Zaštita podataka u uredskom poslovanju

Kopajtić, Hrvoje

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **The University of Applied Sciences Baltazar Zaprešić / Veleučilište s pravom javnosti Baltazar Zaprešić**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:129:953913

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-08-08**

Repository / Repozitorij:

Digital Repository of the University of Applied Sciences Baltazar Zaprešić - The aim of Digital Repository is to collect and publish diploma works, dissertations, scientific and professional publications

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ
Zaprešić

Preddiplomski stručni studij

Poslovanje i upravljanje

HRVOJE KOPAJTIĆ

ZAŠTITA PODATAKA U UREDSKOM POSLOVANJU

STRUČNI ZAVRŠNI RAD

Zaprešić, 2020. godine

VELEUČILIŠTE
s pravom javnosti
BALTAZAR ZAPREŠIĆ

Zaprešić

Preddiplomski stručni studij
Poslovanje i upravljanje

STRUČNI ZAVRŠNI RAD

ZAŠTITA PODATAKA U UREDSKOM POSLOVANJU

Mentor:
dr. sc. Dragutin Funda

Student:
Hrvoje Kopajtić

Naziv kolegija:
UPRAVLJANJE KVALITETOM U UREDSKOM POSLOVANJU

JMBAG:
0082037354

SADRŽAJ

SAŽETAK

Tema ovog završnog rada jest zaštita podataka u uredskom poslovanju. Veoma je bitno da se zaštite podaci, bilo to fizičkom ili elektroničkom zaštitom, kako bi određena organizacija mogla obavljati svoje poslovanje neometano.

U radu se pristupilo definiranju uredskog poslovanja kojeg se može definirati kao rukovanje spisima, zatim njihovo razvrstavanje, evidentiranje, te pretraživanje.

Razlikujemo šest načela uredskog poslovanja: jednostavnost, preglednost, ekspeditivnost, jednoobraznost, ekonomičnost te zakonitost.

Sigurnost podataka te zaštita informacijskih sustava mogu se smatrati kao obveza informatičkih stručnjaka, jer današnji svijet karakterizira informatička nesigurnost, stoga je veoma bitno da se računala, odnosno podaci zaštite na adekvatan način.

Bitno je zaštititi podatke i to fizičkom ili elektroničkom zaštitom. Kada govorimo o fizičkoj sigurnosti, tada se podrazumijeva i zaštita informacija, odnosno infrastrukture, uslijed prirodnih pojava, poput požara, poplava i slično, ali i brigu oko osiguranja adekvatnih uvjeta te odabira pozicije prostorija.

Osim fizičke zaštite podataka u uredskom poslovanju, postoji i elektronička zaštita, pomoću koje se štite podaci od uništenja, neovlaštenih upada i slično. U nastavku su navedene i definirane vrste elektroničke zaštite, poput zaporki, kriptiranje te digitalni vodeni žig.

Hrvatska pošta je najbolji primjer kako treba poslovati jer proteklih godina prolazi kroz sveobuhvatnu digitalnu transformaciju. Njihova usmjerenost na elektroničke usluge i digitalno poslovanje postavlja kibernetičku sigurnost na prvo mjesto, jer znaju da je to veoma bitno ukoliko žele biti sigurni da će svakodnevno moći obavljati svoje poslovanje neometano i bez straha od hakerskih napada.

KLJUČNE RIJEČI: zaštita podataka, uredsko poslovanje, informacijski sustav, fizička zaštita podataka, elektronička zaštita podataka

Title in English: Data protection ih office operations

ABSTRACT

The topic of this final paper is data Protection in Office Operations. It is very important to protect data, be it physical or electronic protection, so that a certain organization can run its business smoothly.

The paper approaches the definition of office operations, which can be defined as the handling of files, then their classification, recording, and search.

We distinguish six principles of office business: simplicity, transparency, expediency, uniformity, economy, and legality.

Data security and protection of information systems can be considered as an obligation of IT experts, because today's world is characterized by information insecurity, so it is very important that computers and data are adequately protected.

It is important to protect data with physical or electronic protection. When we talk about physical security, then we mean the protection of information or infrastructure due to natural phenomena, such as fires, floods and a like, but also care about ensuring adequate conditions and choosing the position of the premises.

In addition to physical data protection in office operations, there is also electronic protection, which protects data from destruction, unauthorized intrusions and the like. The types of electronic protection, such as passwords, encryption, and digital watermark, are listed and defined below.

Croatian Post is the best example of how to do business because in recent years it has undergone a comprehensive digital transformation. Their focus on electronic services and digital business puts cyber security first, as they know this is very important if they want to be sure that they will be able to run their business on a daily basis without interruption and without fear of hacker attacks.

KEY WORDS: data protection, office operations, information system, physical data protection, electronic dana protection

1. UVOD

Zaštita podataka u današnjem svijetu je poželjna jer se često događaju napadi na raznorazne podatke. Stoga je veoma bitno na adekvatan način, bilo fizičkom ili elektroničkom zaštitom, omogućiti neometano uredsko poslovanje.

Tema ovog završnog rada je zaštita podataka u uredskom poslovanju. To je poprilično raširena tematika, jer i putem medija može se doznati o napadima na elektroničke podatke, koji ometaju rad organizacija, te im nanose velike štete u financijskom smislu.

Rad je podijeljen na način da se u prvom dijelu rada objašnjavaju uvodni pojmovi o zaštiti podataka u uredskom poslovanju, potom se u drugom dijelu definira pojam i načela uredskog poslovanja, te temeljni pojmovi vezani uz uredsko poslovanje. Treći dio rada definira zaštitu podataka u uredskom poslovanju, koja podrazumijeva fizičku i elektroničku zaštitu. Pod fizičkom zaštitom ubraja se zaštita okoline, zaštita recepcije, zaštita prostorije, zaštita opreme, a pod zaštitom opreme razlikuje se još zaštita poslužitelja, te zaštita osobnih računala. Pod elektroničkom zaštitom razlikujemo zaporke te je pod tim definiran odabir, pohrana i alati za odabir zaporke, zatim je definirano kriptiranje te digitalni vodeni žig.

Potom su navedeni savjeti za zaštitu uredskog poslovanja, dok u četvrtom dijelu rada je naveden primjer Hrvatske pošte na koji način štiti svoje uredsko poslovanje, ali i kako su reagirali kada je prošle godine izveden hakerski napada na njihov sustav.

U petom dijelu rada je provedeno istraživanje zbog potreba izrade rada, te dobivenim rezultatima se uočava kako su ispitanici upoznati sa pojmom uredskog poslovanja te da uočavaju koliko je bitna adekvatna zaštita podataka u uredskom poslovanju.

2. UREDSKO POSLOVANJE

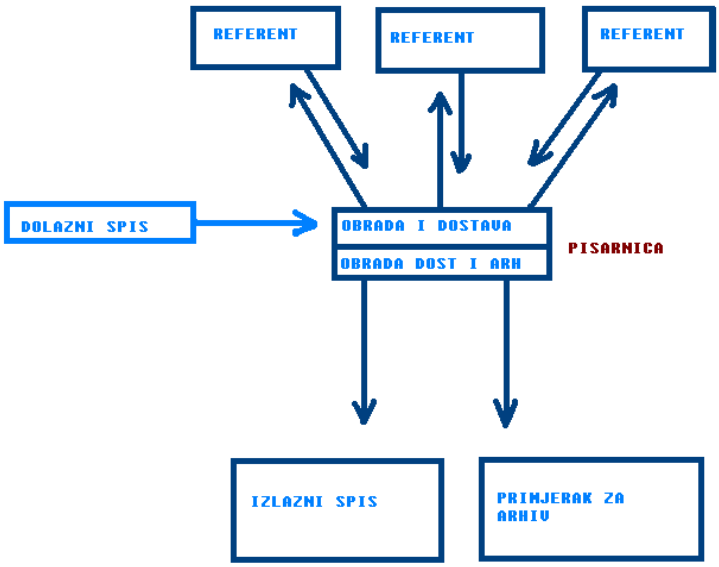
Prema podacima službene mrežne stranice Državnog arhiva Varaždin, „Uredsko poslovanje je rukovanje spisima, njihovo razvrstavanje, evidentiranje i pretraživanje. To su svi oni tehnički postupci na organizaciji dokumenata, pomoćni uredski poslovi koji se svode na upis spisa u knjige, razvrstavanje, praćenje ulaznog i izlaznog prometa spisa i konačno njegovo odlaganje u pismohranu.“ (Državni arhiv Varaždin, n.d.:1)

Prema podacima službene mrežne stranice Ministarstva pravosuđa i uprave, „Uredsko poslovanje je skup pravila i mjera u postupanju s pismenima, koji obuhvaća sljedeće:

- ✓ primanje
- ✓ izdavanje
- ✓ evidencija
- ✓ dostava u rad
- ✓ obrada
- ✓ otpremanje
- ✓ čuvanje
- ✓ izlučivanje i
- ✓ predaja nadležnom arhivu ili drugom nadležnom tijelu.“ (Ministarstvo pravosuđa i uprave, n.d.)

Prema podacima Državnog arhiva Varaždin, „Svrha uredskog poslovanja je evidentiranje i pretraživanje spisa, ne i sadržajna obrada, sadržajnu obradu rade stručne službe stvaratelja, uredsko poslovanje je pomoćna služba i u funkciji je stručne obrade spisa. (…) Središte uredskog poslovanja je pisarnica u kojoj počinje i završava životni put spisa, pisarnica mora imati sustav upravljanja spisima o kojemu zavisi učinkovitost uredskog poslovanja.“ (Državni arhiv Varaždin, n.d.:2-3)

U nastavku je slika koja prikazuje shemu uredskog poslovanja.



