vsak, ki mu je bil zaupan tajni podatek, ali ki se je seznanil z vsebino tajnega podatka, je odgovoren za njegovo varovanje in ohranitev njegove tajnosti.

Poznavanje ZTP je za področje korporativne obveščevalne dejavnosti pomembno zato, ker določa standarde varovanja informacij, ki so bistvene za nacionalno in gospodarsko varnost. Podjetja, ki sodelujejo z državnimi organi ali izvajajo dejavnosti na področju kritične infrastrukture morajo vzpostaviti notranje mehanizme varovanja podatkov skladno z načeli tega zakona.

Tajni podatek: je dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami ter ki je v skladu s tem zakonom določeno in označeno za tajno. Stopnje tajnosti delimo na:

Slika 15: Stopnje tajnosti
Vir: lasten.

Tajni podatki predstavljajo skrajno stopnjo varovanih informacij. Za KOD to pomeni, da se morajo podjetja zavedati meje in razlik med poslovno skrivnostjo ter tajnim podatkom. *Varnostno preverjanje*: je poizvedba, katere namen je zbrati podatke o morebitnih varnostnih zadržkih.

Varnostni zadržki: so ugotovitve varnostnega preverjanja, iz katerih izhaja, da obstajajo utemeljeni dvomi o zanesljivosti ali verodostojnosti osebe za obravnavanje in varovanje tajnih podatkov. Te dvomi so lahko na primer: lažne navedbe podatkov preverjane osebe

v varnostnem vprašalniku ali v razgovoru za varnostno preverjanje. Določene (neizbrisane pravnomočne) obsodbe. Odvisnost od alkohola, drog in druge podobne zasvojenosti. Članstvo oziroma sodelovanje v organizacijah oziroma skupinah, ki ogrožajo vitalne interese RS in podobno. Pravico dostopa do tajnih podatkov imajo samo tiste osebe, ki imajo dovoljenje in se morajo s temi podatki seznaniti zaradi opravljanja funkcije ali delovnih nalog.

Kot primer bi lahko navedli podjetje, ki ima pogodbo z Ministrstvom za obrambo. Pred vključitvijo novega zaposlenega v projekt mora izvesti varnostno preverjanje v skladu z ZTP, saj bi uhajanje podatkov lahko ogrozilo nacionalno varnost in pogodbeno odgovornost podjetja.

Sistem varovanja tajnih podatkov mora biti integriran v širši okvir informacijske in organizacijske varnosti podjetja. V povezavi z KOD to pomeni, da se morajo podjetja zavedati pomembnosti nadzora nad dostopi, sledljivosti komunikacij in zaščite podatkovnih nosilcev. Sistem postopkov in ukrepov varovanja tajnih podatkov mora obsegati:

- splošne varnostne ukrepe;
- varovanje oseb, ki imajo dostop do tajnih podatkov;
- varovanje prostorov;
- varovanje dokumentov in medijev, ki vsebujejo tajne podatke;
- varovanje komunikacij, po katerih se prenašajo tajni podatki;
- način označevanja stopenj tajnosti;
- varovanje opreme, s katero se obravnavajo tajni podatki;
- način seznanitve uporabnikov z ukrepi in postopki varovanja tajnih podatkov;
- kontrolo in evidentiranje dostopov do tajnih podatkov;
- kontrolo in evidentiranje pošiljanja in distribucije tajnih podatkov.

ZTP vzpostavlja najvišje standarde varovanja informacij v državi. Za korporativno obveščevalno dejavnost predstavlja okvir, po katerem se lahko zgledujejo tudi zasebni subjekti. Povezovanje načel ZTP z notranjimi politikami podjetja se krepi zaupanje partnerjev, zmanjšuje operativna tveganja in povečuje integriteto organizacije na trgu.

6.5 Zakon o delovnih razmerjih (ZDR)

Konkurenčna prepoved – zakonska prepoved konkurenčne dejavnosti: med trajanjem delovnega razmerja delavec ne sme brez pisnega soglasja delodajalca za svoj ali tuj račun opravljati del ali sklepati poslov, ki sodijo v dejavnost, ki jo dejansko opravlja delodajalec in pomenijo ali bi lahko pomenili za delodajalca konkurenco.

V kontekstu korporativne obveščevalne dejavnosti je konkurenčna prepoved ključna za zaščito strateškega znanja podjetja.

Konkurenčna klavzula – pogodbena prepoved konkurenčne dejavnosti: če delavec pri oziroma v zvezi s svojim delom pridobiva tehnična, proizvodna ali poslovna znanja in poslovne zveze, se lahko delavec ter delodajalec v pogodbi o zaposlitvi dogovorita za prepoved opravljanja konkurenčne dejavnosti po prenehanju delovnega razmerja. Dogovor velja za obdobje najdlje dveh let po prenehanju pogodbe o zaposlitvi. Denarno nadomestilo znaša 1/3 povprečne mesečne plače zadnjih treh mesecev.

Konkurenčna klavzula ima dvojno funkcijo, in sicer pravno in strateško. Na pravni ravni varuje interese delodajalca, na strateški ravni pa preprečuje prenos znanja in poslovnih metod h konkurenci, kar lahko neposredno ogrozi konkurenčno prednost podjetja.

Nadomestilo za spoštovanje konkurenčne klavzule zaposleni dobi, če spoštovanje konkurenčne klavzule onemogoča pridobitev zaslužka, primerljivega delavčevi prejšnji plači. Delodajalec mu mora za ves čas spoštovanja prepovedi mesečno izplačevati denarno nadomestilo. Denarno nadomestilo se mora določiti s pogodbo o zaposlitvi in znaša mesečno najmanj tretjino povprečne mesečne plače delavca v zadnjih treh mesecih pred prenehanjem pogodbe o zaposlitvi.

6.6 Zakon o preprečevanju omejevanja konkurence (ZPOmK – 2)

Zakon ureja omejevalna ravnanja, koncentracije podjetij, nelojalno konkurenco, oblastna omejevanja konkurence in ukrepe za preprečitev omejevalnih ravnanj in koncentracij. Kartel pomeni sporazum ali usklajeno ravnanje dveh ali več podjetij, katerega namen je usklajevanje njihovega konkurenčnega ravnanja na trgu ali vplivanje na relevantne dejavnike konkurence. V zakonu so definirane prepovedi, in sicer:

- omejevalnih sporazumov (katerih cilj/učinek je preprečevati, omejevati ali izkrivljati konkurenco);
- zlorabe prevladujočega položaja;
- koncentracij podjetij, ki bistveno omejujejo učinkovito konkurenco.

Zakonodaja je za KOD pomembna, ker določa meje, znotraj katerih je mogoče zakonito zbirati in analizirati podatke o konkurenci. Kot primer lahko navedemo podjetje, ki lahko zakonito pridobiva podatke o konkurenci iz javno dostopnih virov, kot so letna poročila ali javni razpisi, ne sme pa plačevati zaposlenih pri konkurenci za namen posredovanja internih dokumentov.

6.7 Zakon o dostopu do informacij javnega značaja (ZDIJZ)

Zakon ureja postopek, ki vsakomur omogoča prost dostop in ponovno uporabo informacij javnega značaja, s katerimi razpolagajo državni organi, organi lokalnih skupnosti, javne agencije, javni skladi ter druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb. Organi so dolžni redno vzdrževati in na primeren način javno objavljati ter dati na vpogled urejen katalog informacij javnega značaja, s katerimi razpolagajo. Informacija javnega značaja je informacija, ki izvira iz delovnega področja organa, nahaja pa se v obliki dokumenta, zadeve, dosjeja, registra, evidence ali drugega dokumentarnega gradiva, ki a je organ izdelal sam, v sodelovanju z drugim organom, ali pridobil od drugih oseb.

Zakon ima v kontekstu KOD dvojno vlogo. In sicer omogoča pridobivanje podatkov iz javnih virov, hkrati pa določa tudi meje, znotraj katerih se lahko ti podatki uporabljajo. Tista podjetja, ki izvajajo KOD, morajo vzpostaviti notranje smernice za zbiranje in uporabo informacij iz javnih virov, da zagotovijo skladnost z zakonom ter preprečijo nenametno razkritje poslovnih skrivnosti drugih subjektov.

Organ prosilcu zavrne dostop do zahtevane informacije, če se zahteva nanaša na:

- tajne podatke ali poslovne skrivnosti;
- osebni podatek, katerega razkritje bi pomenilo kršitev varstva osebnih podatkov;
- podatek, katerega razkritje bi pomenilo kršitev zaupnosti individualnih podatkov o poročevalskih enotah, davčnega postopka ali davčne tajnosti;
- določene podatke v zvezi s kazenskim pregonom, prekrškovnim, upravnim ali sodnim postopkom;

- podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanje, in bi njegovo razkritje povzročilo motnje pri delovanju organa;
- podatek iz dokumenta, ki je postopku izdelave, in je še predmet posvetovanja v organu, njegovo razkritje pa bi povzročilo napačno razumevanje njegove vsebine;
- podatek o naravi oziroma kulturni vrednosti, ki ni dostopen javnosti zaradi varovanja narave oziroma kulturne vrednote.

Vsak organ je dolžan na splet posredovati naslednje informacije javnega značaja:

- prečiščena besedila predpisov, ki se nanašajo na delovno področje organa, povezana z državnim registrom predpisov na spletu;
- programe, strategije, stališča, mnenja in navodila, ki so splošnega pomena ali so pomembna za poslovanje organa s fizičnimi ter pravnimi osebami oziroma za odločanje o njihovih pravicah ali obveznostnih, študije in druge podobne dokumente, ki se nanašajo na delovno področje organa;
- predloge predpisov, programov, strategij in drugih podobnih dokumentov, ki se nanašajo na delovno področje organa;
- dokumentacijo na področju javnih naročil in javnih razpisov za dodelitev sredstev, subvencij, posojil ter drugih oblik sofinanciranj iz državnega ali občinskih proračunov;
- informacije o svoji dejavnosti ter upravnih, sodnih in drugih storitvah;
- vse informacije javnega značaja, ki so jih prosilci zahtevali najmanj trikrat;
- druge informacije javnega značaja.

6.8 Zakon o informacijski varnosti (ZinfV)

Informacijska varnost je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti ter razpoložljivosti. Kibernetska varnost je sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti ter napadi. Kibernetska obramba pa je celota ukrepov in dejavnosti države, s katerimi odvrača, onemogoča, preprečuje ali odbija kibernetske napade v informacijskem okolju. Varnostno operativni center je notranja organizacijska enota posameznih organov državne uprave, ki se odziva na incidente na področju informacijske varnosti. Izvajalci bistvenih storitev za zagotavljanje informacijske varnosti in visoke ravni varnosti omrežij ter informacijskih sistemov vzpostavijo in vzdržujejo dokumentiran sistem upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanje. Izvajalci bistvenih storitev nacionalnemu CSIRT brez

nepotrebnega odlašanja priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev.

Za korporativno obveščevalno dejavnost je informacijska varnost ključna, saj varuje podatkovne vire, ki so temelj konkurenčnih prednosti. V praksi to pomeni, da mora KOD vzpostaviti integriran sistem zaščite informacij, ki vključuje tako tehnične kot organizacijske ukrepe. S tem se zagotovi, da občutljivi poslovni podatki ne postanejo tarča kibernetskih groženj, saj bi se s tem neposredno ogrozila konkurenčnost podjetja.

6.9 Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)

Posebne vrste osebnih podatkov so osebni podatki, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, obdelavo genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatke v zvezi z zdravjem posameznikov in podatke v zvezi s posameznikovimi spolnim življenjem ali spolno usmerjenostjo. Obdelava teh podatkov je praviloma prepovedana.

V okviru KOD ima obdelava osebnih podatkov poseben pomen pri preverjanju poslovnih partnerjev, zaposlenih ali strank. Zato morajo detektivi in analitiki KOD razumeti, kdaj so podatki občutljive narave ter kdaj njihova obdelava presega zakonite meje. To je bistveno za ohranjanje zakonitosti in zaupanja v delovanje KOD.

6.10 Zakon o zaščiti prijaviteljev (ZZPri)

Zakon določa načine in postopke za prijavo kršitev predpisov, za katere so posamezniki izvedeli v delovnem okolju ter njihovo obravnavo in zaščito posameznikov, ki prijavijo ali javno razkrijejo informacije o kršitvi. Nihče ne sme razkriti identitete prijavitelja brez njegovega izrecnega soglasja nikomur, razen zaupniku in organu za zunanjo prijavo. To velja tudi za vse druge informacije, iz katerih je mogoče neposredno ali posredno sklepati o identiteti prijavitelja.

Vzpostavitev notranje poti za prijavo: notranja pot za prijavo se vzpostavi tako, da se določi poseben elektronski naslov in telefonska številka ali druge kontaktne podatke za prejem prijav, ukrepe za preprečitev razkritja identitete prijavitelja ter da se imenuje zaupnika. Zavezanci za vzpostavitev notranje poti za prijavo so subjekti v javnem in zasebnem sektorju s 50 ali več zaposlenimi.

Zunanja prijava: prijavitelj informacijo o kršitvi poda neposredno z uporabo zunanje poti za prijavo, če notranja pot za prijavo ni vzpostavljena, če notranje prijave ne bi bilo mogoče učinkovito obravnavati, ali če prijavitelj meni, da v primeru notranje prijave obstaja tveganje povračilnih ukrepov.

Za KOD ima zakon poseben pomen, saj prijavitelji pogosto predstavljajo dragocen vir informacij o notranjih tveganjih, korupciji ali varnostnih pomanjkljivostih. Sistem prijav omogoča pridobivanje podatkov, ki so ključni za prepoznavanje groženj, pri tem pa mora KOD zagotavljati visoko raven anonimnosti in zaupanja.

6.11 Zakon o detektivski dejavnosti (ZDD-2)

Detektivska dejavnost je zbiranje, obdelava, posredovanje podatkov in informacij ter svetovanje na področju preprečevanja kaznivih ravnanj. Opisno zakon opredeljuje, kaj detektivska dejavnost je – zbiranje in obdelava podatkov. normativno pa določa, kako se ta dejavnost lahko izvaja, torej pod katerimi pogoji ter znotraj katerih pravnih omejitev. Upravičenja detektiva so:

- pridobivanje podatkov od oseb ali iz javno dostopnih virov;
- pridobivanje podatkov iz evidenc;
- pridobivanje podatkov z osebno zaznavo;
- uporaba tehničnih sredstev.

6.12 Zakon o zasebnem varovanju (ZZasV-1)

Zakon ureja pravice in obveznosti na področju varovanja, ki ga ne zagotavlja država. V kontekstu korporativne obveščevalne dejavnosti ima zakon pomembno vlogo pri vzpostavljanju varnostnega okvira, znotraj katerega organizacije varujejo svoje zaposlene, premoženje, informacije, vire in podatke. S tem zakon posredno prispeva tudi k zaščiti informacijskih in konkurenčnih prednosti podjetja. Zasebno varovanje je varovanje ljudi in premoženja na varovanem območju, določenem objektu ali prostoru pred nezakonitimi dejanji, poškodovanjem ali uničenjem z varnostnim osebjem ter sistemi tehničnega varovanja. V praksi to pomeni, da podjetja uporabljajo različne oblike zasebnega varovanja za zmanjševanje varnostnih tveganj, ki lahko vplivajo na poslovne informacije, neprekinjeno poslovanje in tudi ugled. Na primer, kombinacija fizičnega in tehničnega varovanja omogoča zaščito prostorov, kjer se obdelujejo poslovno občutljivi podatki.

Oblike zasebnega varovanja so:

- varovanje oseb oziroma ljudi in premoženja;
- prevoz in varovanje gotovine ter drugih vrednostnih pošiljk;
- varovanje javnih zbiranj in prireditev v gostinskih lokalih;
- upravljanje z VNC;
- načrtovanje in izvajanje sistemov tehničnega varovanja.

Iz vidika KOD so ti ukrepi ključni za preprečevanje industrijskega vohunstva, kraje informacij in notranjih groženj. Detektivske in varnostne storitve se pogosto dopolnjujejo, detektiv zbira podatke ter preiskuje nepravilnosti, medtem ko varnostno osebje preprečuje fizične vdore in nadzira izvajanje varnostnih protokolov.

Odgovorite na vprašanja

Kaj določa Splošna uredba o varstvu podatkov (GDPR)?

Kaj ureja Zakon o varstvu osebnih podatkov?

Kje ni dovoljeno izvajati videonadzora?

Kaj je poslovna skrivnost po Zakonu o poslovni skrivnosti?

Kdaj je pridobitev poslovne skrivnosti zakonita?

Kdaj je uporaba ali razkritje poslovne skrivnosti protipravno?

Kaj vključuje celoten sistem varovanja poslovne skrivnosti?

Kaj je določeno z Zakonom o tajnih podatkih?

Katere stopnje tajnosti poznamo?

Kaj je konkurenčna prepoved po Zakonu o delovnih razmerjih?

Kaj je konkurenčna klavzula?

Kaj določa Zakon o dostopu do informacij javnega značaja?

Kaj opredeljuje Zakon o informacijski varnosti?

Analizirajte slovensko in evropsko zakonodajo, ki ureja pridobivanje in uporabo informacij. Na podlagi izbranih zakonodaj pripravite kratek pregled, kako pravni okvir vpliva na izvajanje korporativne obveščevalne dejavnosti. Opišite tudi kršitev za podjetje.

