Gospodarska špijunaža kao način ugrožavanja klasificiranih informacija

Slunjski, Marina

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

DIPLOMSKI RAD br. 329/PE/2020

GOSPODARSKA ŠPIJUNAŽA KAO NAČIN UGROŽAVANJA KLASIFICIRANIH INFORMACIJA

Marina Slunjski

Varaždin, listopad 2020. godine

SVEUČILIŠTE SJEVER

SVEUČILIŠNI CENTAR VARAŽDIN

Studij poslovna ekonomija, Turizam

DIPLOMSKI RAD br. 329/PE/2020

GOSPODARSKA ŠPIJUNAŽA KAO NAČIN UGROŽAVANJA KLASIFICIRANIH INFORMACIJA

Student:
Marina Slunjski, 0759/336D

Mentor:
doc. dr. sc. Petar Mišević

Varaždin, listopad 2020. godine

Sažetak

Klasificirane informacije ključni su resurs koji tvrtka posjeduje, a prava informacija u pravom trenutku tvrtki osigurava odlučujuću prednost u odnosu na konkurenciju te opstanak na tržištu. Informacije se prikupljaju različitim načinima i metodama, a koje su ponekad na samoj granici zakona. Jedan od načina zaštite osjetljivih podataka od krađe i neovlaštenog korištenja upravo je i metoda klasifikacije podataka. Gospodarska špijunaža predstavlja nezakonit i neetičan način na koji tvrtke dolaze u posjed klasificiranih informacija, čime se neovlašteno i nezakonito dolazi do ključnih informacija s ciljem stjecanja konkurentske prednosti na tržištu, te ostvarivanjem nepripadajuće financijske koristi. Gospodarska je špijunaža neetična i nelegalna, prisutna u gotovo svim područjima gospodarskog poslovanja, a najviše u visoko profitabilnim granama kao što su zrakoplovna industrija, farmaceutska industrija, auto-industrija, IT industrija i dr. Ugrozama iz područja gospodarske špijunaže uglavnom su izložene najrazvijenije države i velike kompanije, međutim, utvrđeno je kako se gospodarskom špijunažom bave i velike svjetske kompanije i sigurnosno-obavještajne agencije gotovo svih zemalja u cilju zaštite gospodarskih interesa. U ovom je radu predstavljeno istraživanje o zaštiti informacijske imovine i informiranosti ispitanika vezano uz pojmove *poslovna tajna* i *gospodarska špijunaža*, te je prikazan primjer slučaja hakiranja podataka grupacije INA d.d.

Ključne riječi: zaštita podataka, informacijska imovina, klasificirani podaci, poslovna tajna, gospodarska špijunaža

Summary

Information assets (hardware, software and data) are a key resource that a company owns, and the right information at the right moment is the biggest asset. Information is collected in different ways and by different methods, which are sometimes on the very edge of the law. One of the ways to protect data is the method of data classification. Economic espionage is an illegal way for companies to collect data, in order to reduce the cost of research, with the aim of making as much profit as possible. Thus, unauthorized and illegal access to key information is used by unauthorized persons, in order to gain a competitive advantage in the market, and achieve unrealistic financial benefits. It is unethical and illegal, but it is also present in all areas of life, and mostly in highly profitable branches such as the pharmaceutical industry and the auto industry.The paper presents a research on the protection of information assets and information of respondents related to the concepts, trade secrets and economic espionage, and a case study of data hacking of the INA d.d.

Keywords: data protection, information assets, classified data, trade secret, economic espionage

Popis korištenih kratica:

BI	Business Intelligence (poslovna inteligencija)
CERT	Computer Emergency Response Team, (nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u RH)
COMINT	Communications Intelligence (komunikacijska obavještajna služba)
DIKW	Data, Information, Knowledge, Wisdom (Podatak, Informacija, Znanje, Razumijevanje)
ELINT	Electronic Intelligence (obavještajna služba koja se bavi presretanjem elektroničkih signala koji nisu u izravnoj komunikaciji među ljudima)
GDPR	General Data Protection Regulation (Opća Uredba o zaštiti podataka)
ISMS	Information Security Management System
ISO	International Organizacion for Standardization (Međunarodna organizacija za standardizaciju)
NSA	National Security Agency (američka agencija za nacionalnu sigurnost)
RH	Republika Hrvatska
SIGINT	Signal Intelligence (obavještajna služba koja se bavi presretanjem elektroničkih signala u komunikaciji među ljudima)
SOA	Sigurnosno-obavještajna agencija
TECHINT	Technical Intelligence (tehnička obavještajna služba)
UVNS	Ured Vijeća za nacionalnu sigurnost
VSOA	Vojna sigurnosno-obavještajna agencija

Sadržaj:

1. UVOD

1.1. Predmet i cilj rada

Ubrzanim razvojem informacijske i komunikacijske tehnologije i njenom primjenom u digitalnom poslovanju dolazi do sve većeg akumuliranja digitalnih podataka i informacija u informacijskim sustavima u privatnom, javnom i državnom sektoru. U temeljima je informacijske znanosti da se razvoj informacijske znanosti povezuje s razmjenom znanja, komunikacijskim medijima, te metodama i tehnikama obrade podataka. Tržište je globalizirano, većina procesa je automatizirana, a digitalna ekonomija preuzima primat u svim područjima poslovanja.

Informacije predstavljaju okosnicu ljudskog djelovanja u uspostavljanju međuljudskih odnosa, poslovnih odnosa ili međunarodnih odnosa. Informacije su izvor znanja, kao što je voda izvor života, no ono čemu će informacija, znanje i moć poslužiti, ne ovisi o informaciji, nego o čovjeku, njegovoj svijesti i savjesti te načinu upravljanja znanjem i informacijama. Upravo zbog činjenice da se svake godine proizvede više informacija nego u cjelokupnoj prošlosti ljudskog roda, javlja se i problem upravljanja i korištenja tako velike količine informacija. S druge strane, većina tih informacija i podataka dostupno je svakome tko raspolaže odgovarajućim znanjem i tehnologijom, pa se tako pojavljuje prvi globalni komunikacijsko-informacijski problem jer nerazvijene zemlje ne posjeduju ni znanje ni tehnologiju. Informacija postaje najvrjedniji kapital, a onaj tko posjeduje pravu informaciju u pravo vrijeme ostvaruje značajnu prednost pred konkurencijom. Upravo se zbog toga sve više ulaže u suvremene tehnologije i informacijske sustave kojima se prikupljaju, obrađuju i transformiraju informacije.

Špijunaža je raširena po cijelom svijetu, a prvi tragovi dopiru još u antičko doba. Adrienne Wilmoth Lerne[1] u svom radu spominje da je u egipatskim hijeroglifima otkrivena prisutnost sudskih špijuna, te da su na papirusima opisane operacije trgovine robljem. Egipatski špijuni koji su radili za faraona, također su imali zadaću istraživati političku situaciju i strategije Rima i Grčke, te su bili prvi koji su koristili biljne i zmijske otrove kako bi sabotirali svoje protivnike. Grci su, za razliku od egipatskih špijuna, bili poznati po prevarama kojima su se

[1]Izvor: Lerner,raspoloživo na http://www.fags.org.espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html – datum pristupa sadržaju 02.02.2020.

koristili kako bi ostvarili napade na svoje protivnike. Kao primjer možemo navesti da su Grci ušli u grad Troju pomoću drvene konstrukcije u obliku konja koju su im darovali, a u njoj su bili sakriveni grčki vojnici.Grci su lako ušli u grad i potom napali nespremnog protivnika. U starom vijeku Rimljani su imali najrazvijeniju špijunažu, s naglaskom na politiku, te špijunažu susjednih zemalja i plemena koja su pripajali Rimskom carstvu. Osim špijunaže susjednih zemalja, razvila se i špijunaža protivničkih strana unutar samog Rimskog carstva što je dovelo do razvoja prvih protuobavještajnih slučajeva.

Lerner također navodi da je razdoblje renesanse obilježila vladavina Crkve, te dolazi do naglog razvoja špijunaže u Europi, s obzirom na to da je svaki narod imao obavještajnu službu s ciljem da budu bolji u trgovini od svojih susjeda. Kao prvi takav primjer možemo navesti osnivanje centara za prikupljanje, sortiranje, obradu i korištenje informacija o „neprijateljskoj strani“ koji je osnovala Dubrovačka Republika. Senat je na svojoj sjednici od 12. kolovoza 1301., formirao tri centra, i to: Centar za fortifikacije i sigurnost, Centar za naoružanje i Centar za obavještajnu službu, koji je nazvan Centar za sakupljanje vijesti i informacija. Ključni ljudi ovog posljednjeg centra bili su plemići: Miho Procula, Pero Prodanelli i Marin Držić. Republika je uskoro imala 1400 agenata, koji su u trećim državama prikupljali vojne, političke i ekonomske informacije (Dedijer, 2002, u Bazdan, 2009, str. 59).

Prema Lerneru moderna špijunaža javlja se u 18. stoljeću, koje je obilježeno brojnim ratovima. To je ujedno i razdoblje u kojem dolazi do industrijalizacije, ekonomskog i teritorijalnog razvoja, pa je i potreba za špijunažom bila sve veća. Velik broj špijuna doveo je i do potrage za izdajicama koji su zloupotrebljavali funkciju obavještajnih snaga. Razvojem gospodarstva uz vojnu špijunažu razvija se i gospodarska špijunaža, upravo zbog razvoja industrijalizacije i urbanizacije, te razvoja znanosti.

Načelo „totalne špijunaže“ primjenjuje se dolaskom Hitlera na vlast i stvaranjem nacističke Njemačke, a nakon Drugog svjetskog rata dolazi do usavršavanja gospodarske špijunaže. Najprivlačnije su grane za gospodarsku špijunažu upravo one koje su i najrazvijenije, a to su: visoka tehnologija, automobilska industrija, farmaceutska industrija, industrija naoružanja, informacijska tehnologija, svemirski programi i slične grane, stoga one moraju i ulagati značajna sredstva kako bi se zaštitile od krađe informacije bilo u fizičkom, bilo u digitalnom obliku.

Sun Tzu, kineski pisac i general, još je prije 2500 godina rekao: „*Tko ima informaciju, ima* i *moć.“,* a profesor te idejni osnivač gospodarske špijunaže i *Business Intelligence* Stevan

Dedijer u jednom je od mnogobrojnih intervjua zaključio: *„Kada su to shvatile uprave kompanija počele su osnivati centre za obavještajnu službu koji su postali radari svake pametne kompanije*.“ (Klasan, 2011).

Idejni tvorac gospodarske špijunaže Stevan Dedijer tvrdi da je uz prikupljanje i mogućnost pristupa informacijama i podacima, jednako važno znati i interpretirati prikupljene informacije, pa zbog toga tvrtke koje žele biti konkurentne, prikupljene podatke obrađuju i analiziraju. Prema Dedijeru, 1960. godine u svijetu je na gospodarsku špijunažu spadalo 25% od ukupnih špijunskih operacija, a 60% na vojno-obavještajne operacije, dok se 1990. godine taj odnos znatno promijenio, te je samo 15% operacija činila vojna špijunaža, a 60% poslovna, odnosno gospodarska špijunaža.

Primarni je cilj svake organizacije osigurati pravovremene i točne informacije, kako bi osigurali svoju konkurentsku prednost, a sukladno tome i vodeću poziciju na tržištu te povećali profit. U svako doba, a ponajviše sada,u razdoblju stalnih inovacija, važno je na vrijeme znati što konkurencija radi i koje su joj namjere, te doći do njihovih ključnih poslovnih tajni. Motivi i ciljevi mogu biti različiti; od osvajanja novog proizvoda ili tržišta, razvoja nove tehnologije, do povećanja konkurentske prednosti i sl. U tu svrhu tvrtke se često služe gospodarskom špijunažom – prikupljanjem informacija na zabranjen i neetičan način. Naime, takav način prikupljanja informacija iziskuje mnogo manje troškove nego kada bi ulagali u sektor za istraživanje i razvoj te u razvoj stručnih kadrova, što je dug i neizvjestan proces.

Jedan od najčešćih primjera koji se navode kao eklatantan primjer gospodarske špijunaže razvoj je ruskog supersoničnog putničkog aviona, Tupoljev Tu-144 (*Tupolev Tu-144*), koji je nastao kao rezultat špijunaže francuske tvrtke Aerospatiale, u kojoj se proizvodio čuveni avion *Concorde*.

Kada govorimo o špijunaži na višoj razini, tada su u to uključene čitave vlade, preko diplomata te obavještajnih službi. Svaka zemlja štiti svoje nacionalne i gospodarske interese, svim dopuštenim, ali počesto i nedopuštenim, sredstvima. Godine 1981., Pierre Marion, direktor francuske obavještajne službe izjavio je: *„Kad dođe do biznisa – počinje rat!“*, te tako stvorio moto da je špijunaža drugi oblik diplomacije, uveo svijet u novu, sadašnju fazu obavještajne revolucije. Vrlo je teško odrediti granicu između onoga što je dopušteno, a što je zabranjeno prilikom prikupljanja informacija, pogotovo u današnje digitalno doba. No, jedno možemo sa sigurnošću reći; zemlje koje imaju viši stupanj razvijenosti tehnike i tehnologije

posjeduju značajnu prednost u odnosu na zemlje u razvoju. Zemlje koje su svoju poslovnu strategiju nadogradile centrima gospodarsko-obavještajne službe, što nije trošak, nego investicija, imaju veći i brži gospodarski rast. Usto, nužno je spomenuti i gospodarsku diplomaciju, u kojoj izvršnu ulogu moraju imati najistaknutiji političari i stručnjaci iz područja gospodarstva.

Kao primjer istaknutog političara u funkciji protežiranja nacionalnog gospodarstva možemo navesti bivšeg predsjednika Francuske Republike Jacquesa Chiraca , koji je 1997. godine izjavio:*„Kada putujem u inozemstvo nemam nikakvih predrasuda.Idem prodavati francuske proizvode!"*[2]

Cilj je ovog rada objasniti proces nezakonitog prikupljanja informacija kroz gospodarsku špijunažu, te važnost zaštite podataka,informacija i informacijskih sustava u kojima se iste obrađuju. Prezentira se uloga informacijske sigurnosti i načini na koje se klasificirani podaci i informacije štite od neovlaštenog pristupa. Neke su informacije dodatno zaštićene, pa u tom slučaju govorima o klasificiranim podacima i informacijama (u državnom sektoru),dok u javnom sektoru i privatnom sektoru koristimo pojmove kao što su „*poslovna tajna*" ili „*profesionalna tajna*".U okviru zaštite klasificiranih podataka važnu ulogu predstavlja organizacija informacijske sigurnosti koja se planira unutar pet područja: fizička sigurnost, sigurnost podataka, sigurnost informacijskog sustava, sigurnosna provjera i sigurnost poslovne suradnje.

1.2. Sadržaj i struktura rada

Struktura rada podijeljena je na osam dijelova i to redom: uvod, osnovni pojmovi, vrste povjerljivih podataka, zakoni i propisi koji reguliraju zaštitu podataka, uloga i značaj informacijske sigurnosti u zaštiti podataka, špijunaža, studija slučaja, te provedeno istraživanje vezano uz zaštitu podataka.

U uvodnom dijelu rada prikazana je važnost zaštite podataka, organizacija informacijske sigurnosti te špijunaže, kao i mali uvod kroz povijest vezan uz navedene pojmove.

[2]Sidibé, D. i Saner, R. 2012.The Intersection Between the Roles oft he State and of Multinationals, u: Business,Society and Politics: Multinationals in Emerging Markets. Ur. A. Hadjikhani, U. Elg, P. Ghauri, Bingley, 330–1.

Kroz osnovne pojmove objašnjena je važnost, struktura i povezanost pojmova; podatak, informacija, znanje, razumijevanje; kao i njihovo tumačenje kroz zakonske akte Republike Hrvatske.

U trećem djelu rada obrađene su vrste povjerljivih podataka: poslovna tajna, profesionalna tajna i klasificirani podaci. Ovi pojmovi predstavljaju osnovu kasnijeg razumijevanja važnosti zaštite podataka, načina ugrožavanja klasificiranih podataka,te gospodarske špijunaže kao teme ovog rada.

Zakon i propisi koji reguliraju zaštitu podataka obrađeni su u četvrtom dijelu ovog rada i to: Zakon o zaštiti tajnosti podataka, Zakon o tajnosti podataka, Zakon o informacijskoj sigurnosti te dijelovi Kaznenog zakona Republike Hrvatske koji se odnose na teme ovog rada.

Peti dio rada odnosi se na ulogu i značaj informacijske sigurnosti u zaštiti podataka, u kojem su prikazani osnovni pojmovi sigurnosti, informacijske sigurnosti, područja i mjere informacijske sigurnosti, kao i uloga norme ISO 27001.

U šestom dijelu rada, opisan je primarni cilj ovog rada,gospodarska špijunaža; jedan od načina nezakonitog i neetičnog prikupljanja klasificiranih podataka. Objašnjen je pojam špijunaže, povijesni pregled, vrste i metode gospodarske špijunaže, te načini zaštite od špijunaže. Također, opisana je uloga i značaj sigurnosno-obavještajnih agencija u području špijunaže, te prezentirana razlika između Business Intelligence koji predstavlja legalan način prikupljanja podataka i gospodarske špijunaže koja predstavlja nelegalan način prikupljanja podataka.

Kroz studiju slučaja na primjeru nacionalne kompanije INA d.d. prikazana su nedavna zbivanja, prema javno dostupnim izvorima, a vezana uz hakerski upad u informacijski sustav INA d.d. koji se dogodio u veljači 2020. godine.

Kroz provedenu anketu, analizirani su načini zaštite podataka, osobnih i poslovnih podataka tvrtke,te zaštite od krađe poslovnih informacija. Anketa je provedena u pravnim osobama iz javnog i privatnog sektora.

2. OSNOVNI POJMOVI

Kako bismo mogli uočiti važnost zaštite podataka, potrebno je utvrditi osnovne razlike između podataka i informacija koje susrećemo u svakodnevnom poslovanju i životu.

Riječ „***podatak*“** potječe od množine latinskog *datum* što znači dio informacije. Podatak je jednostavna neobrađena izolirana misaona činjenica koja ima neko značenje.Podatak – prema Zakonu o tajnosti podataka (Narodne novine br. 79/07) ima sljedeće tumačenje:

„*...podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti cjelovitosti za svoga vlasnika*.“[3]

Podaci (engl.Data) znakovni su prikaz činjenica i pojmova koji opisuju svojstva objekata i njihovih odnosa u prostoru i vremenu. „*Podatak je nematerijalne prirode, on jednostavno postoji u našim mislima i nema značenje unutar ili izvan svog postojanja ili o samom sebi pa se pridružuje značenju kojim opisujemo svojstva objekata. Može postojati u bilo kojem obliku bio upotrebljiv ili ne. Oblici podataka su zvučni, slikovni, brojčani i tekstualni. Bilježe se na njima sukladne načine. Struktura podatka je apstraktna i čine ju: značenje(naziv i opis značenja određenog svojstva), vrijednost(mjera i iznos) i vrijeme. Podaci u kontekstu i* kombinirani unutar strukture čine informaciju“[4] – prema definiciji Hrvatske enciklopedije.

Osobni podatak prema članku 4, Opće uredbe o zaštiti podataka, ima sljedeće tumačenje: *„...osobni podaci” znači svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik”); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca:“*[5]

---

[3]Podatak, Zakon o tajnosti podataka – raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 05.02.2020.
[4]Podatak, Hrvatska enciklopedija – Leksikografski zavod Miroslav Krleža – raspoloživo na https://www.enciklopedija.hr/natuknica.aspx?id=6404 – datum pristupa sadržaju 05.02.2020.
[5]Osobni podatak; prema GDPR, Opća uredba o zaštiti podataka, raspoloživo na https://eur-lex.europa.eu/legalcontent/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR – datum pristupa sadržaju 07.02.2020.

Riječ ***„informacija“*** potječe od lat. *Informare*,što znači informiranje, obavještavanje. Informacija (engl. Information) rezultat je analize i organizacije podataka tako da primatelju daje novo znanje. Informacija je raznolikost poruka od pošiljatelja do primatelja. Ona postaje znanjem kad bude interpretirana, odnosno stavljena u kontekst ili kad joj je dodano značenje. Informaciju čine podaci kojima je dano značenje putem relacijskih veza, odnosno organizirani podaci koji su uređeni za bolje shvaćanje i razumijevanje. Značenje informacije može biti korisno, ali i ne mora – prema definiciji Hrvatske enciklopedije.[6]

Poslovna informacija predstavlja najvrjedniji resurs svakog poduzeća, te poduzeće koje posjeduje pravu informaciju u pravo vrijeme ostvaruje znatne prednosti pred svojom konkurencijom. Prava informacija u pravo vrijeme predstavlja ujedno i moć nad konkurencijom. Kako bi menadžment mogao donositi odluke o upravljanju i razvoju poduzeća mora raspolagati svim dostupnim informacijama u realnom vremenu. Ako nam informacije nisu dostupne u realnom vremenu – možemo donijeti najbolju odluku, ali kada za to bude prekasno. Menadžeri koji posjeduju više informacija i koji imaju veću kontrolu nad njima, imaju i veću prednost u odnosu na ostale u donošenju svojih odluka. Prema tome, možemo zaključiti da poslovna uspješnost poduzeća znatno ovisi o poslovnim informacijama, informacijskoj tehnologiji, te o korištenju istih.

Informacije prema Javoroviću i Bilandžiću možemo podijeliti prema nekoliko kriterija:[7]

1. Informacije prema nastanku:
   - Izvorne
   - Izvedene
2. Informacije prema učinku:
   - Korisne
   - Nekorisne
3. Informacije prema izvoru:
   - Vlastite ili unutarnje
   - Tuđe ili vanjske
4. Informacije prema pojavnom obliku:
   - Glasovne

[6]Informacija, Hrvatska enciklopedija – Leksikografski zavod Miroslav Krleža – raspoloživo na https://www.enciklopedija.hr/natuknica.aspx?id=6404 – datum pristupa sadržaju 05.02.2020.
[7]Izvor: Javorović B., Bilandžić M., (2007), Poslovne informacije i business intelligence, Zagreb: Golden marketing – Tehnička knjiga, str.32–33.