Slika 1: Shema uredskog poslovanja

Izvor: Državni arhiv Varaždin, preuzeto sa http://dav.hr/dokumenti1/UREDSKO%20POSLOVANJE.doc, str.3.

Prema podacima službene mrežne stranice Carnet-a, „Uredsko poslovanje u užem smislu podrazumijeva:

- ✓ zaprimanje i pregleda akata i drugih pošiljki
- ✓ razvrstavanje i raspoređivanje akata
- ✓ upisivanje akata
- ✓ dostavu akata u rad
- ✓ administrativno-tehničku obradu akata
- ✓ otpremu akata
- ✓ razvođenje akata
- ✓ arhiviranje i čuvanje akata.“ (Carnet, 2020)

Što se tiče uredskom poslovanja u širem smislu, ono obuhvaća, prema podacima sa službene mrežne stranice Carnet-a,

- ✓ „(…) periodično izvješćivanje o predmetima i aktima
- ✓ izrada godišnjih statističkih izvješća
- ✓ vođenje evidencija o državnim propisima
- ✓ nadzor i izvješćivanje o provođenju državnih propisa

- ✓ vođenje evidencija o internim propisima.“ (Carnet, 2020)

Autor Odobaša ističe, „U najširem smislu uredsko poslovanje obuhvaća cjelokupni uredski rad, dakle, ne samo rukovanje aktima već i npr. neposredno i posredno (npr. telefonom) komuniciranje sa strankama ili s drugim službenim osobama u organima uprave ili upravnim organizacijama.“ (Odobaša, 2010: 2)

2.1. NAČELA UREDSKOG POSLOVANJA

Razlikujemo šest načela uredskog poslovanja koja su u nastavku navedena i objašnjena:

- ✓ jednostavnost,
- ✓ preglednost,
- ✓ ekspeditivnost,
- ✓ jednoobraznost,
- ✓ ekonomičnost,
- ✓ zakonitost.

Prema riječima autora Smolčić, Andrlić, Hak, „Uredsko poslovanje vodi se prema načelu jednostavnosti, odnosno sve se radnje moraju obavljati na jednostavan i razumljiv način svima koji koriste uredsko poslovanje u svom radu, zatim prema načelu preglednosti, prema kojem se sve radnje moraju obavljati pregledno i logičnim slijedom. Načelo ekspeditivnosti, kao jedno od temeljnih načela uredskog poslovanja, znači da sve radnje u uredskom poslovanju moraju biti završene pravodobno, uz minimalno utrošeno vrijeme ali ne na štetu ispravnosti i kvalitete rada.“ (Smolčić, Andrlić, Hak, 2008)

Autori Smolčić, Andrlić, Hak ističu, „Načelo jednoobraznosti u uredskom poslovanju obavlja se uvijek na isti način, prema propisanim pravilima koja su svima dostupna. Načelo ekonomičnosti u uredskom poslovanju znači da se radnje u uredskom poslovanju obavljaju u što kraćem roku i sa što manje sredstava, ali ne na štetu načela točnosti, jer sve radnje moraju se obaviti točno i nedvojbeno, uglavnom u pisanom obliku, a način utvrđivanja činjenica mora biti siguran i objektivan. (…) izuzetno bitno načelo je načelo zakonitosti koje predstavlja obvezu svih subjekata da se pridržavaju važećih propisa, u prvom redu zakona.“ (Smolčić, Andrlić, Hak, 2008)

2.2. TEMELJNI POJMOVI VEZANI UZ UREDSKO POSLOVANJE

U Uredbi o uredskom poslovanju (NN 7/2009):se navode temeljni pojmovi uredskog poslovanja, te su navedeni u nastavku:

„Pisarnica je posebna unutarnja ustrojstvena jedinica koja obavlja poslove primanja i pregleda pismena i drugih dokumenata, njihovog razvrstavanja i raspoređivanja, upisivanja u odgovarajuće evidencije (očevidnike), dostave u rad, otpremanja, razvođenja te njihova čuvanja u pismohrani.

Pismohrana je dio pisarnice koja obavlja poslove čuvanja i izlučivanja pismena te drugih dokumenata. Dokument je svaki podatak, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, fizički predmet, priopćenje ili informacija, koji sadržajem i strukturom čini raspoznatljivu i jednoznačno određenu cjelinu povezanih podataka.“ (Uredba o uredskom poslovanju, 2009)

„Elektronički dokument je bilo koja vrsta elektroničkog zapisa koji nema svojstva elektroničke isprave. Elektronička isprava je isprava uređena sukladno posebnim propisima. (…) Spis (predmet) je skup pismena, priloga i drugih dokumenata koji se odnose na isto pitanje ili zadaću ili koji na drugi način čine posebnu cjelinu. (…) Brojčana oznaka je identifikacija predmeta odnosno pismena i sastoji se od klasifikacijske oznake i urudžbenog broja. urudžbeni broj označava stvaratelja pismena, godinu nastanka i redni broj pismena unutar predmeta. Klasifikacijska oznaka označava predmet prema sadržaju, godini nastanka, obliku i rednom broju predmeta. Urudžbeni broj označava stvaratelja pismena, godinu nastanka i redni broj pismena unutar predmeta.“ (Ibidem, 2009)

3. ZAŠTITA PODATAKA U UREDSKOM POSLOVANJU

Prema riječima autorice Klasić, „Sigurnost podataka i zaštita informacijskih sustava dugo godina su smatrani ekskluzivnim pravom, ali i obvezom informatičkih stručnjaka. (…) s porastom primjene računala u poslovnoj praksi počeli su se uvoditi prvi standardi koji su se odnosili na siguran rad s računalima i podacima pohranjenim u informacijskim sustavima. U početku je bio presudan značaj fizičke zaštite sustava jer je računalna oprema bila centralizirana, uglavnom u dobro čuvanim posebnim objektima ili prostorima.“ (Klasić, 2007:38)

Autorica Klasić ističe, „Distribucijom opreme i podataka te uključivanjem u internet, potreba za zaštitom sustava postala je još važnijom, ali i znatno složenijom. Prepoznavanje te potrebe ogleda se u izradi i primjeni raznih uputa o zaštiti podataka koji se primjenjuju u poduzećima.“ (Klasić, 2007:38)

Prema podacima Središnjeg državnog ureda za e-Hrvatsku, „U poslovnom procesu (uredsko poslovanje) sigurnost podataka podrazumijeva postojanje sigurnosnih procedura za prijem, rukovanje, pohranjivanje, arhiviranje, uništavanje, distribuciju, umnožavanje, prepisivanje, prevođenje, izdavanje, uvid i objavljivanje podataka. Sigurnosne procedure uključuju i postojanje evidencijskog sustava o kontroli pristupa i izvršenim radnjama, te kretanju (kolanju) i mjestu podataka.“ (Središnji državni ured za e-Hrvatsku, 2005:15)

3.1. FIZIČKA ZAŠTITA PODATAKA

Bitno je zaštititi podatke, prije svega potrebno je provesti mjere fizičke zaštite podataka. Prema podacima Središnjeg državnog ureda za e-Hrvatsku, „Mjere fizičke sigurnosti obuhvaćaju i zaštitu informacija (infrastrukture) uslijed prirodnih pojava (požara, poplave, potresa, oluje), ali i brigu oko osiguranja adekvatnih uvjeta (temperatura, vlaga, neprekidno napajanje, zračenje) i odabira pozicije prostorija.“ (Središnji državni ured za e-Hrvatsku, 2005:15)

U nastavku su navedeni i objašnjeni načini fizičke zaštite, poput zaštite okoline, recepcije, prostorije, te opreme. Što se tiče zaštite opreme, tu razlikujemo zaštitu poslužitelja, te osobnih računala.

Prema podacima Nacionalnog CERT-a, „Okolina objekta je prvi element nad kojim treba provesti postupke fizičke zaštite. (…) Jedan od osnovnih načina zaštite objekta je postavljanje ograda oko područja koje je u vlasništvu organizacije. Time se izravno sprječava prilazak osoba do objekta te zahtjeva najava prije ulaska u prostore organizacije. (…) Postizanje adekvatne

zaštite okoline definirano je kroz CPTED (eng. Crime prevention through environmental design) dizajn.“ (Nacionalni CERT, 2010:13)

Prema riječima autorice Balgač, „Prevencija kriminaliteta kroz dizajn okoliša-CPTED je pristup koji gradskim vlastima, lokalnoj zajednici, policiji, planerima i arhitektima, vlasnicima posjeda, ali i građanima pruža jednostavne i često ekonomične mjere i tehnike, konkretna i praktična arhitektonska i urbanistička rješenja koja dokazano smanjuju prilike i mogućnosti da se kriminal dogodi. Osim smanjenja kriminaliteta CPTED pomaže u smanjenju straha od kriminala i u konačnici unaprjeđuje i poboljšava kvalitetu na nekom području.“ (Balgač, 2013:102)

Što se tiče zaštite okoline, postizanje adekvatne zaštite se postiže i mjerama prirodnog nadzora, prirodnog pristupa, te teritorijalno pojačanje.