Univerzitetna založba
Univerze v Mariboru

7 OSINT in obveščevalni proces

Vsaka organizacija si prizadeva slediti tržnim nišam na področju promocije storitev ali izdelkov, ki jih ponuja. Večina informacij je uporabnikom prosto dostopna v kibernetskem prostoru, zato OSINT kot način pridobivanja informacij velja za eno najpomembnejših in hkrati najučinkovitejših metod. Kar 90 % vseh informacij je javno dostopnih, njihovo pridobivanje pa je zakonito (Lobnikar in Dvojmoč, 2017). Britovšek (2017) navaja, da je kar 86 % vseh informacij, uporabljenih v obveščevalni dejavnosti, pridobljenih prav z uporabo metode OSINT.

V okviru korporativne obveščevalne dejavnosti OSINT predstavlja ključni vir za razumevanje konkurenčnega okolja, gibanj na trgu in zaznavo potencialnih tveganj. Podjetja lahko z učinkovitim zbiranjem javno dostopnih informacij prepoznajo tržne priložnosti in grožnje, kar jim omogoča bolj premišljeno strateško odločanje.

Zavedati se je potrebno, da preko orodij OSINT pridobivamo le surove podatke (angl. *raw data*). Iz tega razloga je potrebno v organizaciji oziroma podjetju dobro analizirati pridobljene podatke. Osredotočiti se je potrebno na določeno bazo podatkov, ki zajema področje, ki je vezano neposredno na napredek organizacije. Dobro je imeti tudi dobro zastavljene in določene dolgoročne in tudi kratkoročne cilje, katerim se lahko s pridobljenimi podatki lažje približamo (Breeden, 2019).

OSINT predstavlja pomembno orodje tudi tistim organizacijam, ki se znotraj korporativne varnosti ukvarjajo z detektivsko dejavnostjo. OSINT za detektive v 21. stoletju ni le možnost, ampak orodje, ki je obvezno potrebno za to, da detektiv kvalitetno opravlja svoje delo (Brock, 2019).

OSINT je tako nepogrešljiv del obveščevalnega procesa v sodobnem poslovnem okolju. V okviru korporativne obveščevalne dejavnosti OSINT omogoča identifikacijo trendov, analizo konkurence, ocenjevanje tveganj ter pravočasno odzivanje na spremembe v okolju.

7.1 Kaj sploh je OSINT?

Beseda OSINT izhaja iz angleščine in je okrajšava za *Open Source Intelligence*, kar pomeni pridobivanje podatkov iz javnih virov. Gre za metodo sistematičnega zbiranja javno dostopnih informacij, ki spada med tri najpomembnejše načine zbiranja podatkov. Gradivo, ki ga zberemo s pomočjo OSINT-a, nam da širši pogled na določen dogodek in razmere. Bistvo OSINT-a je, da pridobimo podatke, ki jih je, kot že omenjeno, treba analizirati, razvrstiti in izluščiti tiste, ki bodo del končne informacije. Uporaba različnih orodij pripomore k povezovanju različnih situacij ali okolja (Koren, 2018).

OSINT je metoda pridobivanja podatkov s pomočjo javnih virov, je proces zbiranja podatkov iz javno dostopnih virov, predstavlja celoten proces pridobivanja oziroma zbiranja in analiziranja javno dostopnih informacij z namenom pridobitve uporabnih obveščevalnih informacij ali izdelkov, so obveščevalne informacije, ki so izdelane na podlagi javno dostopnih informacij (Dvojmoč, 2017).

OSINT je opredeljen tudi kot neuvrščena informacija, ki je pridobljena iz kateregakoli javno dostopnega vira v tiskani, elektronski ali verbalni obliki. Različni viri, kot so radio, televizija, časopis, revije, internet in podobno so lahko uspešno izkoriščene za zbiranje obveščevalnih podatkov (Burke, 2007).

Kot dopolnitev definicije OSINT-a sta pomembna tudi dva izraza, in sicer:

- javni vir: ki je vsaka oseba ali skupina, ki zagotavlja informacije brez posebnih pričakovanj po zasebnosti. Informacije, odnosi in drugi podatki niso zaščiteni pred javnim razkritjem;

- javno dostopne informacije: so podatki, dejstva, navodila in drugo objavljeno gradivo, ki je objavljeno za potrebe širše javnosti. Posamezniki do njih lahko pridejo na zahtevo, stvar zakonito vidijo ali slišijo kot mimoidoči ali pa izvejo na odprtih javnih srečanjih.

Uporablja se na področju nacionalne varnosti, pri organih pregona, na področju korporativne obveščevalne dejavnosti in pri zaznavi ter preiskovanju različnih kriminalnih aktivnosti.

Za korporativno obveščevalno dejavnost to pomeni, da mora organizacija vzpostaviti mehanizme za zakonito, sistematično in etično uporabo teh podatkov. OSINT ne pomeni le zbiranja, ampak tudi selekcijo. To pomeni odločanje, katere informacije so strateško pomembne.

Pri sistematičnem zbiranju javnih virov razlikujemo:

- informacije iz javnih virov ali OSINF (*Open Source Information*) in
- obveščevalne informacije iz javnih virov ali OSINT (*Open Source Intelligence*) (Podbregar in Ivanuša, 2010).

S pomočjo orodij OSINT lahko pridobivamo različne vrste podatkov, ki jih razdelimo na dve skupini. V prvo skupino spadajo podatki, ki so vezani na splošne informacije, v drugo skupino pa specifične informacije, ki zajemajo podrobne informacije o podjetjih ali posameznikih. Razdeljeni pa so tudi na vire, ki so klasični in pa specifični.

Klasični podatki, ki so pridobljeni brez dodatnih orodij, so podatki iz oziroma o:

- javnem arhivu;
- državnih arhivih;
- radiu, televiziji, časopisih in virtualnih novicah;
- strokovnih člankih;
- dogodkih;
- mrliških listinah;
    - finančnih stanjih;
    - socialnih omrežjih.

Specifični podatki, ki so pridobljeni z uporabo posebnih orodij, so podatki o:

- URL-parametrih;
- e-poštnih naslovih, DNS-naslovih in socialnih profilih;
- kibernetskih datotekah;
- geslih in napakah;
- skritih geslih;
- datotekah JAVA;
- globokem in temnem spletu (angl. *deep web in dark web*);
- slikah;
- geolokacijah;
- telefonskih številkah;
- varnostnih sistemih;
- forumih;
- podjetjih;
- zgodovini spletne strani.

Priporočljivo je, da se pri zbiranju podatkov uporabljata oba načina pridobivanja. S tem popolnoma izčrpamo vse vire, ki so nam na razpolago.

V praksi KOD to pomeni, da klasične podatke uporabljamo za osnovno razumevanje trga, specifične pa za poglobljeno analizo konkurence, tehničnih rešitev ali varnostnih ranljivosti. Na primer, pri spremljanju konkurenta lahko organizacija z uporabo orodij OSINT spremlja spremembe spletnih strani, zaposlitvenih objav ali poslovnih objav, kar bi lahko nakazovalo na nove projekte ali premike.

7.2 Zgodovina OSINT

Pridobivanje podatkov iz javno dostopnih virov spada med ene izmed prvih dejavnosti, ki so jih izvajale že najzgodnejše civilizacije. Takšne informacije so prispevale k nadaljnjemu razvoju civilizacij, vojskovanja in gospodarskih razmer ter k boljšemu razumevanju nasprotnih civilizacij (Colquhon, 2016). Osnovni cilj pridobivanja javno dostopnih virov je do danes ostal enak, za prelomnico pa velja Gutenbergova iznajdba tiska leta 1440 (Bižal, 2014).

Hladna vojna velja za zlato obdobje klasičnih OSINT metod, veliko znanstvenikov pa so jo poimenovali tudi vojna obveščevalno-varnostnih služb (Koren, 2018). V vojni sta oba bloka uporabljala različne javne vire podatkov. Le-to je zajemalo časopise, revije, radijske postaje in podobno. Združene države Amerike so metodam OSINT namenile večjo pozornost po terorističnem napadu, ki se je zgodil 11. septembra 2001. Takrat je bil znotraj CIE izoblikovan posebni oddelek, ki je deloval v smeri pridobivanja javno dostopnih virov podatkov in njihovo analizo.

OSINT predstavlja najmlajšo izmed disciplin zbiranja podatkov. Razvoj telekomunikacijskih možnosti je imel za posledico razvoj discipline, saj je tiste podatke, ki so bili prej nedostopni naredil dostopne (Šaponja, 1999). Metoda zbiranja podatkov se je izkazala za zelo učinkovito predvsem pri projektnih delih in kriznem odločanju, dala pa je vpogled na celotno podobo z različnih zornih kotov (Podbregar idr., 2010).

Kot sta zapisala Grozde in Henigman (2008) zbiranje podatkov iz javnih virov obsega ne le prosto dostopnih informacij ter podatkov, temveč tudi nedostopne zbirke, ki so pogosto plačljive. Vseeno gre za javno objavljene podatke, vendar so dostopne le posameznikom pod določenimi pogoji. To so na primer podatkovne baze univerzitetnih knjižnic, do katerih lahko dostopamo le, če smo član knjižnice, ki je članica univerze.