- Pisane
- Slikovne
- Zvučne
- Znakovne

5. Informacije prema vjerodostojnosti:
   - Točne ili istinite
   - Krive ili neistinite
6. Informacije prema području djelovanja:
   - Gospodarske
   - Društvene
   - Političke
   - Odgojno-obrazovne
   - Sigurnosne
   - Vjerske
   - Zdravstvene
   - Kulturne
   - Znanstvene
   - Informacijsko-komunikacijske
7. Informacije prema otvorenosti:
   - Javne
   - Tajne
8. Informacije prema razini:
   - Lokalne
   - Subregionalne
   - Državne
   - Regionalne
   - Svjetske ili globalne
9. Informacije prema sadržaju:
   - Osobne
   - Opće
   - Poslovne
10. Informacije prema dospijeću:
    - Pravovremene
    - Zakašnjele ili zastarjele

Izvori poslovnih informacija mogu biti primarni ili sekundarni. U primarne izvore možemo ubrojiti informacije koje dolaze od rukovodećih osoba u poduzeću (nastupi, govori, intervjui i slično) te javno dostupna analitička izvješća poduzeća. Sekundari izvori informacija su: internet, online i digitalne baze podataka, članci u novinama, monografije, TV ili radijske emisije i slično. Do sekundarnih podataka možemo doći i preko sajmova, burza, stručnih kolegija ili skupova na kojima sudjeluju predstavnici poduzeća.

"Koncept poslovne inteligencije (engl. Business Intelligence), koji govori da inteligentno poslovanje počiva na informacijama koje se transformiraju u znanje, a ono u profit, temelji se na skladnom funkcioniranju pojedinih dijelova informacijskog sustava."[8]

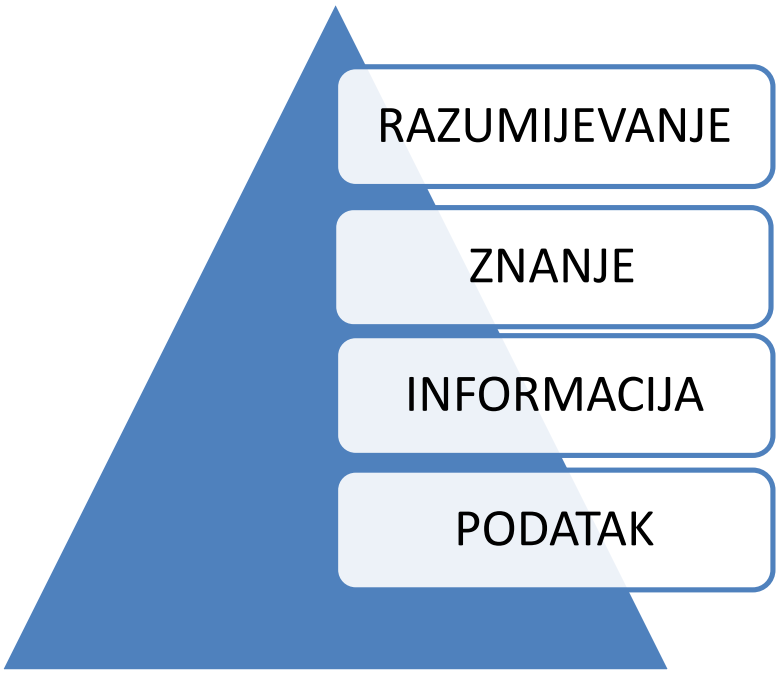
U današnje vrijeme informacije se sve više gomilaju te je teško doći do pravih informacija. Većina podataka i informacija dostupna je svakome tko raspolaže odgovarajućom tehnologijom i posjeduje određenu razinu znanja. Onaj tko posjeduje više informacijsko-komunikacijske sposobnosti i znanja, lakše će se snalaziti u poslovnim, društvenim, gospodarskim, političkim i drugim procesima, te će uvijek biti u prednosti pred onima koji to ne posjeduju. Da bismo ostvarili svoju prednost pred drugim organizacijama, moramo posebnu pažnju posvetiti poslovnim informacijama, što se očituje u sljedećem:

a) izgradnji suvremenih informacijsko-komunikacijskih sustava (utemeljenih na dostignućima informacijske i komunikacijske znanosti, najnovijim informacijsko-komunikacijskim i tehničko-tehnološkim dostignućima, visoko razvijenoj programskoj softverskoj potpori i visokostručnom kadru);
b) stvaranju vlastitih skladišta i baza podataka;
c) uključivanju u šire informacijsko-komunikacijske mreže i sustave uključujući internet
d) obogaćivanju informacijsko-komunikacijske funkcije i sustava uvođenjem posebne poslovno-obavještajne strategije prikupljanja, obrade i korištenja poslovnim podacima i informacijama (Business Intelligence);
e) novim oblicima virtualnog mrežnog poslovnog organiziranja i djelovanja na internetu i preko njega, koji pružaju povezivanje postojećih resursa u snažne sustave itd.

Iz navedenog možemo zaključiti da bi svako poduzeće, da bi ostvarilo svoju prednost pred konkurencijom, moralo težiti izgradnji i razvijanju vlastitih poslovnih podataka i informacija te komunikacijsko-informacijskog sustava.

[8]Čerić, Vlatko, Varga, (2004) Mladen, Informacijska tehnologija u poslovanju, Sveučilište u Zagrebu, Zagreb, 2004., str.25.

Znanje je odgovarajuća zbirka informacija čija je namjera da bude korisna. Znanje čine organizirane informacije koje se mogu koristiti za stvaranje novih značenja i podataka. Znanje je ljudska sposobnost poduzimanja učinkovitih postupaka u raznolikim i neizvjesnim situacijama. Znanje je predodređen proces. Kada netko memorira informacije, skuplja, odnosno gomila znanje. Znanje čine činjenice koje postoje unutar psihičke strukture koju svijest može obraditi. Ljudski um koristi to znanje za biranje između mogućnosti, a time reagiranje i ponašanje postaje inteligentnije. Kada vrijednosti i obveze vode inteligentno ponašanje, ono je zapravo temeljeno na mudrosti. Mudrost je imanje iskustva, znanja i razumijevanja uz moć primjenjivanja svih triju vještina s razboritošću, praktičnošću, diskretnošću i zdravim razumom, odnosno mudrost je sposobnost donošenja ispravnih odluka.[9]



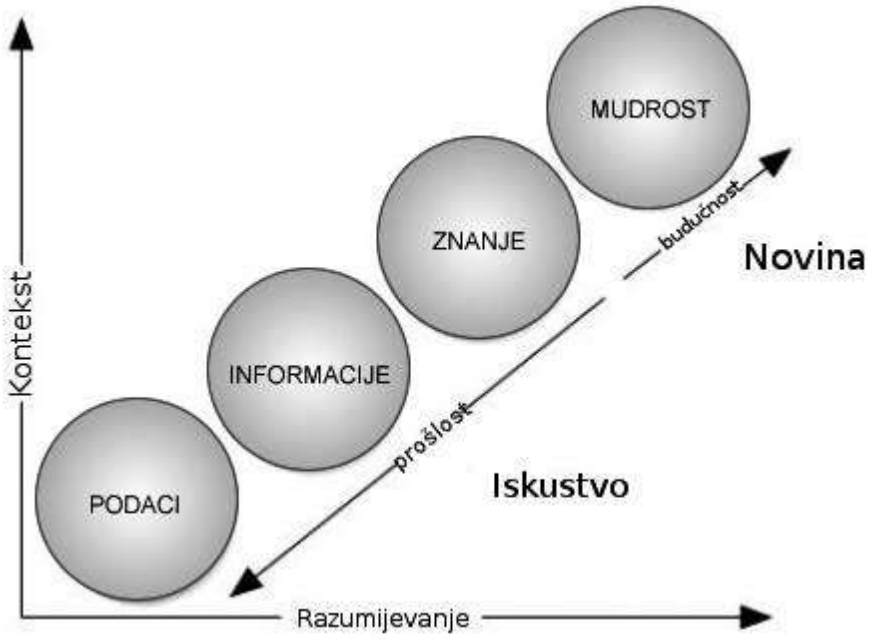
Slika 1:DIKW model – piramida znanja (vlastita izrada)

DIKW (Data, Information, Knowledge, Wisdom Hierarchy) prijedlog je strukturiranja podataka, informacija, znanja i mudrosti u informacijsku hijerarhiju u kojoj svaka razina dodaje određena svojstva onima iznad i ispod nje. Podatak je najosnovnija razina, informacija dodaje kontekst, znanje dodaje kako ga upotrijebiti, a mudrost dodaje kada i zašto ga upotrijebiti.

[9]Znanje, raspoloživo na https://hr.wikipedia.org/wiki/Znanje – datum pristupa sadržaju 25.03.2020.

DIKW model temelji se na pretpostavljanju sljedećeg niza postupaka:

- podatak dolazi u obliku neobrađenih zapažanja i dimenzija,
- informacija se oblikuje analiziranjem veza i odnosa između podataka,
- znanje se oblikuje koristeći informaciju za djelovanje,
- mudrost se oblikuje kroz upotrebu znanja, kroz komunikaciju korisnika znanja i kroz razmišljanja.



Slika 2:Djelomični prikaz DIKW hijerarhije

prema (D. Clarku, 2004)[10]

Na slici 2. prikazano je na još jedan način kako funkcionira piramida znanja prema D. Clarku. Naše iskustvo predstavlja prošlost, dok budućnost predstavlja novu spoznaju o nečemu.Općenita je misao da je podatak manji od informacije, a informacija manja od znanja. Drugim riječima, da bi se kreirala informacija potreban je podatak i samo kada postoji informacija znanje može doći do izražaja.

[10]Clark, Donald. The Continuum of understanding. 2004. – raspoloživo na http://www.nwlink.com/~donclark/performance/understanding.html. – datum pristupa sadržaju 20.03.2020.

2.1. Poslovne informacije kao predmet špijunaže

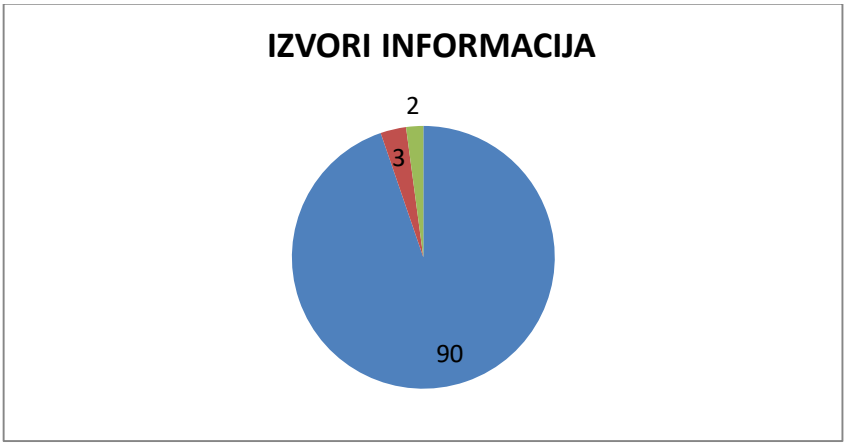
Poslovne informacije, koje su najčešće predmet gospodarske špijunaže, možemo podijeliti na:[11]

1. otvorene informacije ili informacije u bijelim zonama
2. poluotvoreni izvori informacija ili informacije u sivoj zoni
3. zatvorene informacije ili informacije u crnim zonama

Otvorene informacije one su informacije do kojih se može doći legalno i lagano, to su izvori koji su javno dostupni (mediji,internet,javne baze podataka, godišnja izvješća poslovnih subjekata, javni vladini dokumenti, godišnja izvješća s dioničarskih skupština i dr.). Smatra se da je danas oko 90% informacija koje dobivamo iz otvorenih izvora. U ovom slučaju govorimo o legalnom i etičnom prikupljanju podataka i informacija.

Informacije „sivih" izvora nisu tako lako dostupne kao otvorene informacije. Do njih se dolazi dugotrajnim radom, te sudjeluju s oko 3% u ukupnim informacijama za koje su poduzeća zainteresirana te govorimo o informacijama s ruba zakona.

Tajne informacije – top secret informacije, su svega 2% informacija. Do njih se dolazi na zabranjen način, industrijskom špijunažom. Neki od tih načina su; infiltracija, ubacivanje „krtice", prisluškivanjem, špijuniranje, krađom povjerljivih podataka – software.



Slika 3: Izvori informacija (vlastita izrada)

[11]Ibid., 63.

2.2. Metode prikupljanja poslovnih informacija

Uzimajući u obzir cirkulaciju velikog broja informacija na tržištu, sve informacije treba nekako obraditi. Takve aktivnosti danas se više ne smatraju troškom, već investicijama, a sastoje se od prikupljanja, provjeravanja i analiziranja te utvrđivanja vrijednosti i istinitosti informacija i podataka koji su prikupljeni. Prikupljene informacije i podatke je potrebno obraditi i to kroz:

- analizu podataka
- skladištenju podataka
- određivanje kvalitete podataka
- rudarenje podacima
- analitičko obrađivanje podataka

Metode prikupljanja informacija:

1. Skeniranje podataka: skeniranje lokalnih i internetskih datoteka, odnosno memorijskih kapaciteta (dokumenti, liste, popisi, dokumenti posebnih programa kao što su AutoCADi sl.)
2. Pronalaženje lokacije: koriste se podaci s GPS-a, bežičnih lokalnih računalnih mreža i dr. kako bi se ustanovila pozicija osobe, odnosno računala, te kako bi se pratilo eventualno kretanje u prostoru
3. *Bube*: maleni mikrofon koji se skriva u određene dijelove odjeće ili bijele tehnike s ciljem snimanja zvuka
4. Skrivene privatne mreže: zaobilaženje korporacijskih sigurnosnih mreža
5. Kamere: tajno snimanje fotografija i video materijala
6. Keylogger: računalni program koji bilježi svaku vrstu tipkanja na tipkovnici i sprema transkript u samostalni dokument (najčešće Notepad)
7. *Screen Grabber* (nap. prev. *Hvatač ekrana*): računalni program koji periodično slika ono što se nalazi na ekranu određenog računala ili gadgeta
8. Eksfiltracija: diskretno iznošenje informacija iz neke mreže (uglavnom se čekaju momenti velikih prometa po nekom web-mjestu kako bi se teže pratili tragovi iznošenja)
9. Manipulacija materijalima: praćenje izmjena materijala
10. Prisluškivanje mobitela

Mjesta na kojima možemo doći do informacija:

1. Formalni dokumenti (izvještaji,specifikacije proizvoda, radni papiri, tehnička dokumentacija, strateški planovi)
2. Skice (informacije koje se nalaze na skicama vrlo su važne)
3. Državne ustanove (Zavod za statistiku, Zavod za patente, Poslovne udruge i udruženja)
4. Javni servisi (internet, specijalizirane novine, znanstveni članci)
5. Interna korespondencija (zapisnici sa sastanaka, odluke, rješenja)
6. Nevažni komadići papira (računi, putni nalozi i karte)
7. Formalni sastanci (sastanci sa zaposlenicima)
8. Neformalni sastanci (zaposlenici se sastaju poslije radnog vremena i raspravljaju o poslu).

Iz gore navedenih izvora,kao i mjesta na kojima možemo doći do informacija, možemo zaključiti da su to vrlo raznoliki događaji, pa često nismo ni svjesni opasnosti i rizika u kojoj se nalazimo i načina na koji nesvjesno možemo otkriti važne informacije našim sadašnjim ili potencijalnim konkurentima. Zaposlenici često nesvjesno ostavljaju kopije različitih dokumenata na neprikladnim mjestima ili ih bacaju u smeće, a da ih prethodno nisu uništili. Tako u smeću često završavaju i ugovori s našim poslovnim partnerima, koji sadržavaju podatke koji predstavljaju „poslovnu tajnu“ bilo da se odnose na proizvod, cijenu ili neki drugi detalj vezan uz poslovnu suradnju.

3. VRSTE POVJERLJIVIH PODATAKA

3.1. Poslovna tajna

Definicija tajne prema hrvatskom leksikonu; „*...tajna, činjenica poznata užem krugu osoba, za koju postoji opravdan opći ili individualni interes da se znanje o njoj ne proširi. Tajna može biti državna, vojna, službena, poslovna ili osobna.*“[12]

Zakonom o gospodarskoj špijunaži SAD-a[13]iz 1996., koji su pripremili senatori Herb Kohl i Arlen Specter, posebno je definiran institut *poslovne tajne*. A paragraf koji se odnosi na to glasi:

„Poslovna tajna je svaki oblik i svaka vrsta financijskih, poslovnih, znanstvenih, tehničkih, gospodarskih ili tehnoloških informacija, uključujući obrasce, planove, procedure, programe, ili kodove, vidljive ili nevidljive, bez obzira kako su spremljeni, organizirani ili sačuvani, elektronički, grafički, na fotografijama ili napisani – ako je:

1. *vlasnik poduzeo odgovarajuće mjere za očuvanje njihove tajnosti i*
2. *ako informacije predstavljaju neovisnu ekonomsku vrijednost, aktualnu ili potencijalnu, odnosno ako nisu opće poznate i nisu bile prisutne u javnosti na bilo koji način.“*[14]

Prema Zakonu o zaštiti tajnosti podataka (Narodne novine br. 108/96), iz kojeg su preuzete odredbe glave 8 i glave 9; iz 2007 godine, Zakon o tajnosti podataka članak 19. definira:[15]

„Poslovnu tajnu predstavljaju podaci koji su kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.“

[12]Tajna – raspoloživo na https://www.hrleksikon.info/definicija/tajna.html – datum pristupa sadržaju 11.02.2020.
[13]Economic Espionage Act (1996), 18 U. S. C., paragraphs: 1831–1839. , Washington, 3.
[14]Anderson, P. (2009), *Economic Espionage in The World*, Chicago, 56.
[15]Poslovna tajna, Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/748/Zakon-o-za%C5%A1titi-tajnosti- podataka – datum pristupa sadržaju 13.02.2020.

Općim aktom ne može se odrediti da se svi podaci koji se odnose na poslovanje pravne osobe smatraju poslovnom tajnom, kao što se ni poslovnom tajnom ne mogu odrediti podaci čije priopćavanje nije razložno protivno interesima te pravne osobe.

Poslovnom tajnom ne mogu se odrediti podaci koji su od značaja za poslovno povezivanje pravnih osoba ni podaci koji se odnose na zaštićeno tehničko unapređenje, otkriće ili pronalazak.

Poslovna tajna predstavlja način postupanja, poslovnu praksu, "know-how" ili neku drugu informaciju koja pomaže poslovnim subjektima da se natječu s konkurencijom (Zlatović, 2011.).

Poslodavac će posebnim općim aktom, kao autonomnim izvornom radnog i poslovnog prava, urediti pitanja poslovne tajne (Buklijaš, 2008.).

Tajnim podatkom smatra se svaki podatak koji je prema posebnom zakonu određen kao klasificirani podatak (Kazneni zakon, čl. 87, st. 12.).

Tajnom se smatra podatak koji je poznat i koji smije biti poznat samo određenom krugu osoba, pri čemu postoje određene društvene norme koje brane iznošenje takvih podataka izvan tog kruga osoba (Zabel, 1970.).

3.1.1. Odavanje i neovlašteno pribavljanje poslovne tajne

Odavanje i neovlašteno pribavljanje poslovne tajne predstavlja kazneno djelo prema članku 262. Kaznenog zakona Republike Hrvatske koji definira temu „Odavanje i neovlašteno pribavljanje poslovne tajne" na sljedeći način:[16]

1. Tko neovlašteno drugome priopći, preda ili na drugi način učini pristupačnim podatke koji su poslovna tajna, kao i tko pribavlja takve podatke s ciljem da ih preda neovlaštenoj osobi, kaznit će se kaznom zatvora do tri godine.
2. Ako je kaznenim djelom iz stavka 1. ovog članka počinitelj sebi i drugome pribavio znatnu imovinsku korist ili je prouzročio znatnu štetu, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

[16]Odavanje i neovlašteno pribavljanje poslovne tajne, Kazneni zakon Republike Hrvatske stupio je na snagu u svibnju 2015., raspoloživo na http://www.zakon.hr/z/98/Kazneni-zakon– datum pristupa sadržaju 15.02.2020.

3. Ako su definirani pojmovi „poslovno-obavještajna služba“ i „industrijska špijunaža“, ključno je tko sve i kada nastupa kao subjekt. U tom smislu valja razlikovati makro i mikrorazinu aktivnosti. Makrorazina se odnosi na državu koja prikuplja gospodarske informacije na području druge države, bili pritom razlozi političke, vojne ili gospodarske sigurnosti, ili su motivi obavještajni ili protuobavještajni hoće li se te informacije staviti na raspolaganje državnim ustanovama ili se proslijediti nekome od poslovnih subjekata. Razdjelnica je izvor. Naime, ako se to radi uz pomoć zatvorenih izvora, tada je riječ o gospodarskoj špijunaži (Economic Espionage).

3.2. Profesionalna tajna

Profesionalnu tajnu predstavljaju podaci o osobnom ili obiteljskom životu osoba koje saznaju:

- svećenici
- odvjetnici,
- zdravstveni i socijalni djelatnici,
- druge službene osobe u obavljanju svog poziva.[17]

Profesionalna tajna spada u kategoriju privatnih tajni, jer proizlazi iz bliskog odnosa i povjerenja između osoba koje se bave svojim pozivom i njihovim strankama u procesu. Zaštita profesionalne tajne osobito je važna s aspekta osobnog prava na privatnost jer njezinim otkrivanjem može doći do kršenja prava na privatnost.

Neovisno o načinu na koji je tajna otkrivena, Zakonom o zaštiti tajnosti podataka, propisano je da je svatko tko sazna bilo koju vrstu tajne (državnu, vojnu, službenu, poslovnu ili profesionalnu) obvezan čuvati je.

Kao primjer profesionalne tajne možemo navesti – bankarsku tajnu, odnosno povjerljiv odnos između klijenta i bankarskog službenika. Bankarski službenik ima uvid u prihode, troškove, bonitete i ostale povjerljive podatke, pristup PIN-ovima kartica, kao i ostalim osobnim podacima.

[17]Profesionalna tajna, Zakon o tajnosti podataka raspoloživo na https://www.zakon.hr/z/748/Zakon-o-za%C5%A1titi-tajnosti- podataka – datum pristupa sadržaju 22.04.2020.

3.3. Klasificirani podaci

Pojmovi klasifikacije podataka, dodjele stupnjeva tajnosti i pojma neklasificirani podatak uređeni su u Zakonu o tajnosti podataka:

Sukladno članku 2. Zakona o tajnosti podataka**„Klasificirani podatak** je onaj podatak koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje“[18].

„Neklasificirani podatak je podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje“[19].

Klasifikacija podatka je postupak utvrđivanja jednog od stupnjeva tajnosti podatka, s obzirom na stupanj ugroze i područje ovim Zakonom zaštićenih vrijednosti.

Sukladno članku 3. Zakona o tajnosti podataka „Klasificiranim podatkom ne može se proglasiti podatak radi prikrivanja kaznenog djela, prekoračenja ili zlouporabe ovlasti te drugih oblika nezakonitog postupanja u državnim tijelima“.