Prema podacima Nacionalnog CERT-a, „Mjere prirodnog nadzora povećavaju vizualnu percepciju i strah da bi napadač mogao lako biti uočen. Provodi se dizajniranjem prostornih obilježja i aktivnosti na način da se poveća vidljivost i potiču pozitivne društvene interakcije. (…) Mjere prirodnog pristupa kontroliraju granice kako bi se jasno razlikovao prostor javnog i privatnog vlasništva. (…) Teritorijalno pojačavanje promiče društveni nadzor kroz definiranje vlasničke zbrinutosti. Stvaranjem razdvojenosti javnog i privatnog prostora, postiže se osjećaj vlasništva nad privatnim.“ (Nacionalni CERT, 2010:13)

Prema podacima Nacionalnog CERT-a, „U većini organizacija se, odmah nakon ulaska u objekt, dolazi do prostora za informiranje i obavljanje nekih administrativnih poslova - recepcije. (…)Većem stupnju zaštite pridonosi i dizajniranje prostora na način da neautorizirane osobe nemaju pristup dijelu za zaposlenike. Postavljanje računala ne smije omogućiti posjetiteljima pregled sadržaja na njima, niti njihovo korištenje. U područje recepcije moguće je također postaviti alarme, gumbe za slučaj opasnosti i kamere za nadzor.“ (Nacionalni CERT, 2010:14)

Pod zaštitu prostorija podrazumijeva se upotreba kamera koje imaju nadzorne ekrane, te se na taj osim potencijalnih kriminalaca, nadzire rad samih zaposlenika, potom gumbi za slučaj opasnosti, primjerice u situaciji kada se dogodi neki neplanirani događaj poput pljačke, da zaposlenik može pritisnuti taj gumb i obavijestiti nadležne službe da su u opasnosti.

Zatim se može postaviti protuprovalni alarm, pomoću kojeg se čuvaju prostorije koje su zaključane, te prostorije nakon završetka radnog vremena. Mogu se na prozore postaviti brojne prepreke na prozore, ugradnja lokota i slično.

Veoma je bitno pravilno zaštiti opremu i uređaje. Autorica Juran ističe, „Zaštita opreme smatra se najvažnijim aspektom fizičke zaštite informacijskog sustava, ali joj nije usmjerena dovoljna pažnja u obliku načina zaštite. Radi se o tome da se svaka oprema odnosno uređaj vrednuje po svojim karakteristikama i namjeni stoga je razina zaštite različita za različiti uređaj ili opremu.“ (Juran, 2014:52)

Prema podacima Nacionalnog CERT-a, „Poslužitelji predstavljaju vrlo važan aspekt za poslovanje svake organizacije jer mogu sadržavati vrlo važne informacije , a zaposlenici ih svakodnevno koriste. Zbog takvih namjena, najbolja praksa je razdvajanje svakodnevnih funkcija od poslužitelja. To znači da se jedan poslužitelj ne bi trebao koristiti za obavljanje svakodnevnih zadataka. Još jedan od važnih elemenata zaštite predstavlja pravilan smještaj poslužitelja. Najbolje bi bilo poslužitelje izdvojiti u posebnu prostoriju koju je moguće dobro nadzirati. Također, smještaj treba implementirati tako da se spriječi pomicanje i premještanje poslužitelja. .“ (Nacionalni CERT, 2010:15)

Prema podacima Nacionalnog CERT-a, „Najosnovniji način zaštite osobnih računala uključuje dobru edukaciju zaposlenika. Ukoliko su zaposlenici upoznati s pravilnim načinom rukovanja s računalom, rizik od raznih prijetnji znatno je umanjen. Zaposlenicima je potrebno jasno definirati pravila u obliku sigurnosnih politika te ih predstaviti na jednostavan način. (…) Uporaba nadzora u obliku postavljanja kamera i osiguranja može spriječiti zaposlenike pri pokušaju oštećivanja ili krađe računala. Nadzorne kamere potrebno je postaviti na ključna mjesta, koja su u blizini vrijednih uređaja ili računala.“ (Nacionalni CERT, 2010:15)

3.2. ELEKTRONIČKA ZAŠTITA PODATAKA

Osim fizičke zaštite podataka u uredskom poslovanju, postoji i elektronička zaštita, pomoću koje se štite podaci od uništenja, neovlaštenih upada i slično. U nastavku su navedene i definirane vrste elektroničke zaštite, poput zaporki, kriptiranje, te digitalni vodeni žig.

3.2.1. ZAPORKE

Nacionalni CERT ističe važnost zaporki, „Zaporka je oblik tajnog podatka kojeg je potrebno poznavati da bi se pristupilo određenim resursima, informacijama i slično. Zaporka se čuva od onih koji danim resursima ne smiju imati pristup, dok se oni koji pokušavaju resursima pristupiti provjeravaju znaju li lozinku ili ne (prema čemu im se dozvoljava ili odbija pristup). To je kombinacija znakova (slova, simbola, brojeva i tako dalje) koje računalo pamti (ili pamti kako

prepoznati zaporku). Svaki put kad korisnik želi pristupiti podatku pod zaporkom od njega se traži upisivanje iste, čuvajući time njegovu privatnost. Dokumenti se, dakle, mogu zaštititi i dodavanjem zaporke. Na taj se način ograničava pristup dokumentu.“ (Nacionalni CERT, 2010:8)

Veoma je bitno da se na pravilan način odabere zaporka, odnosno smisliti odgovarajuću zaporku koja se ne može saznati. Dakle, ne smije se sastojati od poznatih riječi, datuma rođenja i slično, jer postoji mogućnost da netko tko zna pojedine osobne podatke, može doći do lozinke.

Prema podacima mrežne stranice Infinius, „Osnovna pravila koje vrijede za pravilno postavljanje lozinke su:

- ✓ mora se sastojati od barem osam znakova
- ✓ lozinka mora biti kombinacija slova, znamenki i simbola
- ✓ ne smiju sadržavati osobne informacije (imena, datumi rođendana i sl.)
- ✓ ne smije biti neka riječ iz rječnika.“ (Infinius, 2011)

Prema podacima Centra informacijske sigurnosti, „Moguće je lozinke pohraniti u izvornom obliku ili ih šifrirati jednosmjernim algoritmom stvaranjem sažetka (engl. Hash function). Ukoliko se lozinka pohranjuje u izvornom obliku, sustav prilikom autentifikacije treba samo usporediti jesu li unesena i pohranjena vrijednost identične. Dodatna prednost ovog oblika pohrane je da se u slučaju kada korisnik zaboravi lozinku ona lako može poslati korisniku putem elektroničke pošte.“ (Centar informacijske sigurnosti, 2012:8)

Centar informacijske sigurnosti ističe, „Drugi oblik pohrane lozinki podrazumijeva njihovo šifriranje. Postoje različite metode sigurne pohrane lozinki njihovim šifriranjem. No, sve one uključuju uporabu jednosmjernih funkcija za šifriranje. Samo ime označava kako se radi o jednosmjernoj operaciji. Naime, nakon šifriranja dobiva se sažetak lozinke koji jedinstveno identificira samo tu lozinku. Dodatno, iz sažetka nije moguće rekonstruirati izvornu lozinku. Najpopularnije lozinke za izradu sažetaka su MD5 (engl. Message-Digest 5) i SHA (engl. Secure Hash Algorithm) algoritmi.“ (Centar informacijske sigurnosti, 2012:8-9)

Podaci Centra informacijske sigurnosti govore, „Kako bi se korisnicima olakšao odabir lozinke, postoje mnogi alati koji predlažu lozinke ili ih ocjenjuju. Alat Password Meter daje detaljnu ocjenu kvalitete lozinke. (…) Alat je potpuno besplatan te dostupan u obliku jednostavne i pregledne web aplikacije. Informacije o ocjeni lozinke su vidljive trenutno, a namijenjene su

kako bi korisniku olakšao odabir kvalitetnije lozinke. (…) Osim alata za ocjenu lozinki, postoje i alati za proizvodnju kvalitetnih lozinki. Jedan od najpoznatijih alata za proizvodnju lozinki na sustavima UNIX/Linux je pwgen. Alat proizvodi lozinke koje se lako pamte, dok su istovremeno sigurne i kvalitetne.“ (Centar informacijske sigurnosti, 2012:16)

Prema podacima Centra informacijske sigurnosti, „KeePass predstavlja jedan od najpopularnijih alata otvorenog koda za pohranu lozinki. Omogućuje pohranu svih korisničkih lozinki u jednu bazu podataka koja je zaključana tajnim ključem. Ovaj tajni ključ je poznat isključivo korisniku i mora se zapamtiti. No, pamćenje jednog tajnog ključa je jednostavnije nego pamtiti velik broj lozinki. Baza podataka se šifrira putem popularnih kriptografskih algoritama. Tajni ključ za pristup svim ostalim lozinkama se ne pohranjuje u izvornom obliku već se koristi sažetak (engl. hash) ključa napravljen pomoću algoritma SHA-256.“ (Centar informacijske sigurnosti, 2012:18)

3.2.2. KRIPTIRANJE

Prema podacima Nacionalnog CERT-a, „Postupak kriptiranja uključuje preoblikovanje otvorenog ili jasnog teksta u tekst nerazumljiv osobama kojima nije namijenjen. Osobe kojima je dokument namijenjen i koje ga smiju pročitati moraju posjedovati poseban ključ za pretvaranje dokumenta u jasan tekst, odnosno dekriptiranje. Postoje simetrični i asimetrični kriptosustavi.“ (Nacionalni CERT, 2010:6)