7.3 OSINT v kibernetskem prostoru

Percepcija pridobivanja podatkov iz javnih virov se je spremenila z razvojem kibernetskega prostora, ki pa je vplival tudi na preobrazbo same definicije kaj sploh je podatek. Preobrazba kibernetskega prostora je neposredno vplivala tudi na KOD, saj je omogočila strateško uporabo javno dostopnih podatkov pri prepoznavanju tveganj, analizi konkurence in zaznavanju tržnih priložnosti. Obstoječe tehnike OSINT-a so bile izpodrinjene z novimi tehnikami, ki so bile bolj temeljite, hitrejše in omogočajo pridobivanje mase podatkov. S temi orodji oziroma metodami lahko pridobivamo podatke, za katere si v preteklosti ni bilo mogoče niti predstavljati, da obstajajo. Orodja OSINT se uporabljajo med korporacijami tudi za zbiranje podatkov o konkurenci, trgu in inovacijah. Tudi zasebni detektivi uporabljajo e-orodja OSINT pri opravljanju svojega dela. Slaba stran tega pa je, da so moč javnih virov podatkov začeli uporabljati in izkoriščati tudi hekerji. Le-ti s pomočjo orodij naredijo analizo podjetij in posameznikov ter na podlagi tega najdejo šibko točko le-teh. Zaradi tega so omenjene metode pogosto označene kot negativne, kljub temu pa jih uporabljajo tudi varnostni organi (Galindo idr., 2019).

S pomočjo OSINT orodij je bilo v kibernetskem prostoru veliko prelomnih dogodkov, ki so vplivali na to, da je v zadnjih letih razvoj podobnih orodij doživel razmah. En izmed primerov je bil, ko so varnostni organi razbili kibernetsko mrežo, ki je novačila teroriste (Galindo idr., 2019).

7.4 Pravna ureditev

Pravna ureditev določa meje, znotraj katerih lahko korporativni analitiki zbirajo in obdelujejo podatke iz javnih virov, ter tako zagotavljajo zakonitost in etičnost postopkov. Informacije so v 21. stoletju postale pomemben del oglaševanja, načina prodaje in poznavanja navad ljudi. Piškotki na primer so osnovni primer, kako deluje oglaševanje, ki je vezano na preteklo iskanje po spletu. Piškotki oziroma "cookies" so mehanizmi, ki potrdijo obisk strani na podlagi klika. Na podlagi tega se te informacije shranijo in povrnejo ob naslednjem obisku spletne strani. Piškotki pa shranjujejo tudi brskanje po spletnih straneh, pri čemer je problem predvsem v tem, da te podatke pogosto dobijo velike marketinške korporacije, ki jih uporabljajo za nadaljnje oglaševanje (Panda mediacenter, 2014). Piškotki spadajo pod elektronsko zbiranje podatkov, ki ga morajo podjetja uporabljati skladno z GDPR in Zakonom o varstvu osebnih podatkov (ZVOP-2).

V zadnjem razvojnem obdobju kibernetskega prostora je masivno pridobivanje podatkov postalo eden izmed največjih virov zaslužka. Zaradi tega se je povečala tudi ranljivost posameznikov oziroma uporabnikov. Pridobljeni podatki lahko ogrozijo tudi posameznikovo varnost in predvsem zaradi tega je leta 2016 začela veljati Splošna uredba EU o varstvu podatkov, ki zajema vse evropske države ("Uredba (EU) 2016/679 …", 2016). Poleg Splošne EU uredbe pa imamo v Sloveniji tudi lastne zakone, ki varujejo posameznikove osebne podatke, kot je na primer Zakon o varstvu osebnih podatkov (ZVOP-2). Na področju zbiranja javnih virov podatkov pa se je potrebno posvetiti tudi zakonodaji, ki vključuje dovoljene tehnike pridobivanja.

7.5 Vloga OSINT v obveščevalni dejavnosti

Zbiranje javno dostopnih podatkov (OSINT) je eden izmed načinov izvajanja obveščevalne dejavnosti. S tem obveščevalne službe pridejo do želenih podatkov. Temelji predvsem na spremljanju in zbiranju informacij, ki so javnega značaja (Podbregar, 2008). Klasična obveščevalna dejavnost in OSINT imata ogromno skupnega ter ju med seboj lahko z več vidikov tudi enačimo. Razlika, ki je izredno pomembna pa je ta, da pri metodi OSINT nikoli ne posegamo v človekove pravice in temeljne svoboščine.

OSINT se osredotoča na kvalitetne primarne vire in proces strukturiranja digitalnih podatkov. Razumeti moramo tudi zahtevo po informaciji, ter probleme, ki jih moramo vsebinsko analizirati. Pri tem mora biti določeno in vzpostavljeno tudi sodelovanje med analitikom ter uporabnikom informacije. Pomembno je predvsem to, da analitik razume, kakšno informacijo si uporabnik želi, saj se bo na ta način obrnil in poiskal pravi vir ter primerne podatke. Sodelovanje med njima je potrebno tudi z vidika usmerjanja procesa in povratnih informacij (Podbregar in Ivanuša, 2010).

OSINT ima ključno vlogo v sodobni obveščevalni dejavnosti, saj omogoča pravočasno pridobivanje informacij, ne da bi pri tem kršil zakonodajo. V okviru KOD predstavlja nepogrešljivo orodje za strateško načrtovanje, zaznavanje groženj in krepitev varnostne kulture organizacije.

7.6 Metode in orodja za OSINT analizo

Kot predhodno omenjeno poznamo dve vrsti podatkov, ki jih lahko pridobivamo. To so klasični in specifični podatki.

Za klasične podatke velja predvsem to, da so pridobljeni brez dodatnih orodij, potrebna pa je analiza baz, v katerih so želeni podatki. Vseeno je priporočljiva uporaba dodatnih orodij pri pridobivanju teh klasičnih podatkov, saj pripomore k podrobnejšemu pregledu podatkov, poleg tega pa poteka hitrejše in jih tudi sistematično uredi. Prav tako je z ročnim pridobivanjem nemogoče pridobiti podatke iz vseh mogočih baz, ki jih imamo na razpolago.

Pri klasičnih podatkih je ključnega pomena sistematičnost zbiranja in analiza baz, medtem ko pri specifičnih podatkih večji pomen pridobi uporaba naprednih orodij, ki omogočajo avtomatizirano iskanje ter obdelavo digitalnih vsebin.

Pri pridobivanju specifičnih podatkov pa je uporaba orodij nujna, saj gre za podatke, ki so zapisani v kodah in jih lahko preberejo le določena orodja. To so tisti podatki, ki v praksi predstavljajo največjo dragocenost. Predvsem zaradi tega, ker je njihovo pridobivanje težko ali pa jih ni mogoče pridobiti z ročnim pridobivanjem ali pa vsebujejo podatke, ki niso javno objavljeni. Poleg določenih orodij potrebujemo tudi različne dodatke, ki omogočajo delovanje teh orodij. Kot primer lahko navedemo OSINT preiskave na Deep webu, pri čemer potrebujemo TOR brskalnik, saj drugače ne moremo uporabljati orodij za pridobivanje podatkov iz javnih virov.

Še en način kategorizacije vrste pridobljenih podatkov je deljenje na pridobivanje splošnih ali targetiranih podatkov. Splošni podatki so tisti podatki, ki zajemajo pridobivanje vrednostnih podatkov ne glede na to, kdo je nosilec, bistvo in okolje. To je učinkovito predvsem pri zbiranju oziroma pridobivanju večje mase podatkov, katerih namen je prodaja ali hramba v bazah. Targetirani podatki pa so tisti podatki, ki so vezani na specifično osebo ali organizacijo. Njihovo pridobivanje je tudi najbolj pogosto in hkrati najbolj zahtevno. Poleg načina pridobivanja podatkov lahko razlikujemo tudi namen zbiranja, ki vpliva na izbiro metod in orodij.

Če želimo podatke pridobivati brez orodij, moramo imeti posebna znanja in veščine, na podlagi katerih pridobimo podatke, ki imajo neko določeno vrednost. Pred začetkom pridobivanja informacij je potrebno narediti temeljit načrt, v katerem moramo določiti katere informacije želimo pridobiti, na kakšen način in določiti baze podatkov, v katerih bi podatki lahko bili. Pridobivanje podatkov brez orodij zahteva veliko časa, poleg tega pa pridobimo tudi okrnjeno strukturo podatkov. Orodja OSINT nam omogočijo, da pridobimo vrednostne informacije v krajšem časovnem obdobju (Hassan in Hijazi, 2018).