Zakon o tajnosti podataka propisuje kako je vlasnik klasificiranih podatka nadležno tijelo u okviru čijeg djelovanja je klasificirani ili neklasificirani podatak nastao, a certifikat je uvjerenje o sigurnosnoj provjeri koje omogućava pristup klasificiranim podacima osobama koji rade s klasificiranim podacima.

U odnosu na stupanj ugroze zaštićenih vrijednosti stupnjevima tajnosti iz članka 4. Zakona o tajnosti podataka mogu se klasificirati podaci iz djelokruga državnih tijela u području obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ako su podaci od sigurnosnog interesa za Republiku Hrvatsku.

[18]Klasificirani podatak, Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 15.02.2020.
[19]Neklasificirani podatak, Zakon o tajnosti podataka ,raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 15.02.2020.

Stupnjevi su tajnosti podataka prema članku 4. Zakona o tajnosti podataka[20]:

- vrlo tajno
- tajno
- povjerljivo
- ograničeno

U članku 6., Zakona o tajnosti podataka, stupnjem tajnosti „VRLO TAJNO“ klasificiraju se podaci čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima Republike Hrvatske, a osobito sljedećim vrijednostima:[21]

- temelji Ustavom utvrđenog ustrojstva Republike Hrvatske,
- neovisnost, cjelovitost i sigurnost Republike Hrvatske,
- međunarodni odnosi Republike Hrvatske,
- obrambena sposobnost i sigurnosno-obavještajni sustav,
- sigurnost građana,
- osnove gospodarskog i financijskog sustava Republike Hrvatske,
- znanstvena otkrića, pronalasci i tehnologije od važnosti za nacionalnu sigurnost Republike Hrvatske

U članku 7., Zakona o tajnosti podataka,„stupnjem tajnosti „TAJNO“ klasificiraju se podaci čije bi neovlašteno otkrivanje teško naštetilo vrijednostima iz članka 6. ovoga Zakona.

Članak 8. Zakona o tajnosti podataka,„stupnjem tajnosti „POVJERLJIVO“ klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo vrijednostima iz članka 6. ovoga Zakona.

Članak 9. Zakona o tajnosti podataka, „stupnjem tajnosti „OGRANIČENO“ klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova iz članka 5. Zakona o tajnosti podataka.

[20]Stupnjevi tajnosti podataka ,Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 15.02.2020.
[21]Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka– datum pristupa sadržajuržaju 15.03.2020.

3.3.1. Postupak klasificiranja i deklasificiranja podataka

Klasifikacija podataka obavlja se pri nastanku klasificiranih podataka ili prilikom periodične procjene. U postupku klasifikacije podatka vlasnik podatka dužan je odrediti najniži stupanj tajnosti koji će osigurati zaštitu interesa koji bi neovlaštenim otkrivanjem tog podatka mogli biti ugroženi. Klasificiranje podataka stupnjevima tajnosti „VRLO TAJNO“ i „TAJNO“ mogu provoditi: [22]

- predsjednik Republike Hrvatske,
- predsjednik Hrvatskog sabora,
- predsjednik Vlade Republike Hrvatske,
- ministri,
- glavni državni odvjetnik,
- načelnik Glavnog stožera Oružanih snaga RH i
- čelnici tijela sigurnosno-obavještajnog sustava RH
- osobe koje oni za tu svrhu ovlaste.

Klasificiranje podataka stupnjevima tajnosti „POVJERLJIVO“ i „OGRANIČENO“, pored osoba navedenih pod ovlastima „VRLO TAJNO“ i „TAJNO“ , mogu provoditi i čelnici ostalih državnih tijela. Podaci se klasificiraju za znanstvene ustanove, zavode i druge pravne osobe, kada rade na projektima, pronalascima, tehnologijama i drugim poslovima od sigurnosnog interesa za Republiku Hrvatsku. Za vrijeme važenja stupnja tajnosti podatka, vlasnik podatka obvezan je trajno procjenjivati stupanj tajnosti klasificiranog podatka i izraditi periodičnu procjenu, na temelju koje se može promijeniti stupanj tajnosti ili izvršiti deklasifikacija podatka.

Periodična procjena podataka sukladno članku 14. Zakona o tajnosti podataka provodi se:

– za stupanj tajnosti „VRLO TAJNO“ najmanje jednom u 5 godina,
– za stupanj tajnosti „TAJNO“ najmanje jednom u 4 godine,
– za stupanj tajnosti „POVJERLJIVO“ najmanje jednom u 3 godine,
– za stupanj tajnosti „OGRANIČENO“ najmanje jednom u 2 godine.

[22]Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 16.03.2020.

Način označavanja stupnjeva tajnosti klasificiranih podataka, propisan je uredbom koju donosi Vlada Republike Hrvatske.

Deklasifikacija podataka je postupak u kojem se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak bio označen odgovarajućim stupnjem tajnosti, nakon čega podatak postaje neklasificirani podatak s uporabom isključivo u službene svrhe.Vlasnik klasificiranog podatka dužan je obavijestiti i ostala nadležna tijela o postupku deklasifikacije podataka. Kada postoji javni interes, vlasnik klasificiranog podataka dužan je ocijeniti važnost između prava na pristup informacijama i zaštite tajnosti podatka.

3.3.2. Pristup klasificiranim podacima

Pristup klasificiranim podacima sukladno Zakonu o tajnosti podataka imaju isključivo osobe kojima je to nužno za obavljanje poslova iz njihova djelokruga, te koje imaju izdano Uvjerenje o obavljenoj sigurnosnoj provjeri.

Certifikat izdaje Ured Vijeća za nacionalnu sigurnost na temelju ocjene o nepostojanju sigurnosnih zapreka za pristup klasificiranim podacima.

3.3.3. Zaštita klasificiranih podataka

Zaštita i čuvanje klasificiranih podataka definirana je u članku 26. Zakona o tajnosti podataka kojim se „Dužnosnici i zaposlenici državnih tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravnih osoba s javnim ovlastima, kao i pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima, dužni su čuvati tajnost klasificiranog podatka za vrijeme i nakon prestanka obavljanja dužnosti ili službe, sve dok je podatak utvrđen jednim od stupnjeva tajnosti ili dok se odlukom vlasnika podatka ne oslobode obveze čuvanja tajnosti.[23]

[23]Zaštita klasificiranih podataka, Zakon o tajnosti podataka, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 17.03.2020.

4. ZAKONI I PROPISI KOJI REGULIRAJU ZAŠTITU PODATAKA

4.1. Zakon o zaštiti tajnosti podataka

Zakon o zaštiti tajnosti podataka (Narodne novine br. 108/96), stupio je na snagu 31. prosinca 1996. godine, a prestao važiti 6. kolovoza 2007. godine stupanjem na snagu Zakona o tajnosti podataka, osim odredaba glave 8. i 9. Koje definiraju područje poslovne i profesionalne tajne. Zakonom su definirani pojmovi i obveze čuvanja istih kao i situacije koje se ne smatraju povredom čuvanja poslovne tajne.Glava VIII. Zakona o zaštiti tajnosti podataka, u članku 20 navodi:

Pravna osoba dužna je čuvati kao tajnu i podatke:

1. koje je kao poslovnu tajnu saznala od drugih pravnih osoba,
2. koji se odnose na poslove što ih pravna osoba obavlja za potrebe oružanih snaga, redarstvenih vlasti Republike Hrvatske ili drugih javnih tijela, ako su zaštićeni odgovarajućim stupnjem tajnosti,
3. podatke koji sadrže ponude na natječaj ili dražbu – do objavljivanja rezultata natječaja odnosno dražbe,
4. podatke koji su zakonom, drugim propisom ili općim aktom doneseni na temelju zakona utvrđeni tajnim podacima od posebnog gospodarskog značenja.[24]

4.2. Zakon o tajnosti podataka

Zakon o tajnosti podataka na snazi je od 07. kolovoza 2007. godine (NN br. 79/07, NN br. 86/12).

Sukladno članku 1. Zakonom o tajnosti podataka utvrđuje se „*pojam klasificiranih i neklasificiranih podataka, stupnjevi tajnosti, postupak klasifikacije i deklasifikacije, pristup klasificiranim i neklasificiranim podacima, njihova zaštita i nadzor nad provedbom ovoga Zakona*“:[25]

[24]Zakon o zaštiti tajnosti podataka, NN 108/96, glava VIII, članak 20, raspoloživo na https://www.zakon.hr/z/748/Zakon-o-za%C5%A1titi-tajnosti-podataka – datum pristupa sadržaju 15.04.2020.

[25]Zakon o tajnosti podataka, I. Osnovne odredbe, članak 1, raspoloživo na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka – datum pristupa sadržaju 20.03.2020.

Uredba o načinu označavanja klasificiranih podataka, sadržaju i izgledu uvjerenja o obavljenoj sigurnosnoj provjeri i izjave o postupanju s klasificiranim podacima objavljena u (Narodnim novinama br.102/07).

4.3. Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti (Narodne novine br. 79/07) primjenjuje se u Republici Hrvatskoj kao temeljni zakon koji regulira područje informacijske sigurnosti,te kao dopuna istog zakona Uredba o mjerama informacijske sigurnosti (Narodne novine br. 46/08).

Zakon o informacijskoj sigurnosti u osnovnim odredbama definira pojam informacijske sigurnosti, mjere i standarde informacijske sigurnosti, područja informacijske sigurnosti, središnja državna tijela za provođenje informacijske sigurnosti kao i pravne i fizičke osobe na koja se odnosi, a to su:

1. državna tijela
2. tijela jedinica lokalne i područne (regionalne) samouprave
3. pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke
4. pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.[26]

Središnja državna tijela za informacijsku sigurnost su:

- Ured Vijeća za nacionalnu sigurnost
- Zavod za sigurnost informacijskih sustava
- Nacionalni CERT (engl. *CERT — Computer Emergency Response Team)*

Tehnička su područja sigurnosti informacijskih sustava:[27]

- standardi sigurnosti informacijskih sustava,
- sigurnosne akreditacije informacijskih sustava,

[26]Zakon o informacijskoj sigurnosti, I. Osnovne odredbe, članak 1., raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 17.03.2020.
[27]Zakon o informacijskoj sigurnosti, NN (79/07)

- upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka,
- koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.[28]

4.4. Kazneni zakon RH

Glava I – članak 1, temeljne odredbe, Kaznenog zakona Republike Hrvatske (Narodne novine br. 101/17) definira temelj ovog zakona, odnosno tko i pod kojim uvjetima smije biti kažnjen, te sankcije koje su propisane za određena kaznena djela.

(1) Kaznena djela i kaznenopravne sankcije propisuju se samo za ona ponašanja kojima se ugrožavaju ili povrjeđuju osobne slobode i prava čovjeka te druga prava i društvene vrijednosti zajamčene i zaštićene Ustavom Republike Hrvatske i međunarodnim pravom da se njihova zaštita ne bi mogla ostvariti bez kaznenopravne prisile.[29]

U Glavi dvadeset četvrtoj (XXIV), Kaznenog zakona RH, definirana su kaznena djela protiv gospodarstva, dok je člankom 259. (NN br. 101/17) definirana zlouporaba povlaštenih informacija.

(1) Tko raspolažući povlaštenom informacijom:

2. za vlastiti ili tuđi račun neposredno ili posredno stekne ili otuđi financijski instrument na koji se ta informacija odnosi,
3. neovlašteno otkrije, priopći, preda ili na drugi način učini dostupnom povlaštenu informaciju drugoj osobi,
4. preporuči drugoj osobi ili je navede da stekne ili otuđi financijski instrument na koji se ta informacija odnosi,

- kaznit će se kaznom zatvora do tri godine.

(2) Ako je kazneno djelo iz stavka 1. ovoga članka počinila osoba koja je raspolagala povlaštenom informacijom na temelju članstva u upravljačkim ili nadzornim tijelima

[28]Ivandid Vidovid D., Karlovid L., Ostojid A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 208.
[29]Kazneni zakon RH, temeljne odredbe, glava I, članak 1,raspoloživo na https://www.zakon.hr/z/98/Kazneni-zakon – datum pristupa sadržaju 24.04.2020.

izdavatelja, svojeg udjela u kapitalu izdavatelja, pristupa informaciji kroz obavljanje svog posla ili dužnosti ili počinjenog kaznenog djela,

- kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(3) Ako je kaznenim djelom iz stavka 1. ovoga članka pribavljena znatna imovinska korist ili je drugome prouzročena znatna šteta,

- počinitelj će se kazniti kaznom zatvora od šest mjeseci do pet godina.

(4) Ako je kaznenim djelom iz stavka 2. ovoga članka pribavljena znatna imovinska korist ili je drugome prouzročena znatna šteta,

- počinitelj će se kazniti kaznom zatvora od jedne do osam godina.

Odavanje tajnih podataka – članak 347 Kaznenog zakona Republike Hrvatske[30]definirao je sljedeće:

(1)Tko tajne podatke koji su mu povjereni učini dostupnim neovlaštenoj osobi,

- kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2)Tko pribavi tajni podatak s ciljem da ga on ili druga osoba neovlašteno upotrijebi, ili tko drugome učini dostupnim takav podatak u čiji je posjed došao slučajno,

- kaznit će se kaznom zatvora do tri godine.

(3)Tko djelo iz stavka 1. i 2. ovoga članka počini iz koristoljublja,

- kaznit će se kaznom zatvora od jedne do deset godina.

(4)Tko kazneno djelo iz stavka 1. i 2. ovoga člana počini za vrijeme ratnog stanja ili neposredne ratne opasnosti,

- kaznit će se kaznom zatvora od tri do dvanaest godina.

(5)Tko kazneno djelo iz stavka 1. ovoga članka počini iz nehaja

- kaznit će se kaznom zatvora do tri godine

[30] Odavanje tajnih podataka, Kazneni zakon RH – Zakon.hr, raspoloživo na https://www.zakon.hr/z/98/Kazneni-zakon– datum pristupa sadržaju 17.03.2020.

5. ULOGA I ZNAČAJ INFORMACIJSKE SIGURNOSTI U ZAŠTITI PODATAKA

5.1. Sigurnost

Sigurnost se može definirati kao proces održavanja prihvatljivog nivoa rizika, odnosno sigurnost predstavlja određeni stupanj zaštite od opasnosti, štete, gubitka ili pak kriminalne aktivnosti. Kada je riječ o zaštiti informacijskih sustava i sigurnosti tada postoji nekoliko osnovnih pravila[31]:

- apsolutna sigurnost ne postoji
- uz različite tehničke zaštite potrebno je razmotriti i ljudski faktor sa svim svojim slabostima
- sigurnost je proces, skup usluga, proizvoda ili procedura, te raznih drugih elemenata i mjera koje se konstantno provode

5.1.1. Sigurnost informacijskih sustava

Sigurnost informacijskih sustava predstavlja skup metoda i načina kojima se informacije i informacijski sustavi štite od neovlaštenog pristupa, uporabe, otkrivanja, prekida rada, promjena ili uništenja.[32]

Postoje tri temeljna parametra informacijske sigurnosti:

1. Povjerljivost (engl. confidentiality) – siguran pristup informaciji i informacijskome sustavu isključivo za to ovlaštenoj osobi.
2. Integritet (engl. integrity) – zaštita ispravnosti i cjelovitosti podataka i informacija.
3. Raspoloživost (engl. availability) –ovlaštenoj osobi omogućiti pravodoban i stalan pristup informacijama i informacijskome sustavu.

[31]Pravila sigurnost informacijskih sustava,raspoloživo na http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustava_a_0.pdf – datum pristupa sadržaju 10.02.2020.
[32]Pejić Bach, M. i dr., (2016.),*Informacijski sustavi u poslovanju*, Sveučilište u Zagrebu, Zagreb str 245.

Slika 4: Osnovni sigurnosni trokut

(vlastita izrada)

Sigurnost informacijskih sustava bitna je tema kojoj organizacije diljem svijeta pridaju mnogo pažnje, za što postoji dobar razlog. Upad u informacijske sustave i podatkovne mreže jedan je od najučinkovitijih načina prikupljanja velike količine informacija.

Sigurnosne prijetnje dolaze iz više izvora poput računalnog kriminala, špijunaže, sabotaža i prirodnih nepogoda. Šteta nanesena od strane računalnog kriminala sve je veća, što pokazuju financijski pokazatelji, pa je nužno da provodimo sljedeće radnje kako bismo smanjili rizike od upada:

- definiranje,
- planiranje,
- projektiranje,
- implementiranje,
- održavanje,
- kontinuirano poboljšavanje informacijske sigurnost.

5.2. Pojam informacijska sigurnost

Tijela državne uprave raspolažu s podatcima visokog stupnja tajnosti političkog, vojnog, gospodarskog i drugog karaktera koji mogu biti predmet interesa nekih stranih obavještajnih službi, stranih gospodarskih subjekata, ali i organiziranih kriminalnih i terorističkih skupina.

Sukladno članku 2 Zakona o informacijskoj sigurnosti, pojam informacijske sigurnosti definira se:[33]

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

Osim zakonom, informacijska sigurnost definirana je i ISO 27001 standardom: [34]

„*Informacijska sigurnost podrazumijeva očuvanje povjerljivosti, integriteta i dostupnosti informacije; uključiti se mogu i druge osobine kao što su vjerodostojnost, odgovornost, neporecivost i pouzdanost.“*

Ured Vijeća za nacionalnu sigurnost kao središnje državno tijelo odgovoran je za utvrđivanje i provedbu mjera i standarda informacijske sigurnosti.Razvojem tehnologije sve se više podataka važnih za nacionalnu sigurnost pohranjuje u informacijskim sustavima tijela državne uprave ili se razmjenjuju informacijsko-komunikacijskim kanalima.

Sigurnosno-obavještajna agencija i Vojno-sigurnosno obavještajna agencija zadužene su za otkrivanje i sprječavanje neovlaštenog ulaska u zaštićene informacijske i komunikacijske sustave državnih tijela te odavanje klasificiranih podataka.

Elektronički napadi i ugrožavanja informacijske sigurnosti sve su složeniji te je u odgovoru na njih potrebno stalno učenje, praćenje trendova i inovativnost u rješenjima.[35]

---

[33]Informacijska sigurnost, Zakon o informacijskoj sigurnosti, NN 79/07 – raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 15.03.2020.
[34]Kostanjevec A. i dr.. *Sigurnost informacijskih sustava*, verzija 01012014, FOI Varaždin 2014. str.2.
[35]SOA sigurnosno-obavještajna agnecija, raspoloživo na https://www.soa.hr/hr/podrucjarada/informacijska-sigurnost/ – datum pristupa sadržaju 27.06.2020.

5.2.1. Područja informacijske sigurnosti

U Zakonu o informacijskoj sigurnosti, definirana su područja informacijske sigurnosti, a člankom 8. istog zakona definirana su područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti kroz pet područja:[36]

1. sigurnosnu provjeru,
2. fizičku sigurnost,
3. sigurnost podatka,
4. sigurnost informacijskog sustava,
5. sigurnost poslovne suradnje.

Sigurnosna je provjera područje informacijske sigurnosti koje definira mjere i standarde informacijske sigurnosti koje se primjenjuju na osobe koje imaju pristup klasificiranim podacima. Kako bi osobe imale pristup klasificiranim podacima, moraju imati certifikat, odnosno uvjerenje o obavljenoj sigurnosnoj provjeri kojom se utvrđuje nepostojanje sigurnosnih rizika i zapreka za rad s klasificiranim podacima, dok su tijela ili pak pravne osobe dužne ustrojiti; popis osoba koje imaju pristup klasificiranim podacima, te registar zaprimljenih certifikata s rokovima trajanja certifikata.

Fizička je sigurnost područje informacijske sigurnosti koje utvrđuju mjere i standarde informacijske sigurnosti koji se odnose na zaštitu objekta, prostora i uređaja u kojem se obrađuju klasificirani podaci. Svaki prostor mora se podijeliti na administrativne i sigurnosne zone kako bi se klasificirani podaci štitili od krađe ili neovlaštenog pristupa.

Sigurnost podataka je područje informacijske sigurnosti u kojem se definiraju opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka. Tijela koja koriste klasificirane podatke moraju primijeniti procedure o postupanju s klasificiranim i neklasificiranim podacima, o sadržaju i načinu vođenja evidencije o izvršenim uvidima u klasificirane podatke te nadzoru sigurnosti podataka, propisanim mjerama i standardima informacijske sigurnosti.

[36]Područja informacijske sigurnosti, raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 20.07.2020.

Sigurnost informacijskog sustava područje je informacijske sigurnosti koje definira mjere i standarde informacijske sigurnosti za informacijske sustave u kojima se obrađuju, pohranjuju ili prenose klasificirani podaci.

Sigurnost poslovne suradnje područje je informacije sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom.Pravne i fizičke osobe koje pristupaju provedbi natječaja ili ugovora, obvezne su ishoditi uvjerenje o sigurnosnoj provjeri pravne osobe (certifikat poslovne sigurnosti).

5.3. Mjere informacijske sigurnosti

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji potrebni za zaštitu klasificiranih i neklasificiranih podataka. Zakon o informacijskoj sigurnosti primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima koje u svom djelokrugu koriste klasificirane i neklasificirane podatke, kao i na sve pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima

U Zakonu o informacijskoj sigurnosti (Narodne Novine br. 79/09), definirane su mjere i standardi:[37]

„Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.“

„Standardi informacijske sigurnosti su organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj provedbi propisanih mjera informacijske sigurnosti.“

Također, Zakon o informacijskoj sigurnosti, opisuje radnje koje treba poduzimati, te definira[38]mjere i standarde informacijske sigurnosti koje obuhvaćaju:

- nadzor pristupa i postupanja s klasificiranim podacima,

[37]Mjere i standardi informacijske sigurnosti – raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 27.03.2020.
[38]Mjere i standardi informacijske sigurnosti – raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 27.03.2020.

- postupanje prilikom neovlaštenog otkrivanja i gubitka klasificiranih podataka,
- planiranje mjera prilikom izvanrednih situacija,
- ustrojavanje posebnih fondova podataka za podatke klasificirane u Republici Hrvatskoj, te za klasificirane podatke koje je predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje.

5.4. Kibernetička i računalna sigurnost

Računalna sigurnost je skup mjera i postupaka kojima se osiguravaju podatci pohranjeni u računalima, često dostupni i preko računalne mreže prema definiciji Hrvatske enciklopedije.

Upad u informacijske sustave i podatkovne mreže jedan je od najučinkovitijih načina prikupljanja velike količine informacija. Ujedno, ovaj je način među sigurnijima za „napadače". On se može obavljati iz velike udaljenosti, prikriven brojnim slojevima zaštite prave lokacije, identiteta i namjera „napadača".[39]Zbog navedenih razloga, kao dio ofenzivnog obavještajnog rada, pojedine države prikupljaju podatke o drugim državama provaljivanjem u njihove zaštićene informacijske i komunikacijske sustave kako bi dobile što više podataka o procesima donošenja odluka u tim državama.