Prema podacima Leksikografskog zavoda Miroslav Krleža, „ Simetrični kriptosustavi imaju jednak ključ za kriptiranje i dekriptiranje. Takvi su sustavi konvencionalni (u njih ulaze svi postupci predračunalnoga doba), a sigurnost se postiže osiguravanjem tajnosti ključa, pa se još nazivaju i kriptosustavi s tajnim ključem. Danas je najrašireniji simetrični kriptosustav DES (od engl. Data Encryption Standard).“ (Leksikografski zavod Miroslav Krleža, 2020)

Podaci Leksikografskog zavoda Miroslav Krleža ističu, „Asimetrični kriptosustavi ili kriptosustavi s javnim ključem postavljeni su tako da se ključ za dekriptiranje ne može u prihvatljivom vremenu izračunati iz ključa za kriptiranje. Zbog toga se razmjena tajnih ključeva može obaviti preko nesigurnih komunikacijskih kanala. (…) U asimetričnim kriptosustavima svaki sudionik u komuniciranju mora imati dva ključa: ključ kriptiranja, koji se javno obznanjuje, i ključ dekriptiranja, koji poznaje samo vlasnik. Svatko može kriptirati poruku opće poznatim javnim ključem, ali dekriptiranje može obaviti vlasnik svojega privatnoga ključa.“ (Leksikografski zavod Miroslav Krleža, 2020)

Prema podacima službene mrežne stranice Centra informacijske sigurnosti, „Šifriranje (encryption) je pretvaranje izvornog teksta (plaintext) u šifrirani tekst (ciphertext) pomoću određene šifre (algoritma – AES, 3DES).“ (Centar za informacijsku sigurnost, 2011)

Prema podacima službene mrežne stranice Zavoda za sigurnost informacijskih sustava, „Državna tijela, jedinice lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima koje svoje informacijske sustave javnim i neštićenim komunikacijskim kanalima povezuju s drugim informacijskim sustavima u svrhu međusobne razmjene klasificiranih podataka moraju, pored ostalih mjera informacijske sigurnosti, primijeniti mjere kriptografske zaštite. Osim tajnosti, kriptografske metode osiguravaju i cjelovitost, izvornost i neporecivost pojedinog klasificiranog podatka.“ (Zavod za sigurnost informacijskih sustava, n.d.)

3.2.3. DIGITALNI VODENI ŽIG

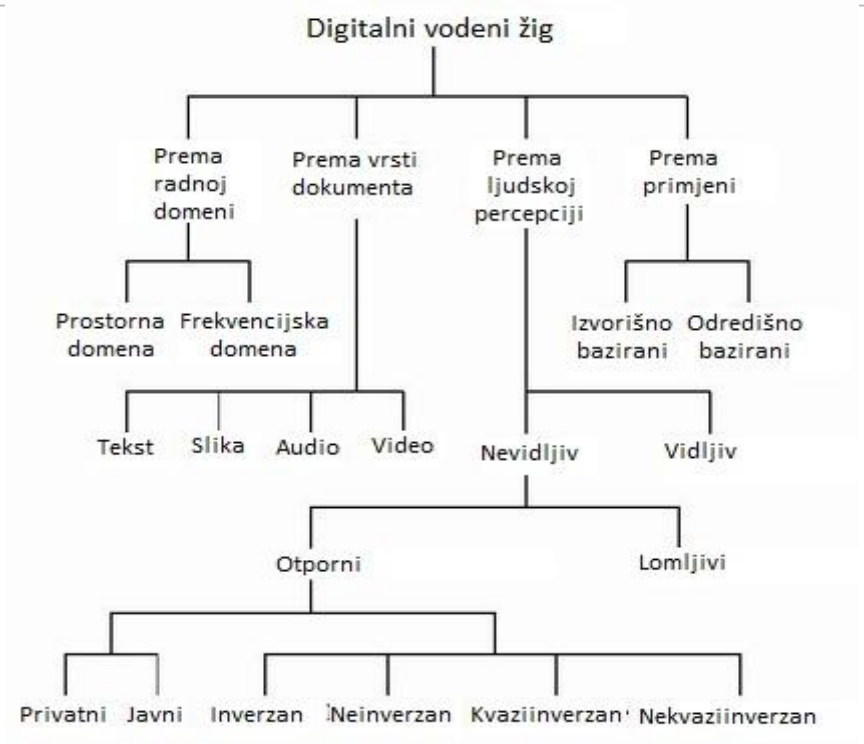
Autor Stančić ističe kako digitalni vodeni žig se može definirati kao signal koji se dodaje digitalnom zapisu. (Stančić, 2009:171)

Prema podacima Nacionalnog CERT-a, „Označavanje digitalnim vodenim žigom je tehnika kojom se mogu zaštiti autorska prava različitih multimedijskih sadržaja. S obzirom da postoji više različitih multimedijskih formata kao što su slike, audio podaci, video podaci te grafički objekti, potrebno je razviti posebne metode za svaki od njih. U usporedbi s istraživanjima o označavanju slika, video i audio podataka, istraživanja o označavanju teksta su malobrojna. Ipak pojavom novih primjena kao što su npr. digitalna knjižnica te knjige u elektroničkom formatu raste interes i za ovo područje.“ (Nacionalni CERT, 2010:10)

Autor Marković ističe, „Vodeni žig bi trebao biti otporan na:

- ✓ Uobičajene geometrijske operacije (rotaciju, skaliranje, translaciju, zrcaljenje);
- ✓ Filtriranje (povećanje i smanjenje razlučivosti, i sl.);
- ✓ Dodavanje šuma slici, dupliciranje linija slike;
- ✓ Mijenjanje boja, promjena kontrasta i svjetline;
- ✓ Kompresiju (JPEG, MPEG, fraktalna kompresija);
- ✓ Digitalno-analogne konverzije i obratno.“ (Marković, 2001)

U nastavku je navedena slika podjele digitalnog vodenog žiga.



Slika 2: Podjela digitalnih vodenih žigova

Izvor: Nacionalni CERT, 2010., str.8.

Na slici se može uočiti kako se žigovi prema radnoj domeni dijele na prostornu i frekvencijsku domenu. Nacionalni CERT ističe, „U prostornoj domeni digitalni vodeni žig se dodaje direktno slici, dok se u frekvencijskoj domeni radi sa spektrima slike i žiga, tj. spektar žiga se dodaje spektru slike.“ (Nacionalni CERT, 2010:10)

Prema vrsti dokumenta dijele se na tekst, sliku, audio, te video. Što se tiče podjele prema ljudskoj percepciji, razlikujemo vidljiv i nevidljiv vodeni žig, sa naglaskom da nevidljivi još može biti otporni, te lomljivi. Otporni vodeni žig može biti privatni, javni, inverzan, neinverzan, kvaziinverzan, te nekvaziinverzan.

4. ZAŠTITA PODATAKA U UREDSKOM POSLOVANJU HRVATSKE POŠTE

Zaštita podataka je iznimno bitna, pogotovo kada se radi o velikoj organizaciji, poput Hrvatske pošte. Stoga je u nastavku definirano sve vezano uz njihovo uredsko poslovanje i zaštitu.

Podaci službene mrežne stranice Hrvatske pošte govore, „Hrvatska pošta kao vodeći logističar na tržištu danas je digitalno inovativna tvrtka koja povezuje korisnike, tvrtke i zemlje. Pošta je najveći davatelj poštanskih usluga u Republici Hrvatskoj i jedini davatelj univerzalne usluge prema odredbama Zakona o poštanskim uslugama te pokriva više od 80 posto tržišta. Danas je Hrvatska pošta svrstana među predvodnike digitalne transformacije u zemlji, a brojna nova rješenja u poslovanju i procesima omogućila su optimalne i modernije usluge te snažno potpomažu rast e-trgovine.“ (Hrvatska pošta, n.d.)

U nastavku je slika koja prikazuje logo Hrvatske pošte.

Slika 3: Logotip Hrvatske pošte

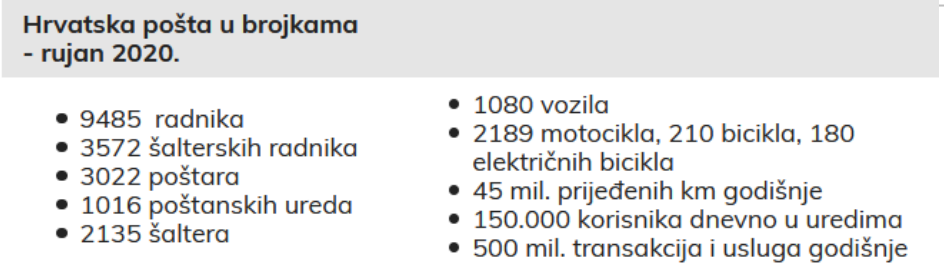
Izvor: Hrvatska pošta, preuzeto sa https://www.posta.hr/logotipi-6497/6497

Prema podacima Hrvatske pošte, „Divizijski ustroj Hrvatske pošte bio jedan od najvećih preustroja trgovačkih društava u Republici Hrvatskoj. Tvrtka je podijeljena u četiri divizije:

- ✓ Divizija pošta
- ✓ Divizija mreža
- ✓ Divizija ekspres
- ✓ Divizija podrška.“ (Hrvatska pošta, n.d.)

Organizacijsku strukturu je najbolje prikazati tabličnim prikazom, koji je naveden u nastavku.