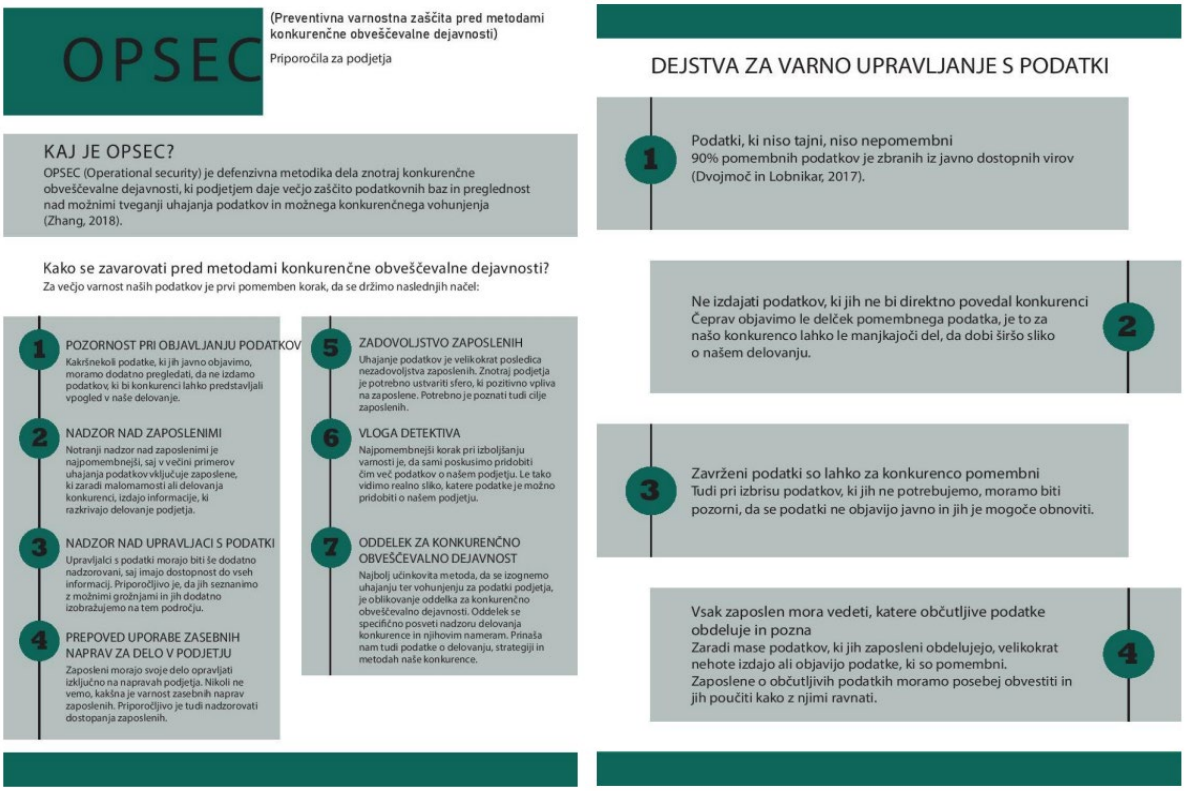
Orodja, ki nam omogočajo pridobivanje podatkov iz javno dostopnih virov nam omogočijo, da pridobivamo specifične podatke, prav tako pa so nam v pomoč tudi pri osredotočanju na našo ciljno skupino. Poznamo tudi orodja, ki nam pomagajo ustvariti shemo o informacijah, ki smo jih že pridobili (Null byte, 2019).

7.7 OPSEC – obrambni mehanizem pred OSINT

OPSEC (angl. *Operational security*) je defenzivna metoda dela znotraj KOD. Podjetjem daje večjo zaščito podatkovnih baz in tudi preglednost nad možnimi tveganji uhajanja podatkov ter mogočega konkurenčnega vohunjenja (Zhang, 2018).

OPSEC lahko primerjamo oziroma kar enačimo s korporativno protiobveščevalno dejavnostjo, saj imata enake cilje. Gre za preventivna varnostna mehanizma, ki nam dajeta vpogled v lastno varnost, raven zaščite in način kako nevtralizirati nevarnost. Potrebno je vedeti in se zavedate predvsem katere grožnje sploh prežijo nad našo organizacijo, kdo predstavlja grožnjo ter kakšni so nameni teh posameznikov (Ivanov in Webster, 2017).

OPSEC je zato ključen element korporativne varnosti, saj dopolnjuje OSINT z vidika varovanja lastnih informacij in zmanjševanja tveganj informacijskega uhajanja.



Slika 16: OPSEC
Vir: lasten.

Odgovorite na vprašanja

Kaj je OSINT? Na kratko zapišite.

Katere podatke pridobivamo preko orodij OSINT?

Opišite OSINT metodo na široko.

Katera dva izraza sta povezana in nekakšna dopolnitev OSINT-a?

Kateri dve vrsti podatkov pridobivamo s pomočjo orodij OSINT in kateri so ti podatki?

Kako se je razvil OSINT?

Kako je OSINT urejen pravno?

Kakšna je vloga OSINT-a v obveščevalni dejavnosti?

Kaj je OPSEC?

Kakšna je povezava med OPSEC in korporativno protiobveščevalno dejavnostjo?

Predpostavite, da želi podjetje spremljati dejavnosti konkurenta s pomočjo odprtih virov. Opredelite, katere javno dostopne vire bi uporabili in pojasnite, kako bi zagotovili zakonitost ter verodostojnost pridobljenih informacij.

Univerzitetna založba
Univerze v Mariboru

8 Tveganja, ki izhajajo iz zlorabe podatkov

Zloraba podatkov predstavlja eno ključnih tveganj sodobnega poslovnega okolja. Informacije, ki jih podjetje pridobi v okviru zakonitega obveščevalnega delovanja, se lahko ob neustreznem varovanju ali namerni zlorabi spremenijo v sredstvo nelojalne konkurence.

Kot je določeno v »Zakonu o preprečevanju omejevanja konkurence« (2008), nelojalna konkurenca predstavlja ravnanje podjetja na trgu, s katerim krši dobre poslovne običaje in s tem povzroči ali bi lahko povzročilo škodo drugim podjetjem. Za dejanja nelojalne konkurence se šteje predvsem posredovanje podatkov o drugem podjetju, če ti podatki škodijo ugledu in poslovanju drugega podjetja ter protipravna pridobitev poslovne skrivnosti drugega podjetja ali neupravičeno izkoriščanje zaupne poslovne skrivnosti drugega podjetja (Dvojmoč, 2019).

Na podlagi pravil Evropske unije o varstvu svobodne konkurence so nekatere prakse še posebej prepovedane. Sankcije za zlorabe so lahko denarne kazni (do 10 % letnega prometa) ali zapor, pri čemer je posebna pozornost namenjena direktorjem podjetij, ki so kršili predpise. Vse članice EU morajo uporabljati in spoštovati pravila konkurence, pri čemer so za nadzor ter spoštovanje pravil pristojna sodišča. Pravila veljajo za vsa podjetja in organizacije, katerih glavna dejavnost je gospodarska (Dvojmoč, 2019).

V okviru pravil konkurence je treba izpostaviti nedovoljene stike in dogovore med podjetji ali organizacijami, imenovane »karteli«, ki omejujejo konkurenco. Najpogostejši primeri takšnih dogovorov so omejitve proizvodnje, cene, delitev trga, razporeditev strank in distribucijski sporazumi med dobavitelji ter prodajalci. Vse izmenjave informacij in dogovori med podjetji ter njihovimi konkurenti se štejejo za protikonkurenčno prakso, ki zmanjšuje strateško negotovost na trgu. Razkritje takšnih informacij po telefonu, elektronski pošti ali na sestanku lahko predstavlja kršitev pravil. Zato je najbolje, da podjetja ne omejujejo proizvodnje, ne izmenjujejo strateških informacij o podjetju, ne postavljajo pogojev poslovanja in cen ter si ne delijo trgov. Kadar so dogovori v korist gospodarstva in potrošnikov (našteti v Uredbi o skupinskih izjemah), niso prepovedani. Če ima podjetje prevladujoč položaj na trgu zaradi velikega tržnega deleža, nima zagotovljene regulacije cen. To pomeni, da podjetje ne sme biti podjetje. Poleg tega podjetje ne sme zaračunavati previsokih cen, postavljati posebnih pogojev poslovanja za poslovne partnerje ali povzročati diskriminacije med potrošniki.

Omejitve konkurenčnega ravnanja določata tudi konkurenčna prepoved in konkurenčna klavzula. Konkurenčna prepoved delavca v delovnem razmerju zavezuje k lojalnosti podjetju, konkurenčna klavzula pa se nanaša na obdobje po zaposlitvi, ko delavec ni več v pogodbenem razmerju s podjetjem. V času trajanja delovnega razmerja se je delavec dolžan vzdržati vseh dejanj, ki bi škodila podjetju, kar pomeni prepoved konkurenčne dejavnosti. Delavec ne sme opravljati nobene dejavnosti ali sklepati poslov za negospodarske ali komercialne dejavnosti za svoj ali tuj račun, dejavnost delavca ne sme vključevati dejavnosti, ki jih opravlja delodajalec in bi lahko predstavljale konkurenco delodajalcu, razen z odobritev delodajalca. Če delavec krši to obveznost, je delavec odškodninsko odgovoren in disciplinsko uveden, kar ima za posledico odpoved pogodbe o zaposlitvi. Po prenehanju pogodbe o zaposlitvi delavca zavezuje konkurenčna prepoved, ki je dopustna le, če je delavec pridobil specifična znanja in stike, s katerimi bi lahko konkuriral prejšnjemu delodajalcu. Njeno delovanje je torej časovno omejeno. Podjetja in organizacije se pogosto srečujejo z vprašanji varovanja poslovnih skrivnosti.

