UNIVERZITET U SARAJEVU
EKONOMSKI FAKULTET

ZAVRŠNI RAD

„USPOSTAVLJANJE STANDARDA SIGURNOSTI INFORMACIJSKIH SISTEMA U ORGANIMA LOKALNE SAMOUPRAVE: STUDIJA SLUČAJA OPĆINA“

Sarajevo, septembar 2024. HANA ZEKOVIĆ

"Grandparents are the perfect blend of
love, laughter, and happy memories."

Za mog dragog dedu ♡

U skladu sa članom 54. Pravila studiranja za I, II ciklus studija, integrisani, stručni i specijalistički studij na Univerzitetu u Sarajevu, daje se

IZJAVA O AUTENTIČNOSTI RADA

Ja, **Hana (Adnan) Zeković**, studentica **drugog (II) ciklusa studija**, broj index-a **5243-74511** na odsjeku **Menadžment**, smjer **Menadžment i informacione tehnologije**, izjavljujem da sam završni rad na temu:

„USPOSTAVLJANJE STANDARDA SIGURNOSTI INFORMACIJSKIH SISTEMA U ORGANIMA LOKALNE SAMOUPRAVE: STUDIJA SLUČAJA OPĆINA“

pod mentorstvom **doc. dr. Kemala Kačapora** izradila samostalno i da se zasniva na rezultatima mog vlastitog istraživanja. Rad ne sadrži prethodno objavljene ili neobjavljene materijale drugih autora, osim onih koji su priznati navođenjem literature i drugih izvora informacija uključujući i alate umjetne inteligencije.

Ovom izjavom potvrđujem da sam za potrebe arhiviranja predala elektronsku verziju rada koja je istovjetna štampanoj verziji završnog rada.

Dozvoljavam objavu ličnih podataka vezanih za završetak studija (ime, prezime, datum i mjesto rođenja, datum odbrane rada, naslov rada) na web stranici i u publikacijama Univerziteta u Sarajevu i Ekonomskog fakulteta.

U skladu sa članom 34. 45. i 46. Zakona o autorskom i srodnim pravima (Službeni glasnik BiH, 63/10) dozvoljavam da gore navedeni završni rad bude trajno pohranjen u Institucionalnom repozitoriju Univerziteta u Sarajevu i Ekonomskog fakulteta i da javno bude dostupan svima.

Sarajevo, 10.09.2024. Potpis studentice:

SAŽETAK

Živimo u vremenu punom tehnologije. Ona je svuda oko nas željeli je mi prihvatiti ili ne. Sastavni je dio naših života, te kao takva ima ključnu ulogu u našem razvoju. Sa jedne strane to zvuči zastrašujuće, dok sa druge nam pruža pozitivne aspekte u bilo kojoj sferi u kojoj nam je potrebna. Da li je riječ o privatnom ili poslovnim pruža nam olakšice u obavljanju bitnih segmenata. Zbog toga je ona važna karika za svakog čovjeka.

Informacioni sistemi kao dio informacionih tehnologija koriste se svakodnevno. Najčešća primjena je u poslovne svrhe u kojim nam olakšava obavljanje posla stvarajući ga što lakšim i jednostavnijim. Posao se obavlja brže, preciznije, te sigurnije što nam je od izuzetne važnosti. Sigurnost informacionog sistema je bitna stavka svakog poslovanja. Koliko god mi mislili da naše informacije nisu nikome važne, varamo se. Svaka informacija koju mi kao zaposlenici neke ustanove posjedujemo može biti iskorištena protiv nas. Zavisnosti samo u čije ruke dospije. Zbog toga, sigurnost informacionog sistema treba biti na prvom mjestu svake kompanije koja želi pozitivno da posluje. Uvođenjem novije vrste zaštite pospiješit ćemo rad cijele kompanije. Standardi sigurnosti informacionog sistema su budućnost, te ga zbog toga trebamo što prije prihvatiti.

Općina kao jedinica lokalne samouprave koristi razne aplikacije informacionih sistema koje im pomažu u poslovanju. Informacioni sistemi se koriste u svakom vidu poslovanja. Bilo da se radi o običnom unosu predmeta, pa sve do finansijskog aspekta prisutni su u cijelom poslovanju. Međutim, kako bi dokumentacije i zahtjevi građana bile sigurnije zaštićene potrebno je uvesti novije vrste zaštite. ISO 27000 je najbolja opcija za to. Kroz analizu i intervju sa zaposlenicima uvidjela sam koliko ima prednosi i nedostataka u njihovoj sigurnosti. Mnogi zaposlenici su zadovoljni sigurnošću koje im antivirusne zaštite pružaju. Međutim, postoje i oni koji smatraju da se trebaju uvesti novije metode zaštite. Slušajući obije strane zasigurno je da se treba doći do modernizacije sigurnosti informacionog sistema prateći novije trendove na tržištu.

Glavni cilj istraživanja ovog rada je istražiti koliko se standardi sigurnosti informacionih sistema ustvari koriste u organima lokalne samouprave, te unaprijediti metodologiju za njegovu upotrebu. Fokus je na zaposlenicima jedne od gradskih Općina u kojoj sam zaposlena.

Iz ovih razloga obavljeno je kvalitativno istraživanje sa uposlenicima kako bi se uvidio stepen zadovoljstva vezan za sigurnost. Analizom podataka utvrdit će se zaključci i rezultati istraživanja, te ispunjenje postavljenjih ciljeva istraživanja.

Ključne riječi: informacioni sistem, informaciona tehnologija, poslovni informacioni sistemi, ISO 27000, standardi sigurnosti, Općina.

ABSTRACT

We live in a technology-filled era. It is all around us whether we choose to accept it or not. It is an integral part of our lives and plays a crucial role in our development. On one hand, it sounds intimidating, but on the other hand, it offers us positive aspects in any sphere where we need it. Whether it is in private or business matters, it provides us with conveniences in carrying out essential tasks. Therefore, it is an important link for every individual.

Information systems, as part of information technology, are used daily. The most common application is for business purposes, where it facilitates the work by making it easier and simpler. Work is done faster, more accurately, and more securely, which is of utmost importance. The security of the information system is a crucial aspect of any business. No matter how insignificant we think our information is, we are mistaken. Every piece of information that we, as employees of an institution, possess can be used against us, depending on whose hands it falls into. Therefore, the security of the information system should be a top priority for any company that wants to operate positively. By introducing newer forms of protection, we will enhance the work of the entire company. Information system security standards are the future, and therefore, we should accept them as soon as possible.

The municipality as a unit of local self-government utilizes various information system applications that assist in its operations. Information systems are used in every aspect of business. Whether it is simple data entry or financial aspects, they are present throughout the business. However, in order to ensure that documentation and citizens requests are more securely protected, it is necessary to introduce newer forms of protection. ISO 27000 is the best option for this. Through analysis and interviews with employees, I have realized the advantages and disadvantages of their security. Many employees are satisfied with the security provided by antivirus protection. However, there are those who believe that newer protection methods should be introduced. By listening to both sides, it is certain that modernizing information system security to follow the latest market trends is necessary.

The main goal of this research is to explore how much information system security standards are actually used in local government bodies and to improve the methodology for their use. The focus is on the employees of the Municipality where I work.

For these reasons, a qualitative study was conducted with the employees to assess the level of satisfaction related to security. By analyzing the data, conclusions and research results will be determined, as well as the fulfillment of the research objectives.

Key words: information system, information technology, business information systems, ISO 27000, security standards, Municipality.

SADRŽAJ

POPIS TABELA

POPIS SLIKA

POPIS PRILOGA

POPIS SKRAĆENICA

IS - Informacioni sistem

ITIL - Information Technology Infrastructure Library

CobiT - Control Objectives for Information and Related Technologies

ISO - International Organization for Standardization

ERP - Enterprise Resource Planning

SCM - Supply Chain Management

CRM - Customer Relationship Management

KBIS - Kompjuterski baziran informacioni sistem

IT - Informacione tehnologije

MRP - Material Requirements Planning

OECD - The Organization for Economic Cooperation and Development

ISACA - Information System Audit and Control Association

NIBIS - NextVIsion Business Information System

DMS - Document Management System

IEC - Importer Exporter Code

ISMS - Information Security management system

ITSMF - IT Service Management Forum

BiH - Bosna i Hercegovina

1. UVOD

U unaprijeđenim državama veliki je značaj informacijsko-komunikacijske tehnologije, posmatrajući je sa privredne, socijalne i političke strane. Vrijeme informacionih sistema je tek stiglo. Informacioni sistem koriste mnoge države, privatne kompanije, međunarodne organizacije, te pojedinci koji vide veliku korist u njima. Kao takvi postali su bitan segment nacionalne i svjetske sigurnosti, trgovine i makroekonomske stabilnosti. Oni predstavljaju veliki problem u nabavci za pojedine segmente rada kao što su zdravstveni sistemi, prenosu električne energije i interakciji. Informaciona sigurnost je proces, što znači da se neprekidno razvijaju noviji sistemi zaštite informacionog sistema. Profić (2018) govori kako je motiv ustvari konstantno stvaranje novih alata koji narušavaju stabilnost informacionog sistema poput „zločudnog softwarea". Oni predstavljaju virus koji ulaskom u informacioni sistem mogu izazvati nepopravljivu grešku kao što je zloupotreba informacija, koji mogu prouzrokovati krađu finansijskih sredstava sa naših računa. Isto tako razvijaju se i novi načini poslovne špijunaže, koja ne mora biti samo računarske prirode (Bogati, 2011).

U današnje vrijeme se mnoge kompanije, kao i njihovi sistemi susreću sa raznim izazovima koji utiču na rad same informacione sigurnosti. Ti izazovi mogu biti kompjuterski zločini, špijunaža, vandalski čin, sabotaža, te požar, potres, poplave i ostale katastrofe koje mogu prouzrokovati poteškoće u radu organizacije. Napadi u vidu kompjuterskih zloupotreba, tačnije virusa, hakiranja, enkripcijske ucjene, te ostale pretnje sa kojima se informacioni sistemi mogu susresti, bivaju sve učestaliji, zahtjevniji i okrutniji. Kompanija koja ima veću korist od informacionog sistema postaje ovisna o samom sistemu gdje kao takva postaje meta napada. Veća opasnost dolazi i povezivanjem privatnih mreža sa javnom mrežom. Jednu od javnih mreža predstavlja i Internet. Isto tako, većina današnjih kompanija čije se filijale nalaze na različitim geografskim područjima imaju veću potrebu za distribucijom informacija, što umanjuje mogućnosti efikasne kontrole.

Sigurnost je, kako navodi Cingula (2019), „osjećaj pojedinca da je zaštićen od fizičke, društvene, duhovne, novčane, političke, ekonomske, osjećajne ili bilo koje druge prijetnje, opasnosti, štete, povrede ili bilo kakvog događaja koji se može tumačiti kao neželjen". Također, Cingula (2019) smatra "da je sigurnost kontrola neizvjesnosti pri čemu se prepoznata opasnost svodi u granice prihvatljivog rizika". "Sigurnost informacionog sistema štiti informacije od širokog spektra prijetnji u cilju osiguranja kontinuiteta poslovanja, te minimiziranja poslovnih šteta, a maksimiziranja povrata investicija i profita", smatra Lagumdžija *et al*. (2008).

Organi lokalne samouprave, u ovom slučaju općine, su mjesto gdje građani najviše i najčešće obavljaju interakciju sa organima državne uprave. To je prvo mjesto podnošenja zahtjeva i molbi upućene državnim organima. Za svakog građanina neke općine izuzetno je važno da organi lokalne samouprave budu što efikasniji u obavljanju svojih poslova, gdje bi i komunikacija s njima bila što jednostavnija. Samim tim, interakcija bi se obavljala u što kraćem vremenskom razdoblju. To ne bi predstavljalo korist samo za građane nego i za

organe lokalne samouprave u cilju obavljanja dužnosti u što kraćem roku. Kaljević *et al.* (2005) smatraju da "implementiranje informacionog sistema u organu lokalne samouprave je jedan od najvažnijih koraka na putu reforme organa državne uprave, kako bi oni iz zatvorenih i relativno tromih sistema prerasli u dobro organizovane, jednostavne i efikasne sisteme okrenute ka korisnicima".

Prilikom realizacije novijih i modernijih informacionih sistema postoje i određeni problemi. Jedan od njih je strah zaposlenika da će vremenom postati tehnološki višak prilikom implementacije novih informacionih sistema. Taj strah je često veoma opravdan, međutim time ugrožavaju i sam proces rada organa lokalne samouprave. Također, još jedan problem je i loša tehnička opremljenost koja sprječava ispravno djelovanje informacionih sistema. Djelimično ili u cjelini, nije bitno. Bitno je da bilo koja smetnja, bila ona cijela ili ne, utiče i pogoršava rad zaposlenika. Sve je teže zadržati obrazovan kadar koji bi održavao opremu, te vršio najosnovniju kontrolu nad informacionim sistemom. Često osobe koje rade u organima lokalne samouprave nisu dovoljno "informatički pismene" kako bi obavljali ovakav tip poslova. Baš zbog navedenih poteškoća sa kojima se zaposlenici svaki dan susreću, sve je veći broj sistema i standarda koji obezbjeđuju sigurnost i kvalitetu u poslovanju. Kada bi gledali gdje se ubrajaju sami standardi, prema Pokorni (2019) bi ih "uvrstili pod kontrolne provedbe sigurnosne informacione politike, odnosno informatičke kontrole koje možemo razvrstati prema okvirima ili normama koje se koriste pri procjeni njihove učinkovitosti i efikasnosti". Okviri i norme koje se najčešće koriste u svijetu, te su kao takvi i najpoznatiji među korisnicima, su: ITIL, CobiT i ISO 27000 norme.

1.1. Predmet i problem istraživanja

Predmet istraživanja u ovom radu je usklađivanje poslovanja sa standardima sigurnosti informacionih sistema (IS) u organima lokalne samouprave, tj. u općinama. Najveći segment bit će posvećen Općini u kojoj sam zaposlena. Sve potrebne informacije ću dobiti na adekvatan način što će mi pomoći prilikom same izrade magistarskog rada. Problem istraživanja je nedovoljna primjena standarda sigurnosti informacionih sistema u organima lokalne samouprave. To rezultira podložnost općina raznim sigurnosnim prijetnjama po njihov informacioni sistem, kao što su kompjuterske zloupotrebe, špijunaže, te razne vrste elementarnih nepogoda koje na najgori način mogu da ugroze rad općina. Nedostatak adekvatne sigurnosti informacijskih sistema može dovesti do štete za organizacije u obliku zlćudnog koda, hakerskih napada, uskraćivanja usluga i krađe podataka.

1.2. Ciljevi istraživanja

Cilj istraživanja je istražiti primjenu standarda sigurnosti informacionih sistema u organima lokalne samouprave, razviti metodologiju za njihovu primjenu, te analizirati postojeće prakse upravljanja sigurnošću informacionih sistema i preventivne zaštite. Također, istraživanje ima za cilj identificirati najčešće izvore sigurnosnih prijetnji s kojima se

uposlenici općina susreću, te predložiti pristup predstavljanja sigurnosnih standarda uposlenicima lokalne samouprave.

1.3. Osnovna istraživačka pitanja

- Koji su međunarodni standardi u području informacionih sistema relevantni za organe lokalne samouprave?
- Kako primijeniti standarde informacionih sistema u organe lokalne samouprave?
- Koje su postojeće prakse upravljanja sigurnošću informacionih sistema u organima lokalne samouprave?
- Kako se provodi preventivna zaštita informacionih sistema i informacija u općinama?
- Koji su najčešći izvori sigurnosnih prijetnji s kojima se uposlenici općina susreću?
- Kako pristupiti predstavljanju sigurnosnih standarda uposlenicima lokalne samouprave?

1.4. Metodologija

Pri izradi ovog istraživanja koristit će se znanstvena i stručna literatura iz područja menadžmenta i informacionih tehnologija, s posebnim fokusom na područje standarda informacionih sistema. Bit će korišteni sekundarni podaci prikupljeni iz naučnih baza podataka koji sadrže relevantne tekstove i radove vezane uz tematsko područje istraživanja. U procesu obrade teme koristit će se sljedeće metode:

- Analiza sekundarnih podataka iz naučnih baza podataka relevantnih za temu istraživanja;
- Metode deskriptivne analize za raščlanjivanje i opis elementarnih cjelina, te utvrđivanje njihovih odnosa;
- Sinteza metoda za povezivanje pojednostavljenih misaonih tvorevina u složenije cjeline;
- Induktivna i deduktivna metoda za izvlačenje općih zaključaka i primjenu zakonitosti na konkretne situacije. Provođenje intervjua sa 10 kolega Općine u kojoj sam obavila intervju, uz prethodnu saglasnost Općinskog načelnika, kao i depersonalizacija podataka.

1.5. Struktura rada

Završni rad će obuhvatati teorijski dio u kom ću obraditi sve tematske cjeline koje su u sklopu naslova magistarskog rada. Drugi dio obuhvata empirijski dio, odnosno opširan pregled i uvid u samu tematiku rada kao i problematiku u istraživanju.

U svom završnom radu obradit ću nekoliko cjelina, odnosno rad čini uvod i 2 (dva) poglavlja, te zaključak provedenog istraživanja. U uvodnom dijelu rada, prvo poglavlje, bit će predstavljen kontekst istraživanja, problematika koja se obrađuje i njena važnost. Također će se postaviti ciljevi istraživanja i objasniti metodologija koja će se koristiti. Uvodni dio će

također sadržiti pregled relevantne literature te definirati ključne pojmove i terminologiji. Drugi dio rada obuhvata teorijske osnove gdje će biti detaljnije razrađene teorijske osnove usklađivanja poslovanja sa standardima sigurnosti informacijskih sistema. Obuhvatit će se osnovni koncepti informacijske sigurnosti, standardi i norme koji se primjenjuju, kao i važni aspekti implementacije i upravljanja sigurnošću informacijskih sistema. Također, bit će opisane relevantne teorije i pristupi koji se koriste u istraživanju. Teorijski dio će obuhvatati drugo poglavlje sa potpoglavljima. U prvom potpoglavlju predstavit ću sistemski pregled literature. Drugo potpoglavlje će se odnositi na informacione sisteme koji su spomenuti u naslovu mog rada. Prikazat ću njegove definicije koje su se evaluacijski mijenjale, te same elemente koje čine uspješan informacioni sistem. Treće potpoglavlje rada će obuhvatati poslovne informacione sisteme, tipove poslovnih informacionih sistema kao što su ERP, SCM i CRM, te njihov uticaj i korist na sam informacioni sistem. Četvrto potpoglavlje će biti o sigurnosti informacionih sistema. Adekvatna zaštita i sigurnosni sistemi koji su nam potrebni za nesmetan rad informacionih sistema, kao i moguće prijetnje s kojima se mi kao korisnici možemo susresti. Ovaj dio rada obuhvatit će i dosta podpotpoglavlja koji su potrebni za sam prikaz zaštite, kao sto su antivirusi, te poteškoće za rad kompanija. Peto će biti o normama, odnosno standardima sigurnosti informacionih sistema kao što su CobitT, ITIL i ISO 27000 i njihova usporedba u ponudama koje nam one nude. Treće poglavlje govorit će o lokalnoj samoupravi. Lokalnu samoupravu koju sam odabrala za svoje istraživanje, te koje ona sisteme rada i zaštite koristi. Empirijski dio, odnosno proces istraživanje će biti dio ovog poglavlja u kojem će se provest istraživanje koje ima za cilj analizirati primjenu standarda sigurnosti informacijskih sistema u organima lokalne samouprave. Metodologija istraživanja bit će detaljno opisana, uključujući prikupljanje podataka, analizu podataka i interpretaciju rezultata. Također, bit će predstavljeni instrumenti ili upitnici koji će se koristiti u istraživanju. Detaljno ću opisati proces intervjua, zašto sam odabrala baš tu metodu za rad, te detaljnu analizu svih intervjuisanih osoba koje su mi pomogle prilikom izrade i istraživanja mog magistarskog rada. Prikazat će se problemi sa kojima se organi lokalne samouprave susreću, restrikcije i prijedlozi koji su otkriveni uz pomoć obavljenog istraživanja. Zaključak će sumirati glavne rezultate istraživanja i izvedene zaključke iz obavljenog intervjua. Bit će razmatrane implikacije dobivenih rezultata i njihova primjenjivost u praksi. Također, moguće će biti identificirane i ograničenja istraživanja, te će se predložiti smjerovi za daljna istraživanja. Na kraju rada, sistemski pregled literature. U ovoj cjelini rada bit će proveden detaljan pregled relevantne znanstvene i stručne literature iz područja menadžmenta, informacijskih tehnologija i standarda sigurnosti informacijskih sistema. Cilj ovog pregleda literature je steći uvid u postojeće spoznaje, istraživanja i prakse vezane uz usklađivanje poslovanja s tim standardima u organima lokalne samouprave. Pregledom literature identificirat će se najvažniji koncepti, modeli, metode i smjernice koje su relevantne za istraživanje.

2. TEORETSKI OKVIR

2.1. Sistemski pregled literature

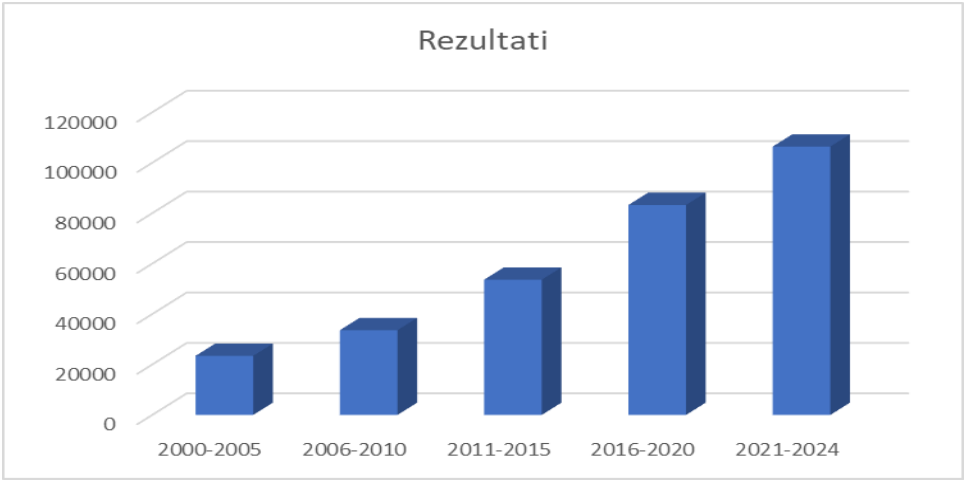
Nalazimo se u vremenu u kojem se susrećemo sa ljudima koji su „informatički opredijeljeni“, tačnije, oni koji dovoljno poznaju tehnologiju i informacione sisteme neophodni za njihov život i poslovanje. Dok sa druge strane, nalaze se „informatički nepismeni“ ljudi koji nemaju dovoljno znanja usmjerenog ka digitalizaciji, pa samim tim i informacionim sistemima koje trebaju da koriste. Tu dolazimo do određenog problema, pogotovo u kompanijama kojima je digitalizacija potreba za obavljanje posla. „Informatički nepismeni“ ljudi nam mogu donijeti dosta problema i poteškoća prilikom rješavanja poslova za kompaniju u kojoj poslujemo i za koju nastojimo da obavimo ključne poslove za njen opstanak. Stoga, treba usmjeriti pažnju na važnost informacionih sistema u poslovanju i izvan njega. Tehnologija napreduje, nalazi se svuda oko nas, te upravo zbog toga ne trebamo sebi dozvoliti da budemo među „informatički nepismenim ljudima“. Informacioni sistemi je izuzeno popularna riječ koja se u zadnje vrijeme sve više koristi. Kao ključne riječi koristit ću „information system“ i „security standards“ jednih od sastavnih riječi teme magistarskog rada.

Prvu bazu pretraga koju sam koristila je Google Scholar ukucavši „information system“ dobila sam ukupno 9.380.000 rezultata u periodu od 2020.-2024. godine. Dok za „security standards“ pikazuje 4.860.000 publikacija u istom intervalu.

Kao drugu bazu pretraga na EBSCOhost na riječ „infromation system“ daje ukupno 100 rezultata zaključeno sa 20.05.2024. godine, a „security standards“ ukupno 56 rezultata.

Treća baza pretrage odnosila se na Science Directs gdje na ključnu riječ „information system“ daje nam ukupno 951.913 rezultata od 2021.-2024. godine. A na „security standards“ 141.837 od istog vremenskog razdoblja.

Slika 1. Rezultati pretraživanja "information systems security standard"



Izvor: Sincedirect

Kucajući zajedno “information systems security standard” imamo ukupno 300.115 rezultata na ovu temu od 2000. godine pa sve do danas (Slika 1.).

Iz Slike 1. možemo da zaključimo da se zadnjih par godina povećala važnost navedenog termina. Kako tehnologija napreduje, tako i značaj standarda sigurnosti informacionih sistema postaje bitnija tema za pisanje. Ovu konstataciju upravo možemo da zaključimo i uz pomoć Slike 1. koja nam detaljno prikazuje povećanje važnosti spomenutih termina. Detaljnijim pregledom rezultata kroz Science Direct uočavamo koliko je ovaj termin važan po određenim oblastima:

- Computer Science,
- Engineering,
- Social Sciences,
- Enviromental Science,
- Economics, Econometrics and Finance,
- Medicine and Dentistry,
- Energy,
- Business, Management and Accounting,
- Agricultural and Biological Sciences,
- Decision Sciences.

Na osnovu navedenih stavki možemo da zaključimo da se standardi sigurnosti informacionih sistema koriste skoro u svim poljima rada.

Standardi sigurnosti informacionih sistema su bitno polje u svim sferama poslovanja. To možemo da vidimo i u prethodnom dijelu rada gdje sam nabrojala 10-ak oblasti u kojim se ovaj termin spominje. Stoga, ne treba ga zanemarivati. Treba ga uvoditi i u ostalim oblastima gdje je manje prisutan, kao i prikazati ljudima sa manjom informatičkom pismenošću šta je to standard sigurnosti informacionih sistema, te kakvu nam korist oni nude.

Na osnovu navedenih ključnih riječi i izvršene pretrage odabrala sam užu sekciju radova koje sam koristila kao osnovu za izradu rada. Ovdje bih izdvojila članak “The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector” od autora Kitsios, Chatzidimitriou i Kamariotou objavljenog 2023. godine koji mi je pomogao u boljem shvatanju standarda sigurnosti informacionih sistema. Prije svega ISO 27001 sistema koji predstavlja najbolji alat za zaštitu od bilo kakvih neželjenih upada, njegovu implementaciju, te primjenu u kompanijama. Pored ovog članka izdvojila bih još i članak od Markgraf, B. (2019). „Importance of Information Systems in an Organization“, prikazujući bitnost informacionih sistema u organizacijama. Zasigurno ovaj članak pokazuje da se informacioni sistemi ne smiju zanemarivati ni u jednoj kompaniji koja nastoji da osigura budućnost svog poslovanja. Pored članaka koristila sam i stručnu literaturu Lagumdžija, *et al.* (2008). Menadžment informacioni sistemi: kompetitivnost i informacione tehnologije, Ekonomski fakultet Sarajevo i Lagumdžija, *et al.* (2021). Menadžment

informacioni sistemi, Ekonomski fakultet Sarajevo koji su mi predstavljali ključne smjernice za izradu strukture rada, kao i pitanja koja sam koristila u obavljanju intervjua.

2.2. Koncept upravljanja podacima i informacijama

Teško je utvrditi, pogotovo danas, šta je to toliko važno da korisnici poznaju iz oblasti informacionog sistema, smatra Anon (2021). Anon (2021) je rekao da je neophodno bolje razumijevanje informacionog sistema kako bi oni mogli egzistirati i opstati. Informacioni sistem je nešto više od samog računara. Njegova efikasna upotreba predlaže bolje shvatanje same organizacije, menadžmenta, kao i same informacione tehnologije prikladne sistemima prikazanim na Slici 2. Informacioni sistemi se mogu dočarati i kao menadžerska i organizacijska objašnjenja na rizike koje im sredina nameće. Kako bi dizajnirali informacioni sistem i efikasno ga primjenjivali moramo razumjeti određene pojmove koji su potrebni za njegovo djelovanje. Ti pojmovi se odnose na prostor u kojem se koriste, strukturu, funkciju i pravila organizacije, samu korist menadžmenta, kao i provođenje odluka u menadžmentu. Pored toga, potrebno je utvrditi učinkovitost, mogućnost i svrhu koju nam omogućava primjena informacione tehnologije, te rješenja koja nam oni nude.

Slika 2. IS kroz tri dimenzije: organizacija, tehnologija i menadžment

Izvor: Lagumdžija et al (2021)

U nastavku rada ću na što jednostavniji način pokušati skrenuti pažnju na neke bitne aspekte u definisanju pojma informacionog sistema. Informacioni sistem prema Lagumdžija *et al.* (2021) možemo definisati kao sistem koji koristi informacije kako bi ispunio informacione prioritete organizacijama. Strauss (2022) ipak smatra da informacioni sistem predstavlja skup alata koji se koriste za skupljanje, analizu, te upravljanje postojećih podataka. Međutim,

"informacioni sistem je skup međupovezanih komponenti koje zajedno rade na prikupljanju, procesiranju, storiranju i distribuciji informacija u cilju podrške odlučivanju i kontroli u organizaciji" smatraju Laudon and Laudon (1984) gdje se ova definicija i dan danas najviše primjenjuje. Informacioni sistem ustvari obuhvata hardver, softver, podatke, ljude, kao i postupke koji zajedno funkcionišu kao jedna cjelina kako bi transformisali podatke u informacije koje su nam potrebne za dalji nastavak posla (TechTarget Contributor, 2023).

Ima mnogo definicija koje se koriste za definisanje informacionog sistema tako da TechTarget Contributor (2023) smatra da često informacione sisteme u literaturi povezuju i sa kompjuterskim sistemima, ali ti sistemi nisu isti. Ustvari i jeste istina da je većinski dio informacionih sistema kompjuterski bazirano, ali isto tako i ne moraju da budu (Rainer i Casey, 2013). Kompjutersko bazirani informacioni sistemi su sistemi koje primjenjuju kompjutersku tehnologiju za izvođenje određenih rješenja ili zadataka potrebnih korisnicima koji ih primjenjuju. S druge strane, Laudon i Laudon (2016) daju širu definiciju koja definira "informacioni sistem kao set međusobno povezanih komponenti koje zajedno rade na prikupljanju, procesiranju, čuvanju i distribuciji informacija s ciljem donošenja odluka i kontroli u organizaciji" prikazano na Slici 3. Dodatno, mnoge kompanije koriste informacione sisteme kako bi obavljale svoje postavljene zadatke. Na taj način oni uspjevaju da komuniciraju sa svojim potrošačima, te budu uspješniji od svoje konkurencije na tržištu (Mukherjee, 2022). Informacioni sistemi služe zaposlenicima da pronađu problem, nađu adekvatno rješenje za njega, te ih riješe uz kreiranje novih brendova pogodnih za njihove krajnje kupce. Osnovne aktivnosti, odnosno procesi koje informacioni sistem prati su ulaz, procesiranje, skladištenje, izlaz, te povratne informacije koje se prikupljaju od korisnika (TechTarget Contributor, 2023).

Slika 3. Funkcije informacionog sistema

Izvor: Autorski rad

2.2.1. Elementi informacionog sistema

Kako bi uspješno obavljali poslove u kompaniji u kojoj radimo, te prikupljali, procesirali, skladištili i dostavljali sve potrebne informacije krajnim korisnicima, informacioni sistem sadrži sintezu od 6 (šest) neophodnih elemenata (Ivković, 2019), a to su (Slika 4.):

- Hardware – su komponente koje lahko možemo dodirnuti i dotaći, dok se ostali elementi nalaze unutar uređaja, a koji se mogu vidjeti prilikom njegovog otvaranja (Ly-Huong T. Pham *et al*., n.d.);
- Software – skup uputa, odnosno programa koji se primjenjuju za rad kompjutera, te obavljanje pojedinih zadataka (Braden, 2024). Drugim riječima, govori kompjuteru (Hardwaru) šta da radi (Ly-Huong T. Pham *et al*., n.d.). Za razliku od Hardwara koji je opipljiv, te ga možemo vidjeti i dodirnuti, softver nije opipljiv;
- Liveware – predstavljaju sve ljudske komponente koje su učestvovale u izgradnji informacionog sistema ili predstavljaju krajnje korisnike koji koriste neki informacioni sistem;
- Orgware – organizuje i povezuje računarsku opremu hardver, programski jezik softver i ljude, koji mogu biti izvršitelji ili krajni korisnici, u jednu skladnu cjelinu (Anon, 2008);
- Netware - pokazuju važnost u međusobnom spajanju različitih komponenti, te osigurava pristup krajnim korisnicima sa različitih mjesta unutar organizacije (TechTarget Contributor, 2023);
- Dataware - imaju važnu ulogu u primjeni informacionog sistema. One predstavljaju skup povezanih tablica, gdje svoje mjesto staništa imaju na disku u kojem su zabilježeni podaci neophodni za kompanije (Ivković, 2019).

Slika 4. Elementi informacionog sistema

Izvor: Autorski rad

Osnovna podjela Dataware je na podatke, informacije i znanje o čemu ću pričati u nastavku rada (Šafar, 2022).

Informacioni sistem će biti uspješan ukoliko svi navedeni elementi budu povezani, podjednakim djelovanjem kao jedna cjelina. Dat ću vam jedan primjer. Recimo da radimo u nekoj manjoj kompaniji koja se bavi proizvodnjom namještaja. Menadžer od nas zahtjeva da upratimo troškove koji su nastali prilikom poslovanja, te nakon određenog vremenskog perioda mu pošaljemo kako bi on mogao izanalizirati gdje se novac najviše utrošio. Kako bih uradila zadani zadatak, prvo mi je potreban laptop ili kompjuter koji ću koristiti za svoj rad, te svi potrebni uređaji uz kompjuter (miš, tastatura, itd.) koji su mi potrebni za obavljanje posla. Nakon toga, moram primjeniti određenu aplikaciju putem koje ću uraditi posao. Odlučila sam se za korištenje Excel aplikacije kako bih napravila tabelu prikupljene liste troškova na svom laptopu/kompjuteru, te poslala svom menadžeru. Da bih poslala menadžeru svoj završni rezultat potreban mi je sistem, laptop ili kompjuter sa pratećom opremom, radna tabela i internet kako bih se priključila na e-mail putem kojeg ću svom menadžeru poslati finalne rezlutate. Kao što sam u prvoj rečenici rekla svih (šest) navedenih elemenata moraju da budu povezani i da rade svoj posao zajedno. Svaka komponenta ima svoj posao koji obavlja, te kad ih zajedno pogledamo daju jednu savršenu cjelinu u obavljanju poslovnih zadataka. To znači da sam uz pomoć Hardware obavila zadan zadatak, ali u tome mu pomaže programski jezik Software, jer Hardware ne razrješava sam zadatke već mu u tome priskače u pomoć Software. Međutim, kako bi Hardware i Software radili bez mene (Liveware) koja upravljam njima i koristim informacioni sistem koji mi pomaže u otklanjanju nedoumica i rješavanju zadatka. Dateware sakuplja, obrađuje informacije koje koristim za pravljenje liste troškova nastalih u posljednjem periodu. Orgware povezuje sve prethodne cjeline u jednu, te uz pomoć Netwera, tj. e-mail adrese prenosim informacije menadžeru. Tako smo moj menadžer i ja prikupili sve potrebne informacije za nastavak rada u kompaniji i donijeli odluke koje će pospješiti bolje i efikasnije buduće poslovanje.

Iz poslovne i organizacione tačke gledišta, informacioni sistem je ustvari nešto mnogo značajnije od procesa ulaza-procesiranja-izlaza smatra Luić (2009). Sa poslovne strane, informacioni sistem je temeljen na informacionim tehnologijama za organizacioni i menadžerski odgovor na izazove koje nam okruženje nameće prilikom poslovanja. Informacioni sistem nam ustvari obezbjeđuje pomoć za sve poteškoće i izazove koje nam okruženje u kojem radimo stvara (Mudželet, n.d.). Da bi shvatili informacioni sistem, šta je ustvari njegova korist i uloga u poslovanju, moramo razumjeti mnogo širu sliku organizacije, menadžmenta i sistemske dimenzije informacione tehnologije, te njegove sposobnosti da spoznaju rješenja za nastale izazove (Luić, 2009).

Informacioni sistem ima veoma važnu ulogu u današnjem poslovanju. U posljednje vrijeme se često spominje digitalna transformacija, tačnije transformacija svakog segmenta poslovanja koje utiče na komponente u poslu koji obavljamo. Pojedinci, kompanije, organi lokalne samouprave, tj. državne ustanove koriste društvene mreže kako bi se povezali sa aktivnostima koje se obavljaju u sferi posla kojim se bave. Pojedinci će koristiti interaktivne alate kao što su telefoni, tablet uređaji, kako bi došli do informacija kome da vjeruju,

odnosno gdje da kupe proizvod koji im je potreban u datom momentu (Giones F, Brem A., 2017). Na taj način oni otkirvaju dosta informacija o kompanijama koje posluju na tržištu, te proizvode koji oni nude. Traže recenzije koje im se nude na internetu kako bi odlučili koja kompanija će na najbolji način zadovoljiti njihovu potrebu.

Međutim, digitalna transformacija ne pomaže samo pojedincima. Ona pomaže i kompanijama koje također koriste digitalnu tehnologiju dovodeći u pitanje njihov odnos sa kupcima, te šta oni u tom trenutku traže. Na taj način kreiraju strategiju koja će im pomoći u diferenciranju na tržištu, te donijeti određenu prednost u odnosu na konkurente. Digitalna transformacija počinje od momenta kad kompanija uvede digitalnu tehnologiju u svom poslovanju (Čakovec, 2021). Pojavom korona virusa digitalna transformacija postala je jedna od najvažnijih elemenata u poslovanju (Oskoruš, 2018) između poslovnih ljudi ili kompanija i krajnjeg korisnika. Omogućila nam je dostupnost usluga i proizvoda koje nam kompanije nude, kao i informacije krajnim kupcima u bilo koje vrijeme i na bilo kojoj lokaciji. Prvo su postojale web stranice koje su nam pružale obavijesti o uslugama, a nakon toga digitalni procesi koji su omogućili interakciju između kupaca (Igrec, 2018). Zbog velike dostupnosti informacija i očekivanja kupci postaju zahtjevniji, jer na efikasan način dolaze do informacija o proizvodima koji im se nude, njihovoj kvaliteti i cijeni. Zbog uvođenja digitalne transformacije u poslovanje način poslovanja se upotpunosti promijenio (Boban M. i Babić A., 2014), jer to nije više izbor koji se mora imati, ona je postala neophodna karika u današnjem poslovanju (Oskoruš, 2018).

Za bolje razumijevanje suštine teme mog magistarskog rada, ali i za dalje razumijevanje funkcioniranja informacionih sistema u kompanijama, tj. organima lokalne samouprave, kao i njihovog korištenja u cilju unapređenja poslovanja, definirat ću osnovne pojmove koji se vežu za moju temu kao i za termin informacioni sistemi: podatke, informacije, znanje, informacione tehnologije i lokalnu samoupravu (Slika 5.).

Slika 5. Proces pretvaranja podataka

Izvor: Autorski rad

2.2.2. Podatak

Prije mnogo godina, Glaser (2001, 2007) je primijetio da su podaci svuda oko nas. Pojam "podatak" ustvari predstavlja zbirku brojeva i simbola bez ikakvog značenja (Cambridge

International Examinations, 2017). Drugim riječim, oni obuhvataju opis događaja ili bilo kojeg drugog dokumenta koji nisu smišljeni tako da posjeduju neko značenje. Podaci su osnovica znanja, jer ustvari kad stvaramo znanje o nečem to doživljavamo kao jedan vid procesa. Zbog toga su podaci ustvari sirovi materijali. Podaci su simboli, karakteri, slike, brojevi. Sve su to podaci koje mi svakodnevno koristimo, a i ne moramo. To su sve ulazni podaci koji su neophodni informacionim tehnologijama za obradu kako bi prešli u naredni korak, a to je stvaranje ključne informacije (Lagumdžija *et al.*, 2021.).

Podaci čine razne oblike informacija koje su obično izgrađene na poseban način (Simplilearn, 2023). Ellö (2022) kaže da "podaci u kontekstu i kombinovani unutar sktrukture čine informaciju". Ustvari pojam informacija vuče korijen od latinske riječi "informare" što u kontekstu predstavlja "obavještavanje" (Faraguna, 2015), odnosno drugim riječima informisanje o nečemu. Informacija je krajnji ishod procjene i organizacije podataka tako što pruža jedinstveno znanje krajnjem korisniku (Muris, 2020). Međutim, korisnici koji koriste informacije ne smatraju da su ljudi dobro informisani sa tim informacijama, jer su proizvedene i isporučene informacije često nepotpune za veći broj korisnika zbog mogućnosti manipulisanja informacijama (Gredelj, 2020). Informacije se publikuju, odnosno daju nam ovlaštenje za njegovo korištenje. Često ljudi miješaju podatak i informaciju, ali između njih postoji velika razlika. Informacije su ustvari podaci kojima se dodjeljuje određeno značenje. Na taj način bismo ih bolje shvatili i razumjeli. Oni pružaju korist podacima kako bi ih mogli upotrebljavati. Informacija je ustvari mnogo više od podatka. U suštini, korist koju imamo od informacija je i glavna razlika informacije od podatka. Podatak je konstatacija obično u obliku neometano ući, obraditi i izaći (Anon, 2012). Sa drugog aspekta, podatak je simbol.

Obrazovani i sposobni ljudi predstavljaju ključnu ulogu u procesu transformacije podataka u krajnju informaciju. D. Radivojević, M. Radivojević (2017) govore da se oni "najčešće sastoje od interpretacije podataka kao činjenica koje imaju smisao u konkretnom kontekstu," kreira neophodan oblik podatka kako bi se tvrdnje na odgovarajući način mogle prezentovati, prikazati.

2.2.3. Informacija

Podaci koji su sprovedeni u smislu da imaju neko značenje, odnosno da ih možemo protumačiti u literaturi su poznate kao informacije (Laudon i Laudon, 2016). Informacije su često pokazatelj obrade podataka, najčešće kompjuterskih. Kao što sam u prethodnom potpoglavlju rekla podatak nema tačno definisano značenja. To su simboli, brojevi, slike, kojim se treba dodijeliti značenje i interpretirati kako bi postali informacija. Oni su ustvari ulazni podaci koji se obrađuju kako bi se stekla informacija sa značenjem. Informacija je obrađen i organizovan oblik podatka (Spilker, 2023). Odnose se na podatke koji su razmatrani, struktuirani i dato im je određeno značenje, odnosno kontekst. Informacije kao takve mogu poslužiti za pružanje odgovora na postavljena pitanja ili uz pomoć njih

donosimo ključne ideje za poslovanje. Važno je samo da ona kao takva bude korisna (Markgraf, 2019).

Iz ovog zaključujemo da informacija predstavlja podatak sa datim kontekstom, odnosno značenjem koje mu se daje i saznanje koje se može proslijediti u pisanom, vizuelnom, elektronskom ili bilo kojem drugom obiku (Spremić,2017).

Informacije su postale veoma važna karika u svakom poslovanju. Od nje ovisi dalji razvoj i opstanak kompanije. Počnimo od nas samih koliko su nam nekad informacije bitne kako bi donijeli neke odluke u životu koje su ključne za nas. Tako je i sa kompanijama. One postaju otvorenije u pružanju informacija dobavljačima i krajnjim korisnicima kako bi ih na taj način privukli i ostvarili saradnju s njima. Potrebno je da kompanija zna kako da koristi informacije u svoje svrhe, te da izvuku najbolje što im ona nudi (Jones,2018). Međutim, ukoliko ih ne upotrebljavamo na pravi način mogu nas dovesti do mnogih problema. Virusi, hakerski napadi i špijunaže su nešto što se može dogoditi ukoliko neko želi pristupiti našim informacijama (Brown, 2022). Zato ih moramo čuvati na adekvatan i prihvatljiv način, te pobjeći od svih prijetnji koje nas okružuju.

Resursi koji odgovaraju određenim grupama neophodno je kategorizirati na mnogobrojne načine (Kovačević, 2008). Informacionom sistemu je ustvari najznačajnija informacija, te je zbog toga nužno uspostaviti adekvatan sistem klasifikacije (Carnet, n.d.). U samom sistemu nalaze se informacije koje su od ključne važnosti za samu organizaciju pa ih tako možemo klasifikovati od onih koje su ključne, pa sve do onih koje su kritične po njih. Zbog toga se upravo koristi klasifikacija kako bi informacije zaštitili na pravi način (Službeni glasnik, 2017). Prilikom postavljanja određenih kriterija pravimo i klasifikaciju informacija, a to je obično prema vrijednostima koje te informacije nude, njihovog uticaja vremena na njenu korisnost, itd. (Kopal i Kortuk, 2012).

U svakoj kompaniji, tako i u organima lokalne samouprave, postoji sljedeća vrsta klasifikacije sistema, i to:

- Javne,
- osjetljive,
- povjerljive i
- tajne (Kovačević,2008).

Javne informacije sama riječ kaže su one infromacije koje mogu biti objavljene i javne za sve građane. One su dostupne javno (Bo Sundgren, 2005). Često se za njih kaže da su to informacije koje se ne nalaze u sistemu klasifikacije jer njihovo objavljivanje ne predstavlja nikakav problem, niti će stvoriti ikakve poteškoće za organizaciju. Zbog toga, kod njih nije potrebno provesti nikakvu sigurnosnu kontrolu.

Važnost zaštite osjetljivih informacija je veoma značajna. Objavljivanje takvih informacija može imati dugoročne posljedice. Zbog toga, one moraju imati veći nadzor kako ne bi došlo do određenih gubitaka u kompanijama. Osjetljive informacije propisuju ko bi mogao imati

pristup tom vidu informacija, u kojim uslovima, prilikama i u kojem momentu (Objašnjeno, 2020).

Povjerljive informacije su one koje su određenim zakonima ili nekim drugim propisima navedene kao povjerljive (Moje znanje, n.d.). Otkrivanjem ove vrste informacija može ugroziti rad kako kompanije tako i zaposlenika. One se upotrebljavaju unutar kompanija koje štite te informacije.

Informacije su tajne, tajne informacije, kada se odnose na osjetljive podatke ili bilo koje nedozvoljene djelatnosti koje su povezane s njima, a mogu izazvati vrlo velike probleme za kompaniju (Kovačević, 2008). To je upravo razlog zbog čega se uvodi odgovarajuća implementacija sigurnosti ovih informacija (Kopal i Korkut, 2012). Implementacija je zaista ključan faktor u održavanju ovih informacija tajnim. Važno ih je zaštititi, te njihov prijenos obaviti na siguran način kako bi osigurali privatnost kompanije i pojedinaca.

Informacije su bitan faktor za kompanije i pojedince. Ona je u suštini poruka koja kao takva ima veliku korist za njih. Informacija podrazumijeva informacioni tok od jednog korisnika do drugog. Najčešće se to odvija u vidu komunikacije koja predstavlja najbolji način za razmjenu informacija među korisnicima. Pošiljaoc kao jedan korisnik, primaoc kao drugi su jedan dio informacionog toka koji im omogućava da prenose znanje, ideje i mnoge druge korisne informacije za njih (Đelmo, 2020). Iako je primalac informacija u većini slučajeva čovjek koji je nadaren da svojim razumom i intelektom primi informaciju, procesira je i na kraju da konačni odgovor na nju, primalac informacije može biti i kompjuterski sistem koji je isto tako u stanju informaciju da primi, te interpretira u skladu sa njegovim mogućnostima. Zato je jako bitno da razlikujemo podatak od informacije koja ima značenje, ali koja ipak ne mora biti istinita i razumljiva za pojedinca koji ga šalje ili prima (Kopal i Korkut, 2012).

2.2.4. Znanje

Rainer i Casey (2013) opisuju znanje kao struktuiranu i procesiranu informaciju i/ili podatak koja pruža mogućnost shvaćanja, znanja i akumuliranog učenja. Ono nam pomaže da otklonimo trenutni poslovni problem koji je nastao unutar organizacije. Znanjem donosimo ključne odluke, te ostvarujemo napredak u raznim poljima poslovanja. Kako bi povezali pretpostavke iz realnog svijeta u podatke pomoću kojih će nastati informacije koje imaju neko značenje, bit će nam potrebno znanje (Anon, 2008). Znanje je svijest i shvaćanje informacija koje omogućavaju spajanje u kontekstu potpore i izvršavanja zadatka.

Slika 6. Proces pretvaranja u informaciju

Izvor: Autorski rad

Slika 7. Proces pretvaranja u znanje

Izvor: Autorski rad

Na slici 6. i slici 7. vidimo da jedno bez drugog ne mogu djelovati jer su sva tri elementa izrazito važna za bolje shvatanje informacionog sistema. Znanje će ostati primarna konkurentska prednost za kompanije, pojedince, pa i samu državu (Cvjetković, 2014). Nove ideje, proizvodi ili nove metode poslovanja su inovacije koje predstavljaju osnovnu pokretačku snagu u kompanijama. Svaki čovjek se obrazuje čime stiče znanje za napredovanjem u kompaniji u kojoj posluje. Time se stvara prilagodba uslovima i hvatanje priključka razvoja postat će prioritet za sve (Šehanović J. *et al.*, 2002).

2.2.5. Informacione tehnologije

Sam naziv informacione tehnologije ili IT odavno se počeo koristiti u poslovanju kompanija i sferi računarstva (Mitchell, 2020). Ljudi obično ovaj termin koriste kada misle o poslovima koji su povezani sa kompjuterima. Člankom iz 1958. godine u časopisu Harvard Business Reviewu počelo se spomunjati da se informacione tehnologije sastoje iz tri osnovna dijela (Mitchell, 2020). Upravo je taj članak skovao taj izraz, te doprinio početak nastanka informacionih tehnologija.

Informacione tehnologije možemo definisati kao mašine, aparate, te njihove aplikacije koje imaju kompjuterske i interakcijske mogućnosti smatra Jokanović *et al.* (2019). Ipak, Lagumdžija *et al.* (2008) ističe da su ustvari informacione tehnologije jedan od velikog broja alata koji su dostupni kompanijama i njegovim menadžerima da se suoče sa problemima koji im nastanu u toku poslovanja. Informacione tehnologije možemo iskoristiti u toku njegovog

kreiranja, skladištenja podataka i informacija, te njihove distribucije koja će nam pomoći u kreiranju znanja (Plojović, 2009). Njegov cilj je upotreba tehnoloških sistema za otklanjanje poteškoća, problema, te upravljanje informacijama (Schulze, 2024). One ustvari predstavljaju najvažniji dio modernog poslovanja. To je spona koja povezuje kompaniju. IT predstavlja instrument pomoću kojeg kompanije nadgledaju i stvaraju svoje aktivnosti. Hardware i Software su sastavni dijelovi informacionih tehnologija, koji služe za prikupljanje, obradu i distribuciju informacija (Jokanović *et al.* 2019).

Smatra se da podaci i informacije pokreću poslove u cijelom svijetu. IT obezbjeđuje sredstva za razvoj, procesiranje, analizu podataka i informacija, gdje bez njega kompanije mogu ostati bez konkretnih mogućnosti prikupljanja i obrađivanja podataka u korisne informacije (Castagna i J. Bigelow, n.d.). Zbog toga, menadžeri u svojim kompanijama trebaju učinkovit informacioni sistem kako bi na što lakši i jednostavniji način bili informisani o poslovanju unutar same kompanije. Bez korisnih informacija teško će se ostvariti željni rezultati, te realizovati poslovne odluke koje imaju za cilj poboljšati konkurentnije pružanje usluga. Kako bi kompanije osigurale svoj opstanak na tržištu moraju prikupljati podatke koji će kasnije postati korisne infromacije sa adekvatnim značenjem za njih. Zbog toga je ključan informacioni sistem koji će omogućiti sigurno procesiranje podataka u informaciju, pa onda u znanje. Kvalitetan je onaj sistem koji zavisi od bezbijednosti tih sistema (Luić 2009).

2.3. Poslovni informacioni sistemi

Mi kao pojedinci svakodnevno koristimo mobilne telefone za rukovođenje bankovnim računom, rasporedom, komunikacijom. Međutim, preduzeća ne mogu svoje poslovne zadatke obavljati putem telefona (UAGC-a, 2023). Tu upravo ključnu ulogu imaju poslovni informacioni sistemi predstavljajući skup hardvera i softvera koji služe za upravljanje podataka kompanija.

Unapređenje informacionih tehnologija doprinijelo je unapređenju mnogih oblika softverskih aplikacija u kompanijama. Razvojem softverskih aplikacija koje se koriste unutar kompanija razvijaju se i poslovni informacioni sistemi koji su korisni u poslovanju. Također, tržišno okruženje postaje vrlo komplikovano zbog sve veće konkurencije i globalizacije, te svega onog što one sa sobom donose. Kompanijama je potrebno sve više podataka i informacija koji će im poslužiti za efikasno donošenje odluka, nabavki, rukovođenjem, distribucijom, te upravljanjem ljudskih resursa (Kaić, 2019). Upravo poslovne informacione sisteme koristimo kako bi organizovali, donijeli odluke, upravljali, te tehnički podržali sve poslovne procese koji se vode unutar kompanije (UAGC-a, 2023).

Kompanije, isto tako i Općine, kako bi poboljšali svoju učinkovitost nastoje reorganizovati poslovne procese kako bi bili jednostavni, produktivniji, prilagodljiviji, fleksibilniji i efikasni. Pored toga, neophodno je dobiti tačnu i korisnu informaciju koja će ovisiti od uspjeha odgovarajućeg toka informacija, upravljanja odnosima s klijentima i dobrima dobavljača (Kaić, 2019).

Poslovni informacioni sistem je skupina međusobno zavisnih komponenti koje služe za prikupljanje ulaznih podataka, obrade, te izlaza podataka i kontrolisanja kako bi podatke transformisali u značajne informatičke proizvode koji će se upotrijebiti za planiranje, organizovanje, kontrolu, donošenje ključnih odluka za kompaniju, te ostalih aktivnosti koji su potrebni kompaniji za uspješno poslovanje (Ivanov, n.d.). To su sistemi koji koriste informacionu tehnologiju u poslovanju radi stvaranja korisnih informacija. Takvi sistemi, ustvari, prihvataju odlučivanje od strane zaposlenika u cilju ostvarivanja njegovih zadataka (Sharma, n.d.). Važno je spomenuti da mnoge kompanije u sklopu informacionih sistema sadrže složene i inovativne sisteme korisne za interakciju i kolaboraciju (Kaić, 2019).

Nalazimo se u vremenu gdje tehnologija napreduje velikom brzinom. Iz dana u dan susrećemo se sa nekim novim izazovima o kojim učimo i usavršavamo se u njima. U savremenom poslovanju mnoge kompanije, industrije, kao i organi državnih institucija najvećom mjerom koriste informacione sisteme uz pomoću kojih postaju konkurentniji na tržištu i ekspeditivniji u poslovnim izazovima koje im nameće okolina, kako bi na zadane zadatke brže i preciznije odgovarali (Lagumdžija *et al.*, 2021.). Menadžeri su upravo ti koji otkrivaju izazove koje im okolina nameće, donose odluke, upravljaju ljudskim resursima, te finansijskim resursima kako bi ostvarili adekvatnu strategiju i nadgledali posao (Skolait, 2021). Posao menadžera je da pruži značenje slučajevima sa kojim se kompanije susreću, te oformi plan kako bi otklonio sve nedoumice i probleme nastale tokom poslovanja. Upravo poslovni informacioni sistem ostvaruje ambicije i snove svakom menadžeru (Skolait, 2021).

Cilj poslovnog informacionog sistema je ostvarivanje dobiti koja će olakšati stvaranje boljeg savremenog poslovanja kroz aplikativna rješenja ostvarenih u kompaniji (Bečejski-Vujaklija, 2008). One obuhvataju veliki skup aplikacija. Od jednostavnih aplikacija koje su složene za korištenje i služe za interakciju i kolaboraciju do onih kompleksnijih aplikacija koje se koriste za najveći obim poslovanja, te spajaju sve segmente poslovanja u jednu grupu. Spomenute aplikacije koriste se odvojeno uz određena vremenska razdoblja tako da ih možemo podijeliti na:

- ERP - Enterprise resource planning;
- SCM - Supply chain management i
- CRM - Customer relationship management.

Poslovne aplikacije se nastavljaju unapređivati nezavisno jedna od druge, ali zavisno od njihove svrhe za što bi se trebale koristiti, odnosno biti korištene. Vremenom aplikacije počinju da se spajaju radi lakšeg poslovanja. Tako, naprimjer dolazi do spajanja finansijskog poslovanja i računovodstva, tj. aplikacija koje su srodne. Unapređenje tih aplikacija i njihovo aktivno korištenje interneta, gigantskim kompanijama nameće spajanje svih aplikacija koje koriste jedan set koji se naziva *"business suite"* kao što imamo meta business suite koji su spojili svoje aplikacije u jednu cjelinu. (Sonnenberg 2022). Tako da u poslovnom svijetu

nekad se svi ovi uzajamni sistemi javljaju u jednom zajedničkom ili se uzajamno modularno isprepliću (Lagumdžija *et al.*, 2021.).

2.3.1. ERP (Enterprise resource planning)

Prije nastanka poslovnih informacionih sistema zaposlenici unutar svojih kompanija koristili su ručnu metodu poslovnog upravljanja. Cijena proizvoda varilala je zavisnosti od troškova radne snage (Samaržija, 2019). U tom periodu manje se pratila količina zaliha, pa su se zahtjevi kupaca najčešće sprovodili direktno iz skladišta kompanije. Uobičajno je bilo da se odgovarajuća količina svakog proizvoda kojeg kompanija pruža krajnjim korisnicima čuva u skladištu (Lukić, 2022). Primjenjivale su se razne metode planiranja koje su svoj fokus stavile na najkorisnije poslovne prakse na način da se rukovodi velikim resursima zaliha (Bertina, 2009). Polako dolazi period kad kompanije nisu imale mogućnost proizvoditi proizvode u velikim količinama, te ih lagerovati u skladište (Lukić, 2022). Proizvodi su se počeli praviti po narudžbama korisnika. Nastankom kompjutera, te poslovnih informacionih sistema koji su omogućili lakše poslovanje, razvija se i sistem upravljanja materijalnim resursima ili MRP koji pomaže da traženi proizvod bude dostupan u traženo vrijeme po najnižim troškovima bez lagerovanja u skladištu (Essex, 2024). MRP sistem nastao je davnih 70-tih godina (Vuković, Džambas i Blažević, 2007). MRP se spaja sa prostim misijama u proizvodnji, te označava razvijeniji model dosadašnjih napora obrade popisa materijala (Rušev, 2017).

Enterprise resource planning, je poslovno planiranje zaliha, temeljeno na MRP, kojem je postojanje zabilježilo 90-tih godina (Pit.ba, 2020). ERP možemo da definišemo kao poslovno rješenje koje pomaže kompanijama u rukovođenju procesima, te usklađivanja pojedinačnih sistema prateći samo poslovanje kompanije objedinjavajući ih u jednu cjelinu kako bi omogućio lakši protok informacija i komunikacije među zaposlenicima. (Ristić, 2017). On se upotrebljava za podršku kompanijama u obavljanju posla, te za korištenje u svim segmentima poslovanja organizacije (Lerotić, 2015). Jednostavnija komunikacija i razmjenjivanje informacija među zaposlenicima omogućava nam upravo ERP aplikacije koje obezbjeđuju da različiti sektori u kompaniji lakše komuniciraju i pristupaju informacijama (C. Kelly i Jiwon MA, 2024).

Zavisnosti od kompanija koji proizvode proizvode, te potreba krajnjih korisnika, ERP sistemi obavljaju poslove objedinjavanja kupaca i dobavljača u cjelovit poslovni sistem, služe za adekvatno donošenje odluka, te upravljaju segmentima u kompanijama kao što su prodaja, nabavka, marketing, ljudski resursi, itd (Pavković, 2020). Njihov cilj je objedinjavanje poslovnih funkcija u jednu korisnu cjelinu temeljenu za stvaranje e-poslovanja. Kvalitetnom primjenom kompanije će pospiješiti proizvodnju, smanjiti troškove, profitabilnost, te bolji protok informisanja i komunikacije kompanije sa krajnjim korisnicima.

2.3.2. SCM (Supply chain management)

Još jedan od navedena tri sistema koji se u praksi često spominje i koristi je SCM ili upravljanje dobavljačkim lancem. Dobavljački lanac je ustvari spajanje sistema poslovnih organizacija, tačnije njihovih zaposlenika, aktivnosti kojim se oni bave, tehnika, tehnologija, te informacionih i drugih potencijala za proizvodnju i transport proizvoda od dobavljača odnosno proizvođača do krajnjih korisnika (Mustapić, 2022). Efikasnost kompanije, gledano u globalu, zavisi od cijelog lanca spoljašnjih faktora, ostalih kompanija, zaposlenika, te ustanova i institucija koji učestvuju u dobavljačkom lancu. Shodno ovome, kompanija neće biti produktivna samo ako obavljaju svoj posao unutar kompanije uspješno. Poredimo li ERP i SCM, ERP koncept je više baziran na sami rad u unutrašnjosti organizacije, dok SCM svoj rad usmjerava i na spoljašnje okruženje.

SCM predstavlja poboljšani način nastanka proizvoda, od momenta nabavke sirovih materijala do njegove finalne proizvodnje, prodaje, te isporuke krajnjim korisnicima (Robinson i Diann, 2024). Može nam pružiti podršku u upravljanju aktivnostima kompanije kako bi otklonio otpad, uvećao vrijednost za krajnje korisnike, te omogućio ostvarenje prednosti na tržištu u odnosu na konkurente (Fernando, 2024). SCM kombinuje sve sisteme u jednu cjelinu okrečući svoj posao na spoljašnje procese u kojem učestvuje kompanija. To su sistemi koji svoju komunikaciju ostvaruju sa ogromnim brojem učesnika u tom dobavljačkom lancu dijeleći veliku količinu podataka i korisnih informacija. Budući da je to izrazito velik potez, svaki učesnik u lancu, od dobavljača, prozvođača, krajnjeg korisnika, trebaju nastojati da komuniciraju i sarađuju zajedno kako bi efikasnost obavljanja posla bila na zavidnom nivou, te se smanjila mogućnost nastavka rizika (Robinson i Diann, 2024). SCM je tipični sistem koji nastoji pratiti i spojiti nabavku, proizvodnju i distribuciju proizvoda i usluga. Kvalitetnim rukovođenjem cijelim procesom unutar kompanije mogu se sniziti troškovi, te umanjiti nepotrebni koraci radi lakše isporuke korisnicima (Fernando, 2024).

Po Laudonu i Travelu (2007.), planiranje u rukovođenju lancem opskrbe i isporuke uključuje više osnovnih modula:

- planiranje proizvodnje proizvoda i usluga,
- planiranje intenziteta ponude i tražnje,
- planiranje isporuke proizvoda i
- planiranje prijevoza.

2.3.3. CRM (Customer relationship management)

Teško je zamisliti život bez mobilnog telefona. Svima nama su upravo oni jako bitna karika u našim životima. Na njima se nalaze informacije koje su nam ključne za poslovne ili private svrhe. Informacije koje mi kao ljudi ne bi mogli zapamtiti u tolikoj mjeri. Isto tako je i sa kompanijama kojima je potrebno više informacija za njihov kvalitetan rad. Kompanije prate

proizvode, kupce, konkurente. Sve su to velike količine informacija koje su potrebne kompaniji da ima adekvatan rad. Za to upravo služi CRM sistem.

CRM je poprilično star sistem koji u zadnje vrijeme postaje sve popularniji pojavom novijih informacionih tehnologija, pogotovo tehnologija koje su bazirane na "Webu", te kao takve obezbjeđuju jedan potpuno nov stepen napredovanja. On kao takav više nije baziran na usluge, već na povećanje odgovornosti za korisnike (Kujović i Dulović, 2011). CRM je ustvari alat koji će nam omogućiti da obezbijedimo sve informacije i spajamo naše odnose sa aktuelnim i potencijalnim partnerima, kupcima, te ostalim kontaktima potrebnim za naše poslovanje (Milanović, 2022). Svaki proizvod koji se proizvede mora biti napravljen po posebnim uvjetima klijetna, odnosno krajnjeg korisnika tih usluga. Zaslugu za to upravo ima inovacija baze podataka koja upravo obezbjeđuje pohranu podataka o korisnicima usluga, kao i aplikativni softveri koji pružaju mogućnost analize i najboljeg načina korištenja svih dobijenih podataka o sklonostima i željama kupaca (Karakostas, Kardaras i Papathanassiou, 2005). Bitno je spomenuti da CRM nije samo običan vid tehnologije. CRM se smatra poslovnim sistemom, odnosno poslovnom filozofijom koja svoj fokus usmjerava na krajnje potrošače (Vasiljev i Milovac, 2010).

Cilj primjene CRM sistema unutar kompanija je poboljšanje načina zapažanja i shvatanja od top menadžera, pa sve do najobičnijeg zaposlenika onog na najnižoj ljestvici hijerarhije u kompaniji (Kujović i Dulović, 2011). Njegovo uvođenje nije nimalo jednostavno. To je ustvari dugotrajan postupak za kojeg ne možemo nikada reći da je upotpunosti okončan. Zahtjev klijenta će se uvećati uporedo sa povećanjem tehnologije, a bitnost korisnika kao najvažnijeg dijela u lancu ne trebamo nikad zanemarivati (Mešić, Lazić i Unkić, n.d.).

2.4. Sigurnost informacionih sistema

Informacione tehnologije se svakodnevno razvijaju. Bilo da smo eksperti u polju IT-a ili obični korisnici, informaciona sigurnost postaje sve aktuelnija tema u poslovanju. Razlog tome su upravo sve češći napadi na sistem koji povećavaju rizik od krađe informacija. Zbog toga nam je upravo potrebna sigurnost informacionih sistema kako bi spriječili krađe i dalje poteškoće za poslovanje. Što smo više usmjereni na stvari koje radimo bez papira, to moramo biti više fokusirani na informacionu sigurnost (Redžibašić i Jašarević, 2021). Nažalost, mnoge kompanije zanemaruju sigurnost informacionog sistema, te se zbog toga vrlo često dese zloupotrebe i štete koje se mogu nanijeti kompanijama u velikoj mjeri. Svjedoci smo sve učestalijih udara na informacione sisteme kompanija kako bi iznudili finansijsku dobrobit, te narušili njihov rad (Mel, 2021). Nepristupačnost podataka predstavlja najveći problem koji su sa ljudskim resursima najbitnija karika lanca neke organizacije.

Informaciona sigurnost je skup postupaka kojima je glavni cilj zaštititi podatke od osoba koje nemaju ovlaštenje njihovom pristupu, od momenta pohrane do momenta prenošenja informacija iz jedne filijale u drugu (Fruhlinger, 2020). Sigurnost informacionog sistema nastoji da zaštiti informacije kompanija od bilo kakve prijetnje koja im može naštetiti poslovanju. Informacije moraju biti sačuvane i zaštićene bezobzira na način prijenosa i

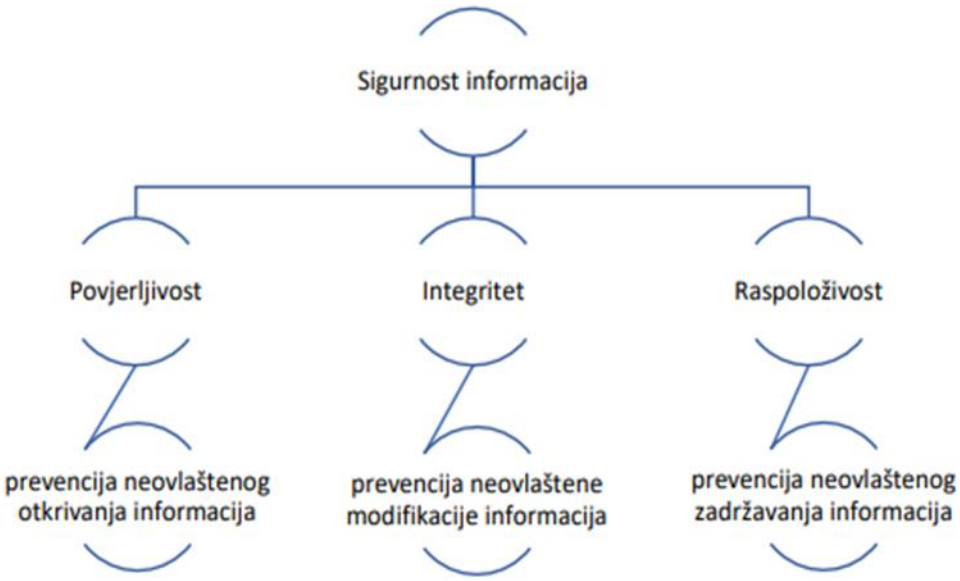
korištenja. Da bi se ta zaštita obezbijedila, svi korisnici informacionog sistema moraju da znaju zaštitne mjere koje im informaciona sigurnost nalaže (Đapić i Lukić, 2007). Kompanije primjenjuju informacionu sigurnost kako bi zaštitili svoje elektronske informacije od hakerskih napada (Yasar, Wright i Teravainen, 2023).

Informaciona sigurnost obuhvata (Marijanović, 2006):

- oporavak informacionog sistema od prijetnji,
- odvraćanje upada i
- upotrebu propisa koji su zakonom određeni, a svoj fokus imaju na zaštiti privatnosti, kompjuterskom kriminali, itd.

Sigurnost je proces koja nastoji da obezbijedi prihvatljiv stepen negativnog efekta (Ćurić, 2017). Sigurnost ne možemo posmatrati kao vid proizvoda ili usluga, to je skup koji ih obuhvata sa još dosta komponenti koje se konstantno odrađuju (Mijić, 2019). Međutim, bitno je spomenuti da ni u jednoj kompaniji nema potpune sigurnosti, jer koliko god kompanija sebe obezbijedila od vanjskog hakerskog uticaja, toliko sebe nije osigurala od unutrašnjeg faktora, odnosno zaposlenika. Informaciona sigurnost tačno naglašava koje informacije moraju biti zaštićene u kompaniji, razlog zbog čega se informacije moraju zaštititi, na koji način, te od kojeg uticaja trebaju biti zaštićene (Lagumdžija *et al.*, 2021). Kako bi došlo do zaštite, te kako bi se adekvatno koristila sigurnost informacionog sistema potrebno je da učestvuju svi zaposlenici unutar kompanije, pa često i pomoć stručnjaka izvan kompanije koji se razumije u informacionu sigurnost sistema (Ćurić, 2017).

Slika 8. Sigurnost informacija



Izvor: "Integrirani okvir za sigurnost i pouzdanost",

Za dobru sigurnost informacionog sistema nije potrebno mnogo. Ona se za mali iznos novca, kao i znanja zaposlenika, može urediti do potpunog savršenstva (Kovačević, 2008). Bezobzira na sve ovo, i dalje je sve veći problem zaštititi podatke unutar kompanije.

Godinama kompanije nastoje da poboljšaju sigurnost informacionog sistema uvodeći firewall, izradu sigurnosnih kopija podataka unutar kompanije, opreme i sl. Svi elementi koji nam služe za zaštitu informacionog sistema su itekako bitni, jer bez njih informacioni sistem ne bi bio adekvatno siguran (Kovačević, 2008). Ipak treba se obratiti pažnja i na znanje i edukaciju samih zaposlenika gdje se u tu sferu ulaže veoma malo, ponekad i ništa. Propuste primjećuju vanjski faktori koji nastoje da unište rad kompanija, te svoje napade usmjeravaju ka sakupljanju informacija uz pomoć kojih će obaviti zlonamjerne poteze.

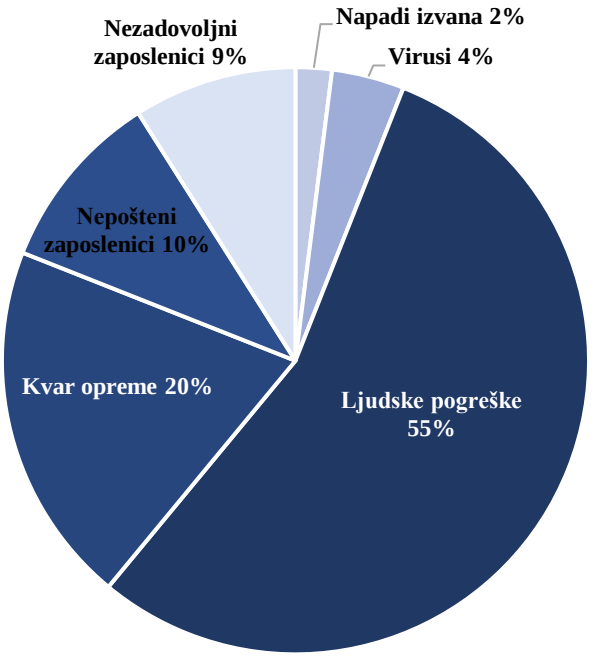
U današnje vrijeme broj osoba koje koriste kompjutere, informacione sisteme, kao i Internet su u znatnom porastu (Smrekar, 2020). Iz dana u dan broj korisnika se povećava. Baš iz razloga što broj korisnika rast, sve se više poslova obavlja putem kompjutera, te je neophodno da svaki čovjek zna osnove kako bi na što kvalitetniji način obavljao svoj posao. Zbog toga, se osobe koje ne znaju koristiti kompjuter smatraju neobrazovane, odnosno nepismene za današnji svijet (Akademija Oxford, 2019).

Svaka komponenta koja ima svrhu da zaštiti informacioni sistem itekako je neophodna za njegov rad jer bez njih informacioni sistem ne bi imao tu sigurnost koju ima s njima. Međutim, veliki problem nastaje u tome što je veoma mala stopa educiranih zaposlenika (Ponjević, 2010). U nekim kompanijama skoro da je i nema. Pored zaposlenika veliku ulogu imaju i sami informacioni sistemi. Njegovim razvojem istovremeno se stvaraju određene slabosti unutar kompanije. Sve kompanije svoje poslove obavljaju putem telekomunikacijskih mreža, tako da velika vjerovatnoća od hakerskih napada i prevara koje će neovlašteno "ukrasti" informacije su u porastu. Prema Lagumdžija *et al.* (2021) opasnost za informacioni sistem u nekim kompanijama odnose se na:

- uposlenike,
- određena pravila i vizije o nužnosti i načinu očuvanja informacija,
- povećanje povezanosti i prenosa obrađenih podataka,
- povećanje složenosti, uspješnosti i pristupačnosti hakerskih alata i virusa,
- Internet i e-mail
- prirodne katastrofe i nezgode.

Mnogi od nas smatraju da prijetnje koje se dese unutar kompanije su prijetnje koje nastaju iz vanjskog okruženja. Međutim, statistički podaci pokazuju suprotno (Slika 9.). Upravo se unutrašnji faktori, odnosno zaposlenici, smatraju najvećim procentom problema sigurnosti uzrokovane ljudskom pogreškom (Kovačević, 2008). Obično se one dešavaju usljed neadekvatne pažnje i loše educiranosti uposlenika. Drugi razlog najčešćih grešaka u kompanijama je zastarjela oprema koja se često kvari, korištenje položaja u kompaniji od strane uposlenika i zaposlenici koji su nezadovoljni svojim položajem u kompaniji ili prema rukovodiocu (Boban, 2014).

Slika 9. Sigurnost informacija



Izvor: Kovačević (2008) "Problemi sigurnosti u velikim kompanijama",

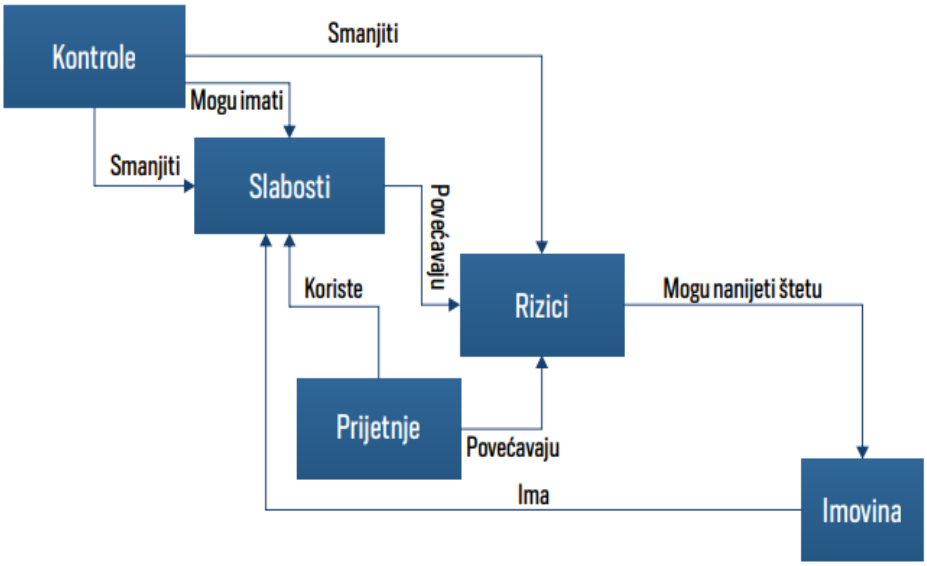
2.4.1. CIA principi

CIA princip je model koji je najpogodniji za obezbjeđenje sigurnosti informacionog sistema. Primjenjuje se za otkrivanje slabosti i metoda za pronalaženje adekvatnog rješenja (Fortinet, n.d.). CIA principi odnose se na:

- Povjerljivost (eng. Confidentiality) - kao prvi elemenat označava zaštitu privatnosti informacija, te omogućava njihovu sigurnost (Irwin, 2023). Informacija treba biti dostupna samo za one osobe koje imaju pravo za njihovo korištenje.
- Integritet (eng. Integrity) - ispravnost i kompletnost informacija su nezaobilazan dio mogućnosti kompanije da nesmetano radi (Hutsix, n.d.).
- Dostupnost (eng. Avaliability) - informacije trebaju biti dostupne osobama koje su ovlaštene za njihov pristup, te kojima su one od ključne važnosti (Hashemi-Pour i Chai, 2023).

Kad su sva tri principa ispunjena u istom vremenskom periodu, sigurnost kompanije je snažnija i kvalitetnije opremljena za upravljanje postojećim prijetnjama (Fortinet, n.d.). Podaci koji prelaze u informaciju, te svi procesi prelaska, sistemi i mreže koje koristimo za njihovu obradu, transport i pohranjivanje predstavljaju važan dio poslovnog procesa (Lemeš i Hamidović, 2023). CIA principi su od izuzetne važnosti za obezbjeđenje "kompetitivne pozicije, stabilnosti gotovinskog toka, profitabilnosti i poslovnog imidža" (Lagumdžija *et al.*, 2021).

Slika 10. Aspekt informacione sigurnosti



Izvor: Lagumdžija et al. (2021)

Za kompaniju neophodno je da svoj fokus usmjeri na prijetnje koje već postoje, a koje mogu iskoristiti ranjivost informacionog sistema neke kompanije. Da bi te prijetnje na optimalan način spriječili potrebno je da ih detektujemo, opišemo i pratimo u toku njihovog djelovanja. Prijetnja nam daje šansu da iskoristimo ranjivost sistema koja može na najprostiji način ugroziti rad kompanije nanosivši joj štete opasne po njih (Lagumdžija *et al., 2021).*

Prijetnje se nalaze svuda. One se mogu pojaviti sa različitih strana, bilo da se radi o ljudskoj ili prirodnoj, neočekivanoj ili namjernoj. Kompanije su te koje trebaju da otklone uzrok i način njegovog nastanka, kao i faktor koji je doprinio stvaranju prijetnje opasne za rad. Vjerovatnoća da će prijetnja koja je nastala unutar kompanije upotrijebiti slabost informacionog sistema predstavlja rizik. Rizik može biti prilika ili gubitak najčešće okarakterisan kao negativan ishod koji može da donese određenu štetu i neželjeni efekat na poslovni rad kompanije (Bedi, 2020). Ukoliko dođe do situacije da prijetnja iskoristi slabost, kompanija mora biti spremna na štete koje se mogu zadesiti unutar nje. Gubitak ili prijetnja koja zadesi kompaniju može uticati na sam rad CIA principa. CIA principi služe kompanijama u uspostavljanju sigurnosti, dok zaposlenici obezbjeđuju izvršavanje dnevnih zadataka (Staff, 2023).

Kako bi uspjeli u namjeri da smanjimo dozu rizika unutar kompanije moramo uvesti kontrolu informacionog sistema. Kontrola nam daje očekivanja da će se poslovni ciljevi koje smo zacrtali i ostvariti, te da će se neželjeni događaji izbjeći i otkloniti (Stanišić, 2014). Kontrolu možemo da razlikujemo prema onoj koje nastoje da spriječe pojavljivanje problema i one koje identifikuju nastali problem. Ako problemi nastanu i pored osnovne kontrole koristi se korektivna kontrola koja će smanjiti negativan učinak nastalih problema, te utvrditi neusaglašenost i način njegovog otklanjanja (Šumić i Petrović, 2008). Sigurnost

informacionog sistema je ozbiljan posao koji zahtjeva savremenu tehnologiju, te vrijeme koje će menadžer i zaposlenici kompanije ustupiti za očuvanje informacija. Pored toga, obično svaka kompanija nastoji da ima firmu namjenjenu za informacionu sigurnost koja će nam pomoći u zaštiti podataka koje se u kompanijama nalaze u velikim količinama (Anon, 2020).

2.4.2. Principi sigurnosti informacionih sistema (prema OECD)

OECD ili The Organization for Economic Cooperation and Development ima svojih 9 principa za sigurnost informacionog sistema, a to su:

- Svijes o infomacionoj sigurnosti - važno je da svaka kompanija koja se bavi poslovima putem kompjutera bude svjesna da je potreba za sigurnošću informacija velika. Sigurnost informacionog sistema i mjere koje se koriste za njihovu zaštitu su od izuzetne važnosti (Lemeš, n.d.);
- Odgovornost - svi članovi i zaposlenici moraju biti najodgovorniji dio sigurnosne zaštite informacionog sistema;
- Odziv - svi članovi i zaposlenici kompanije moraju blagovremeno učestvovati u prevenciji, pronalasku i otklanjanju sigurnosnih poteškoća (Oštrić, 2015);
- Etika - članovi kompanije moraju biti korektni jedni prema drugima;
- Demokratija - kako bi zaštitili informacioni sistem svaka sigurnost treba biti usklađena sa propisima demokratskog društva (Ćurić, 2017);
- Procjena rizika - izuzetno je važno provesti mnogobrojne analize rizika kako bi obezbijedili odgovarajuću zaštitu (Radinić, 2019);
- Dizajn i implementacija sigurnosnih mjera - kontrole koje se sprovode radi obezbijeđenja sigurnosti trebale bi biti neizostavan dio informacionog sistema kako bi obezbijedili sigurnost;
- Upravljanje sigurnošću - kompanije trebaju obezbijediti učinkovit i nedvosmislen pristup rukovođenju sigurnošću (Marijanović, 2006);
- Procjenjivanje - kompanije trebaju nastojati da svakodnevno nadgledaju sigurnost informacionog sistema, te obavljaju neophodnu izmjenu sigurnosnih mjera (Huđek, 2015).

2.4.3. Vrste i izvori sigurnosnih prijetnji

Informaciona sigurnost nam pomaže da zaštitimo informacije u bilo kojem obliku njihovog postojanja**.** To se odnosi na informacije koje kompanije mogu imati u digitalnom ili papirnom obliku. Vrlo često se papirni oblik nalazi u organima državnih institucija zato što se koriste zastarjeli i dotrajali informacioni sistemi. Informacije štitimo od raznih prijetnji. Ne štitimo ih samo od ilegalnih pristupa, nego i od propadanja, kao i neovlaštenih promjena koje se nisu trebale desiti u kompaniji (Jadrić i Ćukušić, 2015). U slučaju informacione sigurnosti imamo unutrašnje i vanjske neprijatelje. Većina napadača se pojavljuju kao vanjski neprijatelju gdje uz pomoć novije tehnologije, kao što je Internet, im obezbjeđuje da

to mogu uraditi iz bilo kojeg dijela svijeta. Međutim, nismo ni svjesni koliko ustvari tih napada dolazi od unutrašnjih neprijatelja. To predstavljaju najteže napade jer se dešavaju od strane zaposlenika koje izuzetno dobro poznaju situaciju unutar kompanije, te kao takvi prouzrokuju veću štetu od vanjskih neprijatelja. Pored toga, postoje i elementarne nepogode na koje kompanije ne mogu da utiču, a koje mogu izazvati potpuni nedostatak informacija (Lagumdžija *et al.*, 2021).

2.4.3.1. Phishing ili krađa identiteta

Phishing je jedan oblik društvenog inžinjeringa za manipulisanje ljudima. To je tip online obmane koja se dešava na internetu uz pomoć kojeg se varaju korisnici da podijele privatne informacije, kao što su korisničko ime, lozinka, sa osobom koja ne treba da zna njihove osjetljive informacije (Hečimović, 2023).

Phishing je nastao 1990-tih godina. Krađa identiteta putem e-maila se predstavlja kao jedna od najčešćih prijetnji putem koje napadač prikuplja informacije žrtve. E-mail će imati sadržaj u poruci koja je isuviše dobra kako bi na što jednostavniji način privukla žrtvu da vjeruje u nju (Anon, 2022). Lažna poruka koja će se poslati tačno određenom korisniku predstavlja prijetnju ne samo po tu osobu, nego i po kompaniju u kojoj ta osoba radi.

E-mail poruka bit će napisana tako da djeluje kao da je poslana od strane pouzdane osobe. Najčešće je hitna kako bi navukla primatelja da je što prije otvori. Uobičajno takav vid e-maila sadrži link putem kojeg će se primatelj prevariti. Taj link često izgleda kao da nas vodi na pravu web adresu, međutim to je krivotvorena web stranica putem kojeg se traži od primaoca da unese svoje korisničko ime i lozinku. Na taj način napadač dobiva sve potrebne podatke koje su mu potrebne za prikupljanje potrebnih informacija. To predstavlja početni stadij gubitka podataka kompanije ili čak i njihovog novca. Hakeri će se često predstavljati kao poznato ime gdje vrlo često poruku možemo da dobijemo od svjetski poznatih brendova (Glamoslija, n.d.). Danas se često ovaj vid napada dešava i na društvenim mrežama gdje korisnici nasjedaju na razne linkove koji im otmu profil.

Phishing se pojavljuje u različitim oblicima pokušavajući da obuhvati što više korisnika. Često su usmjereni na starije ljude, koji slabije znaju za ovaj vid napada, a u svojim „rukama“ imaju veliku finansijsku moć. Napadi putem e-maila i društvenih mreža su najjeftiniji i najučinkovitiji, te kao takvi predstavljaju najzastupljeniju opasnost po sigurnost informacionog sistema (Lagumdžija *et al.*, 2021).

2.4.3.2. Malware i ransomware

Zlonamjerni softver je naziv za sve softvere koji su napravljeni kao ilegalni pristup kompjuterima čiji je glavni i osnovni cilj da nanesu katastrofu korištenjem informacija koje nisu namjenjeni za njih. Ransomware se rasprostire putem phishing e-mail poruke koja sadrži link za krivotvorenu web stranicu ili putem preuzimanja neke dokumentacije kad korisnik posjeti zaraženu web stranicu (Anon, 2024). Tad će se malware preuzeti i instalirati

bez našeg znanja. Zlonamjerni softver označava veliku poteškoću sigurnosti i za korisnike i za kompanije. Nastao je 1980-tih godina sa sličnim karakteristikama ko i većina zlonamjernih softvera (Lagumdžija *et al.*, 2021).

Kompjuterski virusi su prema najnovijim istraživanjima jedni od najčešćih prijetnji za poslovanje gdje kompanije troše velike svote novca za sprječavanje nastale štete koju su prouzrokovali virusi i hakerski napadi. Kompanije koje su napadnute trpe velike novčane gubitke padom sistema. Time im nastaju dodatni troškovi, a samim tim i ugrožava im se poslovanje zbog loše educiranosti zaposlenika. Zarazom sistema, hakeri traže datoteke koje su im korisne za otkrivanje bitnih stvari unutar kompanije, te na taj način blokiraju pristup njihovim informacijama kako bi im prijetili da će biti objavljene (Patrizio, n.d.). Čišćenje kompjutera od zlonamjernog virusa kako bi uklonili nastale štete je dugotrajan proces ukoliko nedostaje odgovarajući alat za njihovo otklanjanje (Lagumdžija *et al.*, 2021). U današnje vrijeme postoji sve više kompanija koje se bave unapređenjem programa za saniranje nastale štete od virusa. To su antivirusni programi koji nas čuvaju i štite od svih zlonamjernih radnji koje se mogu desiti unutar kompanije.

2.4.3.3. Cryptojacking

Cryptojacking je jedan novi oblik zloupotrebe sigurnosti informacionog sistema. On predstavlja nezakonitu upotrebu tuđeg kompjutera za rudarenje bitcoin-a (Sheps, 2023). Pokretanjem web stranice sumnjivog sadržaja (Barney, 2022) možemo nenamjerno instalirati zlonamjerni softver koji će koristiti našu procesorsku energiju za rudarenjem bez našeg znanja ili pristanka na to (Sheps, 2023). Cryptojacking predstavlja najnoviji način narušavanja sigurnosti informacionog sistema. Rudarenje kriptovalutama utiče puno na kompjuterske resurse gdje zbog toga može doći do sporijeg rada računara. Samim tim će sporije obavljati zadatke, jer se u njemu odvija postupak rudarenja kriptovalutama. Ovaj vid rudarenja zauzima dosta memorije, te troši velike resurse energije što će dovesti do pregrijavanja kompjutera čime mu se skračuje vijek trajanja ili ga upotpunosti razoriti. Rudarenje kriptovalutama je skup procesa koji kao takav može imati negativne posljedice. Napadači iskorištavaju slabost sistema kako bi izvršio svoj zadatak. Za razliku od ransomwareom koji je napravljen da privlači pažnju, cryptojacking su nevidljivi i što duže ostanu takvi kvalitetnije će obaviti posao koji su naumili. Napadaju kako pojedinca, tako i kompanije koje se bave malim i velikim poslovima, državne institucije i sl (Rasure i Jackson, 2023).

2.4.3.4. Hakerski napadi

Hakiranje je usmjereno na zlupotrebu kompjutera, mobilnih telefona, te svih onih uređaja koji koriste mrežu kao vid komunikacije radi nanošenja štete i prikupljanja korisnih informacija od strane zaposlenika ili pojedinca (Fortinet, 2023). Haker je osoba koja protivzakonito provaljuje u komunikacionu mrežu s namjerom da nanese štetu pojedincu ili kompaniji. Štete koje hakeri nanesu na sistem je izuzetno ogromna. Pored upada u sistem,

hakeri najčešće postavljaju i viruse koji narušavaju sam rad računara, te usporavaju njegovo funkcionisanje (Lagumdžija *et al.*, 2021).

2.4.3.5. Elementarne nepogode

Elementarne nepogode i ostale prirodne katastrofe narušavaju poslovanje i funkcionisanje kompanije gdje njihove posljedice mogu ugroziti stabilnost cijelog društva (Rebrača, 2018). Kompjuteri, podaci, informacije, te sva tehnološka oprema može biti uništena u momentu elementarnih katastrofa. Katastrofe mogu prouzrokovati prekid rada unutar cijele kompanije. Za oporavak od elementarne nepogode su potrebne velike količine novca i vremena kako bi se sve uništene stvati rekonstruisale i vratile na početno stanje. Iz tog razloga svjetske kompanije izgrađuju i unapređuju pomoćne i rezervne sisteme koji će im omogućiti sigurnost njihovih informacija.

Fault tolerant ili tolerancija grešaka predstavlja kompjuterski sistem koji definiše moć sistema da upravlja greškama i zastojima bez umanjenja funkcionalnosti (Custer, 2023). Sadrži dodatne elemente koji obezbjeđuju nesmetan rad poslovanja kompanije. One obuhvataju adekvatne memorijske čipove i procesore za pohranu podataka koji im kao takvi omogućavaju otkrivanje štete, te momentalno preusmjeravanje na alternativne sisteme podrške (Lagumdžija *et al.*, 2021).

2.4.3.6. Greške

Kompjuteri su uređaji koji mogu dovesti do određenih grešaka prilikom obavljanja poslovnih zadataka. To može ozbiljno naštetiti radu firme, jer se poslovi obavljaju sporije od predviđenog roka. Greške se dešavaju u bilo kojem dijelu obrade informacija (Lagumdžija *et al.*, 2021) bilo da smo na samom početku ili kraju. Zbog toga, trebamo biti oprezni, te svaki nedostatak koji osjetimo prilikom obavljanja poslova što prije prijaviti nadležnoj osobi u IT-u.

2.4.4. Kako provesti informacionu sigurnost?

Kada koristimo informacioni sistem moramo biti spremni na poteškoće koje nas mogu zadesiti, te unaprijed promisliti kako izbjeći nastajanje šteta. Kako bi zaštitili sebe i svoje poslovanje moramo znati od čega se mi čuvamo, odnosno moramo znati sa kojim se to rizicima i posljedicama možemo susresti. Taj proces nazivamo procjenom rizika koji predstavlja osnovni dokument o zaštiti u poslovanju (Krmek, 2022). Unutar njega trebamo sagledati sve informacije koje nam se nude, resurse koje nam obezbjeđuju pohranjivanje, obradu i prijenos informacija, prijetnje bile to vanjske ili unutrašnje, te ranjivost. Pregledom potencijalnih prijetnji, slabosti i ranjivosti dobili smo listu rizika koji se mogu zadesiti u poslovanju (Lagumdžija *et al.*, 2021).

Mjere očuvanja koje se mogu koristiti su:

- svaki zaposlenik ima pravo pristupa informacijama samo onim koje su njemu potrebne za obavljanje posla,
- da se u svakom momentu informacija koja je zaprimljena u kompaniji zna ko je posjeduje bezobzira u kojem se formatu nalazila,
- da se tačno zna stepen povjerljivosti svake informacije,
- jasan postupak kojim će se upravljanje informacijama sa tačnim stepenom povjerljivosti definisati i limitirati,
- da svaki zaposlenik svojim potpisom izjavljuje da je upoznat sa propisima o informacionim sistemima, te da može materijalno i krivično odgovarati u trenutku nepoštivanja istih,
- zaposlenici koji su potpisali izjavu, a prekršili pravila o sigurnosti informacionog sistema, protiv njih će se provesti disciplinski postupak. Tako bi ostali zaposlenici unutar kompanije uvidjeli da su informacije koje oni primaju za obavljanje poslovanja ozbiljne. Samim tim bi se smanjila mogućnost nastanka rizika i prikazala svjesnost mogućih rizika za kompaniju.

2.4.5. Sistem upravljanja informacionom sigurnošću – ISMS (Information Security management system)

Svaki posao koji se obavlja uz pomoć tehnologije podložan je informacionoj nesigurnosti (Raza, 2019). Sistem upravljanja informacionom sigurnošću možemo definisati kao cjelokupni sistem upravljanja koji je usmjeren ka zaštiti bitnih informacija obezbjeđujući povjerljivost, pristupačnost i integritet (Kanade, 2024). Uspjeh ovog sistema je ključan faktor općine koji se ne usmjerava samo na sigurnost nego i na ostale elemente koji su ključni za poslovanje (Hamidović, 2010).

Informaciona sigurnost treba da bude jedan od bitnih komponenti poslovanja kompanija. Menadžeri su ti koji su usmjereni na ISMS iako je on započet po tehničkim aspektima. Nijedan pojedinac, niti ustanova, u današnje vrijeme ne može adekvatno poslovati bez sigurnosti informacionog sistema. Poslovanje je usmjereno na dotok informacija i to u najrazličitijim smjerovima. Tehnologija pomaže ljudima da zajedno dijele informacije, procesiraju ih, te ponovo dostavljaju krajnjem primaocu. Shodno tome, svaki proces od početka preuzimanja informacije do samog kraja mora biti kreiran da loše uticaje po njega svede na minimum. To znači da svi učesnici koji su dio procesa upotpunosti shvataju važnost primjene sistema upravljanja informacionom sigurnošću (Hamidović, 2010).

Ukoliko na adekvatan način primjenimo ISMS on će uspostaviti skup određenih pravila koji mogu unaprijediti poslovanje u kompanijama koje ga primjenjuju. Implementiranje ISMS-a usklađuje svoj rad sa sigurnosnim zahtjevima ISO 27001 (Yasar, 2022). ISMS možemo realizovati u općinama, te ostalim kompanijama koje koriste informacione sisteme za svoje poslovanje (Hamidović, 2010).

2.4.6. Kontrola i revizija informacionih sistema

Revizija informacionog sistema podrazumjeva postupak sakupljanja i analize dokaza uz pomoć kojih možemo presuditi da li je informacioni sistem uspješan ili ne (Bibović, 2013). Odnosno, da li je on uspješan u funkciji održavanja imovine kompanije i cjelovitosti podataka, te da li ostvaruje poslovne ciljeve u poslovanju koristeći same resurse na odgovarajući način. U današnjici, revizija informacionih sistema se tek počela razvijati, te kao takva predstavlja potporu reviziji finansijskih izvještaja koja predstavlja desnu ruku menadžerima u davanju određenih savjeta i rukovođenju informatikom. Revizija informacionog sistema označava sveobuhvatan proces uz pomoć kojeg se procjenjuje da li informatika funkcioniše u skladu sa poslovnim ciljevima koje smo postavili u poslovanju i u kolikoj mjeri ona djeluje i kontroliše informacioni sistem (Kardašić, 2020). Njihov glavni i osnovni cilj je pronalazak rizika, te definisanje njihovog otklanjanja, ciljeve, opseg i metodologiju, kao i ispitivanje rukovodećih kontrola i fizičke sigurnosti, oporavak od nesreća i planiranja budućeg poslovanja (Višnjić, 2021). Također njegov osnovni zadatak je prepoznati njegovo postojeće stanje, otkriti područja u kojima se nalazi rizik, tačnije visinu njegovog rizika, te savjetovati menadžment u pospješivanju njegovog rukovođenja (Spremić, 2017).

Revizija informacionog sistema predstavlja funkciju koja služi za upravljanje. Kao takva omogućava nezavisnu i realnu verifikaciju uspješnosti, odnosno analizu svih postavljenih funkcija, ciljeva informacionih sistema kako bi se na taj način sakupile potrebne informacije koje se razmatraju i kao takve služe kao dobra podloga za ostale tipove revizije. Finalni ishod tih postupaka, koji se temelje na standardima kao što su ISO 27001 norme, ITIL i CobiT, je davanje izvještaja revizora na sljedeće načine: procjena zrelosti korištenja informacionog sistema u poslovanju kompanija prema opaženim oblastima analize poslovnog rizika usmjerenog ka zatečenom stanju i savjeta menadžerima za unapređenje nastalog stanja (Spremić, 2017).

Da bi informacioni sistem bio eksterno efikasan i kvalitetan on mora biti i interno (Anon, 2008). Interna kvaliteta ostvaruje se uz pomoć interne provjere sistema, a obim kvalitete provjerit će se uz pomoć interne revizije. Kako bi ispravno došlo do ocjenjivanja kvalitete tog informacionog sistema koji je prošao kroz internu reviziju neophodno je da prođe i eksternu reviziju nakon koje će se rezultati smatrati vjerodnostojnim za prikaz konačne ocjene kvalitete informacionog sistema kojeg smo posmatrali. Posmatramo li Bosnu i Hercegovinu vidjet ćemo da je revizija informacione tehnologije tek u razvoju i postepenom korištenju. Trenutni period je period u kojem će se napredovati gdje će se revizija informacionih tehnologija morati više koristiti u korporativnom rukovođenju (Isaković, n.d.). Struka revizije informacionih tehnologija napredovala bi znatno brže i uspješnije angažovanjem kompanija, te uspostavljanjem novih zakona, odluka i slično (Spremić, 2017).

Mnoge kompanije u svom poslovanju upotrebljavaju informacione tehnologije za poboljšanje efikasnosti poslovanja, umanjivanje troškova, te omogućavanje tačnih i korisnih informacija. Jedino na taj način će informacione tehnologije pružati veliku dobrobit

poslovanju kompanije. Međutim, one pored koristi mogu donijeti i rizike usmjerene ka tradicionalnom izvršavanju poslovanja. Kompanije moraju biti u mogućnosti da predvide i prepoznaju moguće rizike, te im se kao takvim suprostaviti. Zbog toga se osim razvijanja i napretka informacionog sistema javlja i revizija i provjera informacionog sistema. Revizija informacionog sistema usmjerena je ka ispitivanju i njegovom vrednovanju gdje se uz pomoć upotrebe PC-softvera vrši testiranje i procjena podataka koji su proizvedeni putem kompjutera (Luić, 2009).

Poenta revizije informacionog sistema je uspostavljanje efikasnosti prikazanih informacija u odgovarajućem korporativnom sistemu, kao i postavljanje mjera sigurnosti i očuvanja ključne infrastrukture na svjetskoj osnovi. Menadžeri koji obavljaju posao unutar svojih kompanija moraju biti sigurni da se mogu osloniti na informacione sisteme koji se upotrebljavaju u njihovim kompanijama. U današnje vrijeme kompanije ne mogu da funkcionišu bez informacionih sistema, jer bez njih stvarale bi se određene poteškoće i greške koje bi uzrokovale potpunu katastrofu u poslovanju kompanije. Ne može se ni zamisliti kakve bi poteškoće i posljedice ostavilo po općine da koriste informacione sisteme koji unesene podatke pretvaraju u skroz neku drugu informaciju nepogodnu po njih. Pored problema sa zakonom, zasigurno bi imali većih problema od strane građana čiji se dokumenti, bitne informacije i zahtjevi nalaze upravo u općinama. Zbog toga nam služe menadžeri kako bi svoj posao usmjerili na kontrolisanje i analizu informacionog sistema isto kao i nadzoru i kontrolisanju kvalitete rada poslovnih procesa. Razvoj i unapređenje informacionih tehnologija je pored izmjene na rad menadžmenta uticao i na rad samih ravizionih ustanova. Ranijih godina revizori su svoj posao, procjene i testiranja usmjeravali na finansijskim propisima izvještavanja. Kako su poslovni informacioni sistemi uspostavili napredne tehnologije rukovođenja informacijama, beneficija pribavljanja informacijama što veću vjerovatnoću ovisit će od preciznosti i valjanosti hardvera, softvera, mreža, te ostalih bitnih komponenata za napredniju tehnologiju. Također, ona će zavisiti i od znanja zaposlenika i pojedinaca koji upotrebljavaju tehnologije, rukovođenje informacijama i kompanijske sposobnosti gdje bi se u cjelosti moglo upravljati i nadzirati izmjenama u sistemu i okolini (Luić, 2009).

Iako su se revizori za informacione sisteme fokusirali na kontrole organizacionih, finansijskih i ostalih ključnih cjelina bitnih za obavljanje posla, informacije kao i informacioni sistemi su i dalje predmet manipulacija i zataškavanja istine za menadžere koji nadziru kompanije u kojima obavljaju posao i rukovode informacionim sistemima. Zbog toga, dolazi do neophodnosti za uvođenje novih tehnika i načina pronalaženja korisnih informacija o informacionom sistemu u poslovanju kako bi predstavili vjerodostojan izvještaj i stvorili mišljenje kao jednog od ključnog proizvoda revizorskog posla (Lagumdžija *et al.*, 2021).

Kako bi shvatili osnovne karakteristike revizije informacionih sistema neophodno je i da shvatimo njegovo funkcionisanje i kontrole informacionih sistema baziranih na poslovanju. Svaka revizorska kompanija koja se bavi ovim poslovanjem unaprijedila je svoju vlastitu metodologiju revizije informacionih sistema. Kako bi došlo do unapređenja navedene

metodologije koriste se ISACA standardi (Kirvan, 2023). Revizija nam povezuje ekonomsku sa informacionom stavkom poslovnog informacionog sistema gdje nam kao takva pomaže u pružanju informacija menadžerima u promjeni i unapređenju poslovnih procesa. Posmatrajući sa druge strane, revizija svoju bitnu ulogu ima i za nove poslovne partnere pružajući nam priliku za uspostavljanje saradnje s njima. Uvođenjem određenih načela i postupaka koje bi se usmjerile na formiranje i primjeni informacionih sistem. Time bi se umanjile potencijalne greške, napadi i uništavanje sigurnosti (Luić, 2009). U prošlosti se kontrola upotrebljavala na samom kraju implementacija. Međutim danas sve kompanije zavise od rada informacionih sistema. Te se zbog toga svi rizici i poteškoće moraju što prije predvidjeti i pronaći kako bi kompanije nesmetano mogle da nastave sa svojim radom. Kontrola mora biti bitan dio njegovog dizajna (Luić, 2009).

2.5. Norme/standardi sigurnosti infromacionih sistema

Veoma često informacionu sigurnost poistovječuju sa klasifikovanim podacima i dokumentacijom (Bogati, 2011). Takvo spajanje u današnjici nije tačno jer informaciona sigurnost rukovodi informacionim područjima, te skoro uvijek stavlja u kontekst povjerljivost, cjelovitost i raspoloživost kao ključnu bezbijednost svojstva informacione sigurnosti (Marijanović, 2006). Tajnost se smatra samo jednom od podkategorija povjerljivosti. Povjerljivost kako i sama riječ kaže je nešto što samo određeni ljudi u povjerenju mogu da znaju. Zbog toga, ovaj vid svojstva treba da obuhvata određenu dozu tajnosti i privatnosti između fizičkih ili pravnih osoba, što bi se odnosilo na službene podatke ili neklasificirane podatke. Cjelovitost se ipak odnosi na podatke, te njegova dostupnost klijentima odnosi se na sve podatke čak i na one koje su se javno objavile. Takvi podaci moraju imati vlasnika ili osobu koja vodi računa o podacima u ime vlasnika čiji su podaci. Veoma bitan cilj revizije informacionog sistema je i procjena da li udovoljava sistem smanjenim zahtjevima učinkovitosti. Odnosno, potrebno je izvršiti procjenu usklađenosti kontrole sa svjetski prihvaćenim normama shodno kojima se ovaj vid provjere provodi.

Norme i okviri kao što su CobiT, ITIL i ISO/IEC 17799:2005 i ISO/IEC 27001 norma predstavljaju najbolje svjetske prakse prilikom rukovođenja i revizije informacionog sistema. O ovim normama nešto ću više pisati u nastavku magistarskog rada.

2.5.1. CobiT

CobiT je jedan od svjetski podržanih okvira u kojem se utvrđuju kontrole za rukovođenjem informatikom i određenim informatičkim postupcima. On predstavlja okvir za rukovođenjem IT-a za kompanije koje imaju u planu implementirati, pratiti i unaprijediti najbolju proceduru upravljanja IT-om (Terrell, 2021). CobiT je jako brzo došao do unapređenja, te je bio usmjeren na praćenje razvoja informatike u poslovanju. CobiT v2 koji je nastao 2000-te godine jedan je od najbitnijih koncepta kontrole informacionog sistema (Ćosić i Boban, 2010). Verzija 3 od 2004-te godine usmjerila se na integralni okvir rukovođenja informatikom, dok 4.1 obuhvata jednu od najbitnijeg koncepta provođenja

korporativnog rukovođenja informatikom (Ćosić i Boban, 2010). „CobiT sadrži 4 područja, 34 ključna informatička procesa (cilja kontrole), preko 300 detaljnih informatičkih kontrola, 18 aplikacijskih i 6 procesnih kontrola“ (CIS, 2012). „Svaki od 34 IT procesa CobiT-a “nudi”(Spremić, 2005.):

- modele zrelosti,
- kritične čimbenike uspjeha,
- ključne indikatore ostvarenja cilja,
- smjernice menadžmentu za praćenje performansi i ključne indikatore performansi,
- smjernice menadžmentu za upravljanje rizicima i
- ciljeve kontrole i kontrolne testove.“

Cilj kontrole funkcionalnosti informacionih sistema rasprostranjeni su u četiri kategorije (Spremić, 2005.):

- „Planiranje i organizacija informatike,
- Akvizija (nabava) i implementacija,
- Isporuka i potpora radu, te
- Nadzor i procjena uspješnosti„.

Slika 11. 34 Ključna IT procesa (ili cilja kontrole) prema CobiT metodologiji (napomena: crvenom bojom su istaknuti procesi najvišeg prioriteta)

PLANIRANJE I ORGANIZACIJA (PO)
PO1 Strateško planiranje IS
PO2 Definiranje informacijske arhitekture
PO3 Određivanje tehnoloških smjernica
PO4 Definiranje IT procesa, organizacije i odnosa
PO5 Upravljanje IT investicijama i troškovima
PO6 Komuniciranje prema menadžmentu
PO7 Upravljanje ljudskim resursima
PO8 Upravljanje kvalitetom
PO9 Upravljanje i procjena rizika
PO10 Upravljanje projektima

AKVIZICIJA I IMPLEMENTACIJA (AI)
AI1 Određivanje mogućih rješenja
AI2 Nabava i održavanje aplikacijskih programa
AI3 Nabava i održavanje tehnološke arhitekture
AI4 Korištenje i funkcionalnost rada (obrade)
AI5 Nabava IT resursa
AI6 Upravljanje promjenama
AI7 Instalacija i odobravanje rješenja i promjena

ISPORUKA I POTPORA (DS)
DS1 Definiranje i upravljanje razinama usluga
DS2 Upravljanje vanjskim uslugama
DS3 Upravljanje performansama i kapacitetom
DS4 Osiguranje kontinuiteta usluga
DS5 Sigurnost sustava
DS6 Određivanje i dodjela troškova
DS7 Izobrazba i trening korisnika
DS8 Podrška korisnicima
DS9 Upravljanje konfiguracijom
DS10 Upravljanje problemima i incidentima
DS11 Upravljanje podatcima
DS12 Upravljanje pomoćnom opremom
DS13 Upravljanje operacijama (obradom)

NADZOR I PROCJENA (ME)
ME1 Nadzor i procjena IT performansi
ME2 Nadzor i procjena internih kontrola
ME3 Sukladnost s zakonskim i drugim normama
ME4 Korporativno upravljanjem IT-om

Izvor: Spremić, 2005.

CobiT je izumljen od strane ISACA kako bi se riješili tehnički problemi, otklonili rizici, te održala kontrola (Terrell, 2021). On može biti realizovan u bilo kojoj kompaniji kako bi se obezbijedila kvaliteta i kontrola kompanije koja posluje s velikim informacijama.

2.5.2. ITIL

ITIL predstavlja okvir koji je napravljen za standardizaciju biranja, osmišljavanja, distribucije, održavanja i životnog ciklusa IT usluga u kompanijama (Bigelow i Montgomery, 2022). Iako je nastao krajem 1980-tih godina, prije više od 40 godina, ITIL se tek nedavno počeo koristiti i predstavljati koristan, jednostavan i po svjetskim standardima neizbježan skup sugestija i najbolje prakse prilikom rukovođenja informacionim uslugama. Izumitelji ITIL metodologije je britanska Central Computer and Telecommunications Agency gdje više ne posluju s tim imenom nego imaju novo, a to je Office of Government Commerce (Spremić, 2020). Oni su krajem 1980- tih godina izumili prvu listu uputa koja im prikazuje na koji način se mogu koristiti informatičke usluge kojeg su se svi morali pridržavati. Od tog perioda ITIL se konstantno počeo unapređivati i nadopunjavati gdje danas predstavlja jednu od svjetski prihvaljivih standarda upravljanja informacionim uslugama. Unapređeni su toliko da čak i dobavljači daju svoje usluge u skladu sa ITIL-om (Spremić, 2005). ITSMF je organizacija koja je neprofitna, te kao takva vodi računa o poboljšanju informatičkih usluga, kao i napretka ITIL standarda za upravljanje informatičkih usluga. Pored toga, ITIL će nam omogućiti instrukcije koje su fokusirane na rad zaposlenika, funkcionisanje procesa poslovanja, te upotrebe tehnologije prilikom davanja kvalitetne usluge (Kardašić, 2020). ITIL je skup uputstava koji se zasnivaju na sjajnoj praksi rukovođenja informatičkih usluga bilo da se radi o državnim ili privatnim kompanijama u bilo kojem dijelu svijeta (Grgić, 2019). ITIL predstavlja skup knjiga koje nam pružaju uputstva za obezbjeđivanje vrhunskih informatičkih usluga, opreme i aktivnosti garantujući nam pouzdanu informatičku potporu (Spremić, 2005).

Osmišljen kao skup knjiga, ITIL podrazumijeva najbolji vid pružanja, podrške, distribucije i rukovođenja informatičkim uslugama (Strilic, 2021). Pored toga, ITIL nam omogućava tačne instrukcije na koji način ocijeniti kvalitetu usluge, kako pratiti distribuciju usluge, te rukovoditi cijelim procesom informatičkih usluga (Spremić, 2007). ITIL nam stvara mogućnost da za svaku uslugu možemo ustanoviti kompatibilnost s ITIL preporukama. To se predstavlja uz pomoć ocjene od 0 do 5 kao i kod CobiT-a čime se omogućava provjera zrelosti uslova njegove upotrebe što u konačnici obezbjeđuje procjenu kvalitete informatičke usluge, potpore i rukovođenja. ITIL se najviše koristi u Evropi, najviše u javnom sektoru za čije je prohtjeve i napravljen. Evaluacija ITILA:

- I verzija - Nastao 1986. godine - 40 knjiga
- II verzija - 1999. godine - 8 knjiga
- III verzija - 2007. godine - 5 knjiga

2.5.3. ISO 27000

ISO 27000, koji sadrži svoju porodicu standarda, jedan je od najbitnijih standarda vezanih za sigurnost informacionog sistema. Spomenuta serija normi označava najefikasniji odgovor na buduće napade na kompanije i njihovu sigurnost informacionog sistema, te šta sve menadžer treba da učini da bi svoj posao obavio na kvalitetan način (Kaić, 2019). ISO

17799:2005 i ISO 27001:2005 jedni su od normi koji zahtjevaju najminimalnije kriterije koje kompanije trebaju provesti kako bi došlo do primjene sistema rukovođenja sigurnošću informacija. Govori se o normi koja je najviše usmjerena na sigurnost informacija sa kojima kompanije raspolažu, dok je njegova upotreba najčešća u polju revizije informacionog sistema (Spremić, 2007). To su jedne od rijetkih normi koje u okviru svojih 10 područja imaju preko 100 propisanih provjera uz pomoću koje bi se informacije i informacioni sistemi koji se koriste u kompanijama smatrale sigurne. Međutim, njihov jedini problem je što nema tačnih uputa kako da se koriste u praksi. One s tim mogu utvrditi minimalne provjere zahtjeva, odnosno minimalno provjera koje je potrebno primjeniti u sklopu informacionog sistema kako bi došlo do umanjenja rizika (Spremić, 2007).

ISO 17799 i ISO 27001 podrazumijevaju smjernice, odnosno naglašava koje sve provjere je poželjno implementirati kako bi se rizik umanjio na adekvatnu razinu. Ove norme su atraktivne i najčešće upotrebljene gdje njihovo implementiranje pruža mogućnost dostignuća najznačajnijih ciljeva procesa provjere informacionog sistema (Grgić, 2019). S obzirom na dosta negativnih posljedica prijašnjih normi koje su se koristile i povećale bitnosti rukovođenja informatikom, ISO je saopštio i djelimično proveo preuređenje ovih normi, te uspostavljanje ISO 27000 porodice (Spremić, 2007). Neke od navedenih normi kao što je ISO 27001:2005, su poznate i trenutno aktuelne za korištenje, dok s druge strane ISO 27002, ISO 27003, ISO 27004 i ISO 27005 su jedne od novijih normi koje pored sigurnosti su usmjerene i na rukovođenje rizicima i primjene kontrole nad informacijskim sistemom gdje na taj način osigurava sigurnost sistema u korist postizanja sigurnosnih i drugih rizika (Spremić, 2017).

ISO i IEC zajedno predstavljaju sisteme za regionalnu standardizaciju (Tanović, 2012). ISO norme su usmjerene na ISO 27000 koje se odnose na kontrolu normi u okviru ISO 27000 porodice, ISO 27001 koji je nastao 2006-te godine predstavlja rukovođenje informatičke bezbijednosti, ISO 27002 iz 2007-me je pravilnik postupaka usmjerenih ka rukovođenju informacionog sistema bezbijednosti, ISO 27003 se odnosi na priručnik za uspostavljanje sigurnosti informacionog sistema, te još ISO 27004, ISO 27005, ISO 27006 i ISO 27011 kao dio porodice ISO 27000 standarda (Bogati, 2011).

ISO 27001 je jedan od najpoznatijih standarda koji je dio međunarodnih standarda predstavljen od „Međunarodne Orzanizacije za Standardizaciju“ koji se realizuje rukovođenjem informatičke sigurnosti u kompanijama koje ga primjenjuju (Kosutic, n.d.). Prvi oblik ovog standarda objavljen je 2005-te godine koji je nastao na osnovu poznatog britanskog standarda. ISO 27001 možemo primjeniti u bilo kojoj kompaniji koja ima želju za njegovom implementacijom. Osmišljen je od strane najpoznatijih svjetskih eksperata poznatih u poljima informacione sigurnosti koji propisuju metodologiju za uspostavu rukovođenja informacione sigurnosti u kompanijama. Pored toga, pruža mogućnost kompanijama da dobiju neophodan certifikat čime im se izdaje potvrda da je kompanija realizirala informacijsku sigurnost saglasno sa ISO 27001 normom. Jedan je od najpopularnijih standarda za primjenu u informacionoj sigurnosi u svijetu, te mnoge

kompanije su usmjerene da budu certificirane u skladu s njegovim propisima (Krusha i Mahmutović, 2021).

ISO 27001 usmjeren je na očuvanje tajnosti, cjelovitosti i dostupnosti podataka u kompanijama. To se ostvaruje identifikovanjem mogućih poteškoća koje se mogu desiti podacima, te odrediti šta je potrebno učiniti da se ti problemi zaustave. Dakle, zaključak je da se ISO 27001 usmjerava na rukovođenjem rizika, njegovom otkrivanju i obradi (Bušac, 2016). Zaštitne mjere koje bi se realizovale su najčešće u obliku politike, regulative i tehničke upotrebe (Kos, 2017). Međutim, kompanije koje već imaju svu potrebnu opremu koriste je na veoma nesiguran način. Zbog toga je primjena ISO 27001 standarda usmjerena na određivanje pravila koji su potrebni za sprječavanje štete po informacionu sigurnost (Kujundžić, 2022). Svaka od tih primjena zahtjeva rukovođenje politikom, procedurama, radnicima, te kao takve ISO dočarava na koji način sve navedene elemente uklapa u sistem rukovođenja informacionom sigurnošću.

Rukovođenje informacijskom sigurnošću nije usmjerena samo na sigurnost informacione tehnologije, nego i na rukovođenje procesima, zaposlenicima, fizičku zaštitu i slično (Pokorni, 2019). Ustvari, informacijska sigurnost se odnosi na rukovođenje rizicima u kompanijama, te kompjuterskom sigurnošću, rukovođenje kontinuiteta poslovanja i IT-em (Kos, 2017).

Osigurati kontinuitet u poslovanju je jedan od najbitnijih ciljeva svake moderne kompanije koja želi imati razvijen informacioni sistem. Kako bi ostvarili kontinuitet poslovanja neophodno je da resursi informacionog sistema budu pristupačni, a da sigurnost podataka i informacija koje kompanije posjeduju ne budu ugrožene (Badžim, 2016). Da bi se to ostvarilo bitno je primjeniti sistem rukovođenja sigurnošću informacionog sistema (Bogati, 2011). Taj sistem će nam omogućiti kontinuirano obavljanje posla u kompaniji pomažući nam da se mi kao zaposlenici u svakom momentu možemo suprotstaviti mogućim prijetnjama, te na adekvatan način reagovati na moguće incidente (Gregurić, 2021). Kao takvi postat ćemo puzdan partner u obavljaju posla za bilo kojeg korisnika. Od 1993-će godine u Velikoj Britaniji dolazi do unapređenja novih normi kojim će se osigurati bolja informaciona sigurnost (Bogati, 2011). Unapređenjem informacionih tehnologija dolazi i do uvećanja ukupnog broja normi, kao i mjesta u kojem se oni primjenjuju (Spremić, 2005).

Implementaciju standarda, kao i njegove korake i faze ću prikazati na primjeru uvođenja ISO 27000 u Općini kao jedinici lokalne samouprave u kojoj obavljam poslovne zadatke u cilju rješavanja zahtjeva građana.

2.5.4. Poređenje CobiT/ITIL/ISO standarda

Sva tri navedena okvira i standarda nam nude različite prednosti i nedostatke. Ako se odlučimo za jedan od njih on će nam donijeti određene snage i slabosti, ali nas isto tako dovodi do propusta koji ćemo osjetiti ne koristivši druge standarde i okvire koji imaju svoje bolje strane. Samim tim doći će do nedostatka boljih karakteristika drugih standarda

(Pokorni, 2019). Na primjer, korištenje ITIL-a unutar kompanija omogućava nam detaljne upute o implementaciji procesa, ali njegov glavni nedostatak je slabost u rukovođenju i utvrđivanju ciljeva (Toth, 2022). Dok CobiT, s druge strane, ima svoju jačinu u rukovođenju i utvrđivanju ciljeva, ali ne omogućava nam mnogo detalja o provedbi procesa. Prednost ISO standarda je davanje sažete informacije šta bi IT kompanije trebale raditi, međutim njegov nedostatak se odnosi na premalo smjernica o tome kako on zapravo funkcioniše. Još jedna od razlika između ISO 27001 i CobiT-a je ta što ISO 27001 je više okrenut ka kibernetičkim tehnologijama, gdje je CobiT više usmjeren na omogućavanje usaglašavanja inicijativa IT-a s poslovnim ciljevima kompanije.

U praksi, ukoliko želimo da primjenimo jedne od okvira i standarda neophodno je da sagledamo sve prednosti i nedostatke koje nam one nude. Na taj način će se u budućnosti trošiti mnogo manje vremena, a samo preduzeće će doživjeti svoj pomak u zavisnosti u kojem smjeru žele da napreduju.

3. ISTRAŽIVANJE PROVEDENO U LOKALNOJ SAMOUPRAVI

Organi lokalne samouprave su ustanove koje najčešće komuniciraju sa građanima. To znači da institucije lokalne samouprave moraju ispuniti zahtjeve građana, te svakim danom odgovarati na upite o pružanju usluga stanovništvu, odnosno sprovoditi poslove u cilju zadovoljavanja potreba građana (Mujakić, 2016). Za sve građane je to od izuzetne važnosti gdje sa što kraćom interakcijom uspijevaju doći do potrebnih informacija koje su korisne za njih. Za državu je ipak bitno da taj isti organ precizno izvrši svoju odgovornost, te u relativno kratkom roku riješi sve podnesene zahtjeve od strane građana i drugih državnih organa. Implementacija informacionog sistema u organima lokalne samouprave jedan je od najvažnijih ciljeva uspostavljanja organizovanog i efikasnog sistema usmjerenog ka korisnicima kao najvažnijeg korak ka poboljšanju poslovanja državnih organa (Kaljević, *et al.*, 2005). Međutim, lokalna samouprava susreće se sa mnogim problemima uvođenjem novijeg informacionog sistema. Jedan od njih je relativno nizak procenat informatičke pismenosti kod zaposlenika. Samim tim, to dovodi do nezainteresovanosti zaposlenika za uvođenjem novijeg procesa rada. U organima lokalne samouprave, tačnije općinama, rade zaposlenici starije životne skupine koji poznaju osnove rada na računaru, te bilo kakva promjena koja bi se uvodila za njih bi predstavljala dodatni problem savladavanja iste (Kaljević, *et al.*, n.d.) Procedura po kojoj postupaju dugi niz godina više se ne bi koristila uvođenjem novog informacionog sistema. Često se zbog toga desi i strah kod zaposlenika da će uvođenjem novog sistema postati višak. Gledajući to iz njihove perspektive, istina je da će se smanjiti potreba za ljudskim radom. Uvođenjem noviteta, svi predmeti bi se direktno pohranjivali u informacioni sistem. Time bi se umanjio rad zaposlenika, ali obim posla bi ostao isti. Službenici bi mogli svoje vrijeme usmjeriti na unapređenje usluge koje oni pružanju građanima. Međutim, slaba tehnička opremljenost u općinama dovodi do problema koji postoji već duži niz godina. Loši računari i ostala prateća oprema koja ide uz njih dovodi do toga da nema dobre mreže koja bi mogla izdržati veliki protok podataka. S tim zaposlenici ne bi bili u mogućnosti pružiti kvalitetnu uslugu građanima uvođenjem informacionog

sistema. Sve vuče jedno drugo. Informacioni sistem se ne može implementirate sa lošom tehničkom opremljenošću. A za tehničku opremljenost potrebno je imati edukovano osoblje. Nažalost, ne postoje osobe koje bi opremu stručno održavale jer dosta edukovanog stanovništva napušta granice Bosne i Hercegovine ili svoje znanje usmjeravaju kod privatnika zbog boljeg plaćanja. Sve su to problemi koji se nižu i međusobno povezuju. Uvođenje informacionog sistema u organe lokalne samouprave bi bio dug proces u njihovoj implementaciji. Svi se problemi trebaju svesti na minimum kako bi se bez poteškoća uveo novi sistem koji bi služio ne samo zaposlenicima nego i građanima.

Ustavna pozicija organa lokalne samouprave u Federaciji Bosne i Hercegovine mora biti u skladu sa Ustavom Federacije Bosne i Hercegovine, Kantolanim ustavom i Kantonalnim zakonodavstvom (Paragraf Lex BA - Ustav Federacije Bosne i Hercegovine). Nadležnosti i pitanja koja su bitna za djelovanje organa lokalne samouprave definisana su Zakonom o načelima lokalne samouprave u Federaciji BiH. Sprovođenje nadležnosti koji svaki organ lokalne samouprave ima uređeno je određenim zakonima za svako područje, odnosno općinu, Statutom, Poslovnikom i Pravilnikom. Svaka služba koja obavlja svoj posao u općini služi se određenim Pravilnicima neophodnim za obavljanje poslova koji su im povjereni. Svobuhvatni okvir za unapređenje lokalne samouprave u Bosni i Hercegovini odnosi se na „Evropsku povelju o lokalnoj samoupravi“.

Lokalna samouprava u Bosni i Hercegovini postala je aktuelna 1994-tih godina kada je usvojena Evropska povelja o lokalnoj samoupravi (Mujakić, 2016). Općine kao organi lokalne samouprave danas su veoma popularne ne samo u Bosni i Hercegovini, nego i širom Evrope. One najviše doprinose zadovoljavanju potreba građana. To je prva stanica kojoj će se građani obratiti sa zahtjevom ili potrebom koja im je neophodna. Značaj lokalne samouprave u Bosni i Hercegovini bit će još veći ulaskom BiH u Evropsku uniju, gdje organi lokalne samouprave imaju bitnu ulogu u regulisanju ključnih zahtjeva građana.

Tema za moj magistarski rad koja se odnosi na uspostavu standarda sigurnosti informacijskih sistema u organima lokalne samouprave imat će za cilj pobliži prikaz Općine, u kojoj sam obavila intervju, kao organa lokalne samouprave, te informacione sisteme koje ona primjenjuje. Samim tim ću opisati način implementacije sigurnosnih normi u mojoj lokalnoj samoupravi, odnosno općini, u kojoj sam radila kao volonter/pripravnik, a sad i kao zaposlenik. Pisat ću o pojedinim sistemima koje Službe koriste za obavljanje svojih poslova, te detaljno prikazati intervju sa 10 uposlenika koji su mi pružili informacije potrebne za analizu.

3.1. Jedinica lokalne samouprave

Sarajevski kanton sadrži ukupno devet Općina od kojih sam se ja odlučila za jednu od njih. Ona ujedno predstavlja i jednu od četiri gradske Općine u kojoj se nalaze Općina Novi Grad, Općina Stari Grad, Općina Novo Sarajevo i Općina Centar. Obuhvata centralni dio grada Sarajeva najpovoljnijeg dijela za život građana. Jedna je od najnaseljenijih općina koja predstavlja najbolje mjesto za življenje stanovnika, bilo da se radi o mlađoj populaciji ili

starijoj životnoj dobi. Na usluzi je svojim građanima nastojivši svakodnevno da implementira nove inicijative. Skoro se implementirao i E-registar koji pruža sve potrebne informacije građanima na jednom mjestu.

Općina na raspolaganju svojim građanima pruža 16 Službi, te Ured za internu reviziju i Pravobranilaštvo. Mjesne zajednice kao dio Službe za poslove Općinskog vijeća i lokalnu samoupravu su u najvećoj interakciji sa građanima putem kojih građani podnose svoje zahtjeve i žalbe. Sve Službe rade po Statutu, Poslovniku i Pravilnicima koji su ključan segment njihovog poslovanja. Svaki zahtjev ima svoj tok koji prolazi od njegovog prijema pa sve do njegovog zatvaranja. To je dugotrajan proces koji nekad zna da traje duži vremenski period. Kako bi smanjili čekanje predmeta da dođe do Službe koja je za njega zadužena potrebno je uvesti adekvatan informacioni sistem. Informacioni sistem bi ubrzao samu prodecuru rada, te proces zahtjeva građana. Sistem kojeg je Općina koristila za upravljanje poslovnog sadržaja je DMS o kojem ću nešto više pisati u nastavku, a danas koriste OCEAN.

3.2. Primjer informacionog sistema u javnoj upravi

3.2.1. Document Management System - DMS (upravljanje dokumentacijom)

DMS sistem je poslovanje bez papira, odnosno upravljanje dokumentacijom koja služi za praćenje životnog vijeka svakog dokumenta koji uđe u općinu. Svaki dokument skeniranjem se unosi unutar sistema, tako da se dalja procedura obavlja isključivo elektronskim putem. Uz pomoć njega zaposlenici štede svoje vrijeme traženjem informacija o određenom predmetu (Edops, n.d.). DMS sistem odgovara svim kompanijama bezobzira na njihovu veličinu. Bitna je količina papirologije kojom kompanije upravljaju i raspolažu. Document Management System se koristi i kao arhiva gdje trajno vršimo pohranu dokumentacije na siguran način.

Kada zahtjev bude podnešen na protokol Općine, zaposlenik ga prima, te dostavlja u dalji proces rada. Tačnije, svaki pristigli zahtjev se signira na odgovarajuću Službu zaduženu za taj predmet. Svi dokumenti koji su podneseni uz zahtjev se skeniraju i prilažu u DMS kao jedan predmet pod određenim brojem. U tom momentu zahtjev sa svim podnesenim dokumentima postaje vidljiv i dostupan zaposlenicima kojima je taj predmet signiran. Time se tačno vidi koja je osoba zadužena za koji predmet. Nakon toga predmet ide u dalju proceduru zavisnosti od Službe koja je nadređena za njega. Pisanjem i pravljenjem određene dokumentacije, kao što su: Zaključaka, Ugovora, Odbijenica, i sl., se skenira i postavlja u DMS sistem. Zatvaranjem predmeta ručno, samim tim ga zatvaramo i u DMS sistemu kako bi finiširali obavljanje posla.

Fizički proces kretanja dokumenta u kompaniji sa sobom donosi brojne probleme. Rizik od gubitka dokumenta je velik. Kako bi izbjegli nastajanje problema DMS nam služi za uvid u zaprimljenu i urađenu dokumentaciju u elektronskoj formi. Samim time, omogućava se ubrzan proces pristupa dokumentaciji, te dodatno printanje i skladištenje predmeta. Štedi

nam naše vrijeme u pronalasku potrebne dokumentacije samo uz par klikova. Uz pomoć DMS-a tačno se zna čiji je predmet, u kojoj je proceduri, te kad je došao u svoju završnu fazu.

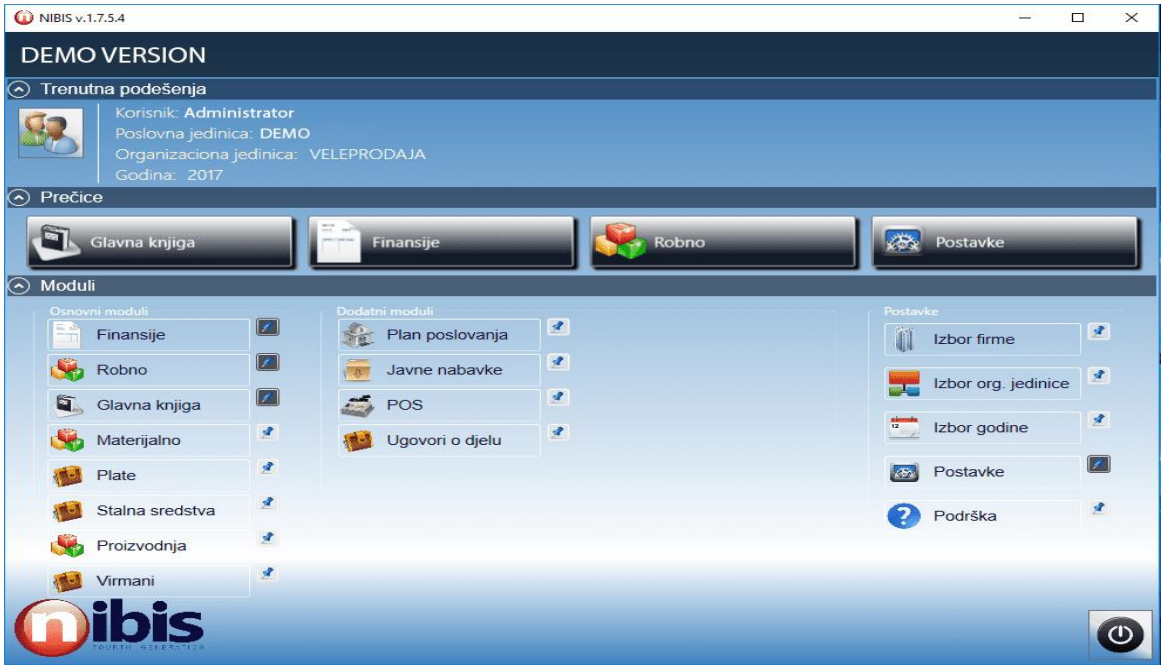
DMS je aplikacija koja pojednostavljuje poslove i pouzdano obrađuje pristiglu dokumentaciju. Sva dokumentacija koja je pristigla u kompaniju treba se na efikasan način prikupiti i pohraniti u DMS. Na taj način se izbjegavaju svi potencijalni problemi velike količine sadržaja u kojem bi njegova organizacija oduzela previše vremena. Primjenom razvrstavamo zahtjeve po Službama gdje bi DMS ove zahtjeve pojednostavio i ubrzao (Đivić, 2008).

Nažalost primjena DMS sistema u Općini je stala prije 2 godine. Koristi se drugi, zastarjeli sistem kojeg je DMS stavio po strani dok se upotrebljavao. Riječ je o Ocean informacionom sistemu kojeg upotrebljavaju samo određene Službe unutar općine.

3.2.2. NextVIsion Business Information System - NIBIS

Poslovni informacioni sistem NIBIS koriste srednje i velike kompanije koje imaju veći obim poslovanja. Napravljen je od polja tako da će svako polje biti upotrebljeno kao samostalni odjeljak gdje će biti međusobno uvezana. S tim bi svaki zaposlenik unutar kompanije bio upućen u poslove koje njihove kolege obavljaju. NIBIS na što jednostavniji i efikasniji način omogućava kontrolu poslovanja (Nibis, n.d.). Osnovni cilj sistema je da nam olakša i ubrza poslovanje, pojednostavi rad zaposlenicima kompanija koje koriste NIBIS kao informacioni sistem za poslovanje, te pojednostavi pristup svim poslovima unutar njega.

Slika 12. NextVIsion Business Information System



Izvor: Unimatrix (n.d.) "NIBIS – NextVIsion Business Information System",

NIBIS je sistem kojeg skoro sve Službe unutar Općine koriste za obavljanje poslova. Raspoređen u određena polja napravljen je da na što lakši i jednostavniji način zaposlenici rade u njemu. Najviše ga koristi Služba za privredu, budžet i finansije gdje sve svoje finansijske poslove obavljaju putem njega. Svaki zaposlenik ima pristup svom polju kako ne bi napravio problem u dijelovima u kojima on nije nadležan. Kroz njega prolaze svi napravljeni Ugovori, plaćanja, javne nabavke, te ostali većinom finansijski izvještaji. Finansijski poslovi usmjereni su na praćenje toka plata radnika, plaćanja, faktura gdje kroz godine možemo biti upućeni u finansijske tokove. NIBIS je omogućio jednu potpuno novu dimenziju, gdje na brži način svi poslovi mogu biti obavljeni u trenu.

3.3. Uspostavljanje standarda sigurnosti sa informacionim sistemom lokalne samouprave

Informacije su jedne od ključnih faktora i najbitnija imovina za svaku kompaniju, te ih je zbog toga neminovno sačuvati od bilo kakvog problema koji nas može zadesiti (Kitsios, Chatzidimitriou i tou, 2023). Kako bi se olakšalo obavljanje posla bržim pronalaskom dokumentacije većina svjetskih kompanija svoje informacije čuva u elektronskom obliku. Ipak, ovo sa sobom nosi određene rizike po kompaniju. Kako bi se spriječile određene prijetnje, kompanije moraju svoje informacije zaštititi uz pomoć strategije kojom bi sačuvali postojeće klijente, te stvorili kontakt sa novim. Upravo tu bitnu ulogu ima ISO 27001 uz pomoć kojeg se identifikuje i pronalazi strategija suočavanja sa svakom opasnošću koja nas može zadesiti (Kitsios, Chatzidimitriou i Kamariotou, 2023).

Kako bi ISO 27001 uveli u Općinu prvo je potrebno pažljivo uvidjeti da li je navedeni primjerak norme adekvatan za primjenu, te njegovo certicifiranje u općini. Nakon prvog i osnovnog koraka za nastavak uvođenja ISO standarda neophodno je pregledati dostupnu literaturu zbog prevelike količine informativnih naslova koji nam mogu biti od koristi prilikom uspostavljanja ISO 27001 norme. Poslije se formira tim koji će se baviti implementacijom ovog standarda (Christino, 2023). U timu trebaju biti edukovani ljudi o informacionim sistemima. Menadžer koji će upravljati cijelim procesom rada, te ostatak tima koji će pridonijeti realizaciji započetog projekta. Za ovaj pomak potrebno je da svi unutar općine budu saglasni za uvođenje ISO 27001 norme, pogotovo menadžer, tj. načelnik općine. Ipak, postoji mogućnost plaćanja konzultantske firme koja se bavi implementacijom ISO 27001. Ali bezobzira na to i dalje nam treba određen broj ljudi iz općine koji će pridonijeti realizaciji projekta, unajmili mi firmu da nam sprovede projekat ili ne. Okupljanjem tima potrebno je izanalizirati nedostatke sa kojim smo se susretali u toku poslovanja. Svaki nedostatak koji ne otkrijemo na vrijeme može ugroziti implementaciju. Zbog toga, neophodno je primjeniti kontrolu za sprječavanje rizika prije njegove identifikacije i primjene ISO 27001. Identifikacijom rizika moramo pokazati spremnost za rizike koje možemo tolerisati i one na koje moramo obratiti pažnju. Sve rizike moramo adekvatno definisati i prikazati jasne smjernice o ažuriranju sigurnosne politike.

Nakon toga se pravi adekvatna strategija koju ćemo primjenjivati tokom cijelog procesa realizacije projekta. Strategijom se definišu ciljevi i smjernice, organizira informaciona

sigurnost, te trajanje realizacije projekta i potrebni troškovi za njega (Kantor, 2021). U ciljeve i smjernice tačno se određuju koje informacije unutar općine je bitno zaštiti. Zbog velikog broja dokumenata koje općina zaprima i ima u svom informacionom sistemu neophodno je zaštititi sve informacije kojima općina raspolaže (Christino, 2023). To nije lagan proces. Zbog toga nam sigurno treba i do tri mjeseca kako bi se strategija napravila na adekvatan način, te započeli dalji koraci implementacije (Kantor, 2021). Razvijanje ključne politike, implementiranje kontrole ublažavanja rizika, periodična evidencija sve su to bitne stavke ažuriranja ISO 27001 standarda smatra Kantor (2021) za koje je potrebno i do 6 mjeseci realizacije.

Jako je bitno provesti obuku među svim zaposlenicima o upravljanju i korištenju informacijske sigurnosti. Time će svi razumijeti bitnost sigurnosti i njezinog segmenta u održavanju ispravnosti. Pored toga, da bi općina dobila Certifikat moramo vršiti zapise događaja prateći svakodnevnu rutinu. Uz pomoć toga će se dokazati da se poslovi obavljaju u skladu sa implementiranim standardom. Vršenje interne revizije, praćenje i mjerenje su koraci uz pomoć kojih potvrđujemo da li su naši ciljevi s početka dobro realizovani (Christino, 2023). Otprilike njegovo vrijeme realizacije je jedan do dva mjeseca. S praćenjem ćemo otkloniti novonastale probleme, te neusklađenost otkrivene tokom interne revizije. I za kraj, potrebno je odabrati certifikacijsku kuću koja će nam pomoći u dobijanju Cerfitikata. Općina će biti dužna da kontinuirano prati i unapređuje svoju informacionu sigurnost, a u tom poslu će im pomoći upravo adekvatna certifikacijska kuća. Razvojem poslovanja dolazi do pojave novih i opasnijih rizika za koje možda naš informacioni sistem neće biti prikladan za otklanjanje problema.

Postoje tri faze implementacije. Prva faza odnosi se na provjeru postojanja i neophodne dokumentacije nužne za primjenu sistema rukovođenja informacionom sigurnošću. Na taj način se osiguravaju organizacijske izjave o primjeni kontrole, kao i načinu tretiranja rizika. Druga faza usmjerena je na testiranje ISMS-a nasprem zahtjeva ISO 27001. Revizori zahtjevaju neophodne informacije koje dokazuju da menadžment sistem nezavisno djeluje. Dizajniran je na adekvatan način, primjenjen i kao takav funkcionalan. Revizije se obično obavljaju uz pomoć certificiranih vodećih revizorskih kuća. Dobijanjem certifikata za ISO 27001 norme dobija se uspješan prolaz druge faze implementacije. Sam proces procjene i upravljanja rizikom informacione sigurnosti je kontinuiran, a ne jednokratan proces, baš kao što se teoretski smatra da sistem upravljanja informacionom sigurnošću nikada nije u potpunosti uveden nego se radi o konstantnom procesu evaluacije, te traženja mogućih neusklađenosti i njihovog ispravljanja. Treća faza obično se odnosi na konstantne provjere čime se potvrđuje da kompanije rade u skladu sa postavljenim normama. Kako bi se certifikat zadržao potrebne su povremene kontrole revizije kojim se prikazuje da ISMS radi u skladu sa postavljenim pravilima. Rezivije se obavaljaju jednom godišnje, međutim njihova kontrola je moguća i prije ako se standard sigurnosti tek uspostavio. U ovoj fazi provjerava se da li općina koja je dobila certifikat svoj posao obavlja u skladu sa ISO normom. Ona se obavlja povremeno, te se na taj način provjerava da li ISMS funkcioniše kako je i napisano u dokumentaciji prije njegove implementacije.

Uspostavljanje ISO 27001 nije lagan proces, već je dugotrajan, te ga kao takvog trebamo ozbiljno shvatiti za njegovu implementaciju.

3.4. Obrazloženje procedure obavljanja intervjua

Za istraživački dio rada na temu „Uspostavljanje standarda sigurnosti informacijskih sistema u organima lokalne samouprave: studija slučaja općina“ odlučila sam se da to bude Općina u kojoj sam zaposlenik. Radi lakšeg prikupljanja informacija, razgovora sa kolegama, te informacija koje već znam kao zaposlenik i pripravnik, gdje sam u Općini radila godinu dana, mogu sa sigurnošću reći da ću na kvalitetan način pristupiti ovom dijelu rada.

Istraživački dio rada ću obaviti intervjuišući kolege iz različitih Službi u Općini kako bih prikupila što potpunije informacije. Kolege posjeduju dugogodišnje iskustvo u obavljanju svog posla, te će odgovori na pitanja koja im postavim zasigurno biti odgovorena na adekvatan način. Prva tačka od koje sam započela svoj proces istraživanja je sačinjavanje liste pitanja koja ću postavljati kolegama u cilju dobijanja što više korisnih informacija od njih (Prilog 1). Kompletirala sam listu od ukupno 11 pitanja. Neka pitanja imaju i potpitanja radi lakšeg shvatanja glavnog pitanja i detaljnijeg i šireg odgovora. Napisana su tako da svaki zaposlenik koji ne obavlja posao u IT sektoru općine može odgovoriti na njih. Nakon sastavljenih pitanja bila mi je potrebna Saglasnost Načelnika. Da ne bi došlo do određenih problema i pobune među zaposlenicima sastavila sam Saglasnost zamolivši Načelnika da mi izađe u susret kako bih sa uposlenicima Općine obavila intervju potreban za pisanje magistarskog rada (Prilog 2). Saglasnost, zajedno sa pitanjima, sam predala na protokol 12.02.2024. godine. Odgovor da li je Načelnik saglasan bio je dostavljen u moju Službu dva dana nakon podnošenja zahtjeva 14.02.2024 godine. Donesen je u vidu predmeta da je Načelnik saglasan za obavljanje intervjua. Sa predmetom sam bez problema mogla da uđem u bilo koju kancelariju, te zatražim informacije potrebne za istraživački dio rada.

Radi ponavljanja odgovora na postavljena pitanja intervju sam obavila sa 10 uposlenika. Uposlenici su bili iz Službe za zajedniče poslove, odjel IT i Javne nabavke, Službe za Privredu, budžet i finansije, te Službe za opću upravu. Pretežno muška populacija zaposlenika odgovarala je na pitanje pa je omjer bio 9:1. Prilikom obavljanja intervjua svim kolegama sam pokazala da je Načelnik saglasan da se ispitivanje obavi u cilju pisanja master rada, te uz to priložila papir o Saglasnosti za učešće gdje svojim potpisom zaposlenik daje saglasnost da njihove odgovore sam u mogućnosti iskoristiti u svrhu istraživačkog dijela rada (Prilog 3). U Saglasnosti o učešću detaljno je opisana tema, cilj prikupljanja informacija, te njihova mogućnost da u svakom momentu mogu odustati od spomenutog istraživanja.

Početak svakog intervjua započinjao je pozdravom i uvodnim dijelom moderatora, koji je svaki put naglasio o kojoj se temi radi, objasnio razlog intervuisanja, te istaknuo da ime i prezime zaposlenika neće koristiti u svrhu istraživanja. Moderator započinje sa prvim pitanjem, a to je godište zaposlenika radi upoređivanja odgovora između starije i mlađe populacije zaposlenika, kao i dalje analize dobivenih informacija. Nakon uvodnog pitanja

moderator je postavljao jedno po jedno pitanje, sa potpitanjima. Učesnici su davali precizne i koncizne odgovore koje ću prikazati u nastavku rada. Cijeli razgovor od pozdrava moderatora do kraja je snimljen radi dokaza o obavljenom intervjuu.

U nastavku istraživanja, a ujedno kao zaključnu riječ i odgovore na postavljena istraživačka pitanja, obavljeni intervju sa kolegama sam prikazala u potpoglavlju 3.5. Analiza podataka intervjuisanih zaposlenika. Sva dokumentacija od predaje na protokol, saglasnosti učesnika, kao i ostalih povjerljivih dokumenata bit će priloženi na CD-u.

3.5. Analiza podataka intervjuisanih zaposlenika

Nakon istraživanja 10 zaposlenika Općine u kojoj sam obavila intervju konstatujem da su odgovori na pitanja dosta slično odgovorena i uzajamno povezana. Iz tog razloga sam ostala na obavljanju intervjua sa 10 uposlenika koji su mi dali konkretne odgovore na postavljena pitanja. Uz pomoć njih sam uspjela doći do zaključaka i odgovora na istraživačka pitanja.

Tabela 1. Tabelarni prikaz istraženih zaposlenika

ISPITANIK	GODIŠTE	ZANIMANJE
I1	1974	Stručni savjetnik za informacione sisteme
I2	1970	Stručni saradnik za informacione sisteme
I3	1995	Stručni saradnik za opću upravu i personalne poslove
I4	1987	Šef Odsjeka za budžet
I5	1999	Viši referent administrator računarske mreže
I6	1990	Stručni saradnik za izvršenje budžeta
I7	1990	Viši stručni saradnik za javne nabavke
I8	1960	Viši referent za održavanje računarske opreme
I9	1983	Viši referent-sekretar mjesne zajednice - Vraca
I10	1998	Viši referent za administrativno- tehničke poslove

Izvor: Autorski rad

Isto tako, kroz analizu godišta (Tabela 1.) uviđam da se počelo zapošljavati dosta mlađe populacije u Općinu, koji žele da postignu napredak u sferi informacionih sistema. Mlađih zaposlenika će kroz par godina sve više biti, tako da smatram da novine koje se planiraju implementirati bi mogle biti od velikog značaja. Iako je ovo samo mali broj intervuisanih zaposlenika i dalje je tu većinom starija populacija koje svoj posao obavljaju mehanički. Uvođenje ISO 27000 intervjuisanim zaposlenicima se izuzetno svidjelo, te se nadaju da će kroz par godina doći do njegove implementacije.

Važnost postojanja sigurnog informacion sistema za rad u lokalnoj samoupravi svim zaposlenicima je od izuzetne važnosti. On je ključ uspjeha svakog poslovanja, te uz pomoć njega svoje poslove obavljaju na brz i siguran način.

„Siguran IS je veoma važan uvijek, što podrazumijeva sve nivoe vlasti tako i lokalnu samoupravu jer podatke pohranjene i obrađene u IS-u, kao i rezultate te obrade koriste, ne samo građani sa područja općine već i šireg teritorija, uključujući i uposlenike." (I1)

"Sigurnost informacionog sistema je od izuzetne važnosti ne samo za Općinu nego i za ostale kompanije koje posluju na tržištu…Uz pomoć njih ćemo i na brži i na lakši način obavljati sve postavljene zadatke…" (I2)

"Ja vjerujem da je važno imati siguran informacioni sistem za rad u lokalnoj samoupravi. Prvenstveno zbog zaštite podataka, a isto tako istakao bih i zbog brzine razmjene informacija na pouzdan način." (I7)

"Važno je imati siguran informacioni sistem mislim za rad u lokalnoj upravi, zbog povjerenja podataka, zbog njihovog skladištenja, zbog naknadne obrade tih podataka i svega što se u njima nalazi" (I10)

Brzina razmjene informacija među zaposlenicima je od krucijalne važnosti ne samo za zaposlenike nego i građane. Bitnost informacija i dokumentacije građana im je na prvom mjestu. Poslovi se obavljaju u cilju zadovoljavanja građanskih potreba i prioriteta. Zato informacioni sistem ima svoju važnost. Pored toga, on je neophodan i za obavljanje poslova zaposlenika jer im pruža dozu sigurnosti. Svaki obrađen zahtjev mora biti adekvatno zaštićen. Jedino na taj način se uposlenici lokalne samouprave mogu osjećati bezbijedno da predmet koji oni obavljaju neće doći u ruke trećeg lica koji sve te informacije može iskoristiti protiv njega.

"…organ uprave radi sa strankama, građanima koji pogotovo, konkretno posao kojim se ja bavim, radi se o ličnim podacima ljudi koji su zaštićeni Zakonom o ličnim podacima i veoma je bitno da se to sačuva. To su strogo povjerljivi podaci na osnovu Zakona i koji ne smiju da dolaze u dodir sa trećim licem." (I3)

"…zbog toga što siguran informacioni sistem obezbjeđuje zaštitu informacija, podataka, bolje funkcionisanje poslovnih procesa, sigurnost svih učesnika u tom samom procesu" (I6)

"…jedinice lokalne samuprave često rukuju osjetljivim podacima građana, uključujući lične podatke, finansijske informacije i neke druge povjerljive podatke, a siguran informacioni sistem pomaže u zaštiti tih podataka od neovlaštenog pristupa. To je vrlo važno zbog povjerenja javnosti, jer kada građani znaju da se njihovi podaci sigurno čuvaju, to može povećati njihovo povjerenje u lokalnu samoupravu." (I9)

Skoro svaka Služba ima neki svoj informacioni sistem, tj. aplikaciju koju koristi za obavljanje poslovnih zadataka. Par ispitanika spomenulo je kako za svoj rad koristi NIBIS informacioni sistem koji je usmjeren ka finansijskom praćenju podataka. Sastavljen je od određenih modula koji prije svega pomaže Službi za privredu, budžet i finansije u obavljanju finansijskih poslova. Svaki modul je međusobno povezan, te kao takav daje širu sliku o finansijskim tokovima svim zaposlenicima koji ga koriste.

“Za svoj rad koristimo finansijski softver od kompanije Next Vision, NIBIS. To je jedan finansijski softver koji objedinjuje više modula. Objedinjuje cijelo finansijsko poslovanje od plata, od planiranja budžeta, finansija, plaćanja faktura, ulaza tih samih faktura, planiranje Javnih nabavki, odnosno cijelo finansijsko poslovanje naše ustanove je na tom softveru.” (I6)

Pored njega tu su i OCEAN informacioni sistem za praćenje toka predmeta. Od njegovog ulaza u Općinu do zatvaranja i arhiviranja predmeta.

“Mi koristimo IVIS i koristimo OCEAN.” (I3)

Kadrovska evidencija sa personalima zaposlenika o svim dokumentima koji su bili neophodni za njihovo zaposlenje. Matična evidencija, aplikacija za nekretnine, poslovnih prostora i još dosta njih uz pomoć kojih zaposlenici detaljno obavljaju sve što im je zadato.

“Mi u Općini imamo jako dosta aplikacija informacionog sistema kao što je naprimjer NIBIS koji služi za praćenje finansijskih podataka, novčanih tokova. Informacioni sistem za praćenje toka predmeta, kadrovska evidencija, čitav personal gdje su svi podaci zaposlenih sa PIO/MIO podacima eventualno socijalnim podacima broju djece i slično. Matična evidencija koja je pod posebnim zakonima, u matičnim knjigama gdje možeš otići u bilo koju općinu i uzeti Izvod iz matične knjige rođenih, državljanstvo. Aplikaciju za nekretnine, registar imovine, poslovnih prostora. Sve su to aplikacije informacionih sistema koje mi kao zaposlenici koristimo za lakše obavljanje posla.” (I2)

Od izuzetne važnosti i uticaj na rad imaju informacioni sistem koji utiče efikasno na obavljanje posla lokalne samouprave. Efikasno pomaže zaposlenicima da rad sa strankama obavljaju lakše, te pruža uvid u njihove lične podatke.

“To znači integrisani sistem za prikupljanje, obradu i prezentaciju podataka. To je top svega. Znači prikupiti i obraditi te podatke sa stručne strane i prezentirati te podatke onome ko donosi odluke za provođenje djela iz same aplikacije je top, vrh. Ne može biti bolje. Znači veoma je bitno za efikasnost rada lokalne samouprave.” (I8)

“…efikasan je, i u informacionom sistemu utiče na produktivnost u poslovniku, utiče na raspoloživa sredstva, resurse, skraćuje vrijeme zahtjeva za obradu itd.” (I5)

“Informacioni sistem može značajno uticati na poboljšanje, odnosno efikasnost rada, lokalne samouprave, na više načina...” (I9)

Ubrzava proces pružajući mogućnost da svaki podatak koji je unešen ne mora ponovo da se unosi. Time se skraćuje vrijeme rada ubrzavajući sam proces. Smanjuje se mogućnost grešaka koje mogu stvoriti zaposlenici. Svi poslovi koje obavljamo uz pomoć informacionog sistema se nalaze na jednom mjestu. Tako informacioni sistem prati naš rad, te nas upozorava o grešakama koje su nastale u obavljaju posla.

“Ali definitivno ono što bih rekao da se može skratiti vrijeme rada, proces rada može biti brži, bolji. Može se doći do informacija na lakši način, može se proces rada smanjiti ali eto o čemu težimo tako da to je sigurno korisno.“ (I7)

“Svi obavljeni poslovi se nalaze na jednom mjestu. Informacioni sistemi prate naš prethodni rad.” (I2)

“Osnovno je zato što to može ubrzati procese i generalno po meni svrha bilo kojeg informacionog sistema u ovom slučaju, posebno je finansijskog, da jednom uneseni podatak se ne mora ponovo unositi, gubiti na vremenu već da se jednom uneseni podatak uz dobre kontrole verifikuje i onda u bilo kojem daljem procesu koristi. Tako da informacioni sistem svakako utiče na efikasnost rada prije svega kroz brzinu, a naravno i kroz pouzdanost.” (I4)

Koliko je informacioni sistem bitan pokazuje i to da se planira uvođenje novog informacionog sistema za obavljanje posla u Općini, a to je Eveve. Uz pomoć ovog sistema građani bi na jednostavan način mogli preuzeti JMBG (jedinstveni matični broj građanina). Samim tim bi se skratila procedura čekanja u redovima i dobivanje dokumenta koja se trenutno izuzetno komplikovana.

“Također radi se sada i na novom uvođenju informacionog sistema Eveve kako bi građani na veoma lakši i brži način dobili JMB (jedinstvene matične brojeve) jer skratila bi se procedura u samom dobijanju JMB (jedinstvene matične brojeve) koja je sada veoma komplikovana.” (I3)

Prijetnji po informacioni sistem i na posao unutar općine nema. Zaposlenici se nisu susretali ni sa kakvim vidom prijetnji po njihov rad. Tačnije, kolege iz IT-a nagovještavaju da prijetnji ima, ali da nijedna nije do kraja ostvarena i realizovana. Prijetnje su prikazane na ruteru, napadi su učestali s tim da nijedna nije narušila njihov rad.

“Napadi, vanjski, na IS Općine su učestali i svakodnevni, ali zahvaljujući postojećim sigurnosnim mjerama neuspješni i Odsjek za informacioni sistem se trudi da zadrži taj status.” (I1)

“Ima zabilježenih napada, ali nijedan napad nije do kraja izvršen. Vidi se na ruteru da je pokušaj s vana sa određene adrese, konstantno se registruje pokušaj ali nema ulaska.” (I2)

Time možemo da uvidimo da zaposlenici iz drugih Službi apsolutno nisu upoznati sa tim informacijama o napadima što je izuzetno dobro. Njihov rad je zaštićen gdje su samim tim sigurniji i opušteniji u obavljanju svog posla.

“Pa, u radu u Općini nismo imali često prijetnje koje su meni poznate.” (I4)

“Pa evo koliko ja znam u zadnje vrijeme nije nešto bilo tih nekih napada, ugrožavanja sigurnosti tih podataka. I koliko ja znam, ne znam da je bio neki uspješan napad.” (I6)

“Ono generalno vam ne bih mogao previše reći. Ono što znam da kolege iz Odsjeka IT-a rade na informacionom sistemu tako da i vode računa da se redovno sprečavaju sve prijetnje koje prilaze s unutra ili s polja.” (I7)

“Znači prijetnji ja zaista ne znam koliko imamo pretnji i da li je bilo uopšte pretnji.“ (I8)

“Lično nisam upoznat sa napadima na baze podataka koje postoje u Općini, te da li su bili uspješni ili ne.” (I9)

“Nemamo česte napade…” (I10)

Zamislite samo da znaju da su ti napadi svakodnevni. Zasigurno nijedan od zaposlenika ne bi bio siguran da svoje informacije ostavlja u računaru. Izuzetno se vodi računa da je svaka informacija zaštićena jer to su, prije svega, dokumenti građana, pa tek onda zaposlenika.

Najčešće prijetnje i izazovi u području sigurnosti informacija, odnosno da li veću prijetnju stvaraju vanjski (hakeri) ili unutrašnji faktor (stručni kadar) su podijeljena. Neki zaposlenici smatraju da veću prijetnju stvaraju vanjski hakeri, dok neki ipak smatraju da su to unutrašnji, tj. zaposlenici općine. Vanjski haker treba tačno da zna šta želi i šta traži od dokumentacije, dok unutrašnji su upoznati sa svim procedurama koje su postavljene unutar općine.

“…tu dolazi više po meni i mom mišljenju to je do vanjskih hakera, odnosno do vanjskog uticaja.” (I3)

“Pa, prije svega mislim da je to u pitanju vanjski faktor odnosno pristupi, neovlašteni pristupi izvan sistema.” (I4)

“Pa ja vjerujem da veću prijetnju stvaraju vanjski faktori.” (I6)

“Veću prijetnju predstavljaju vanjski napadi od strane hakera, jer uposlenici su dužni da poštuju propisane procedure.” (I9)

Unutrašnji faktori i jesu nekad veća prijetnja od vanjskih. Svojim nemarnim radom i greškama mogu da naruše cijeli rad informacionog sistema. Nekad smatram da to urade ne namjerno. Padom koncentracije i u velikoj brzini dosta se desi grešaka koje mogu da naruše radu informacionog sistema. Pogotovo jer svaki zaposlenik polaže Zakletvu o čuvanju povjerljivih informacija. Međutim, ima sigurno izuzetaka koji će sa određenom namjerom naškoditi radu ne samo informacionog sistema, nego i ostalih zaposlenika.

„Mislim da zaposlenik nekad ni ne shvata da je načinio grešku prilikom obavljanja posla. Tako da nekad štetniji mogu biti unutrašnji faktori. Jer ljudi smo. Svako od nas griješi i svako od nas može stvoriti određeni problem za Općinu. Zavisnosti samo u kojoj mjeri. A da je neko to namjerno uradio stvarno nisam upućen u to. Svi na početku svog rada u državnoj instituciji dajemo Zakletvu, tako da svi moramo i da radimo u skladu s njom.“ (I2)

„Pa možda zbog nekog da kažem nestručnosti ili iz nekih drugih da kažem razloga, svakakvi mogu da budu razlozi možda su i unutrašnji faktori nekad veća po meni prijetnje.“ (I7)

„Najveći problem za sigurnost su naši unutrašnji. Ljudi koji rade na obradi unosa i na obradi podataka. Ili mehanički to jest fizički faktori koji mogu uticati na nešto da se desi u transportu podataka.“ (I8)

„Veće prijetnje mogu unutrašnji faktori, zato što prilikom svog rada mogu da odaju neke stvari koje mogu danas sutra koristiti tim nekim hakerima koji žele da naprave neku zbrku.“ (I10)

Tehničke mjere koje preventivno koristi općina za zaštitu informacija usmjerene su na to da svaki računar koji zaposlenik dobije za obavljanje svog posla u IT sektoru prolazi kroz određen vid zaštite i programe. Tačnije, svaki dio informacionog sistema je provučen kroz određen vid zaštite. Zaposlenici da bi pristupili svojim dokumentima u računaru imaju korisničko ime i lozinku. Pored toga, svaki e-mail ima zaštitnu lozinku i korisničko ime. Kartice koje se koriste za otkucavanje ulaska i izlaska sa radnog mjesta imaju u sebi lozinku i ime zaposlenika. Njome se može pristupiti printeru, te ulasku u prostorije općine u kojima je ulaz nezaposlenika zabranjen. Zbog toga je od izuzetne važnosti da se čuvaju od gubitka kako ne bi došlo do zloupotrebe istih.

“Svaki novi računar prolazi kroz jedan vid zaštite. Svaka komponenta informacionog sistema je uvućena kroz antivirusni sistem. Ruter, virtualne mašine imaju svoje korisničko ime i lozinku. Stranice sumnjivog sadržaja se ne mogu otvoriti jer zahtjevaju dodatne provjere. Pored toga imamo i zaštitu protiv požara. Matični ured ima svoju zaštitu koja je određena zakonski. Videonadzor, protivprovalna, protivpožarna vrata sve je to dio zaštite.” (I2)

“…logički pristup znači username, password, autentifikacija za svaku aplikaciju i nemogućnost pristupa. Znači čim mi ne dozvolimo, ne damo nekome da može pristupiti našim podacima zaštićeni na više načina serverski. Znači da bi neko došao da radi mora znati username i password i logovati i način na koji sve to može uraditi. Tako da je onaj naš sistem jako dobro zaštićen, samim tim logičkim stvarima fizičkom zaštitom i username i password za pristup i računaru i sistemu.” (I8)

Na svim računarima instaliran je antivirusni sistem, kao i Bitdefender kojeg kontroliše Odsjek za IT. Backup podataka koji je izuzetno bitan prilikom pada sistema na računaru, kao i firewall kako bi cijeli informacioni sistem bio što sigurniji. Pored ovog postoji zaštita i od elementarnih nepogoda. Kamere, protivprovalna i požarna vrata sve je to dio zaštite kako bi se osiguralo sigurno čuvanje dokumentacije građana istražene Općine.

“Na svakom računaru i opremi u mreži instaliran je antivirusni sistem i obavezna je provjera stanja i statusa opreme sa aspekta virusa od strane Odsjeka za informacioni sistem. U toku je konfigurisanje i postavka firewall-a kako bi sigurnost cijelog IS-a bila na još većem niovu. Odsjek koji se bavi matičnim knjigama je pod posebnim nadzorom u skladu sa zakonskim odredbama i podliježe dodatnim vidovima zaštite.” (I1)

“Pa, koliko je meni poznato tu je prije svega firewall, ovaj, antivirusni programi i što mi je možda poznato meni iz prakse da se uvijek pravi i ovaj hajde da kažemo backup podataka…” (I4)

Umjetna inteligencija nije od izuzetne važnosti za rad u organima lokalne samouprave. Kao prvo, nije dovoljno ispitana ni u drugim aspektima poslovanja.

“Što se tiče umjetne inteligencije ja mislim da to još uvijek, to polje nije dovoljno istraženo i samim tim, je li, ono ima određene rizike. Ali što se tiče same Općine kao Organa uprave nije toliko primjenljiv, primjenljiva umjetna inteligencija na same naše poslovne procese.” (I6)

Ona radi po pitanjima i nalozima ljudi koji upravljaju s njom. Slaba razvijenost ne omogućava robotu da svoj posao obavi samostalno nego ga obavlja uz pomoć zaposlenika koji rukovodi njime. Drugo, mnogi od njih smatraju da AI ne bi imao nikakav uticaj na rad u lokalnoj zajednici. AI nije neophodan za rad u Općinama. S njim dolazi dosta rizika koji mogu ugroziti rad općinskih službi. To su većinom poslovi koji mogu samo ljudi da obavljaju.

“Lični stav, nedovoljna ali i prekomjerna upotreba umjetne inteligencije je mjesto za potencijalne propuste i nosi rizike… uviđenje na mjestima gdje je ljudski faktor neizbježan, poželjan i daje bolji efekat od umjetne inteligencije.” (I1)

“Smatram da u našem poslu AI nije potreban. Može nam malo umanjiti obim poslovanja, ali i dalje je tu potreba za ljudskim radom.” (I2)

“…što se tiče same Općine kao Organa uprave nije toliko primjenljiv, primjenljiva umjetna inteligencija na same naše poslovne procese. Nažalost što je to tako. Još uvijek što se tiče finansijskog softvera sve se oslanja na rad službenika. Na njihov da kažem fizički rad. To se ne može još u toj mjeri prepustiti umjetnoj inteligenciji zbog same, kao što sam već rekao, mogućnosti greške.” (I6)

“…ali definitivno čovjek mora kako da kažem uključiti svoj mozak da bi se to sve realizovalo. Tako da je opet čovjek tu ključan faktor.” (I7)

Dosta papirologije, dokumentacije i poznavanje Zakona ne omogućava korištenje umjetne inteligencije. Zasigurno da AI umanjuje obim poslovanja, ali nam je i dalje neophodan ljudski rad. I treći je usmjeren na lošu edukovanost ljudi za uvođenje umjetne inteligencije.

“U svakom slučaju potrebno je educirati populaciju, posebno starije generacije u benefite umjetne inteligencije.” (I1)

“…također imamo ima uticaj to što ljudi ne poznaju tu umjetnu inteligenciju ni njegove dobre stvari, a ni loše stvari.” (I3)

Zaposlenici se prvo trebaju upoznati i naučiti osnove korištenja AI-a kako bi se on uveo u njihov rad. Možda kad dođe do poboljšanja informacionog sistema da se i uvede ovaj vid napretka. Ali sad intervjuisani zaposlenici ne vide korist od toga. Ili se pak boje da će biti smjenjeni?

Postoje različiti vidovi obuka koje zaposlenici prolaze. Jednom godišnje Agencija za državnu službu raspisuje edukacije u svim poljima poslovanja, čak i onih koji su vezani za IT, gdje se zaposlenici svojevoljno prijavljuju na takav vid educiranosti. Kolege iz IT-a više podliježu obukama uvođenja standarda sigurnosti informacionog sistema za rad u lokalnoj samoupravi. Oni su ti koji teže ka uvođenju i unapređenju ovog vida napretka za rad u općini. Iako bi se i ostali zaposlenici trebali posvetiti ovom segmetnu, jer ona predstavlja budućnost za ostvarivanje adekvatne sigurnosti za njihov rad. Što se zaposlenici prije informišu o tome, prije će standardi sigurnosti biti do kraja implementirani. Dobra edukacija zaposlenika je samo jedan od dodatnih bonusa za sigurnost informacionog sistema i rad u njima.

“Konstantnom edukacijom uposlenika na temu sigurnosti, slanjem informativnih e-mailova sa mogućim posljedicama nenamjernog i namjernog napada na sistem, navođenjem stvarnih primjerima iz prakse i nastale štete na većem nivou, podiže svijest kod uposlenika.” (I1)

“Mi imamo u sklopu Organa uprave plan edukacija u toku godine kojima mi idemo i završavamo, idemo na edukaciju. Također imamo neke privatne edukacije koje želimo da idemo.” (I3)

“…edukacije da kažem, ovaj, neke radionice, timski, timski sastanci te obrade podataka.” (I4)

“Imamo online edukacije. Imamo edukacije u saradnji sa Agencijom za državnu službu koja konstantno nudi programe napretka, naprednog office paketa osnova rada na računaru.” (I6)

Važnost uvođenja standarda sigurnosti informacijskih sistema u organizacijama, te kako će ono uticati na svakodnevne radne zadatke, zaposlenici daju jasan odgovor. Da, važno je. Važno je u svakom aspektu poslovanja. Važno je za sprječavanje neovlaštenog upada, krađe i iskorištavanja informacija. Najvažniji je sa finansijskog aspekta zbog plata zaposlenika i ostalih novčanih mogućnosti koji zahtjevaju određen standard sigurnosti.

“Važnost uvođenja standarda kod nas, evo u finansijskom softveru NIBIS, evo koji sam spomenuo je veoma bitna…” (I4)

Pored toga, za sprječavanje zloupotrebe položaja kojim bi se više poštivala dobivena dokumentacija. Time bi se dobio jedan lijep, upakovan paket koji bi omogućio efikasnije obavljanje posla. Uvođenje ISO 27000 će pružiti dodatnu korist u radu IT sektora. Prvo, omogućila bi im lakše obavljanje posla sa aspekta sigurnosti, a drugo, sigurnost uposlenika bila bi na većem nivou. To je standard koji bi donio dodatne pogodnosti. Iako njegova uspostava zahtjeva veliku svotu novca, te jako puno vremena za njegovu uspostavu njega

trebamo da gledamo kao jednu dobru investiciju koja će trajati duži niz godina. Jer sa ISO 27000 teško je da će doći do zloupotrebe podataka.

Trenutno, Općina koju sam uzela za istraživanje ima ISO kontrolu. Ona se odnosi na kontrolu predmeta. Način na koji se dobiveni predmeti realizuju od strane zaposlenika. Svaki uposlenik može proći kroz kontrolu čime se uviđa njegova spremnost i obavljen posao. I to je jedan segment sigurnosti koji doprinosi boljem poslovanju.

“E sad također imamo veće distance koji nas kontrolišu. Kao što su ISO standardi. Mi imamo koje moramo poštovati. Imamo godišnji, polugodišnji. Također mi imamo jasno definisana pravila i procedure kojih se moramo držati.” (I3)

“…sad mi imamo svakodnevno ISO kontrole. Kako eksterne, tako interne. Koje gledaju niz elemenata i faktora rada.” (I7)

Uvođenje sigurnosnih normi smatra se od izuzetne obaveze po svaku ustanovu i instituciju koja se bavi sa osjetljivom dokumentacijom građana.

“Veoma je, veoma je nužno i bitno je da se uvede. Olakšava funkcionisanje softvera informacionog sistema. Konkretno uvođenje, upravljanje procesa je također ovdje vama značajno.” (I6)

“Tako da je uvođenje sigurnosnih normi jako bitno da ne bi bilo promjene, manipulacije ili zloupotrebe tih podataka koji se inače koriste u organima uprave.” (I8)

“Normalno da je nužno jer može doći do to mi zovemo lika podataka, tj da podaci mogu iscuriti gdje ne treba tako da je nužno.” (I10)

Bitno je zbog ne dovođenja određenih promjena, manipulisanja ili zloupotrebe informacija koje su neophodne za svakog zaposlenika. Bitno je da svaki organ lokalne samouprave posjeduje standarde koji će im pomoći u radu i nadgledanju softvera, tačnije bilo kojeg informacionog sistema koji se koristi u općini.

Općina nedovoljno potiče i informiše građane o planiranim izmjenama, pogotovo informatičkih. Informišu se za druge vidove informacija koje su bitnije za građane i građanke općine. To se najčešće dešava putem web stranice koja se svakodnevno ažurira sa novim podacima. Tu su i Facebook i Instagram kao društvene mreže pogodne i za stariju i za mlađu populaciju. Pored toga, YouTube kanal na kojem se prenose sjednice Općinskog vijeća i ostale bitnije informacije po Općinu i građane. Ugovori sa pojedinim medijskim kućama i sa novinama putem kojih sve informacije dođu do željne adrese. Putem Javnih rasprava gdje i stanovnici mogu dati svoje mišljenje o željnim promjenama, te dati neku svoju ideju. To je jedini način gdje odmah dolazi do interakcije zaposlenika Općine sa građanima tog mjesnog područja.

“…informiše ih putem zvanične web stranice kao i putem drugih društvenih mreža.” (I5)

Sve bitne informacije vezane za ISO standarde objavljuju se na našoj web stranici.

Planovi za poboljšanje informacione sigurnosti u budućnosti, intervjuisani zaposlenici su dali mnoštvo ideja. Ispitanici kroz razgovor sa mnom su uvidjeli da je implementacija ISO 27000 od izuzetne važnosti za sigurnost cijele Općine, te se nadaju da će u skorije vrijeme doći i do njegove realizacije.

"…ali smatram da bi uvođenje standarada ISO 27000 značajno se riješilo pitanje sigurnosti informacionog sistema. Implementacija ovog standarda podrazumijeva analizu rizika sigurnosti, obuku osoblja na čemu stalno treba potencirati, kao i implementaciju tehničkih sigurnosti i mjera, kao i redovno ažuriranje ISO standarda. Implementacijom ovog standarda omogućilo bi se lokalnoj samoupravi da bolje zaštiti osjetljive podatke i informacije, te minimizira rizike od cyber napada, a posljedično osigura povjerenje građana u sposobnost upravljanja informacionom sigurnošću." (I9)

ISO 27000 treba podići sigurnost u Općini na neki viši nivo i to vjerovatno čekajući mlade ljude koji polako popunjavaju radna mjesta ili nove izbore da bi došlo do njegove implementacije. Pored toga, uz pomoć njega bi se svi uposlenici edukovali o izuzetnoj važnosti sigurnosti za njihov rad. Postojale bi određene procedure koje svaki uposlenik mora proći kako ne bi pravio greške u toku svog rada. Time bi se smanjio rizik i potencijalne prijetnje. Definisali bi se svi standardi i norme zaštite informacione sigurnosti. To je dugotrajan proces ali ne i nemoguć. Stoga, trebamo ići ka nekim boljim i inovativnijim stvarima.

"…edukacije zaposlenika i svih ostalih koraka neophodnih za njegovu implementaciju." (I2)

Uvođenje unapređenog firewall-a, zapošljavanje dodatnog kadra u IT sektoru, novog backupa podataka, te unapređenje redovnog održavanja postojećeg informacionog sistema jedni su od ključnih komponenti za bezbijednost dokumentacije.

"Uvođenjem firewall-a, zapošljavanjem dodatnog kadra u Odsjek za informacioni sistem, nadogradnja i unaprjeđenje kao i redovno održavanje postojećih aplikacija, mrežnih segmenata i opreme, te implementacija standarda i normi koji se bave sigurnošću…" (I1)

Pored toga, jedan od ispitanika je dao jedan dobar prijedlog, a to je da se Zakonski uvedu neke obaveze jer nažalost u organe lokalne samouprave najlakše je uvesti neku novinu kad se to definiše određenim Zakonima.

"…trebalo bih se uvesti neka i zakonska obaveza, jer nažalost u većini institucija, posebno ovih državnih organa, najlakše je nešto promijeniti kada se to zakonom definiše." (I4)

3.6. Diskusija rezultata

Koji su međunarodni standardi u području informacionih sistema relevantni za organe lokalne samouprave?

Međunarodni standardi u području informacionih sistema relevantni za lokalnu samoupravu obično se odnose na upravljanje informacionom sigurnošću i upravljanje sistemima informacione tehnologije. Lokalne samouprave mogu odabrati relevantne standarde ovisno o svojim potrebama, ciljevima i vrsti informacija koje obrađuju. Implementacija ovih standarda pomaže u osiguranju visokih standarda sigurnosti i učinkovitog upravljanja informacionim sistemima. Standard ISO 27000 je najrelevantniji za lokalnu samoupravu. Uz pomoć njega sve bitne informacije i dokumentacija bila bi sačuvana na adekvatan način. Pored toga, zaposlenici bi se više informisali o bitnim aspektima sigurnosti za lokalnu samoupravu. Jer ta sigurnost nije neophodna samo nama, nego i građanima čiji se bitni zahtjevi i dokumenti nalaze u prostorijama Općine. Zbog toga, ISO 27000 je odličan model gdje bi njegova implementacija mnogo poboljšala očuvanju sigurnisti i obavljanje posla.

Intervjuisanjem zaposlenika Općine, i uz razgovor sa njima, uvidjeli su bitnost sigurnosti. Koliko ustvari nisu ni razmišljali o tome dok im ja nisam postavljala pitanja. Dosta su se zapitali da li su oni zaista sigurni? Upravo zbog toga smatram da svaki zaposlenik treba da prođe obuku standarda informacionih sigurnosti koji bi mu pružio ISO 27000. Na taj način oni bi obavljali svoj posao bez ikakvog straha od zloupotrebe.

Kako primijeniti standardne informacijskih sistema na organ lokalne samouprave?

Općinski organi imaju velik doprinos u razvoju lokalne zajednice. Kroz planiranje i integrisanost projekta, podržavaju infrastrukturni razvoj, socijalne programe i privredne inicijative. Također, slušajući potrebe građana, prilagođavamo se potrebama i zahtjevima građana, u domenu svojih ovlasti, naravno.

Njegovo primjenjivanjena na organe lokalne samouprave nije lagan zadatak. Potrebno je dosta novca, vremena i obrazovanog kadra koji će omogućiti njegovu implementaciju. To je dugotrajan proces, ali ne i nemoguć. Uz adekvatan stručni kadar, obučen upravo za ovu namjenu, moguće je izvršiti njegovo uvođenje u lokalnu samoupravu. Pronalaskom rizika i postavkom strategije uz obuku svih zaposlenika u Općini moguće je izvesti ovu situaciju. To bi, samim tim, ostvarilo veću sigurnost i sigurnije obavljanje poslova.

Koje su postojeće prakse upravljanja sigurnošću informacijskih sistema u organima lokalne samouprave?

Serija standarda ISO 27000 je međunarodni set normi koji se odnose na upravljanje informacionom sigurnošću. Ključni standard u ovoj seriji je ISO/IEC 27001, koji pruža okvir za uspostavu, implementaciju, održavanje i poboljšanje sistema rukovođenja informacijskom sigurnošću (ISMS) u organizaciji. ISO/IEC 27001 pruža organizacijama strukturirani pristup za identifikaciju, procjenu i upravljanje rizicima vezanim uz informacijsku sigurnost. Implementacija ovog standarda pomaže osigurati da organizacije uspostave odgovarajuće sigurnosne kontrole i prakse kako bi zaštitile osjetljive informacije.

Nažalost u istraženoj jedinici lokalne samouprave trenutno nema implementiranog ISO 27000. Dosta im je bila nepoznanica dok im ja nisam isprezentovala i uputila ih na ovaj

standard. Time su uvidjeli koliko je on ustvari neophodan za rad zaposlenika. Jer uz pomoć njega bi se osiguralo očuvanje svi bitnih dokumenata građana. Time zaposlenici ne bi strahovali od mogućih hakerskih napada na informacioni sistem za matični ured. Iako nemaju uveden ISO 27000 Općina i dalje ima dobro praksu upravljanja sigurnošću informacionog sistema. Tu postoje username i passwordi za pristup uređajima, aplikacijama, printerima. Posjeduju kartice koje im omogućavaju ulazak u posebne prostorije u koje ne smiju uči nezaposlene osobe. Pored toga, firewall koji nastoje da poboljšaju i unaprijede, antivirusi, backup podataka u slučaju pada sistema, te razni informacioni sistemi koji omgućavaju brže i sigurnije obavljanje posla. Sve su to jedni od mjera zaštite kojim se Općina služi kako bi sa sigurnošću upravljala informacionim *sistemima.*

Kako se provodi preventivna zaštita informacijskih sistema i informacija u općinama?

Preventivnu zaštitu provodimo raznim kontrolnim provjerama, ograničavanjem pristupa određenim sektorima naše općine, postavljanjem jakih lozinki, kontrolom uvođenja novih promjena, redovnim ažuriranjem, raznih antivirusnih programa, analizama rizika i slično. Oprema kojom raspolažemo u našem sektoru je kvalitetna i u skladu je sa svjetskim novitetima i preporukama vezano za kvalitet i sigurnost informacionih sistema. U skorijem periodu nastoji se poboljšati informaciona sigurnost poboljšanjem server sale koja je ključna za funkcionisanje svih sistema u Općini. Unaprijedit će se i aplikacije informacionog sistema koje više neće biti zastarjele nego će se omogućiti instalacija najnovijeg oblika aplikacije. Implementacija firewall-a, te konstantna kontrola rada zaposlenika i njihovih e-mailova, kao i provjera pristupu neadekvatnim stranicama koje uposlenici posjećuju. Na takav način informacije i informacioni sistemi su zaštićeni od bilo kakvog mogućeg napada na njih. Da je sigurnost u Općini na zadovoljavajućem nivou pokazuje i činjenica da nijedan napad koji je zabilježen na ruteru nije ostvaren. Zbog toga, Općina je sigurna, te se zaposlenici i građani ne moraju brinuti oko dokumentacije koja se nalazi unutar nje.

Koji su najčešći izvori sigurnosnih prijetnji s kojima se uposlenici općina susreću**?**

Po odgovorima zaposlenika na pitanja koja sam im postavljala mišljenja su podijeljena. Neki misle da su to više vanjski faktori koji nastoje da dođu do informacija koje su pogodne po njih kako bi onesposobile rad Općine. Dok drugi ipak misle da veću prijetnju stvaraju unutrašnji faktