Operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija

Jurjević, Ante

Master's thesis / Specijalistički diplomski stručni

2017

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

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:620973

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ante Jurjević

OPERATIVNA I TEHNIČKA ZAŠTITA POVJERLJIVIH POSLOVNIH I/ILI PROIZVODNIH INFORMACIJA

ZAVRŠNI RAD

Karlovac, 2017.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Ante Jurjević

OPERATIONAL AND TECHNICAL PROTECTION OF CONFIDENTIAL BUSINESS AND/OR PRODUCTION INFORMATION

Final paper

Karlovac, 2017.

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Ante Jurjević

OPERATIVNA I TEHNIČKA ZAŠTITA POVJERLJIVIH POSLOVNIH I/ILI PROIZVODNIH INFORMACIJA

ZAVRŠNI RAD

Mentor:

Davor Kalem, struč. spec. crim

Karlovac, 2017.

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

HRN EN ISO 9001:2009

VELEUČILIŠTE U KARLOVCU

Studij: Specijalistički diplomski stručni studij sigurnosti i zaštite

Usmjerenje: Zaštita na radu

ZADATAK ZAVRŠNOG RADA

Student: Ante Jurjević **Matični broj**: 0420414017

Naziv završnog rada: Operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija.

Opis zadatka: Utvrditi na koji se način provodi zaštita povjerljivih poslovnih i/ili proizvodnih informacija u poduzećima, te koliko je operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija važna za osiguranje adekvatne razine informacijske sigurnosti u poduzeću.

Zadatak zadan:	Rok predaje rada:	Predviđen datum obrane:
09/2016	lipanj 2017	14. 7. 2017

Mentor:	Predsjednik ispitnog povjerenstva:
Davor Kalem, struč. spec. crim	dr. sc. Zlatko Jurac, prof. v. š.

PREDGOVOR II

Ovim putem se želim zahvaliti mojoj obitelji, prijateljima i supruzi koji su mi bili najveća potpora tijekom studiranja, te su u teškim trenutcima školovanja koje zahtjeva mnogo odricanja bili veliki poticaj za daljnji rad i završetak studija.

Zahvaljujem se svom mentoru Davoru Kalemu na pomoći tijekom pisanja diplomskog rada koji mi je svojim stručnim savjetima i kvalitetnim sugestijama uvelike pomogao.

Zahvaljujem se i svim profesorima Veleučilišta u Karlovcu, Odjela Sigurnosti i Zaštite, koji su me u dvije godine školovanja mnogočemu naučili, na način da su svoje znanje i iskustvo kvalitetno prenosili nama studentima i hvala svim ostalim djelatnicima Veleučilišta u Karlovcu na pomoći, ljubaznosti i razumijevanju.

Od srca Vam hvala!

SAŽETAK III

Operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija važna je za osiguranje adekvatne razine informacijske sigurnosti u poduzećima. Motivacija za odabir predmeta istraživanja proizlazi iz činjenice da upravljanje informacijskom sigurnošću postaje sve složenije, a time i važnije uslijed ubrzanog napretka informacijsko-komunikacijske tehnologije, ali i rapidnog porasta računalnog ili kibernetičkog kriminala. Istraživanje je provedeno uporabom sekundarnih izvora podataka iz relevantne literature. Rezultati istraživanja pokazuju kako je na razini poduzeća nužan proaktivan i sustavno razrađen plan informacijske sigurnosti poduzeća kojim se definiraju povjerljivi podaci i način postupanja s istima.

Ključne riječi: intelektualno vlasništvo, poslovna tajna, povlaštene informacije, informacijska sigurnost, UVNS

SUMMARY

Operational and technical protection of confidential business and/or production information is important to ensure an adequate level of information security in enterprises. The motivation for the research subject stems from the fact that information security management is becoming more complex, and thus more important due to the rapid progress of information and communication technologies, and the rapid increase in computer or cybercrime. The study was conducted by using secondary sources of information from the relevant literature. The research results show that it is necessary for companies to develop proactive and systematic plan of information security that defines confidential data and way of dealing with it.

Keywords: intellectual property, trade secret, inside information, information security, UVNS

SADRŽAJ IV

1. UVOD

Informacijska sigurnost postaje temeljni preduvjet uspješnog poslovanja poduzeća u uvjetima porasta uloge intelektualnog vlasništva u stvaranju konkurentske prednosti. Iz tog je razloga ključno razviti plan informacijske sigurnosti poduzeća unutar kojeg su propisani ciljevi, aktivnosti i mjere kojima se postiže sigurnost povjerljivih poslovnih i/ili proizvodnih podataka.

1.1. Problem i predmet istraživanja

Brojna poduzeća u globalnom okruženju izložena su sve većem broju računalnih sigurnosnih incidenata što ukazuje na činjenicu da postoje propusti u sustavu informacijske sigurnosti. Iz opisanog problema proizlazi predmet istraživanja, a to je operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija u poslovanju.

1.2. Ciljevi istraživanja

Opći cilj istraživanja je utvrditi na koji se način provodi zaštita povjerljivih poslovnih i/ili proizvodnih informacija u poduzećima. Iz općeg cilja proizlaze i sljedeći specifični istraživački ciljevi:

- definirati pojam intelektualnog vlasništva i poslovne tajne,
- utvrditi koji je način uređena zaštita klasificiranih podataka na međunarodnoj i nacionalnoj razini,
- istražiti ulogu pojedinih elemenata Plana informacijske sigurnosti poduzeća.

1.3. Metodologija istraživanja

Prilikom provedbe istraživanja korišteni su sekundarni izvori podataka. To su relevantne i recentne knjige, udžbenici, članci te internetske stranice koje obrađuju pitanje informacijske sigurnosti poduzeća.

1.4. Struktura rada

Rad se sastoji od osam cjelina. Nakon uvoda, definiran je i klasificiran koncept intelektualnog vlasništva. Pojam i povijesni razvoj poslovne tajne definirani su u trećoj cjelini, a zaštita poslovne tajne predmet je četvrte cjeline. U petoj cjelini se obrađuju kaznena djela vezana uz odavanje poslovne tajne. Djelatnost Nacionalnog vijeća za sigurnost s naglaskom na operativno-tehničku koordinaciju predmet je šeste cjeline. Uloga i elementi plana informacijske sigurnosti poduzeća opisani su u sedmoj cjelini. Osma cjelina je zaključnog karaktera.

2. POJAM I POJAVNI OBLICI INTELEKTUALNOG VLASNIŠTVA

Intelektualno vlasništvo je skup ekskluzivnih prava na određene kreacije koje predstavlja unikatno pravno sredstvo kojim se postiže uskraćivanje drugima prava da se bez dozvole koriste tim kreacijama. Danas je intelektualno vlasništvo jedini monopol koji društvo prihvaća i podržava.

Intelektualno vlasništvo je sklop prava kojima se štite i potiču ljudska inovativnost i kreativnost. Pod intelektualnim vlasništvom podrazumijevaju se rezultati nematerijalnog, umnog ili intelektualnog ljudskog rada. Iako neopipljivo u fizičkom smislu, intelektualno vlasništvo ima sve karakteristike imovine, pa se ono može kupiti, prodati, licencirati, zamijeniti, pokloniti, založiti, biti predmetom ovrhe, naslijediti kao i svako drugo vlasništvo.

Prema Svjetskoj organizaciji za intelektualno vlasništvo (*engl. WIPO – World International Property Organisation*[1]), intelektualno vlasništvo dijeli se u dvije osnovne skupine[2]:

- industrijsko vlasništvo, koje obuhvaća: patente, žigove, industrijska obličja, oznake zemljopisnog podrijetla proizvoda i planove rasporeda integriranih sklopova,
- autorsko i srodna prava: autorsko pravo odnosi se na intelektualne tvorevine kao što su osobito: književna djela, računalni programi, glazbena djela, dramska i dramsko-glazbena djela, koreografska i panto-mimska djela, djela likovnih umjetnosti iz područja slikarstva, kiparstva i arhitekture, djela primijenjenih umjetnosti, fotografska djela, kinematografska djela, prijevodi i druge prerade djela, zbirke djela i baze podataka,
- srodna prava odnose se na: izvedbe umjetnika-izvođača, fonograme i videograme, emitiranja radija i televizije.

U suvremenom poslovnom okruženju razvijaju se i brojni noviji oblici prava poput poslovne tajne. Taj se proces i nadalje intenzivno nastavlja. Intelektualno vlasništvo, u širem smislu, tako obuhvaća i zaštitu od nepoštenog tržišnog natjecanja, zaštitu povjerljivih podataka,

[1] Svjetska organizacija za zaštitu intelektualnog vlasništva predstavlja globalni forum za politike i usluge intelektualnog vlasništva te ima snažnu nadnacionalnu informacijsku i kooperacijsku funkciju. Osnovana je 14.07. 1967. U svrhu mjerenja vrijednosti intelektualnog vlasništva, WIPO je utemeljila globalni inovacijski indeks.

[2] Benčić, Zvonko. (2001). Intelektualno vlasništvo, suvremeni resurs za postizanje globalne tehnološke kompetitivnosti. *Automatika 42*, 3-4, 199-206.

poslovne tajne, zaštitu tvrtke, znanje i iskustvo (know-how), zaštitu biljnih sorti itd. Za zaštitu povjerljivih podataka, poslovnu tajnu, zaštitu tvrtke, te zaštitu znanja i iskustava ne postoji posebni formalizirani postupci zaštite. Opseg i djelotvornost zaštite tih prava ovisi o načinu čuvanja njihovih sadržaja i ugovorima između strana kojima su ti sadržaji dostupni.

Da bi se efikasno zaštitilo i ostvarivalo pravo iz intelektualnog vlasništva, potrebno je taj proces sustavno planirati. Postupci za zaštitu intelektualnog vlasništva često su financijski vrlo zahtjevni pogotovo ako je riječ o rješavanju sporova ili traženju zaštite u drugim zemljama i drugim pravnim sustavima ili na međunarodnim arbitražnim sudištima. Zbog toga je dobra praksa svakog poslovnog subjekta da unaprijed predvidi moguće situacije i slučajeve u kojima bi moglo doći do pokretanja postupka s područja intelektualnog vlasništva i u skladu sa svojim potrebama pripremi sredstva za uspješno vođenje i okončanje postupka. Biti unaprijed pripremljen može biti ključno za uspjeh eventualnog postupka, koji zauzvrat može biti presudan za daljnje poslovanje. Isto tako, osim osiguranja financijskih sredstava, dodatan potrebni resurs su zaposlenici ili vanjski suradnici poput odvjetnika, zastupnika s područja industrijskog vlasništva i drugih koji mogu biti od ključnog značaja za uspjeh postupaka i minimizaciju troškova.

2.1. Autorsko i srodna prava

Autorsko pravo i srodna prava su prava koja imaju svi autori autorskih djela, a to mogu biti književna, znanstvena i umjetnička djela. Nositelji autorskih i srodnih prava imaju isključivu mogućnost korištenja djela, a djelo se može ustupiti drugima na korištenje uz isključivu dozvolu autora ili drugog nositelja autorskog prava (primjerice nasljednika autora). Autorska i srodna prava razlikuju se od drugih oblika intelektualno vlasništvu po tome što autora štiti sam čin stvaranja znanstvenog, književnog ili umjetničkog djela te stjecanje autorskog prava nije ovisno o provedbi posebnih postupaka stjecanja, odnosno registracije autorskog prava kao oblika intelektualnog vlasništva. „Komercijalni položaj autora počeo se mijenjati tek u 19. stoljeću s masovnom proizvodnjom papira, boljim mogućnostima tiskanja, opismenjavanjem i pojavom profesionalnih pisaca, dok razvojem masovnog tržišta za tiskanu

i kasnije snimljenu i emitiranu riječ, autori dobivaju ekonomsku ulogu kakvu nikada prije nisu imali.“[3]

Područje srodnih prava ubrzano se razvilo u proteklih 50 godina. Srodna prava razvila su se uz autorsko pravo i najčešće su vezana uz omogućavanje priopćavanje autorskog djela javnosti. Autorsko pravo prvotno se razvilo u francuskom pravu te je postupno prošireno na europsko pravo, a danas predstavlja vrlo značajan izvor povlaštenog pravnog i ekonomskog položaja autora na globalnoj razini.

2.2. Prava industrijskog vlasništva

Prema klasifikaciji Svjetske organizacije za industrijsko vlasništvo, pojam industrijskog vlasništva obuhvaća: 1) patente, 2) žigove i industrijska obličja, 3) oznake zemljopisnog podrijetla proizvoda i 4) planove rasporeda integriranih sklopova.

Ad. 1) "Patent je dokument koji izdaju državni uredi nakon podnošenja zahtjeva, koji opisuje izum i stvara pravne preduvjete u kojima patentirani izum mogu biti eksploatirani (proizvedeni , korišteni, prodani ili uvezeni) uz odobrenje vlasnika patenta. Vijek trajanja patenta uobičajeno je ograničen na period od 20 godina.“[4] Patent predstavlja pravo koje proizlazi iz intelektualnog vlasništva izumitelja. Pravni proces zaštite izuma putem patenta koji predstavlja industrijsko vlasništvo u Republici Hrvatskoj provodi Državni zavod za intelektualno vlasništvo kao ovlaštena agencija. Zavod osigurava svim prijaviteljima izuma stručnu potporu u procesu priznavanja i odobravanja patenta te, u konačnici, dodjeljuje prava na patente kojima se izumitelju dodjeljuje pravna zaštita i priznaje vlasništvo nad izumom (invencijom). U uvjetima globalna konkurencije, osobito je važno naglasiti da je Državni zavod za intelektualno vlasništvo u RH dio mreže sličnih zavoda koji djeluju diljem svijeta te blisko surađuje s ostalim Zavodima putem Svjetska organizacije (WIPO). Na ovaj način olakšava se proces pravne zaštite izuma, proces patentiranja izuma, na nadnacionalnom nivou.

[3] Pažur, Ivana. (2004). Autori znanstvenih radova i autorsko pravo. *Vjesnik bibliotekara Hrvatske*, *47*(1-2), 95-108.
[4] Bhawan, Anusandhan. (2001). Intellectual property rights and the Third World. *Current Science*, *81*(8), 955-965.

U Hrvatskoj je postupak prijave i odobravanja patenta uređen Zakonom o patentu[5]. Sukladno Zakonu prijava patenta mora sadržavati: zahtjev za priznavanje patenta, opis izuma, zahtjev za zaštitu izuma (patentni zahtjev), crteže koji se pozivaju na opis izuma te sažetak izuma. Nakon postupka priznavanja patenta, patent se upisuje u registar. Kriteriji koji se koriste prilikom definiranja koji izum može, a koji ne može biti patentiran su da izum mora biti nov te mora imati industrijsku vrijednost (dakle, izum koji se može patentirati je onaj koji se može proizvesti u bilo kojoj industrijskoj grani, dok se izumi koji postoje samo na razini teorijskog otkrića ne mogu patentirati). Patent je kategorija intelektualnog vlasništva koja generira ekonomsku korist za izumitelja, odnosno nositelja patenta. Nažalost, proces patentiranja izuma se u Hrvatskoj rijetko provodi na institucionalnoj razini, a patente prijavljuju uglavnom pojedinci što ukazuje na zanemarenost intelektualnog vlasništva kao ekonomske kategorije. Kada je patent odobren kao dokument koji nositelju omogućuje pravo na eksploataciju izuma, on postaje ekonomska kategorija koja se može egzaktno izraziti u bilanci poduzeća kao dugotrajna nematerijalna imovina.