»Za poslovno skrivnost se štejejo vsi podatki, ki jih kot take določi vodstvo podjetja s pisnim sklepom. O takšni odločitvi je treba obvestiti družbenike, delavce, člane organov upravljanja in druge osebe, zavezane k varovanju poslovne skrivnosti. Tudi če podatek z odločbo iz prejšnjega odstavka ni opredeljen kot poslovna skrivnost, se za poslovno skrivnost štejejo tudi podatki, za katere je očitno, da bi nastala večja škoda, če bi bili razkriti nepooblaščeni osebi. Družbeniki, delavci, člani organov upravljanja in druge osebe so odgovorni za razkritje poslovne skrivnosti, če so vedeli ali bi morali vedeti za naravo teh podatkov.« (»ZGD-1«, 2006, 39. člen) Podatki poslovne skrivnosti imajo dve glavni

značilnosti. Podatki so zaupni in znani določeni skupini oseb, zato bi morali biti znani le tej vnaprej določeni skupini oseb, ki teh podatkov ne sme posredovati ali razkriti tretjim osebam ali jih kakor koli drugače uporabiti. Razlog za zaupnost poslovne skrivnosti mora imeti tržno vrednost.

Kadar se s pisno odločbo določi poslovna skrivnost, je treba natančno določiti krog oseb, ki so seznanjene s to skrivnostjo, njihove odgovornosti in način varovanja poslovne skrivnosti. V tem primeru zakon opredeljuje tri kategorije oseb, ki so dolžne varovati poslovno skrivnost: osebe v podjetju (zaposleni, družbeniki ipd.), osebe, ki za podjetje delajo na podlagi civilnopravnih pogodb in osebe zunaj podjetja, ki so seznanjene s konkretno poslovno skrivnostjo (Dvojmoč, 2019).

Zloraba podatkov in razkritje poslovnih skrivnosti predstavljata eno največjih groženj sodobnim podjetjem. Kljub obstoječi zakonodaji se tveganja povečujejo predvsem zaradi digitalizacije poslovnih procesov, razširjene uporabe kibernetskih orodij in večje povezanosti organizacij. Zato je ključno, da podjetja vzpostavijo notranje nadzorne mehanizme, redno posodabljajo varnostne politike in izvajajo preventivno izobraževanje zaposlenih o varstvu podatkov.

Odgovorite na vprašanja

Kaj je nelojalna konkurenca po Zakonu o preprečevanju omejevanja konkurence?

Kakšne so sankcije za zlorabe?

Kdo je lahko seznanjen s poslovno skrivnostjo?

Predpostavite, da podjetje obdeluje velike količine občutljivih informacij o partnerjih in strankah. Pripravite načrt upravljanja s podatki, ki vključuje razvrščanje po občutljivosti, določitev dostopov in postopke za odzivanje ob kršitvah varnosti.

Univerzitetna založba
Univerze v Mariboru

Literatura

Ahdil, I. (2024). Economic Intelligence tools at the service of strategic efficiency. *International Journal of Applied Management and Economics, 2*(08), 275–283. https://doi.org/10.5281/zenodo.12528428

Ajayi, V. O. (2023). A review on primary sources of data and secondary sources of data. SSRN electronic journal, 2(3).

AJP – 2 Skupna zavezniška obveščevalna, protiobveščevalna in varnostna doktrina. (2003). NATO Standardisation Agency.

Andrew, C. (2018). *The secret world: A history of intelligence.* Yale University Press.

Anžič, M. (2010). *Konkurenčna obveščevalna dejavnost gospodarskih družb* [Magistrsko delo]. Fakulteta za družbene vede.

Bartes, F. (2011). Intelligence analysis – the royal discipline of competitive intelligence. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 59*(7), 39–56.

Bernhardt, R. (2003). *Competitive intelligence: How to acquire and use corporate intelligence and counter-intelligence.* FT Prentice Hall.

Bižal, S. (2014). *Obveščevalna dejavnost javnih virov – OSINT* [Diplomsko delo]. Fakulteta za varnostne vede.

Breeden, J. (2019). *Open source intelligence isn't just for spies.* https://www.nextgov.com/emerging-tech/2019/11/how-agencies-can-use-opensource-intelligence-close-cybersecurity-loopholes/161580/

Britovšek, J. (2017). Zasebna obveščevalna dejavnost v Republiki Sloveniji – teoretični, pravni in praktični vidiki. V T. Pavšič Mravlje idr. (ur.), *Zbornik povzetkov. 18. slovenski dnevi varstvoslovja, Maribor, 7. in 8. junij 2017* (str. 101). Univerzitetna založba Univerze v Mariboru.

Britovšek, J. (2025). Definicija obveščevalne dejavnosti. *Sodobni vojaški izzivi, 26*(4), 185–198.

Brock, E. (2019). *What is OSINT and Why Is It Important To A Private Investigator?* https://rootinvestigations.com/what-is-osint-and-why-are-public-records-iimportant-to-a-private-investigator/https://rootinvestigations.com/what-is-osint-and-why-are-publicrecords-iimportant-to-a-private-investigator/

Burke, C. (5. 1. 2007). *Freeing Knowledge, telling secrets: Open source intelligence and development.* Bond University. https://pure.bond.edu.au/ws/portalfiles/portal/28737919/Freeing_knowledge_telling_secrets.pdfhttp://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1010&co ntext=cewces_papers

Bush, T. (2016). *PESTLE Analysis: Economic Factors Affecting Business.* https://pestleanalysis.com/economic-factors-affecting-business/

Calof, J. L., in Wright, S. (2008). Competitive intelligence: A practitioner, academic and inter-disciplinary perspective. *European Journal of Marketing, 42*(7/8), 717–730.

Cekuls, A. (2023). Business intelligence factors for decision making. *Journal of Intelligence Studies in Business, 12*(2), 4–5.

Choudhry, R. M., Fang, D. in Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. *Safety science, 45*(10), 993–1012. https://doi.org/10.1016/j.ssci.2006.09.003

Colquhoun, C. (2016). *A Brief History of Open Source Intelligence.* https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-ofopen-source-intelligence/

Čaleta, K. in Čaleta, D. (2012). Vpliv kadrovskega menedžmenta na krepitev varnostne kulture v korporativnovarnostnem okolju. *Sodobni vojaški izzivi, 14* (4), 101-122.

Črnčec, D. (2008). *Obveščevalna dejavnost v javnem in zasebnem sektorju (gospodarska vs. konkurenčna obveščevalna dejavnost).* [Doktorska disertacija]. Fakulteta za družbene vede.

Davenport, T. H. in Prusak, L. (1998). Working knowledge: How organizations manage what they know. *Ubiquity,* 1–15.

Diyaolu, A. M. (2019). The role of competitive intelligence in provision of quality information services. *Library Philosophy and Practice, 1–9*.

Duh, M. (2015). *Upravljanje podjetja in strateški management*. GV Založba.

Dvojmoč, M. (2017). Integralna korporativna varnost. *Varstvoslovje, 19*(3), 252–272.

Dvojmoč, M. (2019). Corporate intelligence as the new reality: the necessity of corporate security in modern global business. *Varstvoslovje, 21*(2), 205–223.

Dvojmoč, M. (2021). *Politika varovanja informacij*. Skupina Infocenter – MD svetovanje.

Dvornik, F. (1974). *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, and Japan*. Rutgers University Press.

Dvoršak, A. (2003). Zbiranje relevantnih podatkov o proizvodnji, konkurenci in poslovanju/Industrial Intelligence & Competitive Intelligence & Business Intelligence/. V M. Pagon (ur.), *Dnevi varstvoslovja* (str. 1 – 8). Visoka policijsko-varnostna šola.

Egan, J. (2001). Competitive intelligence. *The Electricity Journal, 14*(2), 84–85. https://doi.org/10.1016/S1040-6190(01)00171-3

Ezendu, E. (2010). *Competitive intelligence*. https://www.slideshare.net/ezendu/competitive-intelligence-2814940

Fleisher, C. S. in Bensoussan, B. (2003). *Strategic and competitive analysis: methods and techniques for analyzing business competition*. Prentice Hall, Upper Saddle River.

Fleisher, C. S. in Bensoussan, B. (2007). Business and competitive analysis: effective application of new and classic methods. *Revista Inteligencia competitiva, 2*(2), 1–5.