Tablica 1: Hrvatska pošta u brojkama



Izvor: Hrvatska pošta, preuzeto sa https://www.posta.hr/organizacijska-struktura-32/32

Hrvatska pošta ističe, „Poštanski uredi su u mnogim sredinama mjesta na kojima građani mogu blizu svojih domova obaviti usluge koje im svakodnevno trebaju. (…) Radnici Hrvatske pošte sastavni su dio svake zajednice i zato je ulaganje u njihova znanja i socijalnu sigurnost važan dio razvojne Strategije Pošta2022. Hrvatska pošta kao jedan od najvećih poslodavaca u Hrvatskoj posvećuje veliku pozornost razvoju i dobrobiti svojih radnika.“ (Hrvatska pošta, n.d.)

Zatim, Hrvatska pošta naglašava kako, „(…)programima stipendiranja visokog obrazovanja brine o mladima kao budućim naraštajima poslovno aktivnih građana. (…) U mnogim dijelovima društvenog života, pa tako i u izvanrednim situacijama, Hrvatska pošta sudjeluje brojnim aktivnostima.“ (Hrvatska pošta, n.d.)

U srpnju ove godine, autor Tomić je proveo intervju sa voditeljicom odjela cyber sigurnosti Hrvatske pošte, Danijelom Marijanović. Ističe kako je sigurnost podataka ključ uspješnog poslovanja. U Hrvatskoj pošti su osnovali poseban odjel kojemu je svrha implementacija najnovijih tehnoloških rješenja.

Prema podacima ICT business, voditeljica odjela cyber sigurnosti Hrvatske pošte naglašava, „Hrvatska pošta protekle tri-četiri godine prolazi kroz sveobuhvatnu digitalnu transformaciju. Posebnu pozornost posvećujemo tehnologiji i rješenjima modernog doba jer je za nas digitalizacija filozofija razvoja i pokretač brojnih projekata u poslovanju. Usmjerenost na elektroničke usluge i digitalno poslovanje stavlja kibernetičku sigurnost na vrh liste prioriteta Hrvatske pošte. Podatci, odnosno informacije su u današnjem digitalnom dobu najvrjedniji resurs i iznimno ih je važno zaštititi i pravilno osigurati. Stoga je početkom ove godine u Hrvatskoj pošti osnovan Odjel za kibernetičku sigurnost koji se, kao što sam naziv govori, bavi samo kibernetičkom sigurnosti. Implementirali smo najnovija tehnološka rješenja koja štite sustav i korisnike tog sustava, a u konačnici i sve korisnike naših usluga.“ (ICT Business, 2020)

Što se tiče rješenja u svrhu zaštite podataka u Hrvatskoj pošti, prema podacima mrežne stranice ICT Business, „Rad sustava svakodnevno se nadzire i sva odstupanja u radu cjelokupne mreže

ili dijela mreže prate se uz pomoć implementiranih alata koji detektiraju potencijalne opasnosti. Vrlo bitan faktor u efikasnoj zaštiti i sigurnosti informacijskog sustava uvijek je ljudski faktor.“ (ICT Business, 2020)

Podaci ICT Business mrežne stranice naglašavaju kako Hrvatska pošta redovito provodi razna testiranja informacijske sigurnosti, surađuju sa nacionalnim tijelima u cilju održavanja izvrsne informacijske sigurnosti, koriste antivirusne programe, vatrozide, koriste složene lozinke, te ih često mijenjaju. Zatim, imaju riješen business continuity i disaster recovery, koji su potrebni za uspješno poslovanje, jer u slučaju da dođe do prekida rada sustava, to uzrokuje ogromne ekonomske troškove, a samim time i reputacijski rizik. Osim toga, Hrvatska pošta je uvela GDPR u svoje poslovanje i to još 2018.godine, jer na taj način osiguravaju da su sva rješenja u skladu sa propisima.

Godina 2020. je svakako godina za pamćenje, jer je to godina kada se svi bore sa pandemijom COVID-19, samim time su pred poslovanja postavljeni brojni izazovi. Hrvatska pošta se vrlo brzo prilagodila novonastaloj situaciji, te su prilagodili poslovne procese, zaposlenici rade u timovima, te je obavezno nošenje maski, upotreba dezinfekcijskih sredstava. Osim toga, uvedene su promjene vezane sa održavanje sigurnosti sustava, te su donesene stroge procedure spajanja na internu mrežu iz kućnog okruženja putem VPN-a, ali je pojačan i awareness i nadzor sustava. (ICT Business, 2020)

Godine 2019. je zabilježen hakerski napad koji je „pogodio“ hrvatske državne službe, Jutarnji list ističe, „Napadači su ciljali na žrtve koristeći phishing metodu koja je oponašala obavijesti o pristigloj e-pošti iz Hrvatske pošte i drugih maloprodajnih usluga. U tim je e-mailovima bila i poveznica na web stranicu na kojoj se korisnike tražilo da skinu Excel dokument. U tom se dokumentu nalazio zlonamjerni kod, naizgled kopiran s interneta. Ako bi žrtve to skinule, makroskripta bi tada na njihovo računalo instalirala zlonamjerni softver u sustav. Tijekom tih su napada otkrivena dva različita skupa zlonamjernih programa (malware). Prvi je bio „Empire backdoor“, a drugi „Silent Trinity“.“ (Jutarnji list, 2019)

Nakon tog napada, Hrvatska pošta je promptno reagirala, pokrenuli su korake za uklanjanje zlonamjernih internetskih stranica, te poslužitelja.

5. PROVEDENO ISTRAŽIVANJE

Zbog potrebe za izradom završnog rada, dana 14.10.2020. godine provedeno je istraživanje na temu Zaštite podataka u uredskom poslovanju, na uzorku od 80 ispitanika. U nastavku su prezentirani dobiveni rezultati.

Istraživanje koje je provedeno sastoji se od sljedećih hipoteza:

- Hipoteza 1: Građani su upoznati sa pojmom Uredskom poslovanja

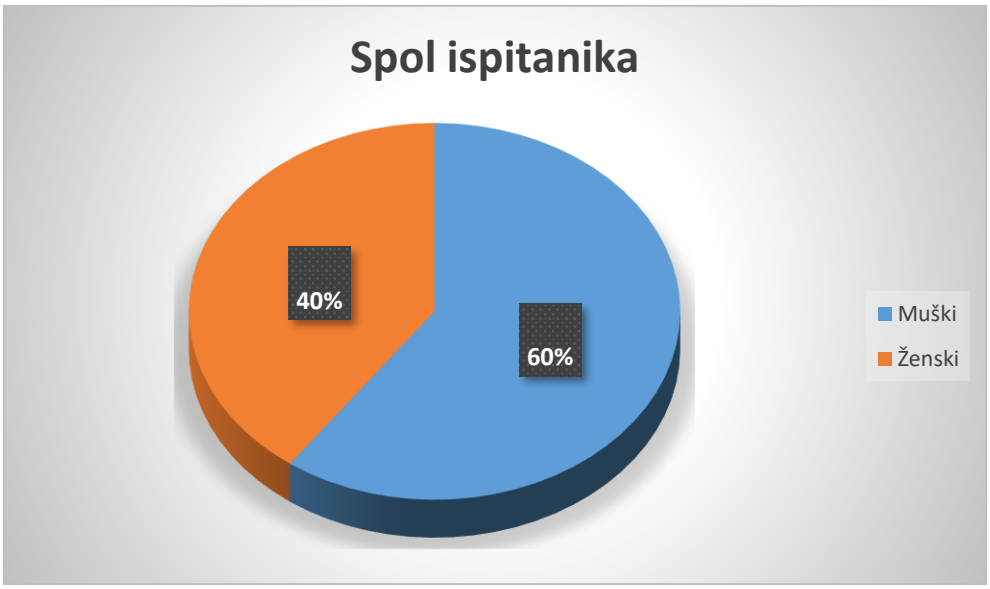
- Hipoteza 2: Veoma je bitno zaštititi podatke u uredskom poslovanju.

Izabrana metoda ispitivanja je provođenje ankete na uzorku od 80 ispitanika, te je sve u skladu sa istraživačkom etikom. Anketa je provedena na način da su anketna pitanja napisana u Google obrascu, te putem društvene mreže Facebook je poslan zahtjev za sudjelovanjem u anketiranju, te je naglašeno da je poželjno da sudjeluju osobe koje znaju što je to uredsko poslovanje.

U nastavku su navedeni grafikoni koji prikazuju rezultate istraživanja.

Više od polovice ispitanika, točnije njih 60%, je muškog spola.

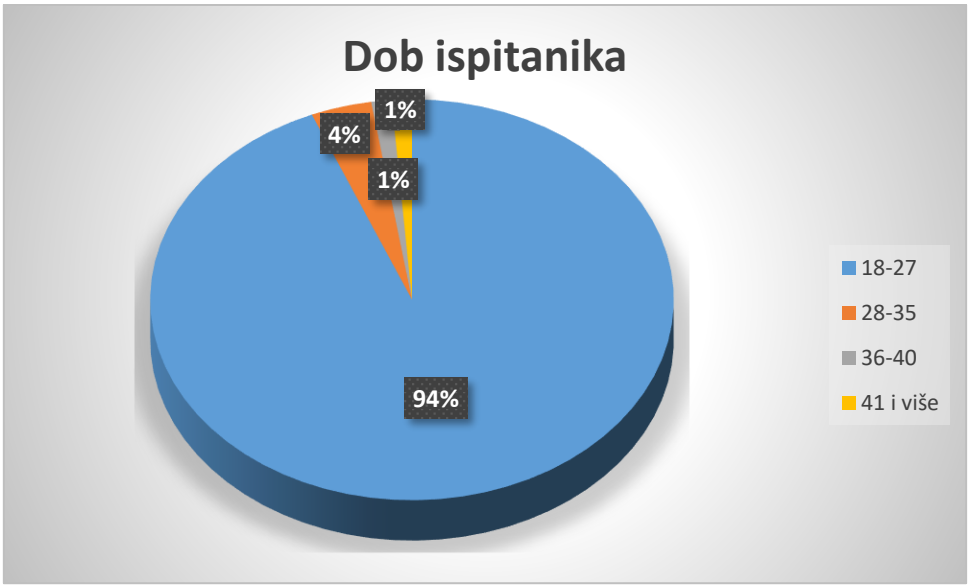
Grafikon 1: Spol ispitanika



Izvor: Izradio autor

Čak 94% ispitanika je u dobi u rasponu od 18 do 27, njih 4% od 28 do 35, 1% ispitanika je u dobi od 36 do 40 godina, te njih 1% ima 41 i više godinu.

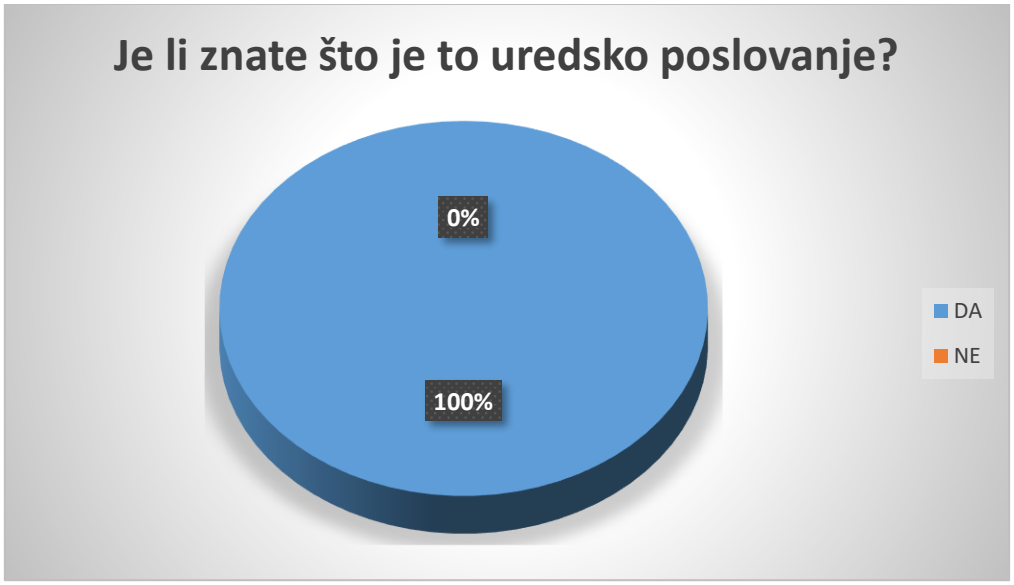
Grafikon 2: Dob ispitanika



Izvor: Izradio autor

Svi ispitanici su upoznati sa uredskim poslovanjem.

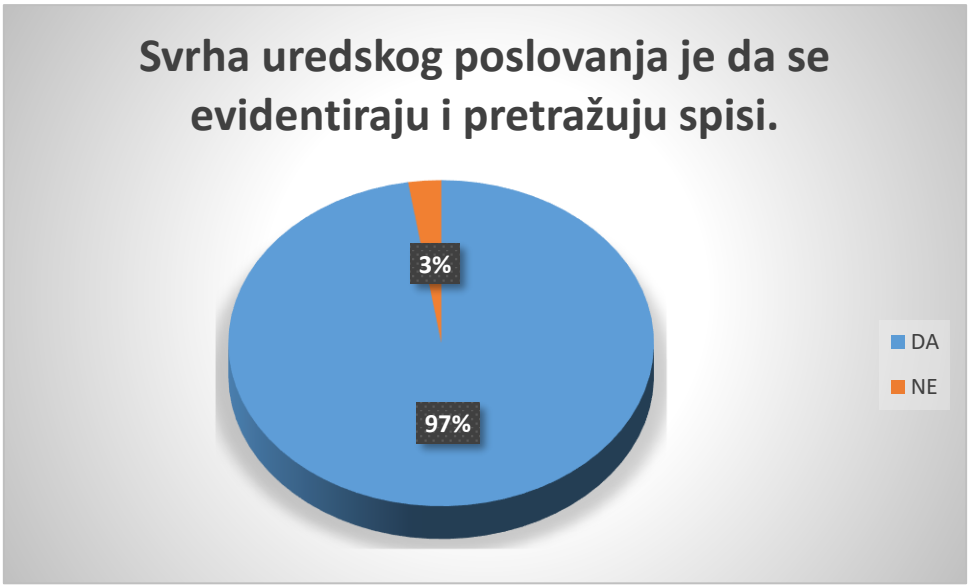
Grafikon 3: Znate li što je to uredsko poslovanje?



Izvor: Izradio autor

Gotovo svi ispitanici, njih 97%, smatraju da je svrha uredskog poslovanja evidentiranje i pretraživanje spisa.

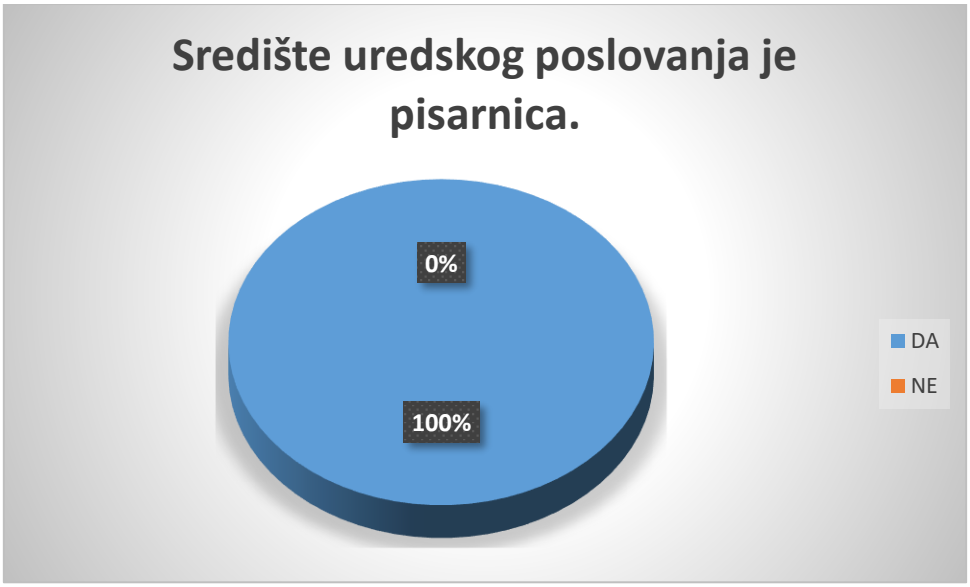
Grafikon 4: Svrha uredskog poslovanja je da se evidentiraju i pretražuju spisi.



Izvor: Izradio autor

Svi ispitanici su složni u tome da je središte uredskog poslovanja pisarnica.

Grafikon 5: Središte uredskog poslovanja je pisarnica.



Izvor: Izradio autor

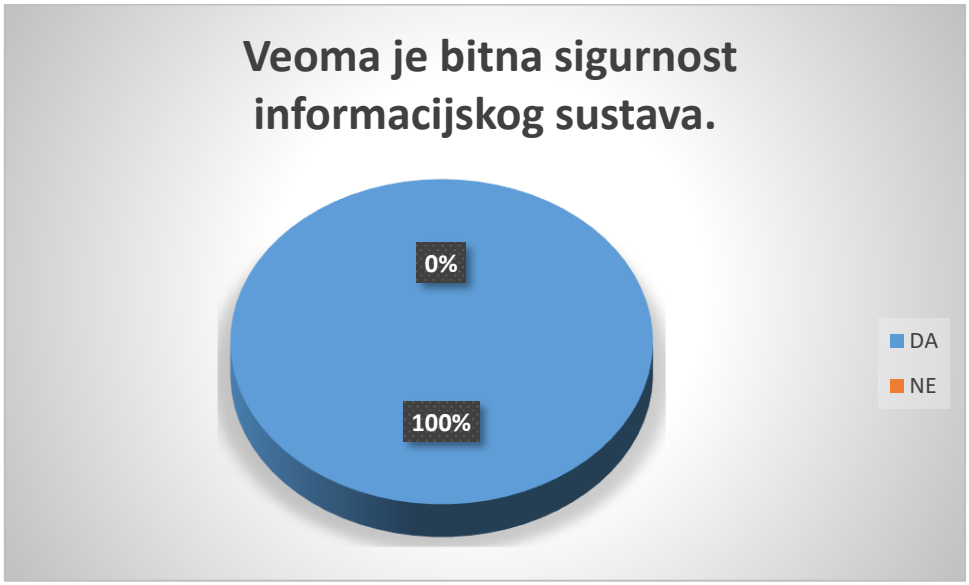
Čak 85% ispitanika smatra kako se bilježi sve veći porast krađa elektroničkih podataka.