Ad. 2) Prema čl. 2. Zakona o žigu[6], kao žig se može zaštititi svaki znak koji se može grafički prikazati, osobito riječi, uključujući osobna imena, crteže, slova, brojke, oblike proizvoda ili njihova pakiranja, trodimenzionalne oblike, boje, kao i kombinacije svih naprijed navedenih znakova, pod uvjetom da su prikladni za razlikovanje proizvoda ili usluga jednoga poduzetnika od proizvoda ili usluga drugoga poduzetnika. Dakle, prema ovoj zakonskoj definiciji žig je subjektivno pravo iz područja industrijskog i intelektualnog vlasništva, koje za predmet zaštite uzima znak kojim nositelj žiga označava svoje robe ili usluge u gospodarskom prometu, čineći ih različitima od iste ili slične robe ili usluga drugog poduzetnika. Žigom se dakle mogu štititi znakovi, osobito riječi, uključujući osobna imena, crteže, slova, brojke, oblike proizvoda ili njihova pakiranja, trodimenzionalne oblike, boje, pod uvjetom da su razlikovni, kao i kombinacije svih naprijed navedenih znakova. Nositelj žiga ima sukladno odredbi čl. 7. ZOŽ-a isključivo pravo na obilježavanje žigom proizvoda ili usluga za koje je žig priznat i isključivo pravo uporabe žiga za te proizvode ili usluge. Nositelji žiga mogu biti pravne ili fizičke osobe koje se bave registriranom gospodarskom, proizvodnom i/ili uslužnom djelatnošću.[7]

[5] Zakon o patentu, pročišćeni tekst zakona, NN 173/03, 87/05, 76/07, 30/09, 128/10, 49/11, 76/13.
[6] Zakon o žigu, pročišćeni tekst zakona NN 173/03, 54/05, 76/07, 30/09, 49/11.
[7] Zlatović, Dragan. (2009). „Pravni aspekti parodije "i intelektualno vlasništvo. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, *30*(1), 725-766.

Ad. 3) Označavanje prehrambenih proizvoda oznakama zemljopisnog porijekla i izvornosti uređeno je na nadnacionalnoj razini, odnosno na razini Europske unije, i to Propisom o zaštiti geografskog porijekla za poljoprivredne i prehrambene proizvode (No. 2081/92) koji je stupio na snagu 1993. godine. Navedene oznake imaju za cilj jačanje konkurentnosti proizvoda na tržištu, i to osobito na međunarodnom tržištu. Oznaka zemljopisnog porijekla i oznaka izvornosti predstavljaju pojavne oblike industrijskog vlasništva kojem je cilj zaštititi proizvode s jedinstvenim značajkama kakvoće. Navedeni oblici industrijskog vlasništva osiguravaju nositeljima navedenog oblika vlasništva stjecanje pozitivne razlikovne prednosti olakšavaju provedbu procesa zaštite proizvoda žigom ili *trademarkom.*[8] Na osnovu garancije kvalitete koju pružaju oznake zemljopisnog porijekla i oznake izvornosti, potrošači su spremni platiti premijsku cijenu pri kupnji istih. „Oznaka zemljopisnog podrijetla je naziv zemljopisnog područja ili neki drugi znak koji ukazuje da neki proizvod ili usluga potječe iz određenog zemljopisnog područja, te da posjeduje određenu kvalitetu i svojstva koja se pripisuju tom podrijetlu.“[9] Kako bi se proizvoda zaštitio navedenom oznakom, nužno je da potječe iz regije kojom je označen te da ima razinu kakvoće i ugleda koja se pripisuje prehrambenim proizvodima iz te regije. Odredbe o zaštiti zemljopisnog porijekla i izvornosti zajamčene su odredbama Pariške konvencije[10], Lisabonskog sporazuma[11] kao i TRIPS *(engl. The Agreement on Trade-related aspects of Intelectual Property Rights)*[12] sporazumom koji je aneks ugovora o osnivanju Svjetske trgovinske organizacije.

Ad. 4) Četvrtu skupinu prava industrijskog vlasništva čine usko specijalizirana prava, tzv. *sui-generis* ekskluzivna prava, poput dizajna elektroničkih sklopova i prava vezanih uz informacije iz baza podataka.[13]

[8] Duraković, Mia (2009). Pregled razvoja autorskog prava u Republici Hrvatskoj s naglaskom na promjene uvjetovane usklađivanjem s pravnom stečevinom EU. *Zbornik radova Pravnog fakulteta u Splitu*, *46*(3), 613-630.

[9] Oznaka zemljopisnog porijekla. Preuzeto s: http://www.dziv.hr/hr/intelektualno-vlasnistvo/oznake/ (25.11.2016.)

[10] Pariška konvencija o zaštiti industrijskog vlasništva iz 1883. godine

[11] Lisabonski sporazum je sporazum kojim se mijenja i dopunjava Ugovor o Europskoj uniji i Ugovor o osnivanju Europske ekonomske zajednice (EEZ).

[12] TRIPS sporazum je sporazum o trgovinskim aspektima prava intelektualnog vlasništva.

[13] Katulić, Tihomir. (2005). Intelektualno vlasništvo danas. *Edupoint: časopis o primjeni informacijskih tehnologija u obrazovanju*, *5*(36).

3. POSLOVNA TAJNA KAO OBLIK INTELEKTUALNOG VLASNIŠTVA

Poslovna tajna predstavlja povjerljive informacije od velike komercijalne važnosti, a to su poslovne informacije i know-how. Otkrivanje poslovne tajne predstavlja nepoštenu konkurenciju. Poštena igra na tržištu se ne može osigurati samo zaštitom industrijskog vlasništva pa su doneseni zakoni koji štite proizvođače i potrošače od nepoštene konkurencije. Kategorije djela nepoštene konkurencije su stvaranje zabune (korištenje sličnog izgleda proizvoda ili sličnog žiga), krivo navođenje (stvaranje krivog dojma o proizvođaču ili njegovim uslugama, diskreditiranje konkurencije (iznošenje netočnih tvrdnji o konkurenciji), odavanje tajnih podataka i usporedno reklamiranje (iznošenje podataka da je neki proizvod bolji od sličnog proizvoda na tržištu).[14]

3.1. Pojam i povijesni razvoj koncepta poslovne tajne

Poslovna tajna je način postupanja, poslovna praksa, „know-how" ili neka druga informacija koja pomaže poslovnim subjektima da se natječu s konkurencijom. Poslovna tajna je onaj element poslovanja koji utječe na uspjeh nekog poslovnog poduhvata kada su svi ostali resursi ekvivalentni, to je ono specijalno znanje koje omogućava jednom poslovnom subjektu da se nametne drugima i stekne konkurentsku prednost na tržištu.

Poslovna tajna je podatak koji je kao poslovna tajna određen zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavlja proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te drugi podatak zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.[15] Prema Zakonu o tajnosti podataka[16], podatak se može klasificirati sa četiri stupnja tajnosti, a to su vrlo tajno, tajno, povjerljivo i ograničeno.

[14] Mintas – Hodak, Ljerka. (2010). *Pravno okruženje poslovanja*, Zagreb: Mate, str. 398.-402.
[15] Cvitanović, Leo, Novoselac, Petar. (2002). *Rječnik kaznenog prava*. Zagreb: Masmedia, str. 321.
[16] Zakon o tajnosti podataka, NN 79/07.

Poslovna tajna obuhvaća sve podatke određene općim aktom društva ili propisom ali u širem smislu i podatke djelovanja nekog subjekta čije bi priopćenje trećoj osobi moglo nanijeti štetu interesima i poslovnom ugledu društva. Takvi podaci mogu biti različite isprave i činjenice koje se odnose na proizvodni postupak, sastojke određenog proizvoda, popis i odnose s klijentima, sadržaj ugovora, poslovnu politiku, podatke sadržane u internom izvješćivanju itd. Poslovnu tajnu dužne su čuvati sve osobe zaposlene u društvu, te članovi društva osoba, članovi uprave i nadzornog odbora kapitalnih društava, i to i za vrijeme radnog odnosa, i nakon prestanka radnog odnosa, odnosno dužnosti koje obnašaju. Poslovnu tajnu mogu trećim ovlaštenim osobama (mjerodavnim organima i sl.) na njihov opravdani zahtjev otkriti samo osobe ovlaštene općim aktom društva.

Točna definicija poslovne tajne često varira od pravnog sustava do pravnog sustava. Ipak, može se slobodno zaključiti kako postoje neke osobine koje su zajedničke. Tako se može zaključiti kako se većina pravnih poredaka slaže da je poslovna tajna takva informacija koja nije poznata stručnoj javnosti, koja na određeni način donosi gospodarsku korist svom nositelju, te čiju tajnost nositelj pokušava u razumnim okvirima sačuvati. Poslovne tajne se nalaze obično u slijedećim oblicima:[17]

- računala, formalni dokumenti, skice i radni papiri,
- interno korespondiranje,
- državne kartoteke,
- publikacije i ostali javni izvori informacija,
- formalni i neformalni sastanci i
- svakodnevni razgovori

U anglosaksonskoj pravnoj literaturi, pojam poslovna tajna odnosi se na proces, formulu, dizajn, praksu, instrumente, skup informacija ili obrazaca na temelju kojih poduzeće može zadržati svoju konkurentsku prednost. Poslovna tajna obično se veže uz pojam „povjerljive informacije“, a u pravnu praksu je uvedena u Engleskoj 1817. godine u slučaju Newbery protiv Jamesa. Predmet spora bila je uporaba naziva proizvoda Dr. James od strane proizvođača Newbery-a.

[17] Zemljić, Marija. (2014). *Industrijska špijunaža* (završni rad). Varaždin: FOI, str. 34.

Postoje tri važne sastavnice poslovne tajne sukladno anglo-saksonskom pravu, prema kojem je poslovna tajna informacija koja[18]:

- nije poznata javnosti,

- sadrži neku vrstu potencijalne financijske koristi za njezina imatelja i

- zahtijeva ulaganje resursa kako bi se zaštitila i održala na povjerljivoj razini.

Općim aktom se ne može odrediti da se svi podaci koji se odnose na poslovanje pravne osobe smatraju poslovnom tajnom niti se poslovnom tajnom mogu odrediti podaci čije priopćavanje nije razložno protivno interesima te pravne osobe. Poslovnom tajnom ne mogu se odrediti podaci koji su od značenja za poslovno povezivanje pravnih osoba niti podaci koji se odnose na zaštićeno tehničko unapređenje, otkriće ili pronalazak.

Poslovne tajne nisu zaštićene zakonima na isti način poput žigova ili patenata (jer ne prolaze proces registracije), a nisu niti predmet javnih ili manje javnih registara poput onih koji se primjerice vode pri hrvatskom Državnom zavodu za intelektualno vlasništvo. Jedna od osnovnih karakteristika ove vrste intelektualnog vlasništva zacijelo je činjenica da se poslovna tajna štiti tako da se niti u kojem trenutku ne odaje. Ovo je fundamentalna razlika prema ostalim vidovima intelektualnog vlasništva, a najviše prema žigovima i patentima.

Poslovne su tajne zakonom zaštićene, a praksa mnogih država, pogotovo onih angloameričkog pravnog kruga (iako se to počinje pojavljivati i u nas) govori i o čestoj upotrebi ugovora o tajnosti podataka, odnosno tzv. Non-Disclosure Agreements - NDA (ugovor o neotkrivanju) koji za stranke donose vrlo rigorozne financijske kazne u slučaju odavanja tajni.[19] Takvi se ugovori često primjenjuju i tokom pregovora prije zaključenja neke poslovne transakcije, pogotovo ako ugovorne strane ne dođu do sporazuma.[20] Isto tako, NDA ugovori su i instrument za prenošenje tajnih znanja i informacija, kako bi se kontroliralo njihovo daljnje stavljanje u promet.

[18] Trade Secret. Preuzeto s: http://www.yellowhours.com/store_2919343/Trade-Secret_269-329-1939_Portage_Michigan_USA.html (19.11.2016.)

[19] Carlsson, Bo, Fridh, Ann- Charlotte. (2002). Technology transfer in United States universities. *Journal of Evolutionary Economics*, *12*(1-2), 199-232.

[20] Jedan od primjera neovlaštenog otkrivanja poslovnih tajni je krađa 100.000 povjerljivih dokumenata koje su bivši zaposlenici otkrili prilikom prelaska iz tvrtke AMD u konkurentsku tvrtku Nvidia. Stoga je tvrtka AMD tužila bivše zaposlenike za krađu patenata.

Zbog ranjivosti i relativno laganog otkrivanja poslovnih tajni pomoću zakonitih i manje zakonitih postupaka, ova vrsta intelektualnog vlasništva prilično je osjetljiva materija. U doba kada industrijska špijunaža uzima maha zahvaljujući brojnim tehnološkim sredstvima koja nikad nisu bila toliko raširena i dostupna kao danas, teško je očekivati da će bilo koji način postupanja, poslovna praksa ili „know-how" dugo trajati.

Osim trgovačkih društava koja ulažu znatne napore u očuvanje tajnosti svojeg poslovanja, u posljednje vrijeme velike napore ulažu i zakonodavci. Samo u Sjedinjenim Državama, zemlji specifične pravne tradicije koja nove zakone donosi rijetko i vrlo oprezno, u proteklom je desetljeću doneseno nekoliko novih propisa koji štite sve oblike poslovne tajne, a istovremeno podižu industrijsku špijunažu na razinu kaznenog djela kažnjivog po federalnim zakonima što je jasan signal inače vrlo pragmatičnog i konkretnog zakonodavca.

Poslovna tajna i pravo na razlikovne oznake u odnosu na konkurenciju bili su poznati instituti još u rimskom pravu. Naime, rimski je vlasnik svojim znakom bio zaštićen od nepoštene konkurencije drugih vlasnika. Smatra se da je institut čuvanja poslovne tajne u rimskom pravu uveden aktom „actio servi corrupti" ili aktom o koruptivnim akcijama. Tu ideju predstavio je 1929. godine A. Arthur Schiller[21] u članku „*Trade Secrets and the Roman Law; the Actio Servi Corrupti"*[22]. Ovim aktom, Rimljani su štitili svoje društvo od krađe i oštećenja imovine.

U 19. stoljeću, Zakon o poslovnoj tajni donesen je u Engleskoj 1817. godine. Ovim zakonom stvaraju se temelji razvoja modernog koncepta Zakona o poslovnoj tajni. Prvi slučaj neovlaštenog objavljivanja poslovne tajne dogodio se 1820. godine u slučaju Yovatt protiv Winyarda.[23] Autor Yovatt je smatrao kako je Winyard neovlašteno kopirao informacije iz njegove osobne knjige, konkretno Yovattove formule i instrukcije. Sudac Chancellor je presudio u korist Yovatta naglasivši da je Winyard prekršio načela povjerenja i diskrecije te je zabranio Winyardu objavu formula i instrukcija koje je neovlašteno preuzeo. Zakon o poslovnoj tajni uvozi se u Sjedinjene Države iz Engleske 1868. godine. Zakon o poslovnim tajnama dalje se razvijao na teritoriju Sjedinjenih američkih država. 1939. godine, u SAD-u se uvodi naknada štete za one koji prekrše obvezu čuvanja poslovne tajne. Danas se samo četiri države - Massachusetts, New Jersey, New York, i Texas - još uvijek oslanjaju na navedeni zakon.

[21] Abraham Arthur Schiller (1902-1977) bio je profesor prava na Sveučilištu Columbia od 1928. do smrti. Specijalizirao se za rimsko pravo, pravo afričkih zemalja, pravo zemalja u razvoju i vojno pravo.
[22] Watson, Alan. (1996). Trade Secrets and Roman Law: The Myth Exploded. *Tul. Eur. & Civ. LF*, *11*, 1.
[23] The property rights – origin of private rights. Preuzeto s: https://fee.org/articles/the-property-rights-origins-of-privacy-rights/ (20.11.2016.)