Fuld, L. M. (1995). *The new competitor intelligence: the complete resource for finding, analyzing, and using information about your competitors*. J. Wiley.

Furgison, L. (2020). *SWOT Analysis Step 4: How to Identify Threats*. Bp plans.

Galindo, J. P., Nespoli, P., Marmol, F. G. in Pérez, G. M. (2019). OSINT is the next Internet goldmine: Spain as an unexplored territory. V *Actas de las V Jornadas Nacionales de Ciberseguridad Junio 5-7*, Cáceres (str. 102–109). Servicio de Publicaciones.

Gomezelj Omerzel, D. (2010). The impact of knowledge management on SME growth and profitability: A structural equation modelling study. *African journal of business management, 4*(16), 3417–3432.

Grozde, J. in Henigman, Ž. (2008). Uporaba javnih virov pri obveščevalnem vrednotenju geografskega prostora. V J. Šifrer (ur.), *Javna in zasebna varnost*: *9. slovenski dnevi varstvoslovja, Bled, 5. in 6. junij 2008*. Fakulteta za varnostne vede. http://www.fvv.uni-mb.si/dv2008/zbornik/index.html

Hao, M., Dayal, U. in Hsu M. (2000). Visual data mining for business intelligence applications. *Web-Age Information Management (konferenca),* 3–14. https://doi.org/10.1007/3-540-45151-X_1

Harbulot, C. in Baumard, P. (1996). *Intelligence économique et stratégie des entreprises : une nouvelle donne stratégique*. Economica.

Hassan, N. A. in Hijazi, R. (2018). *Open source intelligence methods and tools*. Apress Berkeley.

Havenga, J. in Botha, D. (2003). *Developing Competitive intelligence in the knowledgebased organisation.* Academia. https://www.academia.edu/737439/Developing_competitive_intelligence_in_the_knowledge_based_organization

Hayes, A. (2023). Code of Ethics: Understading Its Types, Uses Through Examples. V *Investopedia.* https://www.investopedia.com/terms/c/code-of-ethics.asp

Henschke, A. (2024). Moral risk, moral injury, and institutional responsibility: ethical issues in HUMINT. *International journal of intelligence and counterintelligence, 38*, 1231–1248.

Heywood, A. (1997). *Politics* (4th ed.). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-25543-6

Hrastelj, T. (1995). *Podjetniški izzivi mednarodnega poslovanja*. Gospodarski vestnik.

Hromozdova, L., Dubrovyl-Rokhova, A. in Pravorskyi, R. (2021). Economic intelligence in the system of international economic relations: characteristics of the current situation and problems of development. *Technology audit and production reserves, 4*(4(60), 29–33.

Hughes, D. E., Le Bon, J. in Rapp, A. (2013). Gaining and leveraging customer-based competitive intelligence: the pivotal role of social capital and salesperson adaptive selling skills. *Original Empirical Research, 41*, 91 – 110.

Hughes, S. (2005). Competitive intelligence as competitive advantage: The theoretical link between competitive intelligence, strategy and firm performance. *Journal of Competitive Intelligence and Management*, *3*(2), 3–18.

Infocenter. (2023). *Zakaj je zaščita podatkov tako zelo pomembna*. https://infocenter.si/zakaj-je-zascita-podatkov-tako-zelo-pomembna/

Isson, J. P. in Harriott, J. (ur.). (2013). The competitive intelligence mandate. V *Win with Advanced Business Analytics: Creating Business Value from Your Data* (str. 271–284). John Wiley & Sons. https://doi.org/10.1002/9781119205371.ch13

Ivanov, S. in Webster, C. (2017). *The robot as a consumer: a research agenda* [predstavitev prispevka]. Konferenca "Marketing: experience and perspectives", 29-30. junij 2017, Ekonomska univerza - Varna, Bolgarija.
Johnson, L. K. (2024). *National security intelligence: Secret operations in defense of the democracies* (3rd ed.). Cambridge: Polity Press.
Johnson, L. K. (Ed.). (2007). *Handbook of Intelligence Studies*. Routledge.
Joia, L. A. (2000). W3E – a web-based instruction system for leveraging corporate intelligence. *Journal of Workplace Learning, 12*(1), 5–13. https://doi.org/10.1108/13665620010309747
Kahaner, L. (1997). *Competitive intelligence: How to gather, analyze, and use information to move your business to the top.* Simon and Schuster.
Kaptein, M. in Schwartz, M. S. (2007). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of business ethics, 77*(2), 111–127.
Kendrick, T. (2007). The winning mindset. *Business Information Review, 24*(4), 228–235. https://doi.org/10.1177/0266382107084890
Kent, S. (1966). *Strategic intelligence for American world policy*. Princeton University Press.
Kenton, W. (2023). SWOT Analysis: How To With Table and Example. V *Investopedia.* https://www.investopedia.com/terms/s/swot.asp
Koren, B. (2018). *Osnove Obveščevalne dejavnosti* [Povzetek predavanj]. Ljubljana.
Lobnikar, B in Dvojmoč, M. (2017). *Korporativna obveščevalna dejavnost* [Povzetek predavanj]. Fakulteta za varnostne vede.
Lönnqvist, A. in Pirttimäki, V. (2006). The measurement of business intelligence. *Information systems management, 23*(1), 32–40.
Lowenthal, M. M. (2019). *Intelligence: From secrets to policy* (8th ed.). CQ Press.
Madureira, L., Popovič, A. in Castelli, M. (2021). Competitive intelligence: A unified view and modular definition. *Technological Forecasting & Social Change, 173,* 1–17. https://doi.org/10.1016/j.techfore.2021.121086
Makos, J. (7. 2. 2024). Economic factors affecting business in PESTLE analysis (examples). *PESTLE analysis.* https://pestleanalysis.com/economic-factors-affecting-business/
Martre, P. (1994). *Rapport au Premier Ministre: La politique de sécurité économique et industrielle*. La Documentation Française.
Maune, A. (2014). Competitive intelligence and firm competitiveness: An overview. *Journal of Governance and Regulation, 3*(3), 91–103.
Mihelič K. K. in Culiberg B. (2014). Turning a blind eye: a study of peer reporting in a business school setting. *Ethics & Behavior 24*(5), 364-381.
Mohd Asri, M., in Abdul Mohsin, A. (2020). Competitive intelligence practices and organizational performance linkage: A review. *International Journal of Business and Society, 21*(2), 555–569.
Mwakibete, A. A. (2019). *The corporate security: critical issues on enforcement of internal corporate security*. University of Tanzania.
Noe, J. (2011). *Range operations group, operations security (OPSEC) guide.* https://apps.dtic.mil/dtic/tr/fulltext/u2/1038572.pdf
Null byte. (2019). *Find Passwords in Exposed Log Files with Google Dorks*. https://null-byte.wonderhowto.com/how-to/find-passwords-exposed-log-fileswith-google-dorks-0198557/
Olszak, C. M., & Ziemba, E. (2007). Approach to building and implementing business intelligence systems. *Interdisciplinary Journal of Information, Knowledge, and Management, 2*, 135–148. https://doi.org/10.28945/105
Gill, P. in Phythian, M. (2018). *Intelligence in an insecure world (3rd ed.).* Cambridge: Polity Press
Panda mediacenter. (2014). *How do cookies work?* https://www.panda security.com/mediacenter/security/cookies/
Parsons, N. (20251). What is a SWOT Analysis and How to Do It Right (With Examples). *LivePlan.* https://www.liveplan.com/blog/what-is-a-swot-analysis-and-how-to-do-it-right-with-examples/
Pellissier, R. in Nenzhelele, T. E. (2013). Towards a universal competitive intelligence process model. *SA Journal of information management, 15*(2). https://doi.org/10.4102/sajim.v15i2.567
Phillips, P. J. in Pohl, G. (2024). Industrial espionage: window of opportunity. *Information security journal: a global perspective, 34*, 143–155.
Podbregar, I. (2008). Nekateri elementi obveščevalne dejavnosti. V I. Podbregar in T. Ivanuša (ur.), *Vohunska dejavnost in gospodarstvo* (str. 21–73). Fakulteta za varnostne vede.
Podbregar, I. (ur.). (2008). *Vohunska dejavnost in gospodarstvo.* Fakulteta za varnostne vede.
Podbregar, I. in Ivanuša, T. (2010). Javni viri in analitika v obveščevalni dejavnosti. *Revija za kriminalistiko in kriminologijo, 61*/2, 191–198.

Podbregar, I., Mulej, M., Pečan, S., Podbregar, N. in Ivanuša, T. (2010). *Informacije kot "bojna" podpora kriznemu odločanju, krizni komunikaciji in delovanju*. Zavod za varnostne strategije pri Univerzi Maribor.

Popovici, V. (2014). Economic intelligence – Theoretical and practical aspects. *Annals – economy series, 6*, 286–288.

Porter, M. (1980). *Competitive advantage: Creating and Sustaining Superior Performance; and Competitive Strategy: Techniques for Analyzing Industries and Competitors*. Free Press.

Potparič, D. in Dvoršek A. (2012). Oblikovanje osnovne terminologije na področju kriminalistično obveščevalne dejavnosti. *Revija za kriminalistiko in kriminologijo, 63*(1), 39–49.

Priročnik za delo z izpisi klicev. (2010). Ministrstvo za notranje zadeve.

Prislan, K. in Bernik, I. (2013). Kompromisi pri zagotavljanju informacijske varnosti v organizacijah. V *14. Dnevi varstvoslovja*. Fakulteta za varnostne vede. https://www.fvv.uni-mb.si/DV2013/zbornik/informacijska_varnost/Prislan_Bernik.pdf

Prislan, K. in Bernik, I. (2013). Socialno-psihološke implikacije kibernetskega terorizma. *Varstvoslovje, 15*(3), 357–369.

Prislan, K. in Bernik, I. (2016). Dejavniki sprejemanja odločitev pri urejanju učinkovite informacijske varnosti v organizacijah. *Varstvoslovje, 16(*1), 50–67.

Purg, A. (2002). *Primerjalni obveščevalni sistemi*. Visoka policijsko-varnostna šola.

Raščan, S. (2005). *Spremembe varnostne politike ZDA po 11. septembru 2001*. Fakulteta za družbene vede.

Rouach, D. in Santi, P. (2001). Competitive intelligence adds value. *European Management Journal, 19*(5), 552–559. https://doi.org/10.1016/S0263-2373(01)00069-X

Schermerhorn, J. R. (2002). *Management*. Wiley.

SPOT. (2023). *Analiza poslovnega okolja in konkurence*. http://evem.gov.si/info/razmisljam/analiza-poslovnega-okolja-in-konkurence/

Šaponja, V. (1999). *Taktika dela obveščevalnovarnostnih služb*. Visoka policijsko-varnostna šola.

Thinkcurity. (2022). *How to Perform a SWOT Analysis on Your Security Firm*. https://www.thinkcurity.com/articles/how-to-perform-a-swot-analysis-on-your-security-firm

Todorović, G. (29. 11. 2023). *Primerjalna analiza (benchmarking)*. Kabi. https://www.kabi.info/Novice/primerjalna-analiza-benchmarking/

Trim, P. R. J. (2002). Counteracting industrial espionage through counterintelligence: the case for a corporate intelligence unit and collaboration with government agencies. *Security Journal, 15*(4), 7–24.

Ulcej, D., Britovšek, J. in Sotlar, A. (2011). Obveščevalna dejavnost v gospodarstvu: pojmovne opredelitve. V T. Pavšič Mrevlje (ur.), *Smernice sodobnega varstvoslovja: 11. Slovenski dnevi varstvoslovja, Ljubljana, 3.–4. junij 2010*. Fakulteta za varnostne vede. http://www.fvv.uni-mb.si/DV2010/zbornik/nacionalna_varnost/britovsek_ulcej_sotlar.pdf

Uredba (EU) 2016/679 Evropskega parlamenta in sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) . (2016). *Uradni list Evropske unije,* (L 119).

Vedder, R. G. in Guynes, S. (2001). A study of competitive intelligence practices in organizations. *Journal of computer information systems, 41*(2), 36–39.

Vršec, M. (2003). Uvajanje sodobnih varnostnih mehanizmov v poslovne procese gospodarske družbe in gospodarske javne službe. V M. Pagon, *Dnevi varstvoslovja: 4. slovenski dnevi varstvoslovja, Bled, 5. do 7. junij 2003* (str. 150–151). Visoka policijsko-varnostna šola.

Warner, M. (2002). Wanted: A definition of "intelligence". *Studies in Intelligence, 46*(3), 15–22.

Warner, M. (2014). *The Rise and Fall of Intelligence: An International Security History*. Georgetown University Press.

Wheelen, T. L., in Hunger, J. D. (2012). *Concepts in Strategic Management and Business Policy*. Pearson Education, Inc.

Whitman, M. in Smith, C. A. (2005). The Culture of Safety: No One Gets Hurt Today. *The Police Chief, 72*(11), 20–24, 26, 27.

Zack, M. H. (1999). Development a knowledge strategy. *California management review, 41*(3), 125–144.

Zakon o delovnih razmerjih (ZDR-1). (2013). *Uradni list RS*, (27/13, 78/13).

Zakon o detektivski dejavnosti (ZDD-2). (2024). *Uradni list RS*, (95/24).

Zakon o dostopu do informacij javnega značaja (ZDIJZ). (2006). *Uradni list RS*, (51/06, 117/06).

Zakon o informacijski varnosti (ZInfV). (2018, 2021, 2022). *Uradni list RS*, (30/18, 95/21, 130/22).

Zakon o poslovni skrivnosti (ZPosS). (2019). *Uradni list RS*, (22/19).

Zakon o preprečevanju omejevanja konkurence (ZPOmK-2). (2022). *Uradni list RS*, (130/22).

Zakon o tajnih podatkih (ZTP). (2006). *Uradni list RS*, (50/06).

Zakon o varstvu osebnih podatkov (ZVOP-2). (2022). *Uradni list RS*, (163/22).

Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD). (2020). *Uradni list RS*, (177/20).

Zakon o zasebnem varovanju (ZZasV-1). (2011). *Uradni list RS*, (17/11).
Zakon o zaščiti prijaviteljev (ZZPri). (2023). *Uradni list RS*, (16/23).
Zhang, E. (2018). *What is Operational Security?* https://digitalguardian.com/blog/what-operational-security-five-step-processbest-practices-and-more

KORPORATIVNA OBVEŠČEVALNA DEJAVNOST: PRAKTIKUM

MIHA DVOJMOČ
Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
miha.dvojmoc@um.si

Korporativno obveščanje bi lahko predstavljalo orodje povečanega ozaveščanja sodobnih organizacij, ki želijo poslovati varno, predvsem z vidika globalnega poslovanja, ob upoštevanju tveganj na trgu, pa tudi priložnosti lastnega konkurenčnega razvoja. Kot orodje za obvladovanje izzivov in nadgradnjo poslovanja z vidika konkurenčnosti in varnosti na trgu predstavlja samo zavedanje o nujnosti korporativne varnosti v sodobnem globalnem poslovanju neizogiben korak h konkurenčnemu in varnemu globalnemu poslovanju, z zavedanjem zunanjih tveganj, izkoriščanjem lastnih prednosti in poznavanjem značilnosti trga. Na splošno korporativna obveščevalna dejavnost izboljšuje delovanje organizacij, pridobiva konkurenčno prednost, obvladuje tveganja, ščiti celotno organizacijo, omogoča hitrejše in bolj celovite odločitve ter zagotavlja trajnostni razvoj organizacije.

DOI
https://doi.org/
10.18690/um.fvv.2026

ISBN
978-961-286-113-5

Ključne besede:
korporativna obveščevalna dejavnost, varnost, organizacije, podatek, konkurenčna obveščevalna dejavnost

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.2.2026

ISBN
978-961-286-113-5

Ključne besede:
corporate intelligence,
security,
organizations,
data,
competitive intelligence

CORPORATE INTELLIGENCE: PRACTICUM

MIHA DVOJMOČ
University of Maribori, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
miha.dvojmoc@um.si

Corporate intelligence could represent a tool for increasing awareness of modern organizations that want to operate safely, especially from the perspective of global business, taking into account risks in the market, as well as opportunities for their own competitive development. As a tool for managing challenges and upgrading operations from the perspective of competitiveness and security in the market, the awareness of the necessity of corporate security in modern global business represents an inevitable step towards competitive and secure global business, with awareness of external risks, exploitation of own advantages and knowledge of market characteristics. In general, corporate intelligence improves the functioning of organizations; gains competitive advantage; manages risks; protects the entire organization; enables faster and more comprehensive decisions and ensures sustainable development of the organization.

University of Maribor Press

Univerza v Mariboru

Fakulteta za varnostne vede

Miha Dvojmoč

je izredni profesor za področje varnostnih ved na Fakulteti za varnostne vede Univerze v Mariboru in zunanji sodelavec Nove univerze ter Fakultete za informacijske študije. Pedagoško deluje na dodiplomskih in podiplomskih programih z različnih področij varnosti. Raziskovalno se posveča zagotavljanju varnosti, predvsem integralni korporativni varnosti, korporativni obveščevalni dejavnosti, kritični infrastrukturi z odpornostjo in robustnostjo, zasebnemu varovanju, detektivski dejavnosti, varnosti informacij in osebnih podatkov, ter celovitemu zagotavljanju varnosti organizacij ter nadzorstvenim institucijam. Njegova bibliografija vključuje znanstvene in strokovne članke, konferenčne prispevke, varnostne načrte, elaborate in izvedenska mnenja. Je tudi recenzent pri revijah Fakultete za varnostne vede, Pravne fakultete Univerze v Mariboru ter Nacionalnega inštituta za javno zdravje.