U prevenciji i suzbijanju kibernetičkih prijetnji središnja državna tijela za informacijsku sigurnost surađuju s nacionalnim tijelima i međunarodnim partnerima te sudjeluju u radu Nacionalnog vijeća za kibernetičku sigurnost i Operativno-tehničke koordinacije za kibernetičku sigurnost čija je zadaća pratiti stanje sigurnosti nacionalnog kibernetičkog prostora i predlagati postupanja u slučaju kibernetičkih kriza.
Svaka organizacija raspolaže velikom količinom informacija koje se često pohranjuju samo na računalima, pa gubitak ili krađa mogu prouzročiti veliku financijsku i reputacijsku štetu. Kako ne bi došlo do gubitaka podataka zbog grešaka na računalu ili tehničkih oštećenja, nužno je izraditi sigurnosne kopije (engl. *backup).* Podaci koji se nalaze na sigurnosnim kopijama moraju se fizički držati odvojeno od izvornih podataka, kako bi se, u slučaju gubitka, mogli nadomjestiti nestali podaci.

[39]Raspoloživo na https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/ – datum pristupa sadržaju 28.03.2020.

Sigurnost podataka od neovlaštena proboja i krađe postiže se autentifikacijom i kriptiranjem, što podrazumijeva prevođenje informacija u kodirani oblik razumljiv samo onima koji posjeduju ključ za njegovo dekodiranje. Kao primjer takvog oblika zaštite podataka možemo navesti primjer iz financijskog sektora; Internet-bankarstvo – bankarsko poslovanje, kod kojega,da bismo pristupili bazi podataka, moramo pristupiti s određenog računala, te određenim zaštitnim PIN-om (engl. *Personal Identification Number),* ponekad i s dvama potpisnicima te dvama zasebnim PIN-ovima. Isto tako možemo navesti primjer poslovanja preko različitih poslovnih baza podataka za koje nam je također potrebna posebna autorizacija; kao što su e-porezna, e-fina, e-mirovinsko i slične aplikacije.

5.5. Norma ISO 27001 – sustav upravljanja informacijskom sigurnošću

Ubrzanim razvojem informacijske tehnologije, digitalnog poslovanja i obradom velike količine podataka umnažaju se i rizici, te ugroze u digitalnom poslovanju što iziskuje kontinuirano planiranje organizacije informacijske sigurnosti u cjelini – kroz sva tri segmenta: povjerljivost, integritet i dostupnost podataka u privatnom, javnom i državnom sektoru. Tajnost podataka predstavlja tek jednu od potkategorija povjerljivosti podataka.

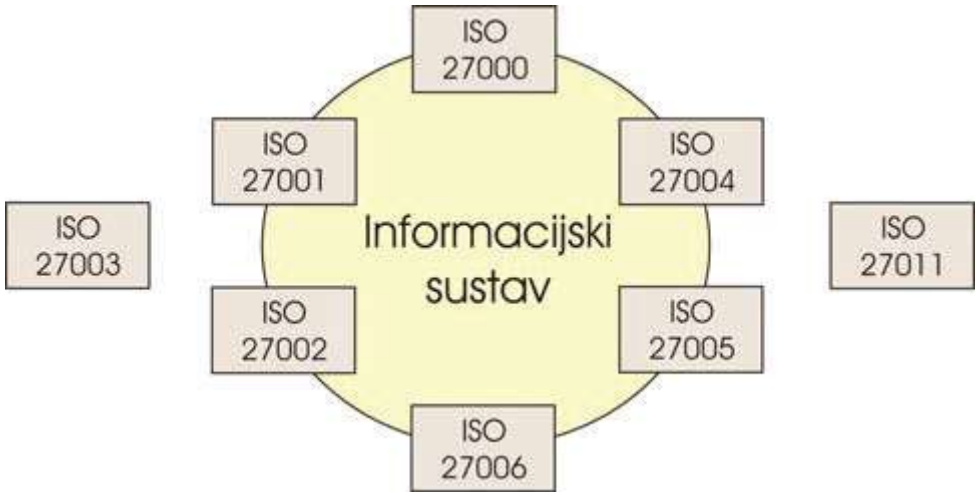
Podaci i informacije ključni su resurs u svakoj organizaciji, pa razvojem informacijske tehnologije i korištenjem podataka i informacija u digitalnom poslovanju, pred svaku organizaciju postavlja se pitanje kako organizirati sustav informacijske sigurnosti koji će jamčiti zaštitu podataka i informacija od krađe i neovlaštenog korištenja. Primjena ISO standarda postala je nužnost u razvoju informacijskih sustava svake organizacije.

Prvi standard razvijen je u Velikoj Britaniji – standard BS 7799, pod nazivom *"Industry Code of Practice"*, 1995. godine. Iz standarda BS 7799 proizašle su ISO/IEC 17799 norme, odnosno ISO/IEC 27001 te ISO/IEC 27002 koje su usvojene kao međunarodne norme, a Republika Hrvatska kao članica Međunarodne organizacije za standarde sa sjedištem u Ženevi, u Švicarskoj, prihvatila je standarde i primjenjuje ih u propisanom formatu. Važno je napomenuti da se sustav normi ne odnosi samo na informacijski sektor, već se njegova primjena danas provodi u svim granama industrije. Isto tako norma ISO 27001 – sustav upravljanja informatičkom sigurnošću nije obvezan, organizacije ga uvode dobrovoljno, no certifikat koji organizacije dobivaju uvođenjem norme, poslovnim partnerima daje dodatna

jamstva, te pruža dodatnu sigurnost u pogledu kvalitete proizvoda. Certifikat ISO 27001 izdaje neovisna međunarodna organizacija ISO (engl. International Organization for Standardization) ili drugo neovisno certifikacijsko tijelo koje je ovlašteno za obavljanje takvih usluga u državama članicama.

ISO (*engl. International Organization for Standardization*) i IEC (*engl. International Electrotechnical Commission*), zajedno čine sustav za međunarodnu standardizaciju. Organizacija ISO objavila je veći broj normi vezanih uz zaštitu i sigurnost informacijskog sustava:[40]

- ISO 27000 – Pregled normi iz ISO 27k serije;
- ISO 27001 – (2006) Sustav upravljanja informatičkom sigurnošću (ISMS);
- ISO 27002 – (2007) Kodeks postupaka za upravljanje sustavom informacijske sigurnosti;
- ISO 27003 – Vodič za uvođenje sustava informacijske sigurnosti;
- ISO 27004 – Mjerenje i metrika efikasnosti sustava informacijske sigurnosti;
- ISO 27005 – Upravljanje rizicima informacijske sigurnosti;
- ISO 27006 – Zahtjevi za postupkom analize i certificiranja standarda;
- ISO 27011 – Upute za uspostavu sustava informacijske sigurnosti u telekomunikacijskom sektoru



Slika 5: Norme informacijske sigurnosti

[40]Norme informacijske sigurnosti ISO/IEC 27K, – pregled normi iz ISO 27K serije – raspoloživo na https://hrcak.srce.hr/file/113574 – datum pristupa sadržaju 15.06.2020.

Izvor: *Norme informacijske sigurnosti ISO/IEC 27K*, Javor Bogadi, univ.spec.oec., *Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica*

Od navedenih normi za upravljanje sigurnošću informacijskih sustava najveću važnost imaju ISO/IEC 27001 i ISO/IEC 27002.Norma IS0 27001 predstavlja međunarodno priznatu normu koja cilja zaštititi informacijski sustav neke organizacije.Predstavlja smjernice i specifikacije za razvoj upravljanja informacijskom sigurnošću ISMS – (engl. *Information Security Management System*).

Primjena ovih normi osigurava usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom(od zaposlenika do informacijskog sustava) kao i povećanje pouzdanosti sustava u slučaju katastrofe te pridonosi povećanju svijesti o nužnosti obuke i osvješćivanja djelatnika vezanim uz informacijsku sigurnost.

Sustav možemo promatrati kao dva bloka i to:

- sustav za upravljanje sigurnošću koji obuhvaća dokumentiranje, pregled, ispitivanje, odgovornost uprava, korektivne i preventivne mjere te stalno poboljšanje sustava
- upravljanje informacijskom sigurnošću koji je ciklus uspostave, implementacije, rukovanja, pregledavanja, ispitivanja i poboljšanja sustava za upravljanje informacijskom sigurnošću (ISMS), a koji je opisan modelom PDCA (*engl.Plan-Do-Check-Act*). Navedeni model predstavlja osnovu za pregled norme BS 7799-2.

Slika 6.: Shema PDCA ciklusa

Izvor: *Norme informacijske sigurnosti ISO/IEC 27K*, Javor Bogadi, univ.spec.oec., *Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica*

Plan-Do-Check-Act ciklus nikada ne završava, nego se njegove aktivnosti ponavljanju kako bi se osigurala ažurnost upravljanja sigurnošću informacijskog sustava.
Faze PDCA ciklusa su:

- PLAN – Uspostava sustava za upravljanje informacijskom sigurnošću;
- DO – Upravljanje sustavom informacijske sigurnosti;
- CHECK – Nadzor i ispitivanje sustava informacijske sigurnosti;
- ACT – Poboljšanje sustava informacijske sigurnosti

Norma ISO/IEC 27001 usvojena je kao hrvatska norma HRN ISO/IEC 27001:2006 pod nazivom "Sustavi upravljanja informacijskom sigurnošću – Zahtjevi", a norma ISO/IEC

27002 usvojena je kao hrvatska norma HRN ISO/IEC 17799:2006 pod nazivom "Kodeks postupaka za upravljanje informacijskom sigurnošću".[41]

Uvođenje norme ISO 27001 koja se sastoji od 11 područja, 39 kontrolnih ciljeva i ukupno 133 kontrole koje pomažu u identifikaciji, upravljanju i smanjenju cijelog niza prijetnji kojima su informacije svakodnevno izložene [42] pomaže organizaciji pri osiguranju zaštite svoga informacijskog sustava. Primjenom norme osigurava se usklađenost aktivnosti unutar organizacije s važećom zakonskom regulativom, kao i povećanje pouzdanosti sustava u slučaju katastrofe. Velika je pozornost posvećena obuci i osvješćivanju djelatnika.

5.5.1. Institucije zadužene za informacija sigurnost

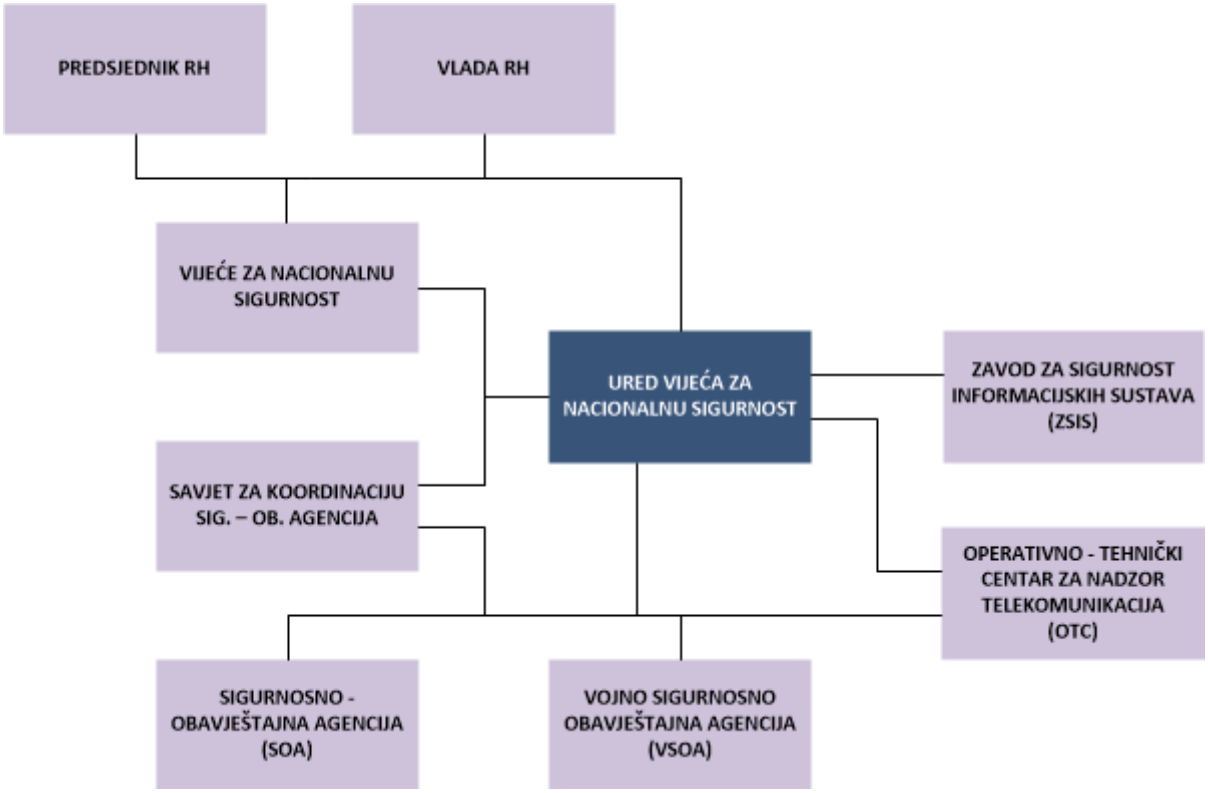
U cilju zaštite klasificiranih informacija i definiranja nadležnosti iz područja informacijske sigurnosti Zakon o informacijskoj sigurnosti (NN br. 79/07) obuhvatio je sljedeća državna tijela:

1. Ured Vijeća za nacionalnu sigurnost
2. Zavod za sigurnost informacijskih sustava
3. Nacionalni CERT (engl.*CERT — Computer Emergency Response Team)*

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost, koje koordinira i trajno usklađuje donošenje i primjenu mjera i standarda informacijske sigurnosti u Republici Hrvatskoj, te u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske te stranih zemalja i organizacija.[43]Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost – hrvatski NSA (engl. National Security Authority).

[41]*Norme informacijske sigurnosti ISO/IEC 27K*, Javor Bogadi, univ.spec.oec.,*Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica – raspoloživo na* https://hrcak.srce.hr/file/113574 – datum pristupa sadržaju 31.03.2020.
[42]*Norme informacijske sigurnosti ISO/IEC 27K*, Javor Bogadi, univ.spec.oec.,*Ministarstvo obrane Republike Hrvatske, Odsjek za poslove obrane Virovitica raspoloživo na* https://hrcak.srce.hr/file/113574 – datum pristupa sadržaju31.03.2020.
[43]Ivandid Vidovid D., Karlovid L.,Ostojid A (2011.),Korporativna sigurnost, Zagreb,UHMS,str 207–208.

Zavod za sigurnost informacijskih sustava(ZSIS) središnje je državno tijelo za tehnička područja sigurnosti informacijskog sustava u državnim i ostalim tijelima koja u svom djelokrugu koriste klasificirane i neklasificirane podatke.[44]



Shema: UVNS u sigurnosno-obavještajnom sustavu RH[45]

Izvor: Republika Hrvatska – Ured vijeća za nacionalnu sigurnost – preuzeto na https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh

[44]Ivandid Vidovid D., Karlovid L.,Ostojid A (2011.), Korporativna sigurnost, Zagreb,UHMS,str. 208.
[45]Ured vijeća za nacionalnu sigurnost – raspoloživo na https://www.uvns.hr/hr/o-nama/shema-uvns-u-sigurnosno-obavjestajnom-sustavu-rh – datum pristupa sadržaju 15.06.2020.

Tehnička područja sigurnosti informacijskih sustava su:[46]

- standardi sigurnosti informacijskih sustava,
- sigurnosne akreditacije informacijskih sustava,
- upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka,
- koordinacija prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

CERT(engl. CERT — Computer Emergency Response Team) nacionalno je tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacija u Republici Hrvatskoj.[47]

Pema Zakonu o informacijskoj sigurnosti u glavi V, članak 20, nacionalni CERT definiran je:[48]

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu: CARNet).

(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.

(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

[46]Zakon o informacijskoj sigurnosti, NN (79/07)
[47]Ivandid Vidovid D., Karlovid L., Ostojid A. (2011.), Korporativna sigurnost, Zagreb, UHMS, str. 208.
[48]Nacionalni CERT - Zakon o informacijskoj sigurnosti, NN (79/07) – raspoloživo na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti – datum pristupa sadržaju 24.04.2020.

6. ŠPIJUNAŽA

6.1. Osnovni pojmovi

Od najdavnijih vremena čovjek je iskazivao interes za druge ljude, skupine, organizacije i države. Razvojem društva i stvaranjem prvih država te ustrojem državnog aparata uočila se potreba za sustavnim i organiziranim prikupljanjem podataka o drugima.

Riječ špijunaža potječe od (njem. *Spionage*< franc. *espionnage*) te označava potajno prikupljanje važnih vojnih, političkih ili gospodarskih podataka.

U pravu, „*….kazneno djelo protiv države koje se sastoji u odavanju podataka stranoj državi ili međunarodnoj organizaciji koji su državna tajna, ili u osnivanju tajne obavještajne službe u korist druge države.*“[49]

U hrvatskom kaznenom zakonodavstvu špijunaža je kazneno djelo protiv Republike Hrvatske, a čini ga onaj tko[50]:

a) državnu tajnu koja mu je povjerena ili do koje je došao na protupravan način učini dostupnom stranoj državi, stranoj organizaciji ili osobi koja za njih radi;
b) prikuplja podatke, predmete, isprave ili saznanja koja su državna tajna kako bi ih učinio dostupnima stranoj državi ili organizaciji;
c) za stranu državu ili organizaciju organizira tajnu obavještajnu službu na području RH, stupi u stranu obavještajnu službu ili joj pomaže u radu.

Objekt špijunaže je državna tajna, to je podatak koji je zakonom, drugim propisom ili općim aktom nadležnoga tijela donesenim na temelju zakona određen državnom tajnom i otkrivanjem kojega bi nastupile štetne posljedice za nacionalnu sigurnost ili nacionalni interes RH. Špijunaža je kazneno djelo slično kaznenomu djelu odavanja državne tajne, od kojega se razlikuje elementom inozemnosti (veza sa stranom državom). Budući da se špijunaža u većini država smatra političkim kaznenim djelom, zahtjev za izručenjem špijuna može biti odbijen ili izručenje može biti podvrgnuto ograničenjima. Špijunažu kao tipično protudržavno kazneno

[49] Špijunaža, *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2020. raspoloživo na http://www.enciklopedija.hr/Natuknica.aspx?ID=59838> – datum pristupa sadržaju 17.06.2020.
[50] Špijunaža, Kazneni zakon RH, raspoloživo na https://www.zakon.hr/z/98/Kazneni-zakon – datum pristupa sadržaju 22.06.2020.

djelo treba razlikovati od tzv. industrijske špijunaže, kod koje se povrjeđuje intelektualno vlasništvo.[51]

Špijunaža kao pojam označava obavještajne djelatnosti koje se sastoje od davanja ili saopćavanja drugoj osobi (ili ratnoj strani, državi ili organizaciji) sakupljene podatke ili činjenice što predstavljaju tajnu (vojnu, službenu, ekonomsku, industrijsku…). Međunarodno pravo regulira špijunažu isključivo u oblasti ratnog prava dok špijunaža u mirnodopskim uvjetima spada pod kazneno pravo pojedine države.[52]

Negativna strana poslovnog obavještavanja krije se u gospodarskoj špijunaži koja predstavlja slučajeve kada države svjesno kršeći međunarodno pravo, kršeći skup pravnih (običajnih i ugovornih) pravila štite svoje poslovne subjekte u globalnoj ekonomiji.

Primjer industrijske špijunaže:

Formula 1, milijunski je sportski biznis. Naime, 2007. godine McLaren kažnjen je sa 100 milijuna dolara uz oduzimanje svih tzv. konstruktorskih bodova za 2007. godine. To se dogodilo nakon što je Međunarodni automobilistički savez (FIA) utvrdio kako su ilegalno došli u posjed tajne tehničke dokumentacije Ferrarija. Ubrzo se otkrilo da je u razdoblju od rujna 2006. godine do listopada 2007. godine Renault neovlašteno došao do McLarenovih poslovnih tajna, uključujući informacije koje se odnose na: dizajn, inovacije, 96 testove, istraživanje i razvoj (R&D) te strategiju za utrke McLarenovih bolida za 2007. godinu.[53]

[51] Špijunaža, *Hrvatska enciklopedija, mrežno izdanje.* Leksikografski zavod Miroslav Krleža, 2020. raspoloživo na http://www.enciklopedija.hr/Natuknica.aspx?ID=59838>. – datum pristupa sadržaju 17.06.2020.

[52] Špijunaža, raspoloživonahttps://hr.wikipedia.org/wiki/%C5%A0pijuna%C5%BEa – datum pristupa sadržaju 24.02.2020.

[53] Schofield, H. (2011.) Renault spy scandal risks denting carmaker's reputation, BBC News, Paris, dostupno na linku http://www.bbc.co.uk/news/world-europe-12732421, Rechtin, M. (2013.) Renault spy scandal: Former COO 'had to leave', Automotive News, raspoloživo na http://www.autoweek.com/article/20130430/CARNEWS/130439995, Mihovilović, M. (2007.) Ucjenjivač Alonso upropastio McLaren, Nacional br. 618, dostupno na http://www.nacional.hr/clanak/37955/ucjenjivac-alonso-upropastio-mclaren, Collantine, K. (2007.) Stories of the season: Hamilton versus Alonso, F1fanatic, dostupno na http://www.f1fanatic.co.uk/2007/10/30/f1-07-review-hamilton-vs-alonso/ – datum pristupa sadržaju 16.03.2020.

6.2. Povijesni pregled

Špijunaža je raširena po cijelom svijetu, a prvi tragovi dopiru još u antičko doba. Adrienne Wilmoth Lerner[54] u svom radu spominje da je u egipatskim hijeroglifima otkrivena prisutnost sudskih špijuna te su na papirusima opisane operacije trgovine robljem. Egipatski špijuni koji su radili za faraona, također su imali zadaću istraživati političku situaciju te strategije Rima i Grčke te su bili prvi koji su koristili biljne i zmijske otrove kako bi sabotirali svoje protivnike. Grci su, za razliku od egipatskih špijuna, bili poznati po prevarama kojima su se koristili kako bi ostvarili napade na svoje protivnike

Špijuniranje je zabilježeno još 1500. godine prije nove ere kada je Mojsije odabrao 12 špijuna i poslao ih u drugu zemlju da razgledaju zemlju, narod, gradove te procijene plodnost zemlje – prema knjizi Brojeva. To se ujedno smatra i prvim spomenom obavještajne službe kao organizacije i kao djelatnosti (Žunec i Domišljanović, 2000: 11).

Gospodarska špijunaža prisutna je još od najstarijih civilizacija, ali u vrlo jednostavnom obliku. Poznat je primjer starog Egipta,u kojemu su pojedini svećenici odlazili u strane zemlje sa zadaćom prikupljanja podataka o gospodarskoj snazi tih zemalja.

Prvi trag špijunaže u Europi pojavljuje se u Dubrovačkoj Republici 1301. godine u kojoj se pojavljuju centri za prikupljanje, sortiranje, obradu i korištenje informacija o „neprijateljima“. 12. kolovoza 1301. godine Senat je formirao tri centra i to:

1. Centar za fortifikacije i sigurnost
2. Centar za naoružanje
3. Centar za obavještajnu službu, odnosno Centar za sakupljanje vijesti i informacija

Ubrzo je Republika imala 1400 agenata koji su u trećim državama prikupljali političke, vojne i gospodarske informacije.[55]
Dolaskom Hitlera na vlast i stvaranjem nacističke Njemačke započinje veliki uspon ratne i industrijske špijunaže, u kojima se primjenjuje načelo „totalne špijunaže“ koje glasi:

[54] Izvor: Lerner,raspoloživo na http://www.fags.org.espionage/Ep-Fo/Espionage-and-Intelligence-Early- Historical-Foundations.html – datum pristupa sadržaju 02.02.2020.
[55]Dedijer, S., Ragusa Intelligence and Security (1301-1806) : A model for the Twenty-First Century?, International Journal of Intelligence and Counterintelligence, Vol XV, No. 1, Spring 2002, p 57.

„*Nema podataka koji nije važan, nema mjesta koje nije interesantno i za špijuna su sposobni svi; djeca, odrasli, vojnici, seljaci, intelektualci.“*

Winston Churchill je 1919. godine osnovao Obavještajni centar za proučavanje industrije u trećim zemljama, u kojima su se nalazili najveći konkurenti. Tu praksu postepeno uvode i druge države, ponajprije Japan pa i ostali kako bi stekli prednost pred svojom konkurencijom.

Stevan Dedijer, poznat kao jedan od utemeljitelja „poslovnog obavještavanja“, u članku objavljenom 1973. godine[56], istaknuo je sve veći značaj prikupljanja podataka poslovne prirode i promijene interesa obavještajnog djelovanja od vojnog k području gospodarske prirode. U vojnu i političku dimenziju obavještajne službe treba uključiti i ekonomski aspekt.Tvrdio je da će gospodarska špijunaža biti tema 21. stoljeća, a napredovat će samo one države čije elite to na vrijeme shvate.

6.3. Međunarodni dokumenti koji definiraju pojam špijunaže

Prikupljanje informacija, što podrazumijeva i prikupljanje informacija gospodarske prirode odnosno poslovnih informacija, jedna je od temeljnih funkcija diplomatske misije koja je regulirana Bečkom konvencijom o diplomatskim odnosima[57] i Bečkom konvencijom o konzularnim odnosima[58].

U Bečkoj konvenciji o diplomatskim odnosima navodi se:

„*….prikupljanje informacija svim dozvoljenim sredstvima o razvoju događaja u državi primateljici i izvješćivanje o tomu vlade države-šiljateljice*“, dok se u Bečkoj konvenciji o konzularnim odnosima preciznije govori upravo o prikupljanju poslovnih informacija:

„ ….prikupljanje informacija svim dozvoljenim sredstvima u svezi s razvojem tržišnog, gospodarskog, konzularnog i znanstvenog života države primateljice i izvješćivanje o tomu vlade države šiljateljice i davanje informacija onima koje to zanima, prvenstveno gospodarskim subjektima.“

[56]Dedijer (1973.), Intelligence policy
[57]Bečka konvencija o diplomatskim odnosima od 18.04.1961. godine (Konvencija je stupila na snagu 24. travnja 1964.), CDR, UNTS, vol.500, str. 75
[58]Bečka konvencija o konzularnim odnosima, CCR, UNTS, vol. 596, str. 261.

6.4. Vrste špijunaža

Prema međunarodnom pravu, špijuni su tajni agenti jedne države ili međunarodne organizacije poslani u inozemstvo s ciljem prikupljanja tajnih informacija.
Sve države „*…stalno ili povremeno šalju špijune u inozemstvo i mada se to ne smatra pogrešno, moralno, politički ili pravno, takvi agenti nemaju priznat status prema međunarodnom pravu jer oni ne predstavljaju agente za održavanje njihovih međusobnih odnosa".*[59]

1. Politička špijunaža – predstavlja interes stranih obavještajnih službi za rad državnih organizacija i njihovih aktivnosti u području vođenja unutarnje i vanjske politike. Posebna pažnja posvećuje se predstavnicima vlade, ministrima i drugim osobama na visokim pozicijama.
2. Vojna špijunaža – predstavlja prikupljanje podataka o oružanim snagama postojećih ili eventualnih protivnika, kao i o oružanim snagama drugih zemalja bilo u cilju svoje obrane ili agresivnih ciljeva[60]. Izuzetak je vojna špijunaža u slučaju rata, koju međunarodno pravo ne zabranjuje.
3. Ekonomska špijunaža – u pravnom smislu ekonomska špijunaža često se naziva i gospodarskom špijunažom, dok se u visoko razvijenim zemljama često koristi i termin industrijska špijunaža. Industrijska špijunaža samo je jedan dio ekonomske špijunaže jer je usmjerena na tehnički i tehnološki razvoj određenih poslovnih subjekata.
4. Elektronska špijunaža – prikupljanje podataka o konkurentnim elektronskim sredstvima i sistemima svih tehničkih i elektronskih oblika komunikacija i veza; (telefoni, telegrafi, teleprinter, radio, računalo, telefaks i slično). Često se koristi u visokorazvijenim zemljama, za prikupljanje podataka u bankarstvu, posebno kod investicijskih banaka, korporacija i slično.

Postoje različita tumačenja špijunaže, pa neki analitičari i stručnjaci pod „industrijskom ili konkurencijskom špijunažom" podrazumijevaju djelovanje konkurentskih tvrtki, dok drugi pod istim pojmom podrazumijevaju obavještajnu djelatnost koja se provodi od strane različitih čimbenika.

[59]Đorđević, O. (1978). Šta je špijunaža. Beograd: Politika, str. 54.
[60]Đorđević, N. (1986). Obaveštajne službe i krivično delo špijunaže. Pravni život, 10, str. 977.

Kako bismo što preciznije mogli definirati granicu između tih pojmova, postoji i sljedeća podjela.

1. Industrijska ili konkurencijska špijunaža - u pravilu cilja na određene proizvode i znanstvene ili poslovne projekte te je najčešće kratkoročne prirode;
2. Gospodarska špijunaža - dugoročno je usmjerena i teži prikupljanju što je moguće opsežnijih informacija iz gospodarskih područja i gotovo uvijek iza nje stoji vlada neke strane zemlje.

Iz prakse se može zaključiti da je vrlo teško odrediti granicu između prikupljanja informacija koje provode državne institucije u državnom interesu te privatnog prikupljanja informacija od strane pojedinih poduzeća koje to rade u privatnom interesu.

Industrijskom špijunažom (*Industrial Espionage*) dolazi se do informacija koristeći se nelegalnim i neetičnim postupcima. Njome se štede milijarde dolara koje bi inače bilo potrebno uložiti u vlastito istraživanje i razvoj, što je neizvjesno i dugoročno. Inače, špijunaža *per se* može se promatrati s dvaju aspekata. Prvi je politički, a drugi pravni.

Gospodarska špijunaža cilja trgovinu za razliku od klasične špijunaže koja cilja državnu sigurnost. Razlog da neka Vlada prati poduzeće, ili obrnuto, svakako je ekonomski interes, u milijunskim ugovorima, o kojima se često radi.

Posljedice gospodarske ili ekonomske špijunaže ogledaju se kroz gubljenje ugovora, poslova i tržišnih udjela, te smanjenjem kompetitivne prednosti za ekonomiju određene zemlje.Razlika između gospodarske, odnosno ekonomske i industrijske špijunaže, u tome je što iza njih svjesno stoje uprave poslovnih subjekata, koje svim sredstvima, a prije svega podmićivanjem nastoje doći do poslovnih tajni.

6.4.1. Tipovi gospodarske špijunaže prema Evanu Potteru;

1. **Primarna i sekundarna gospodarska špijunaža – „zelena“ i „žuta“ zona:**
   Prikuplja informacije iz otvorenih izvora kao što su istraživački centri, sveučilišne baze podataka, knjižnice, trgovačka društva ili udruge, javni mediji, Internet, specijalizirane publikacije, različiti think-tankovi. Često obuhvaća i prikupljanje podataka o različitim makroekonomskim analizama ili trendovima. Osnovna razlika između dviju razina, tj. zelene i žute razine, odnosi se na stupanj težine/lakoće kojom se prikupljaju javni podaci i informacije.
2. **Taktička gospodarska špijunaža – „crvena“ zona**
   Informacije se prikupljaju na relativno osjetljiv način i putem privilegiranih izvora kao što su: osobni kontakti između menadžera pojedinih kompanija tijekom poslovnih susreta, sudjelovanje na usko specijaliziranim simpozijima za strogo određeni krug korisnika, uporaba internih baza podataka u pojedinim kompanijama uključujući analize pojedinih tržišta, interna izvješća o kvaliteti i znanstvenim potencijalima u pojedinim tvrtkama, informacije o budućim projektima određene tvrtke. U obavještajnim krugovima zapadnih zemalja ovaj tip informacija često se označava kao „sakrivena“ informacija. Samo u određenim okolnostima ovakva vrsta špijunaže može se okarakterizirati kao neetička. U ovom slučaju prikupljaju „se sirovi“, odnosno neobrađeni, podaci na nižim razinama. Uz pomoć analitičkih alata kasnije nastaju nove taktike i strategije koje kompanije rabe u svojim aktivnostima na svjetskom tržištu.
3. **Tajna gospodarska špijunaža – „crna“ zona**
   Prikupljanje informacija na nedopuštene i ilegalne načine svim mogućim metodama i sredstvima (tehnička sredstva, ljudski resursi). Ovakve informacije prikupljaju se pomoću specijaliziranih i visokoprofesionalnih skupina kao što su pravnici, stručni i financijski savjetnici, agenti obavještajnih službi itd. Prikupljanjem ovakvih, najčešće strateških informacija, gaze se svi etički standardi, a dolaženje u posjed istih znači za pojedinu tvrtku ili državu komparativnu prednost pred političkim protivnicima ili gospodarskim konkurentima.[61]

[61]Gospodarska špijunaža – paradigma modernog svijeta, Tomislav Đozić, znanstveni članak, raspoloživo na https://hrcak.srce.hr/100731 – datum pristupa sadržaju 26.06.2020.

6.5. Nositelji suvremene gospodarske špijunaže

Nositelji obavještajnih aktivnosti u području industrijske špijunaže najčešće su tvrtke ili kompanije, dok su nositelji aktivnosti u gospodarskoj špijunaži u pravilu političke i/ili gospodarske elite pojedinih zemalja, odnosno države i njihove agencije. Države osnivaju sigurnosno-obavještajne agencije, a privatne tvrtke osnivaju organizacijske jedinice koje se bave Business Intelligenceom te analizama podataka. Gospodarskom špijunažom želi se osigurati gospodarski i industrijski napredak u poslovanju.

Nositelji gospodarske špijunaže nacionalne su obavještajne službe koje rade u skladu sa zadacima i interesima koje su dobili od svojih vlada. Često je vrlo teško odrediti glavnog nositelja obavještajnih aktivnosti; je li to kompanija, tvrtka ili pak obavještajna služba. U globalnom svijetu sve je češći slučaj da obavještajne službe djeluju u interesu nacionalnih kompanija ili korporacija.

Kolika se važnost posvećuje obavještajnim aktivnostima, možemo primjerice zaključiti na temelju toga da je Francuska u listopadu 1997. godine u Parizu utemeljila instituciju pod nazivom „Škola za gospodarski rat“ u području gospodarske špijunaže. Naime, osnivač je škole francusko Ministarstvo obrane, a provodi se teorijska i praktična obuka obavještajnih aktivnosti u skladu s najsuvremenijim obavještajnim tehnikama. Prema kategorizaciji obrazovanja škola spada u kategoriju poslovnih škola, a moto glasi: „znati, predvidjeti, djelovati, reagirati“ prema generalu Charlesu de Gaulleu.

Osim obavještajnih službi, među realizatorima gospodarske špijunaže možemo navesti i tvrtke koje se bave Business Intelligenceom(BI), odnosno pitanjima poslovne sigurnosti. Trend osnivanja BI-tvrtki u SAD-u započeo je sredinom osamdesetih godina, dok je u Europi započeo nešto kasnije, tijekom devedesetih godina prošlog stoljeća. Tijekom 1994. godine BI-tvrtke u SAD-u ostvarile su prihod od 3,3 milijarde USD-a, da bi 2001. godine taj prihod narastao na 4,6 milijarde USD-a.

Premda je poslovanje takvih tvrtki legalno, česti su primjeri u svijetu u kojima njihovo poslovanje zadire u „sivu“ ili pak u „crnu“ zonu nedopuštenog prikupljanja podataka i informacija ili pak transfera zabranjene tehnologije. Iako te tvrtke negiraju da se bave gospodarskom špijunažom, već tvrde da informacije prikupljaju iz otvorenih izvora.

Primjer:

Najveća telekomunikacijska kineska tvrtka HUAWEI bavi se proizvodnjom elektroničke opreme Tvrtka se našla pod istragom u Kanadi i Australiji zbog sumnje da se bavi određenim oblicima špijunaže, a američki Kongres proglasio ih je sigurnosnom prijetnjom jer njihova oprema može poslužiti za *cyber* napad iz Kine. Australska vlada također je zabranila Huaweiju izgradnju brze internetske mreže jer je utemeljitelj Huaweija Ben Zhengfei, bivši inženjer kineske vojske. Dok Kinezi tvrde da se radi o pokušaju suzbijanja konkurencije na tržištu, dio vladajućih političkih elita na Zapadu tvrdi da se radi o pokušaju prikupljanja povjerljivih informacija gospodarske naravi od strane kineske vlade.

6.6. Ciljana područja gospodarske špijunaže

Gospodarska špijunaža usmjerena je na prikupljanje podataka i informacija s područja:

- Financija
- Businessa
- Znanosti
- Tehnike

Osnovni je cilj gospodarske špijunaže stvoriti određene prednosti, kako za vlastitu zemlju, tako i za nacionalno gospodarstvo ili za određene gospodarske grane. Svakodnevno smo svjedoci stalnog napretka tehnoloških i znanstvenih dostignuća koja se primjenjuju u prikupljanju informacija. Upravo stoga, gospodarskoj špijunaži najviše su izložene najrazvijenije zemlje Zapada u kojima je prisutno slobodno kretanje ljudi, dobara i kapitala.

Upravo je stupanj razvijenosti pojedine zemlje glavni kriterij područja gospodarske špijunaže prema kojemu su usmjerene pojedine zemlje. Zapadnoeuropske i američke tvrtke usmjerene su na prikupljanje podataka o posljednjim generacijama tehnologije svojih konkurenata, a zemlje u razvoju (Rusija, Kina, Indija) usmjerene su na software i hardware starije generacije tehnologije koja im omogućavaju jačanje vlastite tehnologije za daljnji razvoj. Dostupnost takve tehnologije moguća je na „crnom tržištu“ na kojemu je cijena takve tehnologije vrlo povoljna i niska. Drugi razlog je što se za tehnologiju starije generacije primjenjuju niži standardi sigurnosne zaštite.

Posebna interesna područja gospodarske špijunaže predstavljaju dual-use tehnologije:

- Zrakoplovna industrija
- Kemijska industrija
- Biomedicina, molekularna biologija, farmacija
- Razvoj i usavršavanje kinetičkih tehnologiji
- Radarski i navigacijski sustavi
- Senzorska i laserska tehnologija
- Svemirski programi i tehnologije istraživanja svemira
- Elektronički i informatički sustavi
- Sustavi vezani uz pomorsku tehnologiju
- Nuklearni sustavi
- Proizvodnja poluvodiča i specijalnih materijala
- Energetske tehnologije i tehnologija zaštite okoliša

6.7. Uloga sigurnosno-obavještajnih agencija u području špijunaže

Sigurnosno-obavještajne službe postoje od davnina. U početku su one prvenstveno bile usmjerene na vojne ciljeve, na osvajanje novih teritorija, dok su s vremenom svoje aktivnosti usmjerile i na političke te gospodarske aspekte. Kao primjer dobro razvijene obavještajne agencije na našim područjima, moramo spomenuti Dubrovačku Republiku u kojoj je Senat na sjednici 12. kolovoza 1301. formirao tri centra, i to: Centar za fortifikacije i sigurnost, Centar za naoružanje i Centar za obavještajnu službu, koji je nazvan Centar za sakupljanje vijesti i informacija. Ključni ljudi ovog posljednjeg centra bili su plemići: Miho Procula, Pero Prodanelli i Marin Držić. Republika je uskoro imala 1400 agenata, koji su u trećim državama prikupljali vojne, političke i ekonomske informacije (Dedijer, 2002, u Bazdan, 2009, p. 59).

Uz razvoj obavještajnih agencija, pojavila se potreba i za osnivanjem protuobavještajne službe, kako bi se zaštitili interesi poduzeća. Cilj je protuobavještajnih službi osigurati sigurnost poduzeća, poslovnih tajni i informacija te intelektualnog vlasništva, a to čine manipuliranjem obavještajnim službama. Cilj je otkrivanje akcije napadača, tj. obavještajnih službi te neutralizirati njihovo djelovanje, a već spomenuto manipuliranje postiže se plasiranjem dezinformacija. (Javorović, Bilandžić, 2007, str. 177–178).

U suvremenom svijetu tajno prikupljene informacije potječu iz tzv. ljudskih izvora, tj. od vlastitih agenata, suradnika i drugih osoba (engl. *Human Intelligence* – HUMINT), ili su rezultat prisluškivanja i praćenja različitih komunikacijskih, radarskih, satelitskih i drugih elektron. sustava (engl. *Electronic Intelligence* – ELINT, *Signals Intelligence* – SIGINT, *Communications Intelligence* – COMINT i dr.). Pojedine države u sastavu obavještajnih službi imaju i posebne poluvojne skupine, a koriste ih za izvođenje subverzivnih i sličnih, tzv. prikrivenih operacija (specijalno ratovanje).[62]

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN br. 79/06, 105/06) definirane su temeljne odredbe, poslovi i ovlasti agencija, obveza suradnje između agencija, kao i njihov ustroj i upravljanje.

U Republici Hrvatskoj postoje dvije sigurnosno-obavještajne agencije, a to su:

- SOA – sigurnosno-obavještajna agencija
- VSOA – vojna sigurnosno obavještajna agencija

U temeljnim odredbama, članak 1, ovog zakona, definiran je razlog osnivanja agencija:

„*.....radi sustavnog prikupljanja, analize, obrade i ocjene podataka koji su od značaja za nacionalnu sigurnost, u cilju otkrivanja i sprječavanja radnji pojedinaca ili skupina koje su usmjerene: protiv opstojnosti, neovisnosti, jedinstvenosti i suvereniteta Republike Hrvatske, nasilnom rušenju ustroja državne vlasti, ugrožavanju Ustavom Republike Hrvatske i zakonima utvrđenih ljudskih prava i temeljnih sloboda te osnova gospodarskog sustava Republike Hrvatske i koji su nužni za donošenje odluka značajnih za ostvarivanje nacionalnih interesa u području nacionalne sigurnosti*“[63]

NSA – National Security Agency – američka nacionalna sigurnosna agencija najmoćnija je špijunska agencija, koja u informacijsko-komunikacijskom prometu nadzire čitav svijet jer posjeduje tehnološke mogućnosti da prati, čuje i vidi sve koji se služe bilo kojim oblikom elektroničke komunikacije. Osim što nadzire komunikacije unutar države i u inozemstvu, također zadužena je i za zaštitu državnih komunikacija i vlade, od sličnih organizacija u

[62]Obavještajna služba, raspoloživo na https://www.enciklopedija.hr/natuknica.aspx?ID=44534 – datum pristupa sadržaju 24.06.2020.
[63]Raspoloživo na https://www.zakon.hr/z/744/Zakon-o-sigurnosno-obavje%C5%A1tajnom-sustavu-Republike-Hrvatske – datum pristupanja sadržaju 22.06.2020.

svijetu.Glavna je zadaća agencije borba protiv terorizma te otkrivanje neprijatelja države. Ova agencija nezakonito se bavila i upadima u računalne programe građana, prvenstveno praćenjem mailova i telefonskih poziva, što se smatra grubim kršenjem ovlasti vlade.Tako je došlo do neovlaštenog praćenja građana i stranaca koji su se našli u SAD-u. U posljednjih 19 godina, od napada 11.09.2001. godine, agencija je modernizirana najsuvremenijom opremom te se ulažu ogromna sredstva u rad agencije.

Uz već spomenutu NSA, neke od najpoznatiji obavještajnih agencija su: Mossad – Izrael, MI6 (Military Intelligence) – Velika Britanija, FAGCI (Federal Agency of Government Communications and Informations) – Rusija, CIA (Central Intelligence Agency) – SAD. Poredane su prema broju zaposlenih i visini budžeta (Bilandžić, 2000: 139).

6.8. Metode i sredstva provođenja gospodarske špijunaže

Sredstva i metode gospodarske špijunaže vrlo su različite te ovise o mogućnostima onih koji je provode, te o njezinim ciljevima. Najlakši izvor informacija su nedovoljno educirani službenici koji otkrivaju poslovne tajne o poslovanju tvrtki i institucija, i to najčešće faksom ili e-poštom, odnosno putem suvremenih komunikacijskih kanala.

Gospodarska špijunaža može se provoditi na nekoliko načina:

- Krađom informatičkih baza podataka (ili nekih njezinih dijelova) uz pomoć unajmljenih hackera;
- Slanjem službenika, poslovnih ljudi ili studenata na specijalizaciju, odnosno školovanje;
- Formiranjem joint-venture tvrtki gdje većinski udio pripada inozemnim vlasnicima;
- Vrbovanjem znanstvenika i stručnjaka koji se bave sofisticiranim tehnologijama ili rade na nekim osjetljivim znanstvenim projektima;
- Sitnim krađama po laboratorijima i institutima
- Klasičnim obavještajnim metodama uključujući i metode elektronskog izviđanja različitih oblika komunikacija;
- Širenjem glasina i dezinformacija s najčešćim temama o:

a) navodnoj „nekvaliteti i nepouzdanosti“ proizvoda čijom proizvodnjom se bavi suparnička tvrtka, i

b) izmišljanjem korupcionaških afera u ciljanoj tvrtki ne bi li se srušio njezin ugled i status na tržištu.