Iako se institut poslovne tajne prvenstveno razvio u okviru običajnog prava, u Sjedinjenim Američkim Državama je 1974. godine Vrhovni sud donio odluku u slučaju Kewanee Oil korporacije protiv Bicron korporacije koja rješava to pitanje i omogućava da države slobodno razvijaju svoje zakone o poslovnoj tajni. Kewanee Oil Corporation je u svojstvu tužitelja poduzela raznovrsne pravne radnje kojima je tražila zabranu uporabe i naknadu štete zbog zloupotrebe poslovnih tajni. Okružni sud je primijenio državni zakon u Ohiju i odobrio trajnu zabranu protiv otkrivanja dvadeset od ukupno četrdesetak poslovnih tajni. 1996. godine 46 američkih država je usvojilo UTSA (*Uniform trade secret law*) ili Jedinstveni zakon o poslovnoj tajni. Taj zakon kriminalizira industrijsku špijunažu koja postaje federalni zločin. Zakon sadrži dvije odredbe kojima kriminalizira povredu čuvanja poslovne tajne[24]:

- kriminalizira krađu poslovnih tajni u korist stranih sila,
- kriminalizira krađu poslovne tajne u komercijalne ili gospodarske svrhe.

Kada su u srpnju 2007. doneseni Zakon o tajnosti podataka i Zakon o informacijskoj sigurnosti, RH je napokon dobila novi, suvremen i vremenu primjeren sustav zaštite tajnih podataka od državnog značenja.

3.2. Izuzeci od čuvanja poslovne tajne

Na sjednicama poduzeća, često je nužno podijeliti poslovne tajne, a ovlaštena osoba upozorenjem naglašava sudionicima sjednica da su određeni podaci tajni i da ih je potrebno čuvati. Navodi se kako osoba koja objavljuje poslovnu tajnu s ciljem zaštite svog radnog mjesta nije počinila povredu čuvanja poslovne tajne. Ova se napomena posebno odnosi na tzv. zviždače, koji svojim postupcima otkrivaju neetične postupke u poduzeću gdje su zaposleni. Zviždači su uglavnom osobe zaposlene unutar tvrtke, a koje svoje zamjerke o postupanju u poslovanju iznose kolegama na radnom mjestu ili svojim nadređenima. Ukoliko se radi o vanjskim zviždačima, isti izvještaje predaju tijelima van tvrtke, primjerice medijima, pravnicima, sudskim instancama i drugim tijelima zakona. Kojoj će se instituciji obratiti eksterni zviždač ovisi uglavnom o prirodi i ozbiljnosti prikupljene informacije.

[24] Legal Information Institute. Preuzeto s: https://www.law.cornell.edu/wex/trade_secret (20.11.2016.)

„Okvir za protukorupcijske mjere u Republici Hrvatskoj svoje uporište nalazi u odredbama kaznenog zakonodavstva, Zakona o USKOK-u te međunarodnim pravnim instrumentima kojima je Republika Hrvatska pristupila. Ključni međunarodni dokumenti su Kaznenopravna konvencija o korupciji, Dodatni protokol uz Kaznenopravnu konvenciju o korupciji, Građanskopravna konvencija o korupciji, te Konvencija Ujedinjenih naroda protiv korupcije.“[25] Ostala zakonska regulativa kojom se u Hrvatskoj određuje ovo područje je: Zakon o sprečavanju sukoba interesa u obnašanju javnih dužnosti, Zakon o odgovornosti pravnih osoba za kaznena djela, Zakon o zaštiti svjedoka, Zakon o sprječavanju pranja novca, Zakon o međunarodnoj pravnoj pomoći u kaznenim stvarima, te Zakon o pravu na pristup informacijama.

[25] Borba protiv korupcije. Preuzeto s: http://www.policija.hr/32.aspx (23.11.2016.)

4. ZAŠTITA POSLOVNE TAJNE U POSLOVNOM PROCESU

Zaštita poslovne tajne u poslovnom procesu može se osigurati na tri načina opisana u nastavku rada, a to su klauzula o poslovnoj tajni u internim aktima poduzeća, Ugovor o povjerljivosti podataka (*engl. NDA – Non-Disclosure Agreement*) i zaštita tajnih podataka sustavom informacijske sigurnosti. Važan aspekt tajnosti u poslovnim procesima ima i zaštita osobnih podataka. Poslovna tajna je važan pojam u poslovanju koji se opisuje i u samom Ustavu RH. Sigurnost i tajnost osobnih podataka je ustavno pravo koje je zajamčeno svim građanima sukladno čl. 37. Ustava RH.[26]

4.1. Klauzula o poslovnoj tajni u internim aktima poduzeća

Poslovna tajna je prvenstveno pitanje samoregulacije unutar poslovnog subjekta. Regulacija poslovne tajne postaje sve važnija jer važnost informacija postaje ključna za poslovanje, a država će je sve manje regulirati prisilnim normama. Trenutno stanje u Hrvatskoj, supsidijarna[27] primjena zastarjelog i nikada dobro uređenog propisa iz 1996., samo je privremeno i loše rješenje[28]. U pravilu se akt donosi u obliku pravilnika, kojim se detaljno uređuju pravni odnosi, pa i tehnička pravila u vezi čuvanja tajnih dokumenata. Osobito je važno definirati što ulazi u poslovnu tajnu i kako se označava, tko je ovlašten za određivanje i što je poslova tajna te kada podatak prestaje biti poslovnom tajnom.

Svako poduzeće koje želi zaštititi tajnost i povjerljivost svojih podataka mora u svojim internim aktima navesti i klauzulu u poslovnoj tajni, koja se, u pravilu uvodi i u pojedinačne (posebno u ugovor o radu) i u opće akte. Pri tome je preporučljivo imati i odredbe o tzv. ugovornoj kazni, koju je prilično jednostavno naplatiti jer se ne zahtijeva dokazivanje štete, nego samo da je netko neovlašteno otkrio poslovnu tajnu. Makar to u zakonu izravno ne stoji, „sudska je praksa zauzela stajalište da su najozbiljnije (najviše) zatvorske kazne uvjetovane nastalom štetom od najmanje 300.000 kuna. Takvih postupaka nema mnogo, i to prije zato što

[26] Ustav Republike Hrvatske, pročišćeni tekst NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.
[27] Supsidijarna primjena označava primjenu određene zakonske norme tek kada i ako ne postoji zakonska norma koja ima prednost. Supsidijarna primjena zakona podrazumijeva primjenu onih odredbi općeg zakona koje nisu u suprotnosti s posebnim zakonskim odredbama.
[28] Mintas – Hodak, Ljerka.: *op.cit.*, str. 407.

stupanj znanja i svijesti koliko je to opasno nije visok nego zato što se poslovne tajne ne zlorabe.“[29]

4.2. Ugovor o povjerljivosti podataka (NDA)

Ugovor o povjerljivosti podataka ili *non-disclosure agreement* (NDA) je dvostrani ugovor kojim se uređuje status povjerljivih podataka (ne samo poslovnih tajni). Ugovorne stranke potpisivanjem ovog ugovora potvrđuju da neće trećim stranama iznositi povjerljive podatke o međusobnoj poslovnoj suradnji.[30] Zajednički cilj ugovornih strana je da pod uvjetima Ugovora o povjerljivosti podataka je da osiguraju zaštitu povjerljivih podataka zadržavajući pritom sposobnost obavljanja svojih poslovnih aktivnosti. Ugovorne strane su suglasne da će se primjenjivati uvjeti NDA ugovora kada jedna ugovorna strana (obznanitelj) obznani Podatke drugoj ugovornoj strani (primatelju). Podaci se mogu obznaniti u pisanom obliku; dostavom predmeta; iniciranjem pristupa Podacima, kao npr. podacima sadržanima u bazi podataka, usmenim ili vizualnim predstavljanjem.

Povjerljivi podaci moraju biti označeni restriktivnom oznakom ugovorne strane koja iznosi podatke. Ako Podaci nisu označeni takvom oznakom/legendom ili su obznanjeni usmeno, podatak može biti identificiran kao povjerljiv u trenutku obznanjivanja. Od primatelja se NDA ugovorom zahtijeva diskreciju u cilju izbjegavanja obznanjivanja, objavljivanja ili širenja povjerljivih podataka druge ugovorne strane kao i prilikom postupanja s vlastitim sličnim podacima koje ne želi obznaniti, objaviti ili širiti.

Primatelj povjerljivih podataka može obznaniti iste svojim zaposlenicima koji ih trebaju znati, kao i zaposlenicima bilo koje pravne osobe koju kontrolira, pod čijom je kontrolom, ili s kojom je pod zajedničkom kontrolom, a koji ih trebaju znati. Primatelj mora osobama kojima obznanjuje povjerljive podatke potpisati pisani sporazum da osigura da ta strana postupa u skladu s NDA Ugovorom. Primatelj može obznaniti podatke u mjeri u kojoj je na to obvezan primjenjivim pravom. Međutim, primatelj je dužan obznanitelju dati promptnu obavijest kako bi mu razumno omogućio pribavljanje naloga o zaštiti podataka. NDA ugovorom propisuje se vrijeme trajanja tajnosti kao i izuzeće od obveze tajnosti.

[29] Za odavanje poslovne tajne i deset godina zatvora. Preuzeto s: http://lider.media/arhiva/32127/ (20.11.2016.)
[30] Mintas – Hodak, Ljerka.: *op.cit*., str. 409.

Tipični sastojci ugovora o povjerljivosti su[31]:

- definiranje ugovornih strana – slično kao i u svakom drugom ugovoru on mora sadržavati ugovorne strane;
- definiranje opsega ugovora – odnosno opsega povjerljivih podataka čija se zaštita ugovara,
- izuzeci na koje se ne primjenjuje ugovor o povjerljivosti,
- rok čuvanja povjerljivih podataka,
- obveze primatelja u vezi s povjerljivim informacijama,
- ugovaranje nadležnog suda ili arbitraže za slučaj kršenja Ugovora o povjerljivosti podataka.

4.3. Zaštita tajnih podataka sustavom informacijske sigurnosti

Prema Zakonu o informacijskoj sigurnosti[32], 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. Mjere informacijske sigurnosti su opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.

Uspostava sustava povjerenja prema osobama čini bitan i nužan element provedbe sigurnosne politike. Tako se, primjerice, u državnoj upravi, osobama koje pristupaju klasificiranim podacima, na temelju sigurnosne provjere izdaje sigurnosno uvjerenje (certifikat) odgovarajućeg stupnja tajnosti, usklađenog sa stupnjem tajnosti klasificiranih podataka kojima trebaju pristupati. Postupak sigurnosne provjere inicira državno tijelo, za svog zaposlenika koji u okviru djelokruga svog radnog mjesta ima potrebu pristupa (engl. *need - to - know*) određenim kategorijama klasificiranih podataka kao što su NATO ili EU klasificirani podaci, ili pojedinim nacionalnim kategorijama klasificiranih podataka, kao što su, primjerice, podaci o klasificiranim ugovorima u okviru nabave (princip razdvajanja nadležnosti).

[31] Mintas – Hodak, Ljerka.:*op.cit*., str. 410.
[32] Čl. 2. Zakona o informacijskoj sigurnosti, NN 79/07.

Izdavanjem sigurnosnog certifikata osobi te potpisivanjem izjave osobe o tome da je svjesna svojih prava i obveza u području tajnosti podataka, rukovoditelji pojedinih službi izdaju formalno odobrenje za pristup određenom fondu klasificiranih podataka ili odobravaju pristup na neformalnoj razini, razvođenjem pojedinog klasificiranog podatka osobi koja ima odgovarajući certifikat i poslovno zaduženje.

Ovakav koncept provedbe sigurnosne politike razvio se tijekom sedamdesetih i osamdesetih godina prošlog stoljeća, isprva u najrazvijenijim državama svijeta, a kasnije i u ostalim demokratskim državama. Tako dolazi do stvaranja jasne i transparentne regulative vezane uz principe klasificiranja podataka, čime se tajni dio tadašnjeg informacijskog prostora transformirao u relativno transparentno, jasno ograničeno područje, odnosno u domenu klasificiranih podataka.

Iznimno brz razvoj informacijske i komunikacijske tehnologije te brzo širenje interneta tijekom devedesetih godina, stvara svijest o specifičnosti zaštite osobnih podataka, što je ubrzo postalo globalna paradigma razvijenog svijeta. Na taj je način domena osobnih podataka postala posebno značajna u informacijskom prostoru jer su korisnici osobnih podataka i državna tijela i druge pravne osobe, a osobni podaci često se razmjenjuju u okviru međunarodne suradnje različitih država.

U RH je povučena poveznica između *Zakona o pravu na pristup informacijama*[33] i *Zakona o tajnosti podataka* (NN 79/07) te je u članku 16. *Zakona o tajnosti podataka* uvedena obveza da vlasnik klasificiranog podatka, koji je od interesa za javnost, provodi ocjenjivanje razmjernosti dva sukobljena interesa tajnosti i javnosti te da u okviru tog procesa zatraži mišljenje Ureda Vijeća za nacionalnu sigurnost, kao središnjeg državnog tijela za informacijsku sigurnost (engl. *National Security Authority - NSA*). *Zakon o tajnosti podataka* u članku 16. stavak 3., ostavlja otvorenim mogućnost naknadnog uvođenja državnog povjerenika za informacije nekim drugim zakonom, jer nije uobičajeno da takav povjerenik, kao procjenitelj zadužen za zaštitu transparentnosti ili javnosti rada državne uprave, bude reguliran *Zakonom o tajnosti podataka*[34].

[33] Zakon o pravu na pristup informacijama, pročišćeni tekst zakona NN 25/13, 85/15 na snazi od 09.08.2015.
[34] Ured vijeća za nacionalnu sigurnost. Preuzeto s: http://www.uvns.hr/main.aspx?id=109 (22.11.2016.)

4.4. Zaštita osobnih podataka u poslovnom procesu

Direktiva 95/46/EZ[35] definira osobne podatke kao bilo koju informaciju koja se odnosi na fizičku osobu koja je identificirana ili se može identificirati (što jest osoba na koju se podaci odnose, odnosno ispitanik), a osobom koja se može identificirati smatra se ona osoba čiji se identitet može utvrditi neposredno ili posredno, a napose putem određenog identifikacijskog broja, ili putem jednog ili više specifičnih elemenata koji su karakteristični za njen fizički, fiziološki, psihički, ekonomski, kulturni ili socijalni identitet.[36]

U praksi se time smatraju, pored uobičajenih identifikacijskih oznaka osoba, kao što su ime, prezime, adresa, ime roditelja i slično, i sve ono što može predstavljati određenu osobu, kao što su audio ili video snimka. To uključuje i snimke putem televizijskih kamera u zatvorenom krugu (nadzorne kamere), sustave videokonferencija ili web kamere.

U brizi za zaštitu privatnosti Vijeće Europe je donijelo Konvenciju za zaštitu pojedinaca pri automatskoj obradi osobnih podataka (1981) i Preporuku o priopćavanju osobnih podataka koje posjeduju javna tijela (1991). Vijeće Europe posvetilo je posebnu brigu i dostupnosti informacija koje nastaju radom javne državne uprave, kao i informacija koje se čuvaju u arhivima. Preporuka o dostupnosti informacija koje posjeduju javne vlasti (1981) afirmira pravo, ali utvrđuje i granice dostupnosti informacija koje nastaju djelatnošću tijela javne uprave, posebno kada je riječ o zaštiti temeljnih državnih interesa i zaštite privatnosti osoba. U Preporuci o europskoj politici o dostupnosti arhivskoga gradiva (2000) rezimira se praksa europskih zemalja o dostupnosti arhivskoga gradiva i daju se smjernice na kojima bi europske zemlje trebale regulirati to pitanje u vlastitim arhivskim zakonodavstvima. I dostupnost arhivskoga gradiva temelji se na zahtjevu demokratskoga prava pojedinca i izraza demokracije svake zemlje, jer ni jedna zemlja ne postaje potpuno demokratska dok svaki od njenih stanovnika ne dobije mogućnost objektivne spoznaje elemenata svoje povijesti. No, i ta preporuka potvrđuje određena dosadašnja ograničenja u korištenju arhivskoga gradiva koje sadrži podatke značajne za obranu temeljnih probitaka države i pojedinaca.