Grafikon 6: Smatrate li da se bilježi sve veći porast krađa elektroničkih podataka?

Izvor: Izradio autor

Svi se slažu u tome da je veoma bitna informacijska sigurnost.

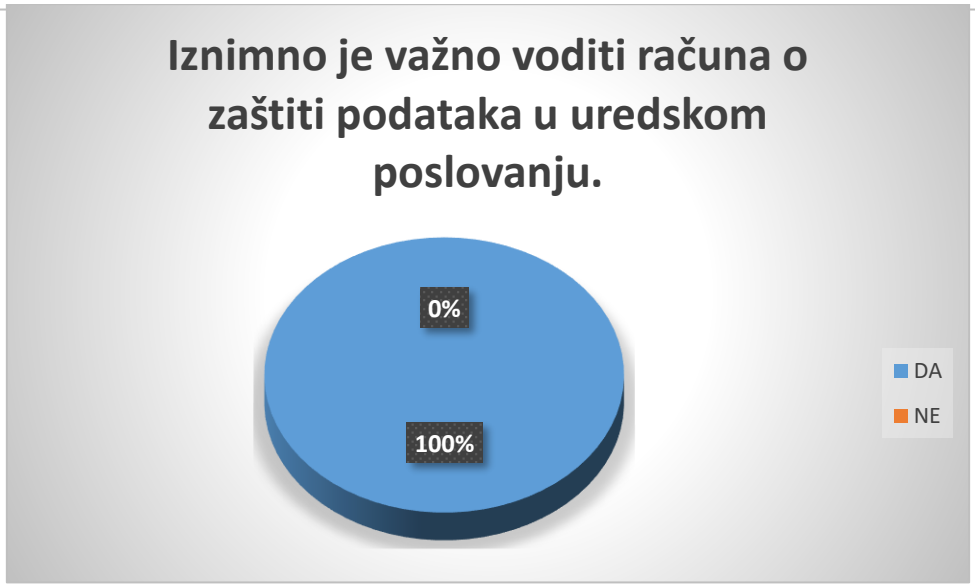
Grafikon 7: Veoma je bitna sigurnost informacijskog sustava.



Izvor: Izradio autor

Također su svi složni u tome da je važno voditi računa o zaštiti podataka u uredskom poslovanju.

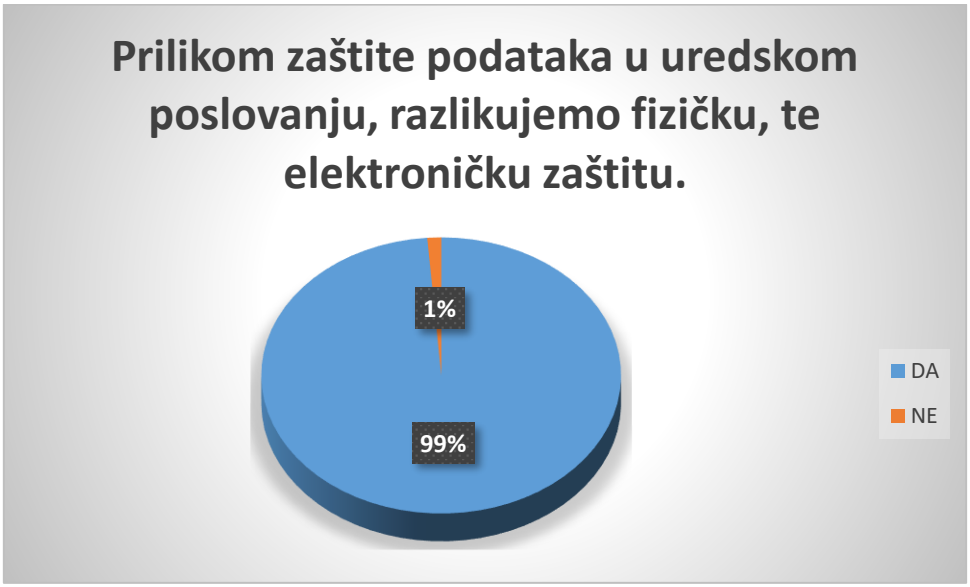
Grafikon 8: Iznimno je važno voditi računa o zaštiti podataka u uredskom poslovanju.



Izvor: Izradio autor

Samo 1% ispitanika je odgovorilo negativno na anketno pitane/tvrdnju o tome da prilikom zaštite podataka u uredskom poslovanju, razlikujemo fizičku, te elektroničku zaštitu.

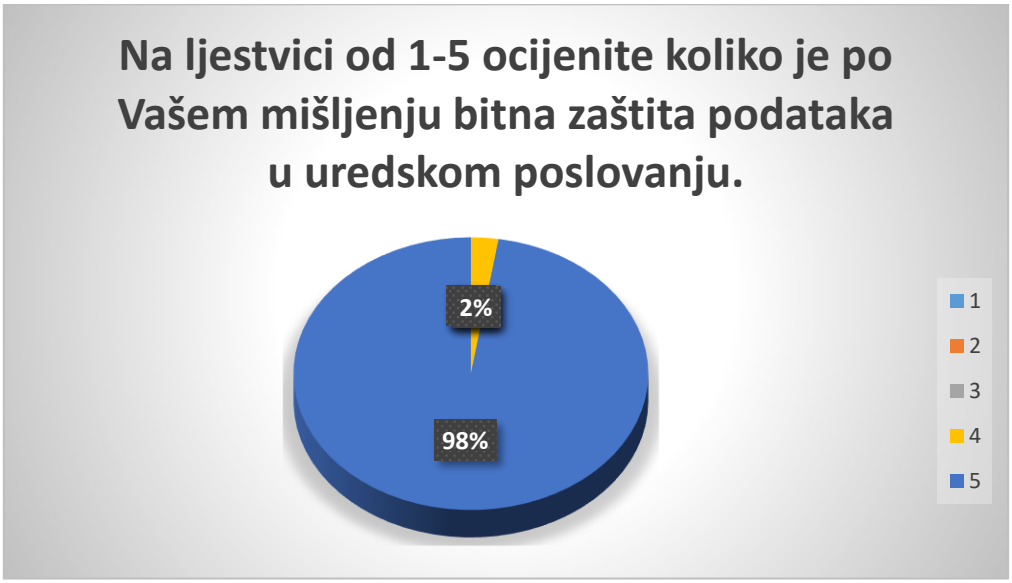
Grafikon 9: Prilikom zaštite podataka u uredskom poslovanju, razlikujemo fizičku, te elektroničku zaštitu.



Izvor: Izradio autor

Što se tiče ocjenjivanja bitnosti zaštite podataka u uredskom poslovanju, njih 98% je dalo ocjenu 5, odnosno smatraju kako je zaštita podataka veoma bitna. Tek njih 2% je dalo ocjenu 4, a ocjene 1, 2, te 3 nije nitko.

Grafikon 10: Na ljestvici od 1-5 ocijenite koliko je po Vašem mišljenju bitna zaštita podataka u uredskom poslovanju



Izvor: Izradio autor

7. ZAKLJUČAK

U ovom radu pristupilo se definiranju zaštite podataka u uredskom poslovanju. Tema ovog završnog rada je veoma aktualna, jer svakodnevno koristimo računala, mobitele, a može se dogoditi da u nekom trenutku se dogodi hakerski napad. Stoga je veoma bitno zaštiti svoje podatke, bilo to osobne ili uredske.

Sigurnost podataka, te zaštita informacijskih sustava su veoma važne, a mogu se smatrati kao obveza informatičkih stručnjaka, jer današnji svijet karakterizira informatička nesigurnost, stoga je veoma bitno da se računala, odnosno podaci zaštite na adekvatan način.

Bitno je zaštititi podatke i to fizičkom ili elektroničkom zaštitom. Kada govorimo o fizičkoj sigurnosti, tada se podrazumijeva i zaštita informacija, odnosno infrastrukture, uslijed prirodnih pojava, poput požara, poplava i slično, ali i brigu oko osiguranja adekvatnih uvjeta, te odabira pozicije prostorija.

Osim fizičke zaštite podataka u uredskom poslovanju, postoji i elektronička zaštita, pomoću koje se štite podaci od uništenja, neovlaštenih upada i slično. Razlikuju se sljedeće vrste elektroničke zaštite, zaporke, kriptiranje, te digitalni vodeni žig.

Hrvatska pošta je najbolji primjer kako treba poslovati jer proteklih godina njihovo poslovanje karakterizira digitalna transformacija. Njihova usmjerenost na elektroničke usluge i digitalno poslovanje postavlja kibernetičku sigurnost na prvo mjesto, jer znaju da je to veoma bitno ukoliko žele biti sigurni da će neometano poslovati.

Zbog potrebe za izradom završnog rada, dana 14.10.2020. godine provedeno je istraživanje na temu Zaštite podataka u uredskom poslovanju, na uzorku od 80 ispitanika. U nastavku su prezentirani dobiveni rezultati. Što se tiče rezultata istraživanja, više od polovice ispitanika, točnije njih 60%, je muškog spola, čak 94% ispitanika je u dobi u rasponu od 18 do 27, njih 4% od 28 do 35, 1% ispitanika je u dobi od 36 do 40 godina, te njih 1% ima 41 i više godinu, središte uredskog poslovanja pisarnica, te su svi ispitanici su upoznati sa uredskim poslovanjem, da je središte uredskog poslovanja pisarnica i da je veoma bitna informacijska sigurnost. Gotovo svi, njih 97%, smatraju da je svrha uredskog poslovanja evidentiranje i pretraživanje spisa, 85% ispitanika smatra kako se bilježi sve veći porast krađa elektroničkih podataka.

Svi su složni u tome da je važno voditi računa o zaštiti podataka u uredskom poslovanju, samo 1% ispitanika je odgovorilo negativno na anketno pitane/tvrdnju o tome da prilikom zaštite

podataka u uredskom poslovanju, razlikujemo fizičku, te elektroničku zaštitu. Što se tiče ocjenjivanja bitnosti zaštite podataka u uredskom poslovanju, njih 98% je dalo ocjenu 5, odnosno smatraju kako je zaštita podataka veoma bitna. Tek njih 2% je dalo ocjenu 4, a ocjene 1, 2, te 3 nije nitko.

8. IZJAVA

Izjava o autorstvu završnog rada i akademskoj čestitosti

Ime i prezime studenta: Hrvoje Kopajtić

Matični broj studenta: 0082037354

Naslov rada: Zaštita podataka u uredskom poslovanju

Pod punom odgovornošću potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada.

Potvrđujem da je elektronička verzija rada identična onoj tiskanoj te da je to verzija rada koju je odobrio mentor.

Datum | Potpis studenta

_____ _____

9. POPIS LITERATURE

9.1. KNJIGE I STRUČNI ČLANCI, RADOVI

- ✓ Balgač, I. (2013). Prevencija kriminaliteta kroz uređenje okoliša i urbani dizajn (CPTED). Ministarstvo unutarnjih poslova Republike Hrvatske. Zagreb.
- ✓ Juran, A. (2014). Sigurnost informacijskih sustava. Pomorski fakultet Rijeka. Rijeka.
- ✓ Klasić, K. (2007). Zaštita informacijskih sustava u poslovnoj praksi. SIGURNOST, Vol.49 No.1 2007.
- ✓ Stančić, H. (2009). Digitalizacija. Zavod za informacijske studije. Zagreb.

9.2. INTERNETSKI IZVORI

- ✓ Carnet (2020). Osnove uredskog poslovanja. Preuzeto s https://loomen.carnet.hr/mod/book/tool/print/index.php?id=130455 (05.10.2020.).
- ✓ Centar za informacijsku sigurnost (2011). Kriptiranje podataka. Preuzeto s https://www.cis.hr/sigurnosni-alati/kriptiranje-podataka.html (15.10.2020.).
- ✓ Državni arhiv Varaždin. (n.d.) Uredsko poslovanje. Preuzeto s http://dav.hr/dokumenti1/UREDSKO%20POSLOVANJE.doc (02.10.2020.).
- ✓ Hrvatska pošta (n.d.). Organizacijska struktura. Preuzeto s https://www.posta.hr/organizacijska-struktura-32/32 (4.10.2020.).
- ✓ Hrvatska pošta (n.d.). Logotipi. Preuzeto s https://www.posta.hr/logotipi-6497/6497 19.10.2020.)
- ✓ Hrvatska pošta (n.d.). Tko smo i što radimo?. Preuzeto s https://www.posta.hr/tko-smo-i-sto-radimo/6501 (12.10.2020.).
- ✓ Hrvatska pošta (n.d.). Zajednica. Preuzeto s https://www.posta.hr/zajednica/6463 (19.10.2020.).
- ✓ Infinus (2011). Odabir lozinke. Preuzeto s http://www.infinius.hr/blog/odabir-lozinke/ (09.10.2020.).

- ✓ Jutarnji list (2019). Misteriozni hakeri napali Hrvatske državne službe Institucije zaražene „nikad prije viđenim“ zlonamjernim programom: „Ovakav alat dosad nije korišten“. Preuzeto s https://www.jutarnji.hr/vijesti/hrvatska/misteriozni-hakeri-napali-hrvatske-drzavne-sluzbe-institucije-zarazene-nikad-prije-videnim zlonamjernim-programom-ovakav-alat-dosad-nije-koristen-9119243 (09.10.2020.)

- ✓ Marković, H. (2001). Detekcija vodenog žiga. Preuzeto s http://sigurnost.zemris.fer.hr/wm/2001_markovic/index.html (12.10.2020.)

- ✓ Ministarstvo pravosuđa i uprave (n..d.). Uredsko poslovanje. Preuzeto s https://uprava.gov.hr/uredsko-poslovanje/12307 (15.10.2020.).

- ✓ Nacionalni CERT (2010). Metode zaštite dokumenata. Preuzeto s https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-04-296.pdf (04.10.2020.).

- ✓ Nacionalni CERT (2010). Fizička zaštita informacijskih sustava. Preuzeto s https://www.cert.hr/fizicka-zastita-informacijskih-sustava/ncert-pubdoc-2010-06-304/ (14.10.2020.).

- ✓ Narodne novine (2009). Uredba o uredskom poslovanju NN 7/2009. Preuzeto s https://narodne-novine.nn.hr/clanci/sluzbeni/2009_01_7_171.html (12.10.2020.).

- ✓ Odobaša, R. (2007). Uredsko poslovanje tijela državne uprave Republike Hrvatske. Preuzeto s https://www.pravos.unios.hr/pfo/sites/default/files/users/user11/UREDSKO_POSLOVANJE-SKRIPTE.pdf (05.10.2020.).

- ✓ Smolčić, J., Andrlić, B., Hak, M. (2008). CRM kao ključ poslovnog uspjeha. Preuzeto s http://www.infotrend.hr/clanak/2008/7/crm-kao-kljuc-poslovnog uspjeha,17,407.html (05.10.2020.).

- ✓ Središnji državni ured za e-Hrvatsku (2005). Nacionalni program informacijske sigurnosti u Republici Hrvatskoj. Preuzeto s https://rdd.gov.hr/UserDocsImages/MURH_migracija%20s%20weba/Arhiva%20projekata/Nacionalni%20program%20informacijske%20sigurnosti%20u%20RH.pdf (17.10.2020.).

- ✓ Tomić, D. (2020). Usmjerenost na elektroničke usluge i digitalno poslovanje stavlja kibernetičku sigurnost na vrh liste prioriteta. Preuzeto s

https://www.ictbusiness.info/poslovna-rjesenja/usmjerenost-na-elektronicke-usluge-i-digitalno-poslovanje-stavlja-kiberneticku-sigurnost-na-vrh-liste-prioriteta (15.10.2020.).

- ✓ Zavod za sigurnost informacijskih sustava (n.d.). Primjena kriptografske zaštite. Preuzeto s https://www.zsis.hr/default.aspx?id=344 (17.10.2020.).

10. POPIS SLIKA, TABLICA I GRAFIKONA

ŽIVOTOPIS

OSOBNI PODACI	
Prezime/ime	Hrvoje Kopajtić
Adresa	Stanka Vraza 9, 10431 Sveta Nedelja
Telefonski broj	091 7629 824
E-mail	hkopajtic@gmail.com
Državljanstvo	hrvatsko
Datum rođenja	05.10.1987.
Spol	muški
Radno iskustvo	01/07/2016 – Administrator u odjelu pravnih poslova EOS Matrix d.o.o., Zagreb (Hrvatska) Administracija u odjelu pravnih poslova 15/08/2014 – 01/072016 Agent u pozivnom centru EOS Matrix d.o.o., Zagreb (Hrvatska) Agent u pozivnom centru 20/03/2014 – 30/07/2014 Administrator i agent u pozivnom centru Modus sustavi d.o.o., Zagreb (Hrvatska) Djelatnik u administraciji i rad u telemarketingu i prodaji 10/11/2013 – 01/02/2014 Administrator Atego d.o.o., Zagreb (Hrvatska) Administrator u agenciji za promet nekretninama 03/11/2010 – 30/10/2013 Radnik u servisu

	T-Hrvatski Telekom, Zagreb (Hrvatska) Rad u servisu T-Hrvatskog Telekoma 30/10/2009 – 25/10/2010 Agent u pozivnom centru T-Hrvatski Telekom, Zagreb (Hrvatska) Agent na telefonskim informacijama
Završeno obrazovanje	09/2017 – Student Menadžmenta uredskog poslovanja Veleučilište s pravom javnosti Baltazar Zaprešić, Zaprešić (Hrvatska) 09/2002 – 06/2006 Maturant opće gimnazije XIII. Gimnazija, Zagreb (Hrvatska) 1997 – 2001 Škola za strane jezike Sova - Škola za strane jezike, Zagreb (Hrvatska) Engleski jezik
Materinski jezik	hrvatski
Drugi jezici	engleski (C2); njemački (pasivno znanje)
Društvene vještine i kompetencije	Dobre komunikacijske vještine stečene radom u pozivnim centrima T – Hrvatskog telekoma i EOS Matrixa te kontaktom s klijentima u agenciji za nekretnine. Odlične komunikacijske vještine stečene radnim iskustvom u prodaji i marketingu tvrtke Modus sustavi.
Računalne vještine i kompetencije	Odlično poznavanje rada sa alatima Microsoft OfficeTM (WordTM, ExcelTM i PowerPointTM te OutlookTM). Osnovno znanje o programima grafičkog oblikovanja (Adobe IllustratorTM, PhotoShopTM). Odlično poznavanje Interneta

Dodatne informacije	i Microsoft Windows-a. Google AdWords certifikat. Uređivanje You Tube kanala. Poznavanje rada u Apple – u. Vozačka dozvola B kategorija