Vrlo je važno istaknuti da se gospodarska špijunaža u većini slučajeva provodi u kombinaciji s legalnim metodama (Business Intelligence) jer ju je teže uočiti te, u slučajevima kada se otkrije, teže ju je pravno sankcionirati jer se jednim dijelom nalazi u zakonskim okvirima.

Metode provođenja gospodarske špijunaže predstavljaju nezakoniti načini i postupci kojima se služe zemlje kako bi došle do željenih podataka.

1. Klasične metode
2. Suvremene metode

Klasične metode predstavljaju postupci koji se svrstavaju u tajne operacije (Cover Operation) upotrebom ljudi, pa se zbog toga ova metoda prikupljanja podataka i informacija naziva i ljudskom obavještajnom službom (Human Intelligence – HUMINT). U ljudske izvore ubrajamo: razne profesionalce, tajne agente, suradnike, ratne zarobljenike, prikrivene informatore; jednim imenom „špijune“.

Metode provođenja gospodarske špijunaže[64]

- Zaposlenici (njihovo znanje ili mogućnost pristupa osjetljivim informacijama)
- Konzultanti ili osobe s posebnim mandatima
  (eksperti koji će imati pristup osjetljivim informacijama)
- Razmjene osoblja (posjeti gostiju, raznih delegacija, razmjene studenata i delegacija)
- Korištenje međunarodnih institucija i organizacija (osoblje te zemlje ima privilegiran pristup informacija)
- Intercepcija komunikacije (slaba točka su računalni sustavi i krađa informacija s računala)
- „kopanje po smeću“ (metoda koja zvuči čudno, ali lako primjenljiva, ako zaposlenici nemaju svijest o čuvanju i uništavanju povjerljivih izvještaja i informacija)

[64]Prema: Anderson, P. (2009.:56) Economic Espionage Today, Chicago.

- Poslovna putovanja (diplomat nerijetko sa sobom prenosi elektronski povjerljive podatke, primjerice u zračnim lukama SAD-a godišnje nestane više od 630 tisuća laptopa)

Slika 4: Metode provođenja gospodarske špijunaže

Izvor: Prilagođeno prema Anderson (Ibidem.:56)

(vlastita izrada)

Također, moramo navesti da u svakoj zemlji postoje specijalisti koji su prošli razne obuke i obrazovanja kako bi bili najbolji u poslovima kojima se služe – tajni agenti, a mogu biti iz različitih područja obrazovanja i obuke kao što su:

- Kriptografija, osobni kontakti, radio-promet,
- Služenje dezinformacijama i dvostrukim poigravanjem, dvostruki agenti i slično
- Obučavanje za davanje seruma istine, posebno za ispitivanje prebjega
- Uporaba infracrvenih kamera za noćno promatranje
- Korištenje „gluhim sobama“ da se onemogući primjena prislušnih uređaja.

Kriptografija je znanstvena disciplina koja se bavi prikrivanjem informacija u porukama, a sastoji se od dvaju podsustava; kriptografije i kriptoanalize. Kriptografija je znanost o zaštiti podataka (šifriranje podataka i enkripcija, te dešifriranje i dekripcija). Kriptoanaliza je znanost kojom se proučavaju metode za otkrivanje izvorne informacije u kriptogramu, bez poznavanja ključa tj. koda.

Suvremene metode zahtijevaju najsuvremenije alate, kod kojih se do tajnih informacija dolazi uporabom tehničkih sredstava, pa stoga govorimo o tehničkoj obavještajnoj službi (Technical Intelligence – TECHINT). Navedene metode napreduju iz dana u dan, a najveći napredak postignut je uporabom satelita. Tajne informacije prikupljaju se tehničkim sredstvima. Pa ipak, ljudski su izvori i dalje krucijalni izvor.

M. Wolf tvrdi: „*Mislim, ipak da rad s ljudskim izvorima – tako dugo dok te službe postoje – nikad neće biti moguće u potpunosti nadomjestiti. Tehničkim sredstvima samo se približno može ustanoviti trenutačno stanje na prostoru što ga se nadzire. Tajni planovi, opcije, i odluke ostaju skriveni i za najrazvijenije satelite*."[65]

Segmenti tehničko obavještajnih službа:

- (Signal Intelligence – SIGINT) metoda je kojom obavještajna služba prikuplja obavještajne podatke presretanjem elektroničkih signala koji su rezultat komunikacije među ljudima. U takvim slučajevima govorimo o komunikacijskoj obavještajnoj službi (Communications Intelligence – COMINT).
- (Electronic Intelligence – ELINT) metoda je kojom obavještajna služba prikuplja obavještajne podatke presretanjem elektroničkih signala koji nisu izravno korišteni u komunikaciji među ljudima

6.8.1. Socijalni inženjering – Social engineering

Socijalni inženjering je metoda nagovaranja ljudi da ispune zahtjeve napadača. Radi se o načinu stjecanja informacija i podataka do kojih napadač legitimnim putem ne bi mogao doći. Pri tome se ne iskorištavaju propusti implementacija operacijskih sustava, protokola i aplikacija, nego se napad usmjerava na najslabiju kariku cjelokupnog lanca – ljudski faktor.

[65]Wolf, M. (2004.), Čovjek bez lica, Zagreb, 310.

Napadač koji provodi napad zasnovan na socijalnom inženjeringu mora posjedovati osobine poput dobrog pamćenja, snalaženja u razgovorima, odgovarajućeg načina razmišljanja i slično, jer mu one donose prednost prilikom izvođenja napada.[66] Socijalni inženjering manipulacija je ljudima (prijevara) u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih manipulator inače ne bi mogao doći.

Pojam socijalnog inženjeringa popularizirao je poznati i osuđeni haker Kevin Mitnick, koji je tvrdio kako je mnogo lakše nekoga tako prevariti nego probiti njegov informacijski sustav. Znači, osnovni je cilj social engineeringa manipulacija ljudima kako bi se neovlašteno pristupilo povjerljivim informacijama. U tu svrhu, često se u e-mailu navode neki poznati podaci o korisniku (njegovo ime, koje može biti poznato jednostavno iz e-mail adrese), datum rođenja i slično ili se pak napadač pretvara da je administrator podataka.

Educiranje zaposlenika o socijalnom inženjeringu kao metodi kojom se nezakonito pribavljaju poslovne informacije predstavlja kontinuiranu obvezu svake organizacije, kao i obvezu zaposlenika o prijavljivanju svakog događaja koji ima obilježje socijalnog inženjeringa u cilju prevencije i izučavanja načina djelovanja napadača.

6.8.2. Phishing napadi

Phishing je jedan od oblika socijalnog inženjeringa u kojem napadači pokušavaju doći do brojeva kreditnih kartica, lozinki različitih korisničkih računa i slično.Nakon virusa, crva, neželjene elektroničke pošte (SPAM-a), hoax poruka i različitih kombinacija ovih prijetnji, u posljednje je vrijeme na Internetu primijećen izniman porast tzv. phishing napada.[67] Pojam phishing napada podrazumijeva aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih web-stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka, kao što su korisnička imena i zaporke, PIN-brojevi, brojevi kreditnih kartica i sl. U doba neprestana porasta popularnosti Internet bankarstva i obavljanja transakcija putem Interneta ovakvi su napadi posebno opasni i posebnu je pažnju potrebno posvetiti metodama njihova sprječavanja. Potrošači često preko različitih aplikacija na internetu kupuju različite artikle, od kojih su neki i većih vrijednosti.

[66] Vrste napada raspoloživo na https://www.cis.hr/www.edicija/Vrstenapada.html – datum pristupa sadržaju 21.0252020.
[67] Phising napadi raspoloživo na https://www.cis.hr/www.edicija/Phishingnapadi.html – datum pristupa sadržaju 24.02.2020.

Prilikom takvih kupnji, obvezni su dostaviti svoje osobne podatke, kao i brojeve svojih bankovnih kartica i računa što predstavlja veliku opasnost i potencijalnu mogućnost krađe osobnih podataka.

6.9. Načini zaštite od špijunaže

Apsolutna sigurnost ne postoji. Usprkos poduzimanju svih organizacijsko – tehničkih mjera nijedna organizacija nije isključena od sigurnosnih ugroza. Važno je napomenuti da se učestalost napada i prijetnji povećava s povećanjem obujma poslovanja i vrijednosti našeg proizvoda ili usluge na tržištu. Međutim, sve organizacije koje se nalaze na tržištu moraju jačati kapacitete u cilju prevencije od gospodarske špijunaže.

Kako bi smanjile rizike od neovlaštenog pristupanja i krađe podataka i informacija, nužno je:

1. Minimizirati izlaganje informacijske mreže poduzeća – podaci koji se šalju unutar i izvan poduzeća moraju biti zaštićeni tako da su minimalno izloženi bilo kakvoj aktivnosti poput krađe, zlouporabe ili presretanja.
2. Sigurna baza podataka –svi podaci i informacije spremljeni su bazi podataka unutar organizacije kojoj pristup iz vanjskog izvora nije moguć. Vrlo je bitno da se pristup podacima odvija samo putem jednog kanala što smanjuje mogućnost krađe podataka presretanjem ili drugim napadima.
3. Podaci koji se koriste nalaze se na sigurnom – u ovom slučaju govorimo o enkripciji podataka, pri kojoj je potrebno mnogo vremena da se početni podaci vrate u izvorni oblik i pročitaju, a znamo da je određeni podatak najveći kapital samo u pravo vrijeme.
4. Zaštita od brisanja i gubljenja podataka – uvijek je potrebno napraviti sigurnosnu kopiju svih verzija podataka jer do brisanja podataka može doći i slučajno, nenamjernim brisanjem osoba koje rade na tim bazama podataka.
5. Zaštita od miješanja podataka i autorizacija – svaki podatak mora imati svoj autentifikacijski „kod“ kojim je on zaštićen, te se tako osigurava teži pristup i mijenjanje podataka od strane kradljivaca ili neželjenih korisnika.
6. Nadziranje podataka – nadziranjem cjelokupnog informacijskog sustava poduzeća, osiguravamo praćenje svakog podatka i njegova pristupa bilo unutar ili van

organizacije. Sustav se svakodnevno provjerava te se nadograđuje kako bi bio sigurniji i efikasniji, a sigurnosni administrator može uvidjeti moguće prijetnje sustavu.

Ulaganje u mjere zaštite treba biti proporcionalno vrijednosti informacije koju želimo zaštititi. Što bolje svaka zemlja štiti intelektualno vlasništvo, imat će više stranih ulaganja i brži ekonomski rast. Žrtve industrijske špijunaže mogu biti gotovo svi, a sigurnosti nikada nije dovoljno.

Neki od načina na koje možemo unaprijediti mjere zaštite od gospodarske špijunaže:

- Imenovati osobu zaduženo za korporativno-informacijsku sigurnost
- Edukacija zaposlenika vezana uz zaštitu podataka u poslovnom komuniciranju
- Pratiti i analizirati studije slučaja iz područja gospodarske špijunaže
- Biti kontinuirano informirani o trendovima i metodama gospodarske špijunaže

6.10. Razlika između gospodarske špijunaže i Business Intelligence

Industrijska špijunaža – predstavlja prikupljanje zaštićenih podataka iz poslovanja neke organizacije od strane neovlaštenih osoba ili organizacija. Predmet industrijske špijunaže je zaštićena informacija, pri čemu postoje dvije ciljane skupine informacija. Prva je informacija o samoj organizaciji (procesi, tehnologija, ideje) dok drugu skupinu predstavljaju operativne informacije usmjerene na kupce, cijene ili tržište. Informacija predstavlja moć. Jedna od najučinkovitijih metoda prikupljanja zaštićene informacije je upotreba insidera, odnosno osoba koje raspolažu informacijama koje predstavljaju poslovnu tajnu.To mogu biti različite osobe, od izvršnih menadžera pa do niže rangiranih zaposlenika koji zbog slabijih primanja pristaju na „prodaju“ zaštićenih podataka konkurentima.

Industrijskom špijunažom mogu se baviti ne samo pojedinci i tvrtke, već i čitave države koje se bave špijunažom radi prikupljanja informacija kako bi pomogle tehnološkom razvoju svoje industrije, radi daljnje trgovine ili kako bi stvorile stratešku političku ili vojnu prednost. Kada govorimo o zaštićenim informacijama u vojnoj industriji – tada govorimo o pitanjima nacionalne, regionalne ili globalne sigurnosti.

Pojam *Business Intelligence* dolazi spajanjem dvaju termina, jednog iz obavještajnog svijeta (intelligence) i drugog iz poslovnog (business). U hrvatskom jeziku ne postoji prijevod

sintagme u općoj upotrebi, pa se najčešće koristi upravo izvorni naziv, premda bi jedan od preciznijih prijevoda glasio „*sustav upravljanja poslovnim informacijama"*.

Međutim, kada govorimo o Business Intelligence i gospodarskoj špijunaži, tada najčešće podrazumijevamo legalne metode djelovanja poslovnih organizacija prilikom prikupljanja poslovnih informacija u svom poslovnom okruženju i na tržištu, dok gospodarska špijunaža predstavlja nedopušteno prikupljanje osjetljivih poslovnih informacija na zabranjen, nezakonit način. Jednu od najtočnijih definicija dao je John F. Quinn[68]koji je tijekom jednog svog predavanja na konferenciji o Business Intelligence u svibnju 1994. godine u Virginiji iznio viđenje; „*proces BI je proces prikupljanja poslovnih ili konkurentskih informacija putem legalnih i etičnih metoda uključujući časopise, novine, internet, te posebne baze podataka, dok gospodarska špijunaža* predstavlja „*potajno prikupljanje osjetljivih, restriktivnih ili posebno klasificiranih informacija", s time da špijunaža obuhvaća i krađu informacija od svojih izravnih poslovnih konkurenata.*

Kanadski stručnjak za međunarodne odnose, Evan Potter daje svoje viđenje pojmova gospodarske špijunaže (*economic espionage* i *economic intelligence*). Prema Potteru, gospodarska špijunaža obuhvaća „*potajna i nedopuštena nastojanja inozemnih zemalja koja u korist vlastitih gospodarskih interesa i pritom se mogu služiti i sabotažama ili nekim drugim nedopuštenim sredstvima, zadiru u gospodarsku sigurnost drugih zemalja*"[69]

Pojam *economic intelligence* prema Potteru obuhvaća politiku ili komercijalno relevantne gospodarske informacije, uključujući financijske, trgovinske i informacije pojedine vlade koje pomažući vlastitim nacionalnim interesima, izravno ili neizravno pomažu u podizanju učinkovitosti i produktivnosti ili pomažu konkurentnosti vlastitog gospodarstva u svijetu. Također, Potter smatra kako economic intelligence može snažno pomoći jednoj državi, na štetu druge države, što se posebno ogleda u različitim poslovima gospodarske prirode, investicijama, produktivnosti, konkurentnosti ili gospodarskom rastu.[70]

[68]John F. Quinn bio je dugogodišnji dužnosnik CIA-e.Predavao je predmet business intelligence BI na sveučilištima u Sofiji i Tokiju, te je bio stručni savjetnik u različitim kompanijama koje se bave BI-om.
[69]E. Potter, Economic Intelligence & National Security, Carlton University Press & The Center for Trade Policy and Low, Canada, 1998.
[70]Ibid.

6.11. Špijunaža – prema kaznenom zakonu RH

Špijunaža je kao kazneno djelo opisana u članku 348. Kaznenog zakona Republike Hrvatske koji detaljno definira počinitelje kao i sankcije koje su predviđene za počinjenje djela iz djelokruga špijunaže i to na sljedeći način: [71]

(1) Tko tajne podatke koji su mu povjereni ili do kojih je došao na protupravan način, učini dostupnim stranoj državi, stranoj organizaciji, stranoj pravnoj osobi ili osobi koja za njih radi, kaznit će se kaznom zatvora od jedne do deset godina.

(2) Tko neovlašteno prikuplja tajne podatke, s ciljem da ih učini dostupnim stranoj državi, stranoj organizaciji, stranoj pravnoj osobi ili osobi koja za njih radi, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(3) Tko za stranu državu ili organizaciju organizira obavještajnu službu na području Republike Hrvatske, ili stupi u stranu obavještajnu službu koja djeluje protiv interesa Republike Hrvatske ili joj pomaže u radu, kaznit će se kaznom zatvora od jedne do deset godina.

(4) Tko kazneno djelo iz stavka 1. i 3. ovoga članka počini u vrijeme rata ili oružanog sukoba u kojem sudjeluje Republika Hrvatska,kaznit će se kaznom zatvora najmanje pet godina.

(5) Tko kazneno djelo iz stavka 2. ovoga članka počini u vrijeme rata ili oružanog sukoba u kojem sudjeluje Republika Hrvatska,kaznit će se kaznom zatvora od tri do petnaest godina.

[71]Špijunaža, Kazneni zakon RH: članak 348. – raspoloživo na https://www.zakon.hr/z/98/Kazneni-zakon – datum pristupa sadržaju 15.04.2020.

7. STUDIJA SLUČAJA –CASE STUDY

„Grupacija INA d.d.“

Slika 9.: zgrada kompanije INA d.d.

Izvor: https://www.ina.hr/home/press-centar/galerija/ dostupno 05.03.2020.

1. Što se dogodilo po mišljenju stručnjaka Gorana Akrapa i kako se to radi:

"Pošiljatelj ili grupa njih pošalje određene mailove poruke s malicioznim sadržajem i lako postoji mogućnost da je netko u tom slučaju kliknuo na mail na koji nije trebao i došlo je do zaraze podataka"[72]

Zaposlenici u svim poduzećima, dnevno dobivaju velike količine mailova, bilo poslovne ili privatne tematike, dobivaju različite reklamne sadržaje i slične pogodnosti koje se nude na tržištu. U nedostatku vremena, često ne pročitamo sadržaj maila, već odmah kliknemo na mail, te takvim postupcima izlažemo poduzeće rizikom od različitih hakiranja ili neovlaštenog upada u baze podataka.

[72] https://dnevnik.hr/vijesti/hrvatska/dnevnik-nove-tv-otkriva-koji-iznos-od-ina-e-traze-hakeri-od-INEhttps://www.telegram.hr/politika-kriminal/inu-su-napali-hakeri-pa-su-u-kompaniji-sad-zabrinuti-da-su-im-možda-ukradeni-osobni-podaci-građana – datum pristupa sadržaju 15.04.2020.

2. Kako je postupila kompanija:

Obavijest grupacije od 16.02.2020.

„*INA Grupa je pod kibernetičkim napadom koji je započeo oko 22 sata 14. veljače 2020. te uzrokovao poteškoće u radu pojedinih informatičkih sistema, što povremeno može utjecati na normalan rad,primjerice, izdavanja bonova za mobitele, elektroničkih vinjeta, plaćanja komunalnih računa. Opskrba tržišta je sigurna. Prodaja goriva na našim maloprodajnim mjestima se nastavlja neometano. Provedba svih plaćanja je sigurna, neovisno o tome radi li se o gotovinskom plaćanju, INA kartici ili bankovnoj kartici.INA poduzima sve kako bi žurno otklonila poteškoće u radu sustava.Ispričavamo se našim kupcima za eventualne neugodnosti koje je ova situacija mogla prouzročiti i molimo za razumijevanje do ponovne pune uspostave sustava. O daljnjem razvoju situacije javnost će biti pravovremeno obaviještena*.“

Dana 17.02.2020. operativni direktor Industrijskih servisa INA d.d., Goran Pavlović, obratio se javnosti te informirao bivše i potencijalne kupce o trenutnom stanju. Zahvalio je svim kupcima na razumijevanju koje su imali i koje pokazuju dok se problemi u potpunosti ne riješe te se ispričao zbog eventualnih poteškoća i neugodnosti. Kupci, bez obzira plaćaju li gotovinom, bankovnim karticama ili karticama Ine, mogu kupovati na siguran način. Sustav koji je napadnut je izoliran, te na slučaju rade najbolji stručnjaci. Poteškoće su se javile jedino kod prodaje bonova za mobitele, elektroničkih vinjeta i plaćanja komunalnih računa.

Dana 21.02.2020. INA Grupa izvijestila je u petak da je u procesu otklanjanja poteškoća u informatičkim sustavima na koje je utjecao kibernetički napad koji se dogodio krajem prošlog tjedna, a kažu i da ne mogu isključiti mogućnost da je uslijed napada došlo i do neovlaštenog pristupa osobnim podacima.

3. Koji je cilj napada na tvrtke po mišljenju stručnjaka

"Onaj tko je napadnut ili plati ili dio ili cijelu otkupninu i onda dobije ključ za dekodiranje zaključanih podataka. Ne možete doći do pouzdanih IP adresa po kojima bi to mogli otkriti

niti možete definirati s obzirom da otkupnine idu u bitcoinima tko je taj koji u konačnici sve naplati“, kaže Goran Akrap, stručnjak

Preko IT krugova do rep.hr-a došla je neprovjerena informacija o iznosu od 1500 bitcoina, odnosno oko 100 milijuna kuna, koje hakeri traže od Ine

Slika 10: Slika INA-ine benzinske postaje

Izvor: rep.hr; dostupno 05.03.2020.

Topić pak napominje kako šteta može biti milijunska.

„ *Mislim da nije samo stvar u materijalnoj šteti, nego je stvar reputacije. INA je kažem jedna velika kompanija koja mora voditi računa i o tom dijelu. Podaci inicijalno mogu otići prema ruskim serverima, ne mora značiti da je to krajnji korisnik tih podataka, može značiti da je samo preko Rusije netko došao do tih stvari, znamo da je Rusija jedan potencijalni kriminalni milje za takve skupine“, kaže Bernard Topić iz Hrvatske udruge.Neke tvrtke ne moraju biti direktno ciljane, mogu biti nasumično. Što je u ovom slučaju bilo teško je reći, to će pokazati analize".*

"Obično najveća šteta je reputacijska zato što financijske štete, imate u krajnjoj liniji osiguranja koja ih pokrivaju, možete se osigurati od šteta zbog informatičkog *kriminala, ali*

ne možete se osigurati od loše reputacije", 73 *navodi Carić stručnjak za informacijsku sigurnost.*

INA je samo jedan od primjera napada koji se svakodnevno događaju u globalnom svijetu, na kojem egzistiraju milijuni tvrtki. I najsuvremenija informatička oprema ponekad nije dovoljna u zaštiti podataka jer je najčešći uzrok ugroza upravo nesavjestan, ponekad nedovoljno educirani ljudski faktor što možemo vidjeti i na opisanom primjeru INA-e d.d.

[73] https://www.rtl.hr/vijesti-hr/novosti/crna-kronika/3648399/hakeri-pokazali-da-ni-velika-ina nije otporna na njihove napade – datum pristupa sadržaju 15.03.2020.

8. ISTRAŽIVANJE

Istraživanje na temu. „Gospodarska špijunaža i krađa poslovnih informacija“ provedeno je na ispitanicima iz privatnog i javnog sektora Istraživanje je provedeno putem ankete koja je poslana na mailove što zaposlenika, što vlasnika i članova uprava.

Neke od tvrtki javnog sektora koje su sudjelovale u anketi:

Hrvatske Vode – Zagreb

Hrvatski sabor – Zagreb

Hrvatski zavod za mirovinsko osigurane HZMO – područna služba Varaždin

Ministarstvo Financija Republike Hrvatske – Carinska Uprava Varaždin

Ministarstvo Pravosuđa Republike Hrvatske – Kaznionica u Lepoglavi

Ministarstvo unutarnjih poslova MUP Republike Hrvatske – PU Varaždin

Neke od tvrtki privatnog sektora koje su sudjelovale u anketi:

ABIT d.o.o. Varaždin

Haitec d.o.o Varaždin

Hrvatske autoceste d.o.o. – podružnica Varaždin

INA d.d. grupacija

KOKA d.d. Varaždin

KTC d.d. Križevci

LESNINA XXL Zagreb

Stočar d.o.o. Varaždin

Veterinarska stanica d.d. Varaždin

Vindija d.d. Varaždin

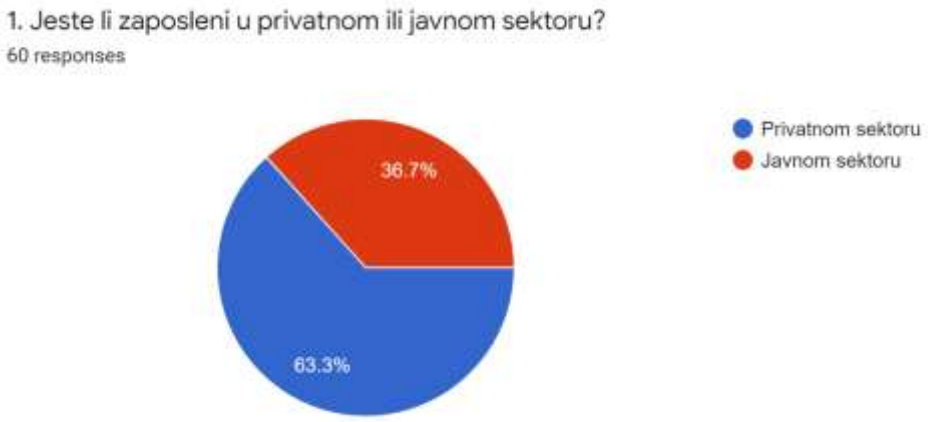
VSV Stočar Novi d.o.o. Varaždin

WIENER osiguranje Vienna Insurance Group d.d.

Anketa se sastoji od sljedećih pitanja:

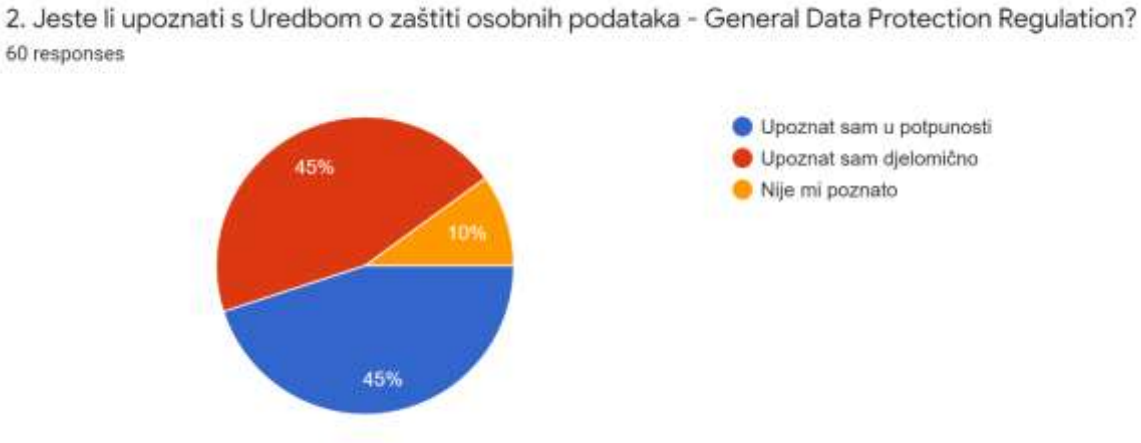
1. Jeste li zaposleni u privatnom ili javnom sektoru?
2. Jeste li upoznati s Uredbom o zaštiti osobnih podataka – General Data Protection Regulation?
3. Jesu li Vam osobni podaci bili ukradeni?
4. Postoji li u tvrtki u kojoj radite pravilnik o zaštiti poslovnih informacija?
5. Jeste li upoznati s pojmom "poslovne tajne"?
6. Jeste li upoznati s time koji su podaci klasificirani u tvrtki u kojoj radite?
7. Dali je tvrtka u kojoj radite bila podvrgnuta hakiranju ili krađi podataka?
8. Jeli računalo s kojeg primate i šaljete podatke zaštićeno sigurnosnom lozinkom?
9. Primate li na službenom računalu neželjenu poštu (reklame, privatne mailove i slično)?
10. Jeli Vam poznat pojam gospodarske špijunaže?
11. Jeli tvrtka u kojoj radite sklona prikupljanju informacija i podataka na zabranjen (nelegalan) način?
12. Razmjenjujete li poslovne podatke s osobama koje nisu vaši suradnici?
13. Jeste li upoznati s kaznenim sankcijama vezanim uz neovlašteno odavanje podataka?
14. Tvrtka u kojoj radim posvećuje pažnju zaštiti informacijske imovine:
15. Koliko je stara računalna oprema na kojoj radite?

ANALIZA ANKETE



Graf 1. – prikaz odgovora na anketno pitanje broj 1
Izrada: vlastita izrada autora

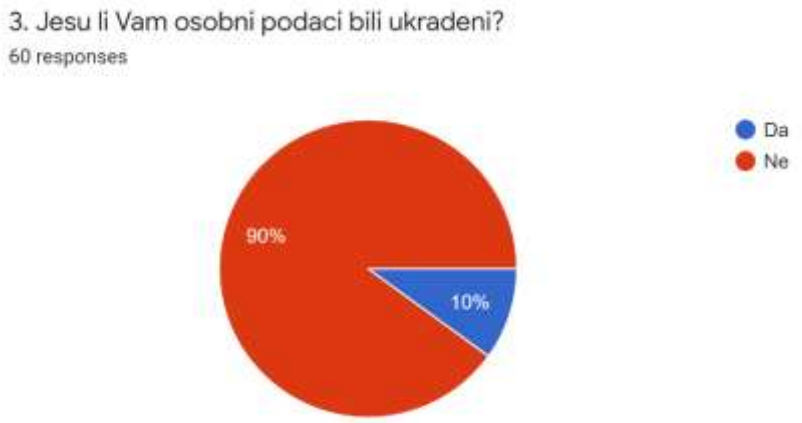
Prvo anketno pitanje postavljeno je sa svrhom analize zaštite podataka i gospodarske špijunaže ovisno o tome radi li se o tvrtkama privatnog ili javnog sektora. 63,3% ispitanika zaposleno je u privatnom sektoru, dok je 36,7% ispitanika zaposleno u javnom sektoru.



Graf 2. – prikaz odgovora na anketno pitanje broj 2
Izrada: vlastita izrada autora

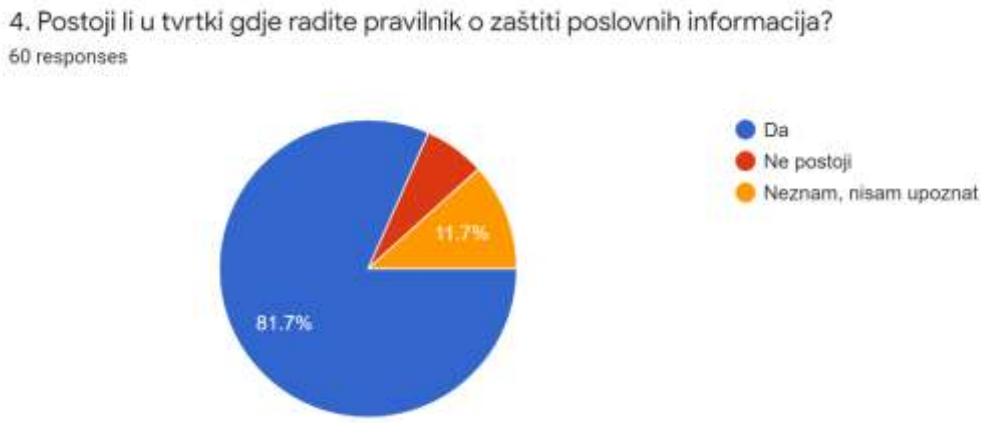
Drugo anketno pitanje usmjereno je na zaštitu osobnih podataka ispitanika u tvrtkama u kojima su zaposleni. S obzirom na to da je od 25.05.2018. godine na snazi Opća uredba o zaštiti podataka (GDPR – General Data Protection Regulation), a primjena je obvezna za sve članice Europske unije, ovo pitanje nam je interesantno zbog zaštite osobnih podataka zaposlenika i članova njihovih obitelji. Iz ankete možemo zaključiti da je 45% ispitanika u

potpunosti upoznato za direktivom te 45% ispitanika djelomično upoznato s direktivom. Samo za 10% ispitanika ova tema je nepoznanica, pa možemo zaključiti da je 90% ispitanika upoznato sa svojim pravima i obvezama vezanima uz zaštitu osobnih podataka.



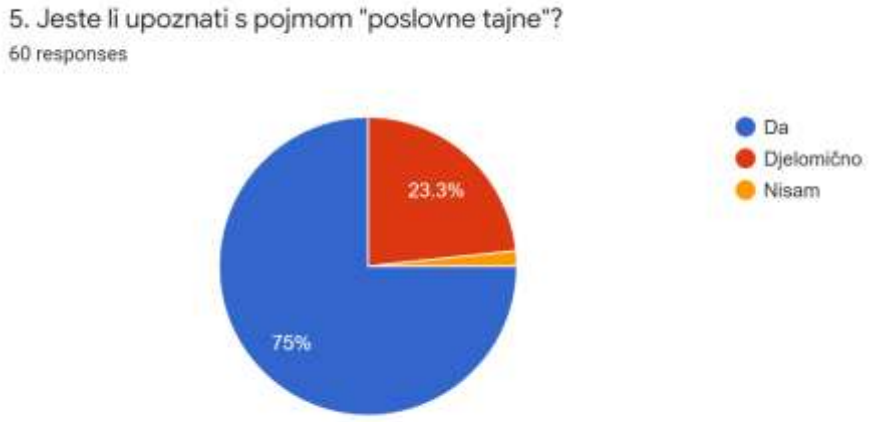
Graf 3. – prikaz odgovora na anketno pitanje broj 3
Izrada: vlastita izrada autora

Na treće anketno pitanje 90% ispitanika je odgovorila da se nije susrelo s krađom osobnih podataka, što je vrlo pozitivno. Samo 10% ispitanika imalo je tu nesreću da su im osobni podaci bili ukradeni.



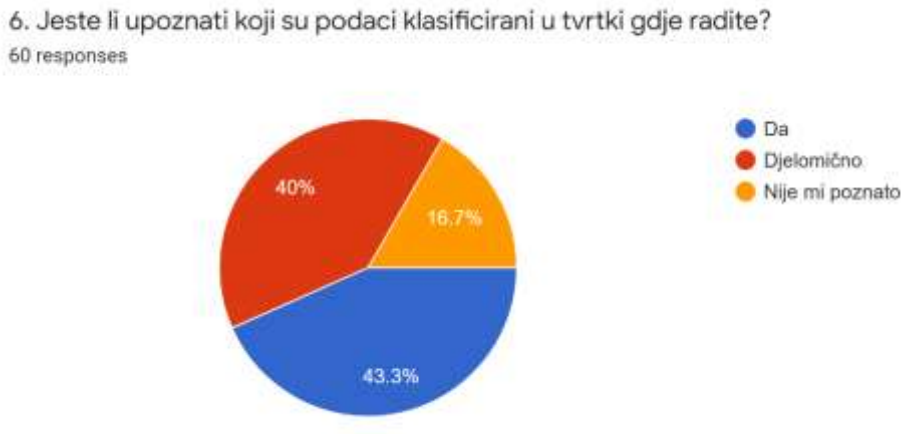
Graf 4. – prikaz odgovora na anketno pitanje broj 4
Izrada: vlastita izrada autora

Svaka tvrtka mora voditi brigu o zaštiti poslovnih informacija te posjedovati pravilnik o istom. 81,7% ispitanika zna da takav pravilnik postoji u tvrtkama u kojima su zaposleni, 11,7% ispitanika nije upoznato sa situacijom, dok je 6,6% ispitanika odgovorilo da u tvrtki u kojoj su zaposleni ne postoji takav pravilnik. Od anketiranih 60 ispitanika, 4 je odgovorilo negativno na to pitanje.



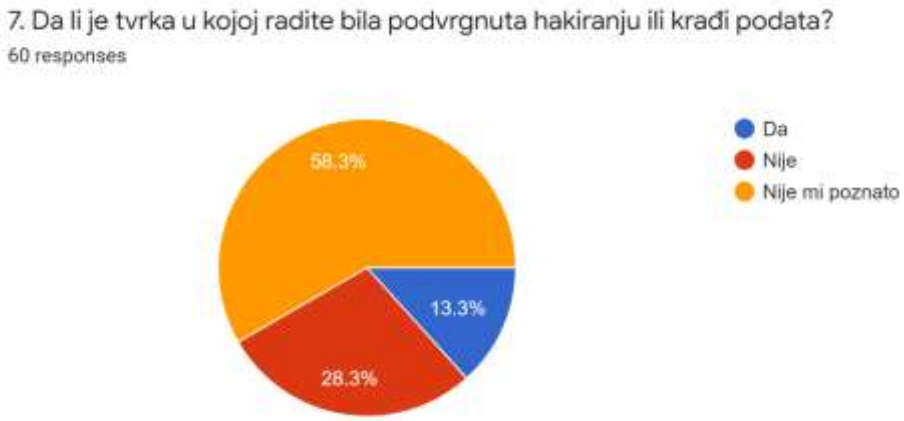
Graf 5. – prikaz odgovora na anketno pitanje broj 5
Izrada: vlastita izrada autora

Na anketno pitanje broj 5, gotovo 75% ispitanika odgovorilo je da su upoznati s poslovnom tajnom, 23,3% ispitanika odgovorilo je da su djelomično upoznati s poslovnom tajnom, dok 1,7% ispitanika ne zna za poslovnu tajnu, odnosno od 60 ispitanika samo jedan ispitanik nije upoznat s pojmom poslovne tajne.



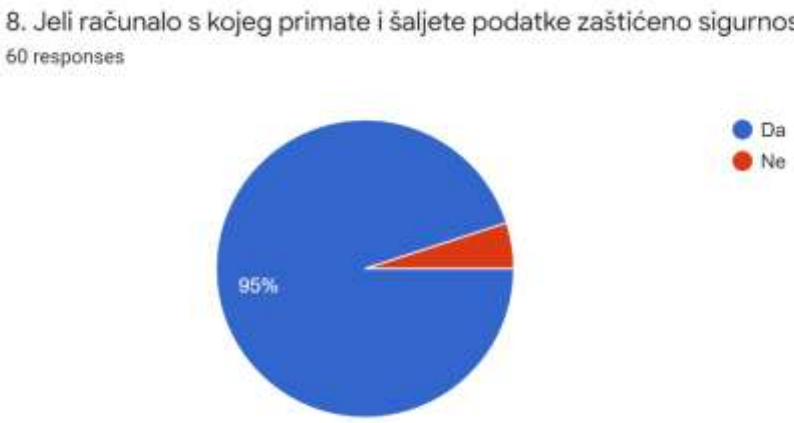
Graf 6. – prikaz odgovora na anketno pitanje broj 6
Izrada: vlastita izrada autora

Na 6. anketno pitanje 43,3% ispitanika odgovorilo je da su upoznati s pojmom klasificiranih podataka te znaju koji podaci spadaju u tu domenu. 40% ispitanika djelomično je upoznato s klasificiranim podacima, dok 16,3% ispitanika nije upoznato s tim podacima. S obzirom na to da je anketirano 36,7% ispitanika iz javnog sektora, gdje je obveza postupanja u pogledu klasifikacije podataka, prisutna je svijest ispitanika u pogledu klasifikacije podataka jer samo mali postotak ispitanika nije upoznat s klasificiranim podacima.



Graf 7. – prikaz odgovora na anketno pitanje broj 7
Izrada: vlastita izrada autora

Na 7. anketno pitanje velik broj ispitanika, 58,3% odgovorio je da nije upoznat s činjenicom je li ili nije tvrtka u kojoj su zaposleni bila podvrgnuta hakiranju podataka ili krađi podataka, 13,3% ispitanika odgovorilo je potvrdno na to pitanje. Iz nedavne prošlosti – veljača 2020. godine, znamo o hakerskom napadu na informatički sustav nacionalne kompanije INA-e te o pokušaju neovlaštenog pristupa osobnim podacima. INA je jedna od tvrtki koja sudjeluje u anketi. Tako 28,3% ispitanika tvrdi da tvrtke u kojima su zaposleni nisu bili izložene takvoj radnji.



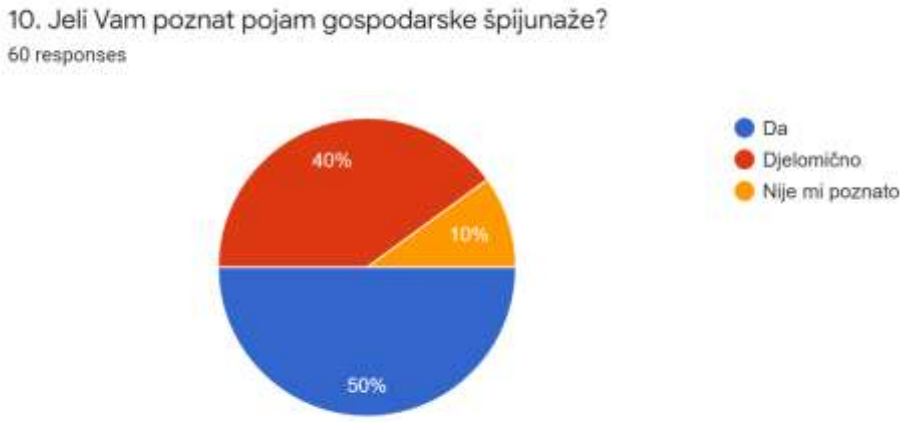
Graf 8. – prikaz odgovora na anketno pitanje broj 8
Izrada: vlastita izrada autora

Na 8. anketno pitanje čak 95% ispitanika je odgovorilo da su računala na kojima rade zaštićena sigurnosnom lozinkom što je vrlo pozitivno. 5% ispitanika ne koristi sigurnosnu zaštitu na računalu.

Graf 9. – prikaz odgovora na anketno pitanje broj 9
Izrada: vlastita izrada autora

Bez obzira na to što su pristupi računalima zaštićeni sigurnosnim lozinkama, čak 58,3% ispitanika odgovorilo je da na službena računala primaju privatne mailove, reklame i drugu neželjenu poštu. Osobno smatram da je taj broj ispitanika trebao biti veći jer smatram da skoro svi u nekom postotku službeno koriste računalo za privatne potrebe, najčešće putem maila. 41,7% ispitanika odgovorilo je da službeno računalo koriste samo u službene svrhe. S

obzirom na to da u anketi sudjeluju ispitanici iz javnog sektora (Hrvatski Sabor, Ministarstva) pristup podacima na njihovim računalima dodatno je zaštićen lozinkama na više razina.

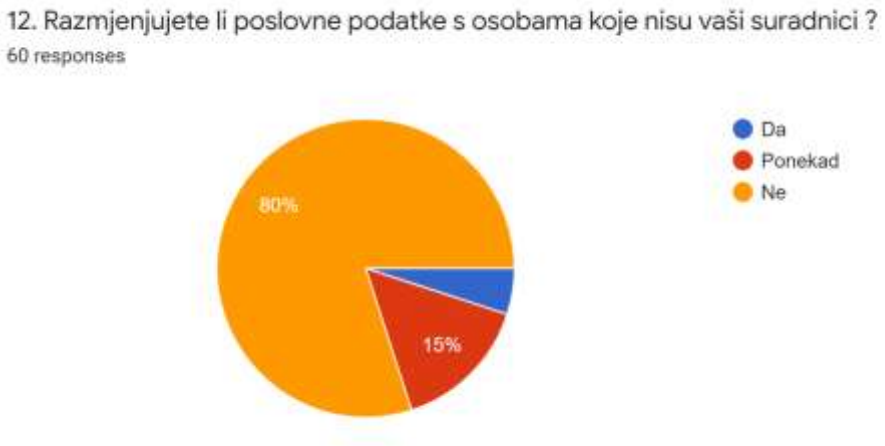


Graf 10. – prikaz odgovora na anketno pitanje broj 10
Izrada: vlastita izrada autora

Gotovo 50% ispitanika upoznato je s pojmom gospodarske špijunaže, 40% ispitanika djelomično je upoznato, dok je 10% ispitanika negativno odgovorilo na to pitanje, odnosno nisu upoznati s pojmom gospodarske špijunaže.

Graf 11. – prikaz odgovora na anketno pitanje broj 11
Izrada: vlastita izrada autora

Na 11. anketno pitanje 61,7% ispitanika odgovorilo je da tvrtke u kojima su zaposleni nikako nisu sklone prikupljanju poslovnih podataka i informacija, na neetičan, odnosno zabranjen način. 33,3% ispitanika odgovorilo je da nisu upoznati s tim podacima, dok je 5% ispitanika odgovorilo pozitivno na to pitanje. Ako znamo da je u anketi sudjelovalo 60 ispitanika, njih troje odgovorilo je pozitivno na pitanje.



Graf 12. – prikaz odgovora na anketno pitanje broj 12
Izrada: vlastita izrada autora

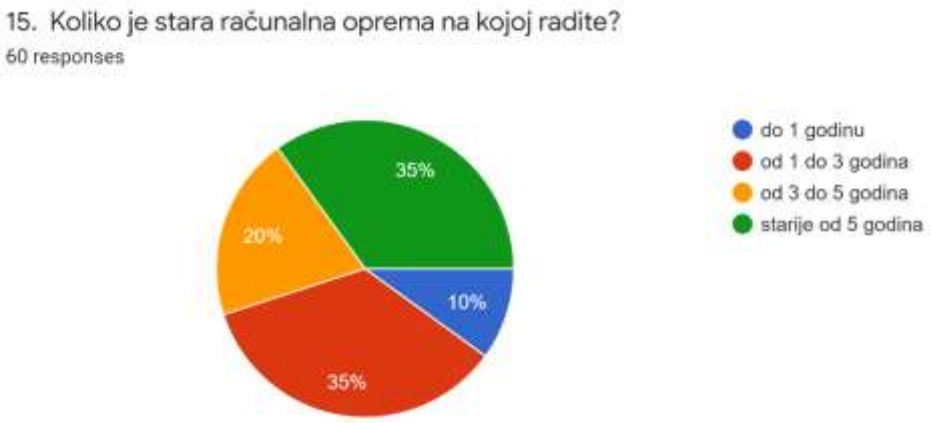
Gotovo 80% ispitanika je na 12. pitanje odgovorilo da ne razmjenjuju poslovne podatke s osobama koje nisu njihovi suradnici. Smatram da ispitanici nisu iskreno odgovorili na ovo pitanje jer svi mi ponekad komentiramo događaje koji se odvijaju u našem poslovnom okruženju, bilo da to radimo svjesno ili nesvjesno. Često svojim ukućanima ili prijateljima nesvjesno prepričavamo poslovne događaje i tako nesvjesno ugrožavamo poslovne podatke te tvrtku činimo ranjivom za neovlašteno prikupljanje poslovnih podataka. 15% ispitanika odgovorilo je da ponekad razmjenjuju poslovne podatke s osobama koje nisu suradnici dok je 5% ispitanika priznalo da to rade.

Graf 13. – prikaz odgovora na anketno pitanje broj 13
Izrada: vlastita izrada autora

Za neovlašteno odavanje poslovnih podataka, zakon predviđa stroge sankcije, što je 56,7% ispitanika svjesno toga. 33,3% ispitanika djelomično je upoznato s predviđenim sankcijama, dok 10% ispitanika nije upoznato sa sankcijama.

Graf 14. – prikaz odgovora na anketno pitanje broj 14
Izrada: vlastita izrada autora

Gotovo 46,7% ispitanika odgovorilo je da tvrtka u kojoj su zaposleni redovito ulaže u zaštitu informacijske imovine, 46,7% ispitanika odgovorilo je da tvrtke ulažu u zaštitu informacijske imovine samo onda kada je to nužno potrebno, dok je 9,6% ispitanika odgovorilo da se vrlo malo ulaže u zaštitu informacijske imovine.



Graf 15. – prikaz odgovora na anketno pitanje broj 15
Izrada: vlastita izrada autora

Na pitanje o starosti računala na kojima rade ispitanici su odgovorili sljedeće: 10% ispitanika radi na računalu starom do godinu dana, 35% ispitanika radi na računalu starom 1–3 godine, 20% ispitanika radi na računalu starom 3–5 godina, dok 35% ispitanika radi na računalu starijem od 5 godina.

Zaključak ankete

Iz provedene ankete možemo zaključiti da je veliki broj ispitanika u potpunosti ili barem djelomično upućen u zaštitu osobnih podataka što je vrlo pozitivno. Isto tako možemo zaključiti da su zaposlenici upućeni u pojmove „klasificiranih podataka“ i „poslovne tajne“ te su svjesni sankcija koje su predviđene za kršenje istih. Informacijska imovina je u većini tvrtki zaštićena, čak njih 95%. Iz ankete možemo također zaključiti da tvrtke javnog sektora više ulažu u informacijsku opremu i sigurnost, kao i velike grupacije privatnog sektora, no to nažalost nije slučaj kod manjih tvrtki privatnog sektora.

Vezano uz odavanje poslovnih podataka osobama koje nisu zaposlene u tvrtkama, situacija nije toliko optimistična. Većina ispitanika razmjenjuje poslovne informacije s ukućanima, prijateljima ili slično što predstavlja prijetnju ugroze. „Gospodarska špijunaža“ pojam je koji je ispitanicima također poznat. Prema odgovorima ankete tvrtke se ne služe neetičnim i nelegalnim postupcima prikupljanja poslovnih informacija ili barem zaposlenici nisu upoznati s tim.

9. ZAKLJUČAK

Cilj rada bio je istražiti i prezentirati gospodarsku špijunažu kao način nezakonitog i neetičnog poslovanja u funkciji krađe klasificiranih informacija i ostvarivanja nepripadajuće materijalne koristi te ostvarivanja prednosti nad konkurencijom i povećanja tržišnog udjela u poslovanju.

Zaštita podataka od gospodarske špijunaže aktualna je tema u svim sferama poslovanja, neovisno radi li se o privatnom, javnom ili državnom sektoru. Svakim danom svijet je sve više globaliziran; informacijski, tehnološki i ekonomski. Svakim danom sve više klasificiranih podataka i informacija akumulira se u informacijskim sustavima i time postaju interesantniji pojedincima, grupama i organizacijama za izučavanje ostvarivanja nezakonitog proboja i njihova otuđivanja.Podaci i informacije koje se obrađuju u organizacijama često su privatne naravi, pa u tom slučaju govorimo i o zaštiti osobnih podataka od gospodarske špijunaže. Sve veća prisutnost interneta, različitih zbirki i registara podataka,te društvenih mreža rezultirala je povećanjem rizika od krađe i gubitka podataka. Svi ti podaci, koje često ostavljamo i na društvenim mrežama, izlažu nas različitim rizicima i ugrozama poput krađe identiteta, što nam može stvoriti velike privatne i poslovne probleme.

Izuzetno je važno da se sve pravne i fizičke osobe koje podatke obrađuju u profesionalne i komercijalne svrhe drže važećih zakona i propisa koji reguliraju područje obrade podataka.

Ustavom Republike Hrvatske,članak 37. navodi se sljedeće:„*Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita osobnih podataka,te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je upotreba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.*“

Gospodarska špijunaža kao način nelegalnog i neetičnog prikupljanja podataka bila je prisutna tijekom cjelokupne povijesti ljudskog društva. Razvojem društva i gospodarstva države i tvrtke u okviru poslovanja kontinuirano pokušavaju doći do klasificiranih informacija o konkurenciji i njihovu poslovanju, čak i na nelegalan način kako bi zadržale uspješnost poslovanja ili je povećale nad svojom konkurencijom.Posebno su ugrozama iz područja gospodarske špijunaže izložene najrazvijenije industrijske zemlje (SAD, Njemačka, Kanada…), međutim, i razvijene zemlje i njihove kompanije dijelom su uključene u nezakonitu i neetičnu obradu klasificiranih podataka.Akteri u primjeni gospodarske špijunaže

često koriste različite načine kako bi postigli željeni cilj: nagrađivanjem, vrbovanjem i ucjenjivanjem djelatnika konkurentskih tvrtki i institucija, probojem u informacijske sustave, krađom informatičke opreme koja sadrži klasificirane podatke, prisluškivanjem, socijalnim inženjeringom i dr. Kada govorimo o organiziranim i sustavnim špijunažama na višoj razini, tada su u njih uključene i obavještajne agencije u svrhu zaštite gospodarskih interesa određene države. Upravo na neetičan i nelegalan način pribavljanjem informacija brojne svjetske kompanije kao i pojedine države uštede milijarde dolara godišnje koje bi inače morale uložiti u istraživanja i razvoj.Provođenjem gospodarske špijunaže ostvaruju materijalnu korist koja im ne pripada, a sve s ciljem ostvarivanja što veće dobiti i dominacije na tržištu koja ima i odraz na jačanje međunarodnog položaja i utjecaja u svijetu. Ako malo bolje proučimo našu okolinu, možemo vidjeti da je špijunaža prisutna u svim područjima našeg života, premda često toga nismo ni svjesni. Upravo zbog imperativa koji vodi današnji svijet; novac, profit i moć, razvijene zemlje često svoju tehnologiju poklanjaju zemljama na nižem stupnju razvoja, kako bi iste učinili tehnološki ovisnim upravo s prikrivenim motivom gospodarske špijunaže.

Mnoge zemlje vode ekonomske ratove u kojima je omiljeno oružje špijunaža.

Sustav informacijske sigurnosti u privatnom, javnom i državnom sektoru treba biti organiziran da štiti klasificirane informacije od gospodarske špijunaže koja se danas odvija na različite načine, a najčešće kroz neovlaštene upade i krađu digitalnih podataka. Kontrole se moraju vršiti na više razina, a najveću prijetnju predstavljaju zaposlenici koji nisu dovoljno educirani o rizicima i ugrozama, neadekvatan selekcijski postupak u području ljudskih resursa, sustav sigurnosnih provjera, primanje i promicanje kandidata mimo standardne procedure, nedovoljnog ulaganja u korporativno-informacijsku sigurnost koja se kod određenih upravljačkih struktura još uvijek smatra troškom, a ne investicijom koja jamči opstanak organizacije na tržištu.

Uzimajući u obzir znanstvena i tehnološka postignuća, ponekad ni sve mjere koje organizacija poduzme nisu dovoljne da je zaštite od nepoželjnih „upada“ u sustav i krađe informacijske imovine.

I na kraju možemo dati generalni zaključak gospodarske špijunaže, koji je napisao Tomislav Đozić u znanstvenom članku naziva *Gospodarska špijunaža-paradigma modernog svijeta* koji glasi:„*Gospodarska špijunaža ne poznaje saveznike. To je rat svih protiv svih, od onih slabije razvijenih zemalja pa do najrazvijenijih zemalja svijeta“*.

10. IZVORI:

KNJIGE I ZNANSTVENI ČLANCI :

1. Anderson, P. (2009.:56) *Economic Espionage Today*, Chicago.
2. Bezdan, Zdravko, *Poslovno-obavještajne službe, industrijska i gospodarska špijunaža u međunarodnoj ekonomiji*, 2016, UDK/UDC:355.40:339.9
3. Bogati, J., *Norme informacijske sigurnosti ISO/IEC 27K*, Ministarstvo obrane RH, Odsjek za poslove obrane Virovitica, Praktični menadžment, Vol.II, br.3, str. 112–117.
4. Dedijer, S. 2002. *Ragusa Intelligence and Security 1301.–1806A Model for theTwenty-First Century?*. International Journal of Intelligence and Counter Intelligence, sv. 15, br. 1, ljeto 2002.
5. Đorđević, N. (1986). *Obaveštajne službe i krivično delo špijunaže*. Pravni život, 10, str. 977.
6. Ivandin Vidović Darija, Lidija Karlović, Alen Ostojić *Korporativna sigurnost*, Zagreb, UHMS, 2011.
7. Javorović B, Bilandžić M, *Poslovne informacije i business intelligence,* Zagreb, Golden marketing – Tehnička knjiga, 2007
8. Klaić B., Rječnik stranih riječi, Nakladni zavod MH Zagreb, 1988. god.
9. Klasić, K., Klarin, K., *Informacijski sustavi : načela i praksa*. Zagreb : Intus informatika, 2009.,
10. Panian, Ž. *Kontrola i revizija informacijskih sustava*. Zagreb : Sinergija - nakladništvo, 2001.
11. Potter, E. *Economic Intelligence & National Security*, Carlton University Press & The Center for Trade Policy and Law, Canada, 1998.
12. Uredba o mjerama informacijske sigurnosti (NN 46/2008)
13. Žunec, O. i Domišljanović, D. (2000.) *Obavještajno-sigurnosne službe Republike Hrvatske*. Zagreb: Jasenski i Turk
14. Wolf, M. (2004.) *Čovjek bez lica*. Zagreb

INTERNET STRANICE :

1. AZOP – Agencija za zaštitu osobnih podataka – dostupno 10.02.2020. na https://azop.hr/zastita-podataka-hrvatska/
2. Boban, M. (2018). Zaštita osobnih podataka i nova EU uredba o zaštiti podataka. Bilten Hrvatskog društva za medicinsku informatiku, 24 (1), 26–40. – dostupno 15.02.2020. na https://hrcak.srce.hr/193680
3. Clark, Donald. The Continuum of understanding. 2004. – dostupno 10.02.2020. na http://www.nwlink.com/~donclark/performance/understanding.html.
4. Gospodarska špijunaža–paradigma modernog svijeta – Hrčak, Tomislav Đozić – dostupno 15.02.2020. na https://hrcak.srce.hr/100731
5. Informacija, *Hrvatska enciklopedija*, Leksikografski zavod Miroslav *Krleža* – dostupno 05.02.2020. na https://www.enciklopedija.hr/natuknica.aspx?id=27405
6. Informacijsko *društvo, Hrvatska enciklopedija*, Leksikografski zavod Miroslav *Krleža* – dostupno 07.02.2020. *na* https://www.enciklopedija.hr/Natuknica.aspx?ID=27411
7. Informatička sigurnost– dostupno 14.02.2020. na https://www.soa.hr/hr/podrucja-rada/informacijska-sigurnost/
8. Kazneni zakon Republike Hrvatske – dostupno 20.02.2020. na https://pravosudje.gov.hr/UserDocsImages/dokumenti/Kazneni%20zakon-neslu%C5%
9. Klasificirani podatak, Zakon o tajnosti podataka – dostupno 15.02.2020. na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka
10. Kibernetička sigurnost – dostupno 10.02.2020. na https://www.soa.hr/hr/podrucja-rada/kiberneticka-sigurnost/
11. Lerner;– dostupno 02.02.2020. na http://www.fags.org.espionage/Ep-Fo/Espionage-and-Intelligence-Early-Historical-Foundations.html
12. Norme informacijske sigurnosti ISO/IEC 27K, –pregled normi iz ISO 27K serije – dostupno 15.06.2020. na https://hrcak.srce.hr/file/113574
13. Podatak, Zakon o tajnosti podataka, – dostupno 05.02.2020.na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka
14. Podatak, Hrvatska enciklopedija – Leksikografski zavod Miroslav Krleža – dostupno 05.02.2020. na https://www.enciklopedija.hr/natuknica.aspx?id=6404
15. Pojam i vrste tajni – dostupno 23.02.2020. na https://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=220761

16. Poslovno-obavještajne službe, industrijska i gospodarska špijunaža u međunarodnoj ekonomiji; Bazdan Zdravko – dostupno 25.02.2020. na https://hrcak.srce.hr/169954
17. Pravila sigurnost informacijskih sustava,– dostupno 10.02.2020. na http://www.veleri.hr/files/datoteke/nastavni_materijali/k_informatika_2/Sigurnost_informacijskih_sustav a_0.pdf
18. Osobni podatak; prema GDPR, Opća uredba o zaštiti podataka, – dostupno 15.03.2020. na https://eurlex.europa.eu/legalcontent/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR
19. SOA – Sigurnosno-obavještajna agencija – dostupno 24.06.2020. na https://www.soa.hr/hr/o-nama/sto-je-soa/
20. Socijalni inženjering – https://www.cis.hr/www.edicija/Socijalniinenjering.html; dostupno 21.02.2020. – Centar informacijske sigurnosti
21. Špijunaža kao oblik ugrožavanja poslovnih informacija – Dejan N. Tepavac; dostupno 12.03.2020.na https://scindeks-clanci.ceon.rs/data/pdf/0042-8426/2019/0042-84261903163T.pdf
22. Špijunaža – dostupno 13.03.2020. na https://www.enciklopedija.hr/natuknica.aspx?id=59838
23. Špijunaža prema Kaznenom Zakonu Republike Hrvatske – dostupno 22.02.2020. na https://www.zakon.hr/z/98/Kazneni-zakon
24. Tuđman, M., Boras, D., Dovedan, Z. (1993). *Uvod u informacijske znanosti* (2. izd.). Zagreb: Školska knjiga–dostupno 14.06.2020. na http://dzs.ffzg.unizg.hr/text/Uvod%20u%20informacijske%20znanosti/
25. Ured vijeća za nacionalnu sigurnost Republike Hrvatske – dostupno 13.06.2020. na https://www.uvns.hr/hr
26. Ustav Republike Hrvatske – Zakon.hr; dostupno 25.04.2020. na https://www.zakon.hr/z/94/Ustav-Republike-Hrvatske
27. Zakon o elektroničkoj ispravi, dostupno 15.02.2020. na https://www.zakon.hr/z/272/Zakon-o-elektroni%C4%8Dkoj-ispravi
28. Zakon o informacijskoj sigurnosti, NN 79/09 – dostupno 17.02.2020. na https://www.zakon.hr/z/218/Zakon-o-informacijskoj-sigurnosti
29. Zakon o tajnosti podataka – Zakon.hr – dostupno 31.01.2020. na https://www.zakon.hr/z/217/Zakon-o-tajnosti-podataka

30. Zakon hr. –kazneni zakon – dostupno 15.02.2020. na https://zakonipropisi.com/hr/zakon/kazneni-zakon/348-clanak-spijunaza
31. Wikipedija –https://hr.wikipedia.org/wiki/Podatak,_informacija,_znanje,_mudrost dostupno 10.02.2020.

11. POPIS SLIKA I GRAFOVA:

12. PRILOZI

Prilog 1. Anketa

Anketa:

1. Jeste li zaposleni u privatnom ili javnom sektoru?
    1. Privatnom sektoru
    2. Javnom sektoru

2. Jeste li upoznati s Uredbom o zaštiti osobnih podataka – General Data Protection Regulation?
    1. Upoznat sam u potpunosti
    2. Upoznat sam djelomično
    3. Nije mi poznato

3. Jesu li Vam osobni podaci bili ukradeni?
    1. Da
    2. Ne

4. Postoji li u tvrtki u kojoj radite pravilnik o zaštiti poslovnih informacija?
    1. Da
    2. Ne postoji
    3. Ne znam, nisam upoznat

5. Jeste li upoznati s pojmom "poslovne tajne"?
    1. Da
    2. Djelomično
    3. Nisam

6. Jeste li upoznati s time koji su podaci klasificirani u tvrtki u kojoj radite?
    1. Da
    2. Djelomično
    3. Nije mi poznato

7. Dali je tvrtka u kojoj radite bila podvrgnuta hakiranju ili krađi podataka?
    1. Da
    2. Ne
    3. Nije mi poznato

8. Jeli računalo s kojeg primate i šaljete podatke zaštićeno sigurnosnom lozinkom?
    1. Da
    2. Ne

9. Primate li na službenom računalu neželjenu poštu (reklame, privatne mailove i slično)?
    1. Da
    2. Ne

10. Jeli Vam poznat pojam gospodarske špijunaže?
    1. Da
    2. Djelomično
    3. Nije mi poznato

11. Jeli tvrtka u kojoj radite sklona prikupljanju informacija i podataka na zabranjen (nelegalan) način?
    1. Da
    2. Nikako
    3. Nije mi poznato

12. Razmjenjujete li poslovne podatke s osobama koje nisu vaši suradnici?
    1. Da
    2. Ponekad
    3. Ne

13. Jeste li upoznati s kaznenim sankcijama vezanim uz neovlašteno odavanje podataka?
    1. Da
    2. Ne
    3. Djelomično

14. Tvrtka u kojoj radim posvećuje pažnju zaštiti informacijske imovine:
    1. Vrlo malu
    2. Samo onda kada je to nužno potrebno
    3. Redovito se ulaže u to područje zaštite

15. Koliko je stara računalna oprema na kojoj radite?
    1. Do 1 godinu
    2. Od 1 do 3 godine
    3. Od 3 do 5 godina
    4. Starije od 5 godina

Sveučilište Sjever
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

UNIVERSITY NORTH

Prijava diplomskog rada

Definiranje teme diplomskog rada i povjerenstva

ODJEL: Odjel za ekonomiju

STUDIJ: diplomski sveučilišni studij Poslovna ekonomija

PRISTUPNIK: Marina Slunjski | MATIČNI BROJ: 0759/336D

DATUM: 13. 03. 2020. | KOLEGIJ: Korporativna sigurnost

NASLOV RADA: Gospodarska špijunaža kao način ugrožavanja klasificiranih informacija

NASLOV RADA NA ENGL. JEZIKU: Economic espionage as a way of compromising classified information

MENTOR: Petar Mišević | ZVANJE: doc. dr. sc.

ČLANOVI POVJERENSTVA:
1. izv.prof.dr.sc. Ante Rončević, predsjednik
2. izv.prof.dr.sc. Anica Hunjet, član
3. doc.dr.sc. Petar Mišević, mentor
4. doc.dr.sc. Mirko Smoljić, zamj.član
5.

Zadatak diplomskog rada

BROJ: 329/PE/2020

OPIS:

Uspješnost i efikasnost organizacije ovisi i o tome koliko su u stanju zaštititi informacijsku imovinu od gubitka i krađe. Organizacije su svakodnevno izložene konkurenciji na globalnom tržištu, u kojem im pravovremeno raspolaganje kvalitetnim informacijama osigurava konkurentsku prednost i bolju poziciju na tržištu. Učestala je pojava da se pojedine organizacije koriste i gospodarskom špijunažom u cilju ostvarivanja određenih poslovnih ciljeva, zadobivanja konkurentske prednosti i ostvarivanja nezakonite financijske dobiti. Gospodarska špijunaža iziskuje puno manje troškove nego što je potrebno uložiti u razvoj i istraživanje. Gospodarskom špijunažom se bave i vlade država i privatne organizacije.
U diplomskom radu je potrebno:
- objasniti pojam i teorijske osnove o gospodarskoj špijunaži, ciljeve i vrste gospodarske špijunaže,
- informacije (poslovne tajne i klasificirani podaci) koje predstavljaju interes u gospodarskoj špijunaži,
- metode i tehnike prikupljanja poslovnih informacija, zakonski propisi koji sankcioniraju kaznena djela iz područja gospodarske špijunaže te načine zaštite informacijske imovine,
- provesti istraživanje vezano uz gospodarsku špijunažu i krađu poslovnih informacija u organizacijama, prikazati i navesti rezultate istraživanja i definirati zaključke diplomskog rada.

ZADATAK URUČEN | POTPIS MENTORA

SVEUČILIŠTE SJEVER

Sveučilište
Sjever

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, Marina Slunjski pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autorica diplomskog rada pod naslovom – Gospodarska špijunaža kao način ugrožavanja klasificiranih podataka, te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Studentica:
(Marina Slunjski)

(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, Marina Slunjski neopozivo izjavljujem da sam suglasna s javnom objavom diplomskog rada pod naslovom – Gospodarska špijunaža kao način ugrožavanja klasificiranih podataka - čija sam autorica.

Studentica:
(Marina Slunjski)

(vlastoručni potpis)