[35] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka.

[36] Dulčić, Katarina, Bodiroga-Vukobrat, Nada. (2008). Zaštita osobnih podataka pacijenata u europskom i hrvatskom pravu. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, *29*(1), 371-411.

Većina odluka koje se repliciraju na pojedinca, u suvremenom društvu temelji se na podacima pohranjenim u automatski vođenim skupovima podataka. Načelo odgovornosti osigurava da na taj način čuvani podaci i njihova uporaba neće posegnuti u pravnu sferu privatnosti pojedinca na kojega se ti podaci odnose. Problem privatnosti ne izvire samo iz uporabe modernih informacijskih tehnologija. Problem privatnosti je vezan uz sakupljanje, obradu, čuvanje i uporabu osobnih podataka. Moderna tehnologija i uporaba moderne informacijske tehnologije je taj problem samo potencirala, jer kompjutorski potpomognuti skupovi podataka omogućuju brzo udruživanje individualnih osobnih podataka na jednom mjestu i povezivanje datoteka koje se nalaze kod različitih službi.

Privatnost ili pravo na privatnost ima u različitim političkim uređenjima različit sadržaj. Ishodišta za zaštitu osobnih podataka jesu osnovna ljudska prava, koja su civilizacijska tekovina. Pravo na privatnost definira se kao pravo pojedinca da zahtijeva, da se podaci koji se odnose na njega ne daju bilo kome.[37] Zaštita osobnih podataka obuhvaća tajnost osobnih podataka (engl. *Data privacy*), koja je u prvom redu pravno pitanje i sigurnost osobnih podataka (engl. *Data security*), čiji je cilj fizičko čuvanje opreme kojom se obrađuju osobni podaci, čuvanje prostorija, obrada podataka i komunikacija[38].

U svezi s informacijskom privatnošću se kao temeljno pitanje postavlja definiranje pojma informacije i pojma podatka. „Podatak se može definirati kao činjenicu ili ideju u formaliziranom obliku, podesnu za komuniciranje i različite operacije. Informacija predstavlja i sadrži značenje koje podatku daje čovjek u određenim okolnostima.“[39] Glede rada UN na području zaštite osobnih podataka, prijelomni trenutak predstavlja godina 1974. Te je godine generalni tajnik UN-a Kurt Waldheim pripremio cjelovit izvještaj na temu "Ljudska prava i znanstveno tehnološki razvoj". U svojem zaključku izvještaj preporučuje državama, koje još nemaju zakonom uređenu zaštitu osobnih podataka, da takav način reguliranja upotrebe osobnih podataka što prije usvoje. Preporuka generalnog sekretara sadrži također i osnovna načela koje bi članice UN trebale uvažavati pri zakonskom uređivanju zaštite osobnih podataka.

[37] Načela i smjernice zaštite osobnih podataka. Preuzeto s: http://www.snz.unizg.hr/wnew/nacela1.pdf (30.11.2016.)
[38] Isto
[39] Pedrycz, Witold. (2005). *Knowledge-based clustering: from data to information granules*. London: John Wiley & Sons, str. 23.

To su sljedeća načela[40]:

- načelo određenosti,
- načelo obavještavanja i
- načelo pristanka.

Načelo određenosti kaže da se mogu sakupljati samo oni osobni podaci, koji su nužno potrebni da bi se postigao cilj zbog kojega se sakupljaju. Načelo obavještavanja govori o potrebi da se pojedinca prethodno obavijesti koji se osobni podaci o njemu sakupljaju. Načelo pristanka kaže da se mogu sakupljati samo oni osobni podaci za koje je pojedinac pristao da se sakupljaju.

[40] Isto

5. KAZNENO DJELO ODAVANJA POSLOVNE TAJNE (INDUSTRIJSKA ŠPIJUNAŽA)

Kazneno djelo odavanja poslovne tajne (industrijska špijunaža) je nelegalno dobivanje poslovnih tajni koje pripadaju konkurentu i koje konkurent štiti, koristeći nepoštena sredstva kao što su zapošljavanje svojih ljudi u konkurentskom poduzeću kako bi odali tajne, korištenje tajnih agenata za prikupljanje informacija o proizvodnim postupcima konkurenata i sl. Najčešće korištene metode kako doći do tajnih podataka o konkurentima mogu se podijeliti u pet grupa[41]:

- metoda trojanskog konja – poduzeće ubacuje svog čovjeka u konkurentsku tvrtku gdje nam on otkriva što to tvrtka čini. Ova metoda špijunaže ima dugu povijest, a jedan od primjera uporabe je evidentira u praksi kompanije East India Co. koja je djelovala u 18. i 19. stoljeću. Kompanija je tada angažirala škotskog botaničara Roberta Fortunea da prikupi uzorke biljki, sjemenja i tajni pripravljanja čaja iz Kine u Indiju koja je tada bila pod britanskom vlašću.
- izdaja - netko je motiviran za izdaju ili se želi osvetiti matičnoj tvrtki, te tako pokazuje podatke drugima. Jedan od takvih slučajeva zabilježen je 1993. kada je General Motors optužio Volkswagen za industrijsku špijunažu. Šef proizvodnje u Opelu Jose Ignacio Lopez napustio je Opel i zaposlio se u Volkswagenu zajedno s još sedam izvršnih direktora. Opel je tada zaključio da su njegove poslovne tajne otkrivene i korištene u Volkswagenu.
- provala - fizički upad u prostorije ili upad u računalnu bazu podataka. Svjetski je poznata operacija Shady Rat tijekom koja se odnosila na računalni napad na više od 70 tvrtki, vlada i neprofitnih organizacija tijekom 2006.
- korupcija namještenika - potplaćeni ljudi odaju tajne matične kompanije.
- komunikološki aspekti - prisluškivanje razgovora, telefona, itd. Tako je 2000. Izvršni direktor Oracle-a Larry Ellison angažirao detektivsku agenciju kako bi prisluškivala i pratila istraživačke organizacije koje su radile za Microsoft.

[41] Zemljić, Marija. (2014). *Industrijska špijunaža* (završni rad). Varaždin: FOI, str. 32.

5.1. Pojam industrijske špijunaže

Pod pojmom industrijske špijunaže podrazumijeva se „nezakonito djelovanje gospodarskih subjekata (tvrtki, institucija, ustanova) na prikupljanju podataka gospodarske naravi radi stjecanja nove i dodane vrijednosti.“[42] Važno je istaknuti da ovo djelovanje nije ni poticano ni potpomognuto od institucija vlasti države iz koje dolazi subjekt koji se time bavi. Metode koje se koriste slične su metodama koje koriste izvještajne službe i ovise o tehničkim, tehnološkim i ljudskim mogućnostima subjekta.

Ciljevi industrijske špijunaže jesu prikupljanje podataka (te po mogućnosti doći u posjed, odnosno ukrasti ih): novim, razvijenijim tehnikama i tehnologijama, poslovnim tajnama konkurentskih gospodarskih subjekata, novim proizvodima i uslugama koje konkurentski gospodarski subjekti namjeravaju plasirati kao i podatci o vremenu i načinu njihova plasmana, osobama koje vode tvrtke, ali i osobama koje vode istraživačke i razvojne dijelove tvrtki koje su cilj napadna djelovanja, dobivanju poslova na natječajima. Veće, snažnije i razvijenije tvrtke prikupljaju podatke strateške važnosti, a manje tvrtke svoje ciljeve postavljaju na nižim razinama važnosti, tehničko-tehnoloških znanja i sposobnosti te vrijednosti.

O potencijalnoj razornoj snazi industrijske špijunaže svjedoči i projekt simulacije špijunaže korištenjem socijalnog inženjeringa. U studiji slučaja nije definirano u kojoj je tvrtki provedena navedena simulacija. Poznate su samo činjenice da se radi o visokotehnološkoj tvrtki koja je sama zatražila simulaciju napada kako bi testirala stupanj vlastite informacijske sigurnosti. Napad je izvršen uz pomoć privremenog zaposlenika koji je krivo prezentirao svoje odgovornosti i ovlaštenja te se koristio zlouporabom fizičkog pristupa i internim hakiranjem uz koordinaciju s djelovanjem eksternih hakera. Primijenjene metode industrijske špijunaže u navedenoj simulaciji generirale su iznimne rezultate. Naime, ukradeno je preko milijardu vrijednih informacija, i to u tvrtki s vrlo sofisticiranim sustavom tehničke zaštite.[43]

Iz opisanog primjera je zaključuje da je objekt radnje kod procesa industrijske špijunaže je zaštićena informacija, tj. informacija iz poslovanja neke tvrtke koja je poduzela razumne mjere da ta informacija ostane tajnom. Inkriminiran je svaki neovlašteni opseg učinjen u cilju prikupljanja takve informacije u korist druge osobe ili tvrtke. Premda je ponekad teško

[42] Ćosić-Dragan, Daniel. (2008). Poslovnost i izvjesništvo. *National security and the future*, *9*(1-2.), 53-76.
[43] Winkler I. Case study of industrial espionage through social engineering. Preuzeto s: https://new.social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html (24.05.2017.)

razgraničiti tzv. javne informacije, tj. one informacije iz poslovanja tvrtke koje su pod jednakim uvjetima dostupne svim tržišnim subjektima, od informacija i podataka koji su poslovna tajna, na industrijsku špijunažu može uputiti i način odnosno metoda prikupljanja takve informacije. Razvojem informatičke tehnologije stvorene su pretpostavke za djelotvornije zloporabe zaštićenih informacija, a razvijene su i brojne tehnike prikrivanja takvih djela i stečene dobiti.

5.2. Kazneno djelo izdavanja i neovlaštenog pribavljanja poslovne tajne

U hrvatskom kaznenom pravu, industrijska špijunaža inkriminirana je propisivanjem kaznenog djela izdavanja i neovlaštenog pribavljanja poslovne tajne iz čl. 262. Kaznenog zakona[44]. U članku se ističe da će se osoba koja 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 nepozvanoj osobi, kazniti kaznom zatvora od jedne do pet godina. Ako je odavanje, odnosno pribavljanje podataka koji su poslovna tajna počinjeno radi njihova odnošenja u stranu državu ili ako je počinitelj za takvo postupanje primio mito, počinitelj će se kazniti kaznom zatvora od jedne do deset godina. Osoba koja kazneno djelo izdavanja i neovlaštenog pribavljanja poslovne tajne počini iz nehaja, može se kazniti novčanom kaznom ili kaznom zatvora do dvije godine. Kazneno djelo izdavanja i neovlaštenog pribavljanja poslovne tajne, MUP je, analizom KZ-a svrstao u kazneno djelo korupcije[45].[46]

5.3. Zaštita od odavanja poslovne tajne (industrijske špijunaže)

Zaštita se treba ogledati u pružanju pomoći u obliku dosegnutom i planiranom stupnju tehnološkog razvoja, strateškoj infrastrukturi, posebnim stručnim znanjima, gospodarskim subjektima, stanju na tržištu, ključnim statističkim pokazateljima stanja gospodarstva te

[44] Kazneni zakon pročišćeni tekst zakona, NN 125/11, 144/12, 56/15, 61/15 na snazi od 30.05.2015.
[45] Korupcija je u najširem smislu svaki oblik zloupotrebe ovlasti radi osobne ili skupne koristi bilo da se radi o javnom ili privatnom sektoru. Korupcija se pojavljuje u gotovo svim područjima života i djelovanja, od javnih institucija, preko politike, do privrede i poslovanja. Korumpiranom osobom se smatra svaka službena ili odgovorna osoba koja radi osobne koristi ili koristi skupine kojoj pripada zanemari opći interes koji je dužna štititi s obzirom na položaj i ovlasti koje su joj povjerene.
[46] Bedi, Davor. (2015). Koruptivna kaznena djela u javnom i privatnom sektoru u Republici Hrvatskoj s posebnim osvrtom na područje Primorsko-goranske županije í studije slučaja. *Policija i sigurnost*, *24*(1/2015), 65-82.

drugim podatcima kojima mogu pomoći svojim gospodarskim subjektima u stvaranju novih vrijednosti te bržem i jeftinijem razvoju novih tehnologija. U cilju onemogućavanja odavanja poslovne tajne postoje određene protuaktivnosti odnosno:[47]

1. Operativne protumjere se odnose na skup mjera sigurnosne provjere zaposlenika i partnera te na jasno definiranje ovlasti zaposlenika u pristupu i raspolaganju pojedinim vrstama informacija s obzirom na stupanj tajnosti;

2. Fizičke protumjere se odnose na skup mjera kojima se prevenira mogućnost fizičkog napada na različite klasificirane informacije putem provala i krađa. Iz tog razloga je nužno osigurati adekvatan sustav kontrole i nadzora u prostorijama gdje su arhivirane klasificirane informacije. To se posebno odnosi na nazor zaposlenika, posjetitelja te partnera organizacije.

3. Posebna mjere vezane za zaposlene se odnosi na provedbu istrage zaposlenika koji imaju pristup povlaštenim informacijama.

4. Tehničke protumjere se odnose na skup mjera kojima se informacijski sustavi poduzeća štite od potencijalnih napada s ciljem krađe informacija. Cilj provedbe tehničkih protumjera je osigurati pouzdanost i sigurnost uporabe informacijskih sustava.

U cilju zaštite od industrijske špijunaže, poduzeće treba angažirati savjetnika u vezi s pravnim definiranjem poslovnih tajni za tvrtke, izrade pravilnika o poslovnim tajnama, podzakonskih propisa te procedura za zaposlenike, kao i konzalting u vezi ostvarivanja organizacijskih i tehničkih uvjeta za dobivanje EU sigurnosnih certifikata. Također je važno izraditi procjenu ugroza. U sklopu prosudbe ugroza sagledavaju se svi oblici ugroza tvrtke, kako ugroze usmjerene prema fizičkoj sigurnosti objekata i zaposlenika, tako i prema cjelokupnoj informacijskoj sigurnosti, na osnovu čega se izrađuju odgovarajuća tehnička i organizacijska rješenja. Sigurnosna politika tvrtke predstavlja temeljni dokument koji određuje pravce, napore, modele i resurse na temelju kojih se provode svi daljnji postupci u svrhu poboljšanja i očuvanja stanja sigurnosti. Poduzimajući odgovarajuće zakonske postupke i procedure, moguće je zaštititi tvrtku i njezine zaposlenike od nelegalnog prikupljanja podataka o poslovnim tajnama tvrtke, osjetljivim i povjerljivim podacima uz kontinuirano podizanje razine svijesti.

[47] Zemljić, Marija. (2014). *Industrijska špijunaža* (zvaršni rad). Varaždin: FOI, str. 38.

6. NACIONALNO VIJEĆE ZA INFORMACIJSKU SIGURNOST I OPERATIVNO-TEHNIČKA KOORDINACIJA ZA INFORMACIJSKU SIGURNOST

Operativno-tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija na nacionalnoj razini osigurana je osnivanjem Nacionalnog vijeća za informacijsku sigurnost kao koordinacijskog tijela sigurnosnog sustava na razini Republike Hrvatske. U nastavku rada opisuje se djelokrug rada Nacionalnog vijeća za informacijsku sigurnost te operativno-tehnička koordinacija za informacijsku sigurnost.

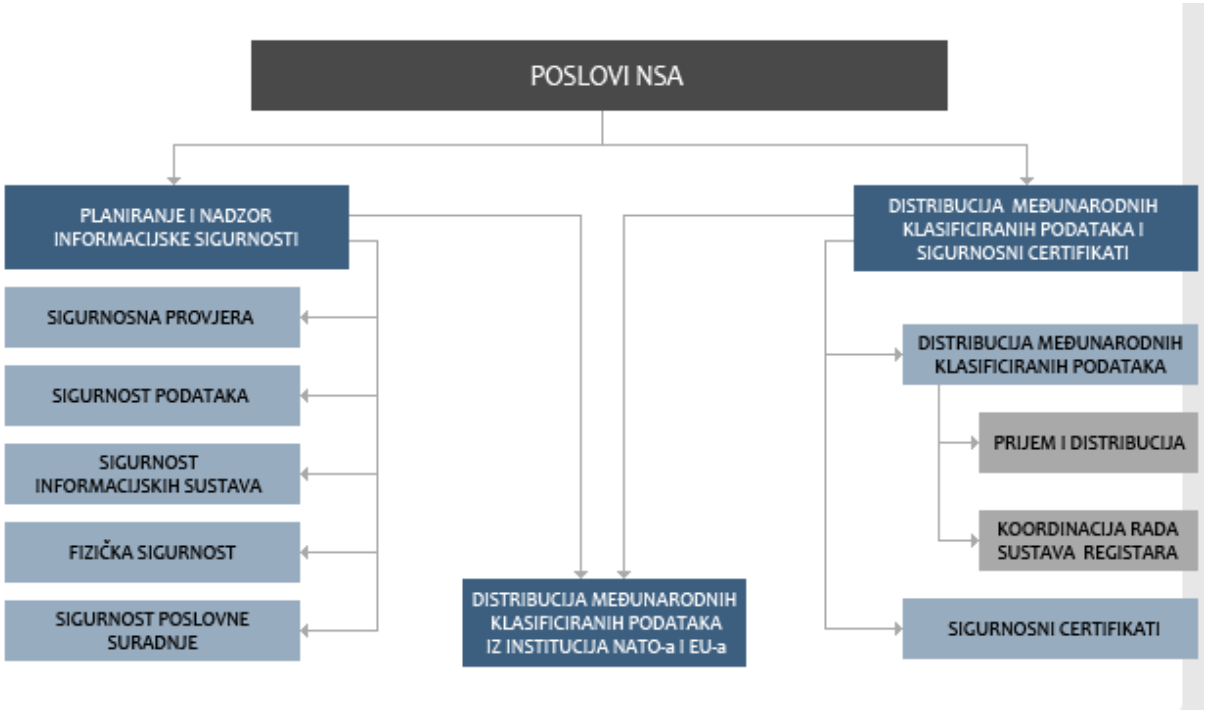
6.1. Nacionalno vijeće za informacijsku sigurnost

Središnje tijelo na nacionalnu sigurnost je Ured Vijeća za nacionalnu sigurnost RH (UVNS). Ured ima zadaću koordinacije i usklađivanje donošenja i nadzora nad primjenom mjera i standarda koje se odnose na informacijsku sigurnost. Pojedini aspekti informacijske sigurnosti čije donošenje koordinira Nacionalno vijeće za informacijsku sigurnost su:[48]

- Sigurnosna provjera,
- Fizička sigurnost,
- Sigurnost podataka,
- Sigurnost informacijskih sustava,
- Sigurnost poslovne suradnje,
- Izdavanje fizičkim i pravnim osobama certifikata za pristup nacionalnim, NATO i EU klasificiranim podacima.

[48] Ured Vijeća za nacionalnu sigurnost. Preuzeto s: http://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa (02.12.2016.)

Vlasnik klasificiranog podatka je multinacionalno, nacionalno ili državno tijelo gdje je podatak nastao. Pravne osobe su dužne primijeniti mjere sigurnosti klasificiranih podataka. Postupak klasifikacije od strane pravne osobe uređen je Naputkom o klasificiranju podataka u projektu i Projektno-sigurnosnom uputom. Naputak o klasificiranju podataka u projektu predstavlja sastavni dio nacionalnih klasificiranih ugovora i podugovora koji definira standarde za zaštitu klasificiranih podataka. Naputak izrađuje državno tijelo koje sklapa ugovor s pravnom osobom. Uputa o klasificiranju podataka u projektu je sastavni dio Projektno-sigurnosne upute, a suglasnost za sadržaj upute daje tijelo UVNS, nadležna tijela druge države ili međunarodne organizacije. Fizičke osobe zaposlene u pravnoj osobi imaju obvezu čuvanja tajnosti klasificiranih podataka za vrijeme i nakon provedbe klasificiranog ugovora. Dakle, podatak se čuva dok je klasificiran nekim od stupnjeva tajnosti. Za prijem i distribuciju međunarodnih klasificiranih podataka zadužen je Središnji registar pri Uredu Vijeća za nacionalnu sigurnost. Na slici 1 prikazan je djelokrug rada Ureda Vijeća za nacionalnu sigurnost u Republici Hrvatskoj.



Slika 1. Djelokrug rada Ureda Vijeća za nacionalnu sigurnost u Republici Hrvatskoj [1]

[1] Izvor: Ured Vijeća za nacionalnu sigurnost. Preuzeto s: http://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa (02.12.2016.)

Na temelju slike 1 se zaključuje kako se temeljni djelokrug rada Ureda Vijeća za nacionalnu sigurnost odnosi na planiranje i nadzor informacijske sigurnosti te na distribuciju međunarodnih klasificiranih podataka i sigurnosnih certifikata, a iz navedenih zadaća ujedno proizlazi distribucija međunarodnih klasificiranih podataka iz institucija NATO I EU. Proces distribucije međunarodnih klasificiranih podataka može se podijeliti na prijem i distribuciju klasificiranih podataka, koordinaciju rada sustava registra i dodjelu sigurnosnih certifikata.

6.2. Operativno-tehnička koordinacija za informacijsku sigurnost

Poslovi operativno-tehničke koordinacije za informacijsku sigurnost koji se obavljaju u sklopu UVNS-a su praćenje stanja sigurnosti Nacionalnog informacijskog prostora, donošenje Izvješća o stanju Nacionalne informacijske sigurnosti i donošenje i implementacija planova postupanja u slučaju informacijskih kriza.

6.2.1. Praćenje stanja sigurnosti Nacionalnog informacijskog prostora

Pojam informacijske sigurnosti definira se kao „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.“[49]

U cilju boljeg razumijevanja koncepta praćenja stanja sigurnosti Nacionalnog informacijskog prostora ključno je definirati pojam informacijskog ili kibernetičkog prostora. „Informacijski prostor predstavlja javni komunikacijski i informacijski prostor, u smislu povezanosti računalnih mreža, baza podataka i općenito izvora informacija, odnosno predstavlja virtualnu mrežnu okolinu koja je globalna i naseljena znanjem u elektroničkom obliku.“ [50] Informacijska tehnologija stvara alternativu stvarnom prostoru i svijetu. Informacijski ili kibernetički prostor mijenja prostorno – vremenske zakonitosti, odnosno briše prostorne i vremenske barijere u komuniciranju i svakodnevnim aktivnostima. Pridjev kibernetički (*engl.*

[49] Zakon o informacijskoj sigurnosti, (NN br 79/2007)
[50] Pal, Nikhil, Pal, Sankar, (1991). Entropy: A new definition and its applications. *IEEE transactions on systems, man, and cybernetics*, *21*(5), 1260-1270.

cyber) prvi je upotrijebio autor znanstvene fantastike William Gibson. Taj se pojam usko vezuje uz kibernetiku, „znanost o općim zakonitostima procesa upravljanja i regulacije te dobivanja pretvorbe, pohranjivanja i prijenosa informacija u sustavima, koji su neovisni o njihovoj fizikalnoj prirodi. Riječ kibernetika dolazi od grčke riječi *kibernein* što znači upravljati. Temelje kibernetike u današnjem obliku je postavio američki znanstvenik Norbert Wiener 1948. godine.“ Kibernetika predstavlja multidisciplinarnu znanstvenu disciplinu koja polazi od informacijsko – sustavne paradigme i donosi svestrani pristup znanstvenoj analizi. Za Wienera, osnova kibernetike je u komunikaciji. On smatra da se „društvo može razumjeti samo putem proučavanja poruka i sredstava komunikacije kojim raspolaže, i da će u budućnosti razvoj poruka i sredstava komunikacije, poruka između čovjeka i stroja, između stroja i čovjeka i između stroja i stroja neizbježno igrati sve značajniju ulogu.“[51] Termin informacijskog ili kibernetičkog prostora danas se široko upotrebljava kada se želi opisati globalna mreža infrastrukture informacijske tehnologije, telekomunikacijski sustav i računalni sustav. U tom prostoru komunikacija je moguća među pojedincima iz udaljenih dijelova svijeta, i to u djeliću sekunde, uz obilježja interaktivnosti i multimedijalnosti. „Pojam »kibernetički« uveden je u pravni poredak RH ratifikacijom Budimpeštanske konvencije o kibernetičkom kriminalu još 2002. godine.“[52]

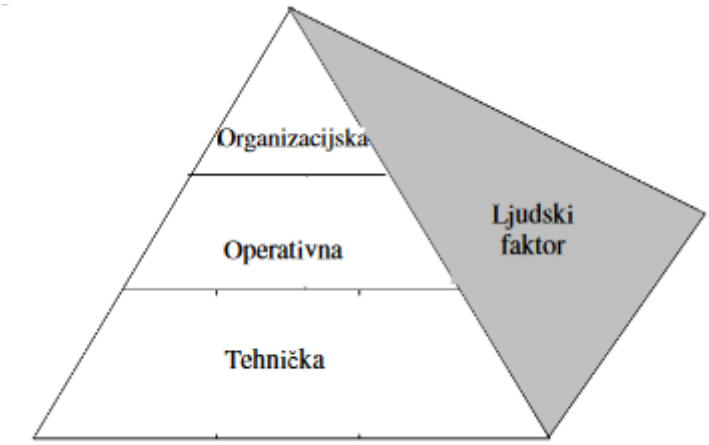
Zadaća praćenja stanja na području informacijske sigurnosti u Republici Hrvatskoj je poduzimanje preventivnih mjera s ciljem sprječavanja ugroza nacionalne informacijske sigurnosti. Pojedini aspekti preventivnog djelovanja s ciljem zaštite sigurnosti nacionalnog informacijskog prostora su:[53]

- praćenje stanja na području računalne sigurnosti i objavljivanje sigurnosnih obavijesti u svrhu priprema za sprečavanje šteta,
- kontinuirano praćenje računalno-sigurnosnih tehnologija te se sva nova saznanja prikupljaju i diseminiraju,
- javno objavljivanje novih informacija u svrhu edukacije najšire javnosti i unapređenju svijesti o značaju računalne sigurnosti,
- provođenje detaljne edukativne obuke za specifične grupe korisnika.

[51] Panian, Željko. (2000). *Poslovna informatika: koncepti, metode i tehnologija*. Zagreb: Potecon doo., str. 32.
[52] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)
[53] Nacionalni CERT. Preuzeto s: http://www.cert.hr/onama (03.12.2016.)

Svrha sustavnog praćenja stanja sigurnosti Nacionalnog informacijskog prostora je osigurati proaktivno i pravodobno djelovanje s ciljem učinkovitog prepoznavanja i sprječavanja potencijalnih ugroza po informacijsku sigurnost u RH. S obzirom da je priroda informacijskog prostora obilježena stalnim promjenama, svrha sustavnog praćenja stanja sigurnosti je ujedno pravodobno prepoznavanje potrebe za modifikacijom zakonskih propisa kojima se regulira pitanje informacijske sigurnosti na nacionalnoj razini.

Praćenje stanja sigurnosti Nacionalnog informacijskog prostora se provodi na više razina kako je prikazano na slici 2.



Slika 2. Dimenzije praćenja sigurnosti Nacionalnog informacijskog prostora [2]

Evidentno je da su dimenzije praćenja sigurnosti Nacionalnog informacijskog prostora organizacijske, operativne i tehničke mjere, a zasebnu dimenziju praćenja stanja nacionalne informacijske sigurnosti čini praćenje ljudskog faktora. Praćenje stanja informacijske sigurnosti na organizacijskoj razini uključuje mjerenje kvalitete procesa i koordinacije sustava. Operativni aspekt odnose se na neposredno mjerenje veličina pojedinih procesa, a tehnički aspekt praćenje brojivih jedinica/mjera.[54]

[54] Sajko, Mario. (2016). Mjerenje i vrednovanje učinkovitosti informacijske sigurnosti. Preuzeto s: https://www.fer.unizg.hr/_download/repository/Mario_Sajko_%5Bkvalifikacijski_rad%5D.pdf

6.2.2. Izvješće o stanju Nacionalne informacijske sigurnosti

Obveza Ureda Vijeća za nacionalnu sigurnost je izraditi godišnja i, po potrebi, izvanredna izvješća o rezultatima praćenja stanja na području informacijske sigurnosti u Republici Hrvatskoj kao i o nadzoru sigurnosno-obavještajnih agencija te Operativno-tehničkog centra za nadzor telekomunikacija. Zadaća UVNS-a je izrađivati objedinjena izvješća i periodične te po potrebi strategijske analize stanja informacijske sigurnosti u Republici Hrvatskoj. Korisnici navedenih izvješća su Predsjednik Republike Hrvatske i Predsjednik Vlade Republike Hrvatske.

Jedna od zadaća UVNS-a je izraditi izvješća o provedenim mjerama kontrole koje su poduzete kako bi se osiguralo poštovanje Ustavom zajamčenih prava građana. Ta se izvješća dostavljaju predsjedniku Hrvatskog sabora i saborskom odboru koji se bavi problematikom nacionalne sigurnosti.

6.2.3. Preventivni i reaktivni planovi u slučaju informacijskih kriza

Krizne situacije nastaju kao rezultat nepovoljnog razvoja događaja. Kriza predstavlja nepovoljan ishod događaja. Ne postoji jedinstvena definicija pojma poslovne krize, no velik broj radnih definicija pojma poslovne krize osigurao je temelje za identificiranje osnovnih obilježja poslovnih kriza. „Etimološki gledano, riječ kriza potječe iz grčkog jezika. U staroj Grčkoj riječ kriza (κριςις) značila je "presudu" ili "odluku", to jest presudni trenutak koji odlučuje o daljnjem pozitivnom ili negativnom razvoju neke stvari ili situacije. Bit krize jest da u određenom trenutku treba odlučiti (ili donijeti odluku), ali da još (uvijek) nije odlučeno." [55] Analogno općoj definiciji krize, informacijska kriza, odnosno kriza informacijske sigurnosti je neplanirani i neželjeni događaj koji predstavlja ugrozu po nacionalnu informacijsku sigurnost, ograničenog trajanja s ambivalentnim ishodom. U Republici Hrvatskoj su donošenjem Zakona o kritičnim infrastrukturama [56] i pratećim podzakonskim aktima stvoreni su legislativni preduvjeti za uspješno upravljanje rizicima

[55] Kešetović, Željko, Toth, Ivan. (2012). *Problemi kriznog menadžmenta: znanstvena monografija*. Veleučilište Velika Gorica, str. 26.
[56] Zakon o kritičnim infrastrukturama (NN 56/13)

kritične komunikacijske i informacijske infrastrukture unutar utvrđenih sektora kritične infrastrukture, u cilju:[57]

- povećanja otpornosti/smanjenja ranjivosti komunikacijskih i informacijskih sustava;
- umanjivanja posljedica negativnih događaja (prirodne i tehničko-tehnološke nesreće) i mogućih napada (namjernih i nenamjernih);
- omogućavanja brzog i učinkovitog oporavka te nastavka rada.

Vlada RH identificirala je informacijsko-komunikacijski sektor kao sektor iz kojeg se određenim metodama utvrđuju nacionalne kritičke infrastrukture. Nacionalnu kritičku infrastrukturu sačinjavaju elektroničko-komunikacijske mreže, infrastruktura i povezana oprema te informatička infrastruktura i sustavi zemaljske radiodifuzije.

Ključni dugoročni interes Republike Hrvatske je kontinuirano poduzimati aktivnosti zaštite kritične informacijsko-komunikacijske infrastrukture kako bi se osigurao kontinuirani rad iste. Prvi cilj je prepoznavanje kritične komunikacijske i informacijske infrastrukture. Nakon što je prepoznata kritična infrastruktura, propisuju se obvezne operativne, tehničke i organizacijske mjere održavanja iste te postupci izvješćivanja o računalnim incidentima koji se provode u suradnji između vlasnika kritične infrastrukture i središnjih tehničkih i sigurnosnih te državnih tijela. Temeljni cilj učinkovitog upravljanja informacijskom, odnosno kibernetičkom krizom je definiranje pravodobnih i učinkovitih akcija kojima će se uspješno odgovoriti na prijetnje i oporaviti infrastrukturu koja je od ključnog sigurnosnog interesa za Republiku Hrvatsku.

Sustav upravljanja u kibernetičkim krizama u RH potrebno je uspostaviti u skladu sa sljedećim zahtjevima:[58]

1. usklađenost s nacionalnim rješenjima upravljanja u krizama,
2. obuhvaćanje zaštite kritične nacionalne komunikacijske i informacijske infrastrukture,
3. usklađenost s međunarodnim sustavima upravljanja u kibernetičkim krizama EU i NATO-a,
4. usklađenost s nacionalnim nadležnostima tijela zakonom zaduženih za koordinaciju prevencije i odgovora na računalne ugroze sigurnosti informacijskih sustava.

[57] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)
[58] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)

Iz navedenih zahtjeva proizlaze i ciljevi upravljanja kritičnom infrastrukturom u pogledu nacionalne informacijske sigurnosti. Prvi je cilj definiranje kriterija na osnovu kojih se utvrđuje koja je komunikacijska i informacijska infrastruktura od kritičnog značaja za Republiku Hrvatsku. Kriteriji za determiniranje kritične informacijsko-komunikacijske strukture detaljno se razrađuju Zakonom o kritičnim infrastrukturama u kojem je propisana metodologija pristupa odabiru kritične infrastrukture, a metodologiju je potrebno sustavno unaprjeđivati u skladu s međunarodnim propisima.

Drugi cilj je definirati obvezne sigurnosne mjere koje je vlasnik ili upravitelj kritičnom informacijsko-komunikacijskom infrastrukturom dužan provoditi kako bi se izbjegli potencijalni računalni sigurnosni incidenti i kako bi se sanirale posljedice nastalih računalnih incidenata. Osobito relevantne sigurnosne mjere koje su dužni provoditi vlasnici i upravitelji kritičnom informacijsko-komunikacijskom infrastrukturom su mjere sigurnosne provjere djelatnika i provedba mjera postupanja s klasificiranim podacima.

Važnu ulogu u preveniranju informacijskih kriza ima uspostava sustava upravljanja rizicima kao treći cilj vezan uz prevenciju računalnih incidenata. Proces upravljanja rizicima sastoji se od identifikacije, mjerenja i kontrole rizika.[59] Primarna korist od primjene sustava upravljanja rizicima proizlazi iz situacijske analize, odnosno prepoznavanja i iskorištavanja prilika, odnosno prepoznavanja i minimiziranja prijetnji u okruženju. Svrha je upravljanja rizicima osigurati adekvatnu pripremljenost na potencijalne računalne ugroze. Priprema za različite scenarije ujedno jača kompetencije zaposlenika i osigurava uspješnu i fleksibilnu prilagodbu te pravodobno reagiranje na računalne incidente. Sektorska procjena rizika uključuje:[60]

1. identifikaciju kritičnih funkcija (službe, podaci, mreže, itd.);

2. identifikaciju prijetnji;

3. procjenu prijetnji, ranjivosti i posljedica;

4. analizu i prioritetiziranje rizika;

5. utvrđivanje prihvatljivog rizika i obradu rizika.

[59] Legčević, Jelena, Taučer, Katarina. (2014). Krizni menadžment u funkciji nove teorije menadžmenta. *Ekonomski Vjesnik/Econviews: Review of contemporary business, entrepreneurship and economic issues*, *27*(1), 199-208.

[60] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)

Četvrti cilj u prevenciji i sanaciji računalnih incidenata se odnosi na jačanje javno-privatnog partnerstva u prevenciji i sanaciji računalnih sigurnosnih ugroza. Učinkovita prevencija i sanacija računalnih incidenata uvjetovana je nadzorom, koordinacijom i razmjenom sigurnosnih podataka između vlasnika i upravitelja kritičnom infrastrukturom i tehničkih te sigurnosnih službi RH. U slučaju računalnog sigurnosnog incidenta potrebno je uspostaviti okvir za suradnju javnih i privatnih tijela s tijelima kaznenog progona. Kako bi se pravovremeno osigurala sanacija posljedica računalnog sigurnosnog incidenta, važno je uspostaviti tehničku koordinaciju s tijelima koja pružaju tehničku podršku pri otklanjanju posljedica nastalog incidenta.

Peti cilj se odnosi na uspostavu Nacionalnog sustava upravljanja u kibernetičkim krizama. Nacionalni sustav upravljanja u kibernetičkim krizama treba osigurati:[61]

1. sustavno praćenje stanja sigurnosti nacionalnog kibernetičkog prostora, u svrhu otkrivanja prijetnji koje mogu imati za posljedicu kibernetičku krizu,
2. periodično izvješćivanje o stanju kibernetičke sigurnosti,
3. učinkovito planiranje postupanja u kibernetičkim krizama,
4. usklađeno i koordinirano postupanje državnih tijela u kibernetičkim krizama.

Sve ostale mjere kojima se osigurava kibernetička sigurnost usko su vezane uz borbu protiv računalnog ili kibernetičkog kriminala i kaznenog progona istog. Računalni ili kibernetički kriminal se odnosi na sve vrste kriminalnih radnji koje se provode posredstvom informacijsko-komunikacijske tehnologije. „Računalni, odnosno kibernetički kriminalitet obuhvaća kaznena djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom komunikacijskih i informacijskih tehnologija i predstavlja prijetnju ostvarenju sigurnijeg informacijskog društva.“[62] „Kod kaznenih djela računalnog kriminala uobičajeno je propisivati kažnjivost pripremnih radnji u nešto većem obujmu nego što je to slučaj kod većine ostalih kaznenih djela. Razlog za takvu zakonodavnu praksu leži u virtualnom karakteru ovih kaznenih djela, zbog čega su mogući problemi u dokazivanju povrede ili ugrožavanja zaštićenih pravnih dobara. Zato je potrebno kaznenopravnu zaštitu

[61] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)
[62] Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)

pomaknuti u što raniji stadij. Široko kažnjavanje pripremnih radnji zahtijeva i čl. 6. Konvencije o kibernetičkom kriminalu.“[63]

Kako bi se osigurala učinkovita borba protiv kibernetičkog kriminala važno je unaprjeđivati zakonodavni okvir i prilagođavati ga brzom trendu rasta i sve većem broju pojavnih oblika kaznenih djela računalnog kriminala, i to u skladu međunarodnim propisima. Prilikom suzbijanja negativnih učinaka računalnog kriminala po nacionalnu sigurnost, važno je uvažavati načela međunarodne suradnje. Potreba za međunarodnom suradnjom pri suzbijanju računalnog kriminaliteta proizlazi iz činjenice da je Internet medij s globalnim dosegom koji ne poznaje nacionalne granice te se stoga i akcije suzbijanja računalnog kriminala trebaju provoditi na međunarodnoj razini. To se osobito odnosi na suradnju između pojedinih država članica EU i NATO-a kao i na suradnju s trećim zemljama. Olakotna okolnost u organizaciji međunarodne suradnje pri borbi protiv računalnog kriminala odnosi se na mogućnost razmjene informacija putem Europola[64] i Eurojusta[65] koji već imaju razrađene kanale za međunarodnu suradnju s ciljem suzbijanja kriminalnih radnji. Svaki računalni incident predstavlja hitnu situaciju koju je potrebno rješavati uvažavajući multidisciplinarni pristup, odnosno koordinacijom tijela koja mogu pridonijeti uspješnom suzbijanju negativnih posljedica incidenta. Učinkovita komunikacija između pojedinih tijela zaduženih za rješavanje posljedica računalnih incidenata omogućuje se uspostavom stalnih kontakt točaka.

S obzirom na činjenica da je računalni kriminalitet sofisticirani oblik kriminalne aktivnosti koji se može provesti samo uz preduvjet da počinitelj(i) posjeduju usko specijalizirana znanja i vještine, nužno je ulagati u edukaciju ljudskih potencijala te razvoj kompetencija i tehničkih mogućnosti s ciljem optimizacije procesa kriminalističkog istraživanja u segmentu računalnog kriminala. Kriminalna istraživanja mogu se kvalitetno provoditi samo uz adekvatne forenzičke alate i sustave koji su prilagođeni razini sofisticiranosti računalnih kriminalnih djela.

[63] Mučalo, Marina, Sviličić, Nikša. (2000). Virtual War. *Politička misao*, *37*(1), 229-242.
[64] Europol je koordinacijsko tijelo na razini Europske unije koje policijama država članica osigurava relevantnu bazu vijesti i informacija s ciljem borbe protiv kriminala.
[65] Eurojust je koordinacijsko pravno tijelo na razini Europske unije osnovano s ciljem osiguranja sigurnosti i pravde u EU. Tijelo je utemeljeno na solidarnom djelovanju s ciljem jačanja borbe protiv međunarodnog kriminala.

Učinkovitu borbu protiv računalnog kriminaliteta kao ozbiljne prijetnje sustavu nacionalne sigurnosti potrebno je provoditi u suradnji s gospodarskim sektorom, a to se posebno odnosi na nezavisne regulatore telekomunikacijskih usluga kao i na suradnju s pravnim osobama koje nude usluge javnih elektroničkih komunikacija te subjekte koji pružaju elektroničke financijske usluge (primjerice usluge Internetskog i mobilnog bankarstva). Razlog navedenoj inicijativi proizlazi iz činjenice da gospodarski subjekti trebaju biti opremljeni adekvatnim sustavima zaštite protiv računalnog kriminaliteta kako bi na mogućnost pojave ili pojavu istog mogli pravodobno upozoriti tijela za kazneni progon. Drugi cilj suradnje s gospodarskim sektorom na području suzbijanja računalnog kriminaliteta proizlazi iz potrebe računalnog opismenjavanja krajnjih korisnika koja se postiže edukacijom i podizanjem razine svijesti o pojavnim oblicima računalnog kriminaliteta i mjerama zaštite protiv te vrste kaznenih djela.

7. PLAN INFORMACIJSKE SIGURNOSTI PODUZEĆA

Osnovni dokument koji definira kritične čimbenike upravljanja informacijskom sigurnošću naziva se plan informacijske sigurnosti. Taj plan mora biti prilagođen organizaciji na koju se primjenjuje i stoga može posjedovati različite razine kompleksnosti. U okviru njega se istražuju rizici koji se mogu pojaviti a imaju utjecaj na poslovni sustav te predložiti određene akcije koje se mogu poduzeti kako bi se oni minimizirali ili u potpunosti izbjegli.[66] Planom informacijske sigurnosti poduzeća klasificira se stupanj povjerljivosti informacija te se definira razina diskrecije. Kako bi se osigurao optimalan ustroj organizacijske komunikacijske sa stajališta informacijske sigurnosti, nužno je ustrojiti organizacijsku komunikaciju prema *„need to know"* načelu i definirati rukovanje dokumentima koji su označeni određenim stupnjem tajnosti. Definiranje i upravljanje rizicima informacijske sigurnosti poduzeća temelje je plana informacijske sigurnosti. U implementaciji informacijske sigurnosti poduzeća potrebno je njegovati suradnički pristup. Posebni aspekti plana informacijske sigurnosti poduzeća su operativna i tehnička zaštita povjerljivih poslovnih i/ili proizvodnih informacija.

7.1. Klasifikacija stupnja povjerljivosti informacija i definiranje razina diskrecije

Klasificirani podatak predstavlja tajni podatak u vlasništvu državne uprave. To je podatak koji nadležno državno tijelo u propisanom postupku označi klasificiranim, jer je za njega utvrdilo zakonsku obvezu određivanja stupnja tajnosti. Klasificirani podatak je i svaki drugi podatak, kojeg nekoj državi tako označenog preda druga država, međunarodna organizacija ili institucija, sukladno odgovarajućem međunarodnom ugovoru o uzajamnoj zaštiti klasificiranih podataka. Zakonom se obavezno propisuju kriteriji klasificiranja, način označavanja, postupanja i zaštite klasificiranog podatka. U RH je postupanje s klasificiranim podacima propisano sa tri posebna zakona: *Zakonom o tajnosti podataka* (NN 79/07), *Zakonom o informacijskoj sigurnosti* (NN 79/07), *Zakonom o sigurnosnim provjerama* (NN 85/08) te nizom pripadajućih podzakonskih akata – uredbi, pravilnika i naputaka.[67]

[66] Informacijska sigurnost. Preuzeto s: www.orkis.hr/Download.ashx?FileID=88e3b8ea-6439-4e55-b89f-054762971b63, (07.12.2016.)
[67] Klaić, Aleksandar, Perešin, Anita. (2011). Koncept regulatornog okvira informacijske sigurnosti. Preuzeto s: https://bib.irb.hr/datoteka/521742.AK_AP_Koncept_regulativnog_okvira_inf_sig_DKU_032011.pdf (06.12.2016.)

Stupnjevi tajnosti klasificiranih podataka su sljedeći:

- Vrlo tajno,
- Tajno,
- Povjerljivo.

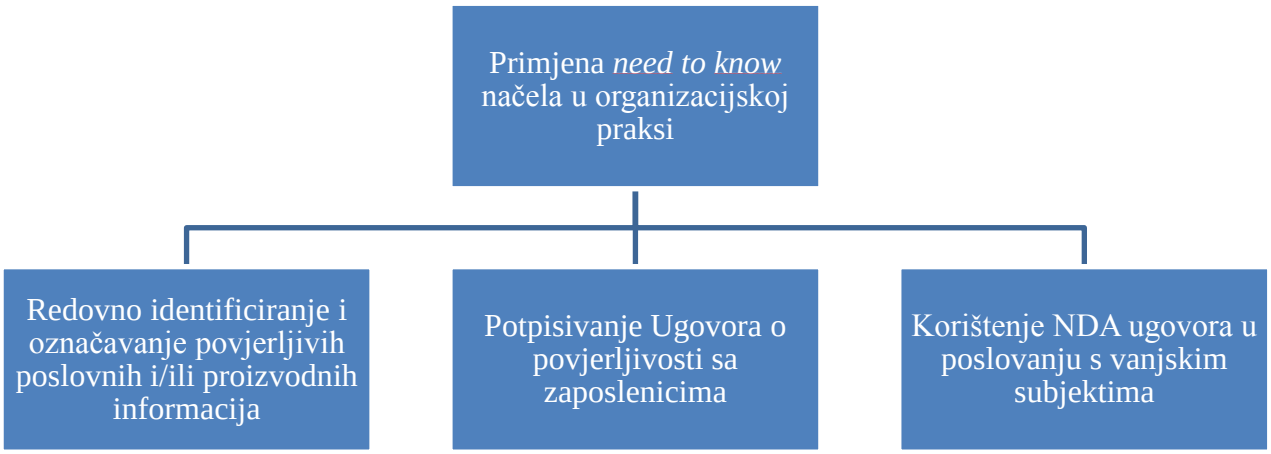
Pristup podacima ima fizička osoba iz pravne osobe koja je sigurnosno informirana i ima odgovarajući certifikat . Klasificiranim podacima za koje je definiran ograničeni pristup, pristup se može osigurati samo fizičkim osobama iz pravne osobe koje su potpisale *Izjavu o postupanju s klasificiranim podacima stupnja tajnosti "ograničeno".*
Oblici povrede sigurnosti klasificiranih podataka su uništenje, otuđenje, gubitak i dostupnost neovlaštenim osobama i medijima. Za podatke stupnja tajnosti "vrlo tajno", "tajno" i "povjerljivo" fizička osoba iz pravne osobe upozorava vlasnika podatka i UNVS te slijedi pokretanje postupka utvrđivanja odgovornosti. Povreda sigurnosti ne uključuje izvanredne situacije, ali je u tom slučajno nužno da osoblje iz pravne osobe koje je izvanredno pristupilo klasificiranom podatku naknadno potpiše *Izjavu o postupanju s klasificiranim podacima*. U slučaju povrede sigurnosti klasificiranih podataka, pravna osoba dužna je izraditi Izvješće o povredi sigurnosti klasificiranih podataka te dostaviti isto Uredu Vijeća za nacionalnu sigurnosti. Rok dostave izvješća je 90 dana od dana obavijesti o povredi sigurnosti klasificiranih podataka.[68]

7.2. Ustroj organizacijske komunikacije prema *„need to know"* načelu

Poduzeća u kojima konkurentska prednost proizlazi iz nematerijalne imovine, odnosno intelektualnog vlasništva često raspolažu visoko osjetljivim informacijama, odnosno poslovnim tajnama. U opisanom okruženju, adekvatan stupanj informacijske sigurnosti je moguće ostvariti samo ukoliko se organizacijska komunikacija organizira prema *need to know* načelu. Primjena načela *need to know* u organizacijskoj praksi je jednostavna. Fizička osoba zaposlena u pravnoj osobi tako može imati potrebna službena odobrenja za pristup određenim osjetljivim i tajnim poslovnim podacima, međutim pristup istima joj se neće osigurati ukoliko za to nema evidentne potrebe, odnosno ukoliko pristup takvim informacijama nije neophodan da bi se uspješno izvršio određeni organizacijski zadatak. Primjena *need to know* načela onemogućuje zaposlenicima pregled osjetljivih poslovnih informacija i poslovnih tajni kako

[68] Vuković, Hrvoje. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. *National security and the future, 13*(3), 12-31.

bi što manji broj ljudi imao uvid u takvu vrstu podataka i informacija. Kako bi poduzeće uspješno implementiralo *need to know* načelo u praksi, potrebno je razviti sustav kontrole pristupa operativnim i dokumentacijskim sustavima.[69] Sustav kontrole pristupa operativnim i dokumentacijskim sustavima definira vlasnik tajnih i osjetljivih podataka na način da jasno odredi tko ima pristup određenoj vrsti podatka i tim zaposlenicima dodijeli ovlasti pristupa tajnim i osjetljivim informacijama. Putem sustava kontrole pristupa operativnim i dokumentacijskim sustavima moguće je onemogućiti neautorizirani pristup poslovnim tajnama, odnosno osjetljivim poslovnim i proizvodnim informacijama s aspekta informacijske sigurnosti. Primjena *need to know* načela u organizacijskoj praksi može se osigurati u tri koraka koja su prikazana na slici 3.



Slika 3. Primjena *need to know* načela u organizacijskoj praksi u tri koraka [3]

[69] Bereš, Paun. (2013). Heuristika i zakonska regulativa u oblasti zaštite tajnih podataka u funkciji edukacije subjekata sistema odbrane. *Vojnotehnički glasnik/Military Technical Courier*, *62*(2), 121-135.

Na temelju slike 3 zaključuje se kako je prvi korak u primjeni *need to know* načela u organizacijskoj praksi redovito identificiranje i označavanje povjerljivih poslovnih i/ili proizvodnih informacija. Tvrtke trebaju redovito identificirati, označavati i revidirati povjerljive poslovne i/ili proizvodne informacije s kojima raspolažu. Pritom je važno razlikovati prava industrijskog vlasništva od poslovnih tajni. Naime, prava industrijskog vlasništva kao što su patenti, autorska prava i zaštitni znakovi moraju biti objavljeni u javnosti. U prvom koraku ujedno je važno odgovoriti na pitanja: tko ima pristup poslovnoj tajni? gdje se nalaze informacije o poslovnoj tajni? koje su mjere primijenjene s ciljem zaštite poslovne tajne, odnosno povjerljive poslovne i/ili proizvodne informacije? Poslovne tajne potrebno je označiti klasifikacijom povjerljivo i definirati ovlaštene zaposlenike s pravom pristupa povjerljivim podacima.

Druga razina zaštite povjerljivih poslovnih i/ili proizvodnih informacija osigurava se putem sklapanja Ugovora o povjerljivosti sa zaposlenicima tvrtke. Naime, zaposlenici igraju ključnu ulogu u održavanju poslovnih tajni povjerljivim podacima. Oni svakodnevno rade s povjerljivim podacima te je stoga nužno poduzeti korake kako bi zaposlenici znali koji su podaci povjerljivi i kako s njima ispravno postupati. Preporučljivo je provoditi redovitu obuku zaposlenika o povjerljivim podacima tvrtke i odgovornosti zaposlenika koji su dužni održavati diskreciju poslovne tajne i drugih povjerljivih podataka.

Treća razina organizacijske komunikacije prema *need to know* načelu regulira odnose s vanjskim suradnicima. Zaštita povjerljivih poslovnih i/ili proizvodnih informacija u poslovanju s trećim strankama osigurava se putem NDA ugovora. U NDA ugovoru s trećim strankama je potrebno precizirati koji zaposlenici vanjske tvrtke će imati pristup povjerljivim informacijama. Uobičajeno je da treća strana ima obvezu vraćanja svih povjerljivih tiskanih i elektroničkih podataka vlasniku podataka po završetku poslovnog odnosa. [70]

7.3. Definiranje rizika i upravljanje rizicima informacijske sigurnosti poduzeća

Rizici informacijske sigurnosti poduzeća su sve vrste rizika koje proizlaze iz ugrožavanja tajnih i povjerljivih podataka uništavanjem, gubitkom ili neovlaštenim pristupom i širenjem povjerljivih informacija. Rizici informacijske sigurnosti poduzeća ujedno se povezuju s

[70] Mintas – Hodak, Ljerka. (2010). Op.cit., str. 403.

ekonomskim gubicima za poduzeće s obzirom da je u suvremenom poslovnom okruženju upravo informacija temeljni resurs u stjecanju konkurentske prednosti. Identifikacija rizika informacijske sigurnosti podrazumijeva definiranje unutarnjih i vanjskih čimbenika koji potencijalno mogu ugroziti diskreciju koja se zahtijeva u postupanju s povjerljivim poslovnim i/ili proizvodnim informacijama. Pritom je potrebno naglasiti da je proces identifikacije rizika informacijske sigurnosti u suvremenom okruženju otežano zbog kontinuiranog napretka informacijsko-komunikacijske tehnologije te je rizike po informacijsku sigurnost potrebno redovno ažurirati. Upravljanje rizicima po informacijsku sigurnost poduzeća odnosi se na postupanje u slučaju:[71]

- Pristupa povjerljivim informacijama od strane neovlaštene osobe,
- Kompromitiranja sigurnosti informacijskog sustava kao rezultat pristupa od strane „hakera“,
- Presretanja podataka tijekom transakcije,
- Gubitka podataka ili povjerljivosti informacija zbog greške korisnika,
- Fizičkog gubitka podataka uslijed katastrofe,
- Nekompletnosti i nedokumentiranosti transakcije,
- Neautoriziranog pristupa povjerljivim informacijama od strane zaposlenika,
- Neautoriziranog zahtjeva telefonom ili emailom za povjerljivim informacijama („phishing“),
- Neautoriziranog pristupa preko papirnih dokumenata i izvještaja,
- Neautoriziranog transfera povjerljivih informacija preko treće strane.

Kako bi se eliminirali ili barem smanjili rizici informacijske sigurnosti, nužno je minimizirati broj ljudi koji rukuju povjerljivim informacijama, ograničiti pristup informacija prema *need to know* načelu kako je opisano u potpoglavlju 7.2. Važan aspekt upravljanja rizicima informacijskog sustava je provedba edukacije osoblja u postupanju s povjerljivim poslovnim i/ili proizvodnim informacijama. Povjerljive podatke potrebno je čuvati od fizičkog uništenja ili gubitka, a nakon što je istekla zakonska ili druga obveza zaštite takvih podataka, poduzeća imaju obvezu uništenja povjerljivih dokumenata. Za proces uništenja dokumenata koji sadrže povjerljive informacije zadužen je vlasnik povjerljivog dokumenta. Poseban aspekt

[71] Heimdal Security. Preuzeto s: https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/ (18.12.2016.)

upravljanja rizicima informacijske sigurnosti odnosi se na sigurnost informacijskih sustava što podrazumijeva:[72]

- kreiranje kriterija pristupa računalnoj mreži (uključuje kontrolu pristupa osobnih računala, mobilnih telefona i prijenosnika korisnika izvan sustava)
- kreiranje korisničkih grupa
- kontrolu pristupa elektroničkoj pošti
- kontrolu pristupa Internet servisima
- kontrolu pristupa telefonskom sustavu
- kontrolu daljinskog pristupa
- kontrolu pristupa preko virtualnih privatnih mreža.

7.4. Suradnički pristup u implementaciji informacijske sigurnosti poduzeća

Pojedine hijerarhijske razine u poduzeću (strateška, taktička, operativna) kao i pojedine poslovne funkcije ne mogu osigurati učinkovit sustav upravljanja informacijskom sigurnošću ukoliko njihovo djelovanje nije integrirano i utemeljeno na načelima suradnje. Dakle, na razini poduzeća kao cjeline je potrebno promicati kulturu sigurnosti. U skladu s holističkim poimanjem kulture sigurnosti, važno je prilagoditi politiku sigurnosti realnim potrebama poduzeća i prirodi interakcije između pojedinih poslovnih jedinica u sklopu poduzeća. Jedino primjenom suradničkog pristupa može se implementirati uspješan sustav informacijske sigurnosti u poduzeću kao set strategija za upravljanje procesima, alatima i politikama potrebnim za sprječavanje i otkrivanje prijetnji po tiskane i elektroničke povjerljive poslovne i/ili proizvodne informacije.

Na svim organizacijskim razinama potrebno je provoditi kontrolu provedbe politika za realizaciju informacijske sigurnosti. Iz tog se razloga izrađuje godišnji izvještaj o stanju informacijske sigurnosti. Godišnji izvještaj o stanju informacijske sigurnosti mora biti odobren od strane odgovarajućeg autoriteta unutar poduzeća, a treba sadržavati sljedeće elemente:[73]

- dodatke planu informacijske sigurnosti koji proizlazi u iz tehnološkog i operativnog razvoja informacijske tehnologije i poslovnih zahtjeva

[72] Isto
[73] Informacijska sigurnost poduzeća. Preuzeto s: http://vjestak-informatika.com/files/Informacijska%20sigurnost%20poduzeca-Sasa%20Aksentijevic.pdf (21.12.2016.)

- procjenu stanja primjene postojećeg plana informacijske sigurnosti
- status primjene postojećeg plana informacijske sigurnosti
- prijedlog mjera za poboljšanje informacijske sigurnosti poduzeća
- vrijeme potrebno za primjenu mjera poboljšanja
- vezane troškove i proračun potreban za primjenu predloženih mjera.

7.5. Primjer postupanja u slučaju krađe tehničke projektne dokumentacije u poduzeću

U hipotetskom primjeru poduzeće se bavi djelatnošću istraživanja i razvoja u području brodogradnje. Poduzeće je specijalizirano za izradu tehničke dokumentacije za izradu specijaliziranih vrsta plovila, a u svojem poslovanju usko surađuje s Hrvatskim registrom plovila koje je certifikacijsko tijelo koje potvrđuje da određen tehnička dokumentacija ispunjava sve potrebne preduvjete kako bi se izradio prototip plovila i krenulo u proces serijske proizvodnje plovila.

Poduzeće izrađuje usluge tehničke projektne dokumentacije za krajnje naručitelje (proizvođače plovila i Hrvatsku mornaricu), a kako se radi o plovilima s određenim stupnjem inovacije, navedeni projekti često ujedno služe kao podloga za pokretanje postupka zaštite intelektualnog vlasništva putem patenta (*eng. patent pending*). S obzirom da tehnička dokumentacija sadrži određeni stupanj inovativnosti u tehnologiji izgradnje plovila, sve projekte nužno je zaštititi određenim stupnjem tajnosti podataka – u poduzeću tehnička dokumentacija je zaštićena oznakom „vrlo tajno“ te je točno utvrđeno tko ima pravo pristupa određenim vrstama informacija vezanim uz projekt. Nužno je naglasiti kako je riječ o poduzeću koje je osnovala jedinica regionalne samouprave s ciljem podupiranja inovacija u poduzetništvo te inovacija u području opreme kojom raspolaže Hrvatska ratna mornarica te stoga poduzeće surađuje s Nacionalnim tijelom CERT (*engl. Computer emergency respones team*) ili timom za hitne računalne intervencije i Zavodom za sigurnost informacijskih sustava Republike Hrvatske.[74]

Kako bi se informacijski sigurnosni rizici smanjili na minimum, utvrđeno je pravilo da određenom projektu može pristupiti isključivo inženjer brodogradnje – projektant koji na njemu radi. Ulazak u računalni sustav u kojem se nalazi baza podataka projekata potrebno je potvrditi korisničkim imenom i lozinkom, a sustav prati aktivnosti svakog pojedinog

[74] Tijela osnovana sukladno Zakonu o informacijskoj sigurnosti (NN 79/07)

korisnika/inženjera projektanta. Pojedini korisnici mogu pristupiti samo onim projektima za čiju su izradu osobno odgovorni. Na ovaj način eliminira se mogućnost preklapanja odgovornosti koja može utjecati na slabiju zaštitu podataka unutar poduzeća. Klasificiranim podacima (tehničkoj dokumentaciji projekta) se, dakle, pristupa prema načelu „jedan projekt – jedna odgovorna osoba“. Značaj osiguranja klasificiranih podataka u poduzeću XY proizlazi i iz činjenice da je tvrtka sa svakim od klijenata potpisala NDA ugovor kojim pod punom pravnom odgovornošću jamči da podaci o projektu neće „iscuriti“ van povjerljivog kruga.

Potpisivanjem ugovora, primatelj informacije (pravna osoba) se obvezuje čuvati povjerljivost dobivenih informacija i ne otkrivati ih trećima. U protivnom može snositi velike novčane kazne. Obveza čuvanja tajnosti podataka proizlazi i iz ugovornih odnosa sa Ministarstvom obrane RH koje je čest naručitelj tehničke dokumentacije plovila u poduzeću.

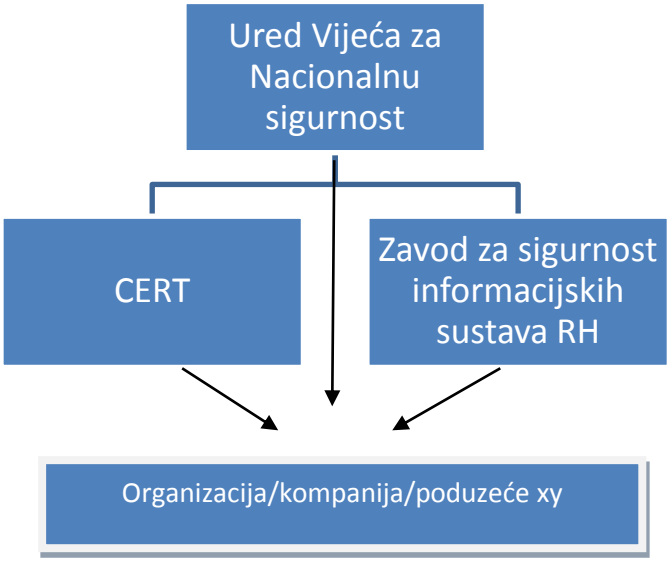
Unatoč visokoj razini zaštite povjerljivih informacija u poduzeću i jasnoj podjeli odgovornosti zaposlenika kada je riječ o pristupu povjerljivim informacijama, u poduzeću je došlo do hakerskog napada i krađe povjerljive projektne dokumentacije. Na taj način je poduzeće po prvi put u svojem poslovanju bilo izloženo računalnom ugrozu i potrebi obrane od istog na temelju koraka utvrđenih Postupkom u slučaju računalnih ugroza. Postupak u slučaju računalnih ugroza u poduzeću XY usklađen je sa smjernicama Nacionalnog tijela CERT pod nazivom *Upravljanje sigurnosnim incidentima*[75]. U konkretnoj situaciji primarni cilj je spriječiti daljnje napade na sustav poduzeća XY s obzirom na informacijsku osjetljivost projekata koje izrađuje, a osobito kada je riječ o projektima čiji je naručitelj Ministarstvo obrane za ratnu mornaricu. Jednaku važnost ima i identifikacija napadača (hakera) s ciljem sprječavanja daljnje distribucije klasificiranih podataka s oznakom „vrlo tajno“, ali i s ciljem provedbe kazneno-pravnih postupaka zbog neovlaštenog pristupa (krađe) povjerljivih informacija putem računalnog kriminala.

Svaki računalni ugroz u poduzeću zahtijeva provedbu detaljne računalne forenzike[76]. Poduzeće informira o incidentu CERT, Zavod za sigurnost informacijskih sustava Republike Hrvatske i krovno tijelo i Ured Vijeća za nacionalnu sigurnost. Navedena vrsta incidenta ne smije se i ne može rješavati bez koordinacije s navedenim tijelima.

[75] Upravljanje sigurnosnim incidentima. Preuzeto s: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-06-266.pdf (22.12.2016.)

[76] Računalna forenzika se bavi prikupljanjem, pretraživanjem, zaštitom i analizom dokaza u digitalnom obliku te uključuje njihovu prezentaciju kao materijalnih dokaza u kasnijim eventualnim sudskim postupcima.

Hijerarhijski ustroj koordinacije između nacionalnih tijela za informacijsku sigurnost i poduzeća prikazan je na slici 4.



Slika 4. Hijerarhijski ustroj u komunikaciji i koordinaciji pri rješavanju problema krađe intelektualnog vlasništva (klasifikacijskog podatka razine „vrlo tajno“) [4]

Izvor: slika koju je izradio autora završnog rada

U navedenoj fazi pokreće se postupak utvrđivanja odgovornosti. Sukladno CERT-ovim smjernicama za upravljanje računalnim ugrozama, konstruiran je životni ciklus upravljanja računalnim ugrozom koji je prikazan na slici 5.

Slika 5. Životni ciklus upravljanja računalnim ugrozom [5]

Postupak pripreme za provedbu forenzične analize računalnog napada na sustav predstavlja esencijalni korak u uspješnoj provedbi te o kvaliteti pripreme uvelike ovisi i sama uspješnost detekcije napadača i sprječavanje daljnjih šteta koje može prouzrokovati širenje vrlo tajnih podataka neovlaštenim korisnicima.

Priprema uključuje:

- Ekipiranje stručnog i kvalitetnog tima za provedbu forenzične analize računalnog napada. Pritom je nužno da osoblje iz pravne osobe koje je izvanredno pristupilo klasificiranom podatku potpiše *Izjavu o postupanju s klasificiranim podacima*,
- Definiranje jasne strukture odgovornosti članova tima naglašavajući potrebu koordinacije s nacionalnim tijelima navedenim u slici 1,
- Alokaciju potrebnih fizičkih resursa (forenzičnih alata) s ciljem uspješne detekcije napadača na računalni sustav i unaprjeđenje stupnja zaštite sigurnosti informacijskog sustava.

Na temelju računalne forenzične analize ispituju se propusti u sigurnosti informacijskog sustava i detektira se izvor računalnog ugroza. Provedba navedene analize ujedno je temeljni dokaz koji se koristi u sudskom postupku protiv osobe koja je neovlašteno pristupila (ukrala) projektne podatke označene oznakom „vrlo tajni“. Kako bi provedba forenzične analize bila uspješna, timu se alocira skup forenzičnih alata, odnosno računalnih programa i uređaja, i to: programski paketi za stvaranje preslika čvrstog diska, alati za rekonstrukciju programskog diska i sklopovlja, alati za dohvaćanje obrisanih podataka, programi za detektiranje zaporki te programi za detekciju izvora hakerskih napada.

Nakon što je računalni ugroz detektiran uporabom sustava za otkrivanje i sprječavanje napada (IDPS [77] sustavom), sprječava se daljnja destruktivna aktivnost napadača unaprjeđenjem postavki vatrozida i antivirusnih programa te se provjeravaju i dovode u ispravno stanje datoteke. Kako bi se sustav u potpunosti zaštitio potrebno je eliminirati (izbrisati) zlonamjerni programski kod koji je korišten za provedbu računalnog ugroza i onemogućiti pristup korisničkom računu s kojeg je obavljena krađa intelektualnog vlasništva poduzeća. Rezultat analize je otkrivanje identiteta grupe napadača i utvrđivanje načina pristupa informacijskom sustavu poduzeća (putem FTP protokola[78]).

[77] IDPS sustav je sustav koji automatizirano prati mrežne i sistemske događaje u svrhu detekcije kršenja sigurnosne politike. To je sustav koji detektira upade u sustav.
[78] FTP protokol je standardni mrežni protokol za premještanje datoteka s jednog hosta na drugi.

Unutar poduzeća izrađuje se izvješće o uzrocima nastanka i tijeku incidenta, identitetu napadača i sigurnosnim propustima informacijskog sustava koje je napadač iskoristio. Također se u izvješću UVNS-u navode mjere koje su se poduzele da bi se eliminirale negativne posljedice napada i kako bi se sustav zaštitio od daljnjih negativnih posljedica širenja zlonamjernog računalnog koda.

Rok dostave izvješća UNVS-u je 90 dana od dana obavijesti o povredi sigurnosti klasificiranih podataka. Dakle, temeljni cilj u razdoblju nakon incidenta je izuzetno poboljšanje preventivnih mjera zaštite informacijskih sustava s ciljem zaštite od daljnjih napada. Međutim, to je samo jedan aspekt djelovanja nakon incidenta. Drugi aspekt djelovanja uključuje provedbu kazneno-pravnih mjera protiv napadača na sustav što se provodi u suradnji s Ministarstvom unutarnjih poslovanja, odnosno nadležnom policijskom jedinicom.

8. ZAKLJUČAK

Suvremeno poslovno okruženje je vrlo složeno i pitanje informacijske sigurnosti postaje sve važnije. Dva su razloga za nastanak opisanog stanja. S jedne strane raste ekonomska vrijednost nematerijalne imovine, odnosno intelektualnog vlasništva i poslovnih tajni jer to postaju primarni generatori konkurentske sposobnosti poduzeća. S druge strane dolazi do kontinuiranog razvoja i napretka informacijsko-komunikacijske tehnologije, a time i do razvoja sve sofisticiranijih oblika računalnog ili kibernetičkog kriminala te su poduzeća suočena sa sve većim izazovima u očuvanju informacijske sigurnosti poduzeća.

Visoka razina informacijske sigurnosti preduvjet je uspješnog poslovanja u javnom i privatnom sektoru. Prilikom suradnje između javnog i privatnog sektora, zaposlenici u pravnoj osobi trebaju imati certifikat na osnovu kojeg im je osiguran pristup određenim klasificiranim podacima. Postupak klasifikacije od strane pravne osobe uređen je Naputkom o klasificiranju podataka u projektu i Projektno-sigurnosnom uputom. Navedena se pravila odnose i na postupanje pravnih osoba sa klasificiranim podacima koje izdaje EU i NATO. Zadaća poduzeća je ujedno osigurati adekvatnu operativnu i tehničku razinu informacijske sigurnosti na intra i interorganizacijskoj razini. Iz tog je razloga nužno da poduzeće definira povjerljive informacije, način njihova čuvanja i da jasno utvrdi tko ima pristup povlaštenim informacijama i u kojim situacijama. Kako bi se osigurao odgovoran pristup prema povlaštenim poslovnim i/ili proizvodnim informacijama, poduzeća sklapaju ugovore o povjerljivosti sa zaposlenicima, dok se u suradnji s trećim stranama sklapaju NDA ugovori kojima se čuva povjerljivost i diskrecija.

Priroda suvremenog poslovnog okruženja nalaže poduzećima potrebu za proaktivnim upravljanjem sustavom informacijske sigurnosti utemeljenim na Planu informacijske sigurnosti poduzeća i dodacima istom. Operativna i tehnička zaštita povjerljivih podataka u poduzeću treba biti nadopunjena sustavnim procesom edukacije kadrova u pogledu rukovanja povjerljivim podacima.

LITERATURA

1. Bedi, Davor. (2015). Koruptivna kaznena djela u javnom i privatnom sektoru u Republici Hrvatskoj s posebnim osvrtom na područje Primorsko-goranske županije í studije slučaja. *Policija i sigurnost*, *24*(1/2015), 65-82.
2. Benčić, Zvonko. (2001). Intelektualno vlasništvo, suvremeni resurs za postizanje globalne tehnološke kompetitivnosti. *Automatika 42*, 3-4, 199-206.
3. Bereš, Paun, (2013). Heuristika i zakonska regulativa u oblasti zaštite tajnih podataka u funkciji edukacije subjekata sistema odbrane. *Vojnotehnički glasnik/Military Technical Courier*, *62*(2), 121-135.
4. Bhawan, Anusandhan. (2001). Intellectual property rights and the Third World. *Current Science*, *81*(8), 955-965.
5. Borba protiv korupcije. Preuzeto s: http://www.policija.hr/32.aspx (23.11.2016.)
6. Carlsson, Bo, Fridh, Ann- Charlotte. (2002). Technology transfer in United States universities. *Journal of Evolutionary Economics*, *12*(1-2), 199-232.
7. Cvitanović, Leo, Novoselac, Petar. (2002). *Rječnik kaznenog prava*. Zagreb: Masmedia, str. 321.
8. Ćosić-Dragan, Daniel. (2008). Poslovnost i izvjesništvo. *National security and the future*, *9*(1-2.), 53-76.
9. Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka
10. Dulčić, K.atarina, Bodiroga-Vukobrat, Nada. (2008). Zaštita osobnih podataka pacijenata u europskom i hrvatskom pravu. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, *29*(1), 371-411.
11. Duraković, Mia (2009). Pregled razvoja autorskog prava u Repuplici Hrvatskoj s naglaskom na promjene uvjetovane usklađivanjem s pravnom stečevinom EU. *Zbornik radova Pravnog fakulteta u Splitu*, *46*(3), 613-630.
12. Heimdal Security. Preuzeto s: https://heimdalsecurity.com/blog/10-critical-corporate-cyber-security-risks-a-data-driven-list/ (18.12.2016.)
13. Informacijska sigurnost poduzeća. Preuzeto s: http://vjestak-informatika.com/files/Informacijska%20sigurnost%20poduzeca-Sasa%20Aksentijevic.pdf (21.12.2016.)
14. Informacijska sigurnost. Preuzeto s: www.orkis.hr/Download.ashx?FileID=88e3b8ea-6439-4e55-b89f-054762971b63, (07.12.2016.)

15. Katulić, Tihomir. (2005). Intelektualno vlasništvo danas. *Edupoint: časopis o primjeni informacijskih tehnologija u obrazovanju*, *5*(36).
16. Kazneni zakon, pročišćeni tekst zakona NN 125/11, 144/12, 56/15, 61/15 na snazi od 30.05.2015.
17. Kešetović, Željko, Toth, Ivan, (2012). *Problemi kriznog menadžmenta: znanstvena monografija*. Veleučilište Velika Gorica.
18. Klaić, Aleksandar, Perešin, Anita. (2011). Koncept regulatornog okvira informacijske sigurnosti. Preuzeto s: https://bib.irb.hr/datoteka/521742.AK_AP_Koncept_regulativnog_okvira_inf_sig_DKU_032011.pdf (06.12.2016.)
19. Legal Information Institute. Preuzeto s: https://www.law.cornell.edu/wex/trade_secret (20.11.2016.)
20. Legčević, Jelena, Taučer, Katarina. (2014). Krizni menadžment u funkciji nove teorije menadžmenta. *Ekonomski Vjesnik/Econviews: Review of contemporary business, entrepreneurship and economic issues*, *27*(1), 199-208.
21. Mintas – Hodak, Ljerka. (2010). *Pravno okruženje poslovanja*, Zagreb: Mate, str. 402.
22. Mučalo, Marina, Sviličić, Nikša. (2000). Virtual War. *Politička misao*, *37*(1), 229-242.
23. Nacionalni CERT. Preuzeto s: http://www.cert.hr/onama (03.12.2016.)
24. Načela i smjernice zaštite osobnih podataka. Preuzeto s: http://www.snz.unizg.hr/wnew/nacela1.pdf (30.11.2016.)
25. Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NN 108/2015)
26. Oznaka zemljopisnog porijekla. Preuzeto s: http://www.dziv.hr/hr/intelektualno-vlasnistvo/oznake/ (25.11.2016.)
27. Pal, Nikhil, Pal, Sankar, (1991). Entropy: A new definition and its applications. *IEEE transactions on systems, man, and cybernetics*, *21*(5), 1260-1270.
28. Panian, Željko. (2000). *Poslovna informatika: koncepti, metode i tehnologija*. Zagreb: Potecon doo., str. 32.
29. Pažur, Ivana. (2004). Autori znanstvenih radova i autorsko pravo. *Vjesnik bibliotekara Hrvatske*, *47*(1-2), 95-108.
30. Pedrycz, Witold. (2005). *Knowledge-based clustering: from data to information granules*. London: John Wiley & Sons
31. Sajko, Mario. (2016). Mjerenje i vrednovanje učinkovitosti informacijske sigurnosti. Preuzeto s:

https://www.fer.unizg.hr/_download/repository/Mario_Sajko_%5Bkvalifikacijski_rad%5D.pdf (04.12.2016.)

32. The property rights – origin of private rights. Preuzeto s: https://fee.org/articles/the-property-rights-origins-of-privacy-rights/ (20.11.2016.)
33. Trade Secret. Preuzeto s: http://www.yellowhours.com/store_2919343/Trade-Secret_269-329-1939_Portage_Michigan_USA.html (19.11.2016.)
34. Upravljanje sigurnosnim incidentima. Preuzeto s: http://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-06-266.pdf (22.12.2016.)
35. Ured vijeća za nacionalnu sigurnost. Preuzeto s: http://www.uvns.hr/main.aspx?id=109 (22.11.2016.)
36. Ustav Republike Hrvatske, pročišćeni tekst NN 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.
37. Vuković, Hrvoje. (2012). Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj. *National security and the future*, *13*(3), 12-31.
38. Watson, Alan. (1996). Trade Secrets and Roman Law: The Myth Exploded. *Tul. Eur. & Civ. LF*, *11*, 1.
39. Winkler I. Case study of industrial espionage through social engineering. Preuzeto s: https://new.social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html (24.05.2017.)
40. Za odavanje poslovne tajne i deset godina zatvora. Preuzeto s: http://lider.media/arhiva/32127/ (20.11.2016.)
41. Zemljić, Marija. (2014). *Industrijska špijunaža* (završni rad). Varaždin: FOI, str. 32.
42. Zlatović, Dragan. (2009). „Pravni aspekti parodije "i intelektualno vlasništvo. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, *30*(1), 725-766.
43. Zakon o informacijskoj sigurnosti NN (79/07)
44. Zakon o informacijskoj sigurnosti, NN 79/07.
45. Zakon o kritičnim infrastrukturama (NN 56/13)
46. Zakon o patentu, pročišćeni tekst zakona, NN 173/03, 87/05, 76/07, 30/09, 128/10, 49/11, 76/13
47. Zakon o pravu na pristup informacijama, pročišćeni tekst zakona NN 25/13, 85/15 na snazi od 09.08.2015.
48. Zakon o tajnosti podataka, pročišćeni tekst zakona NN 79/07.
49. Zakon o žigu, pročišćeni tekst zakona NN 173/03, 54/05, 76/07, 30/09, 49/11.

POPIS SLIKA

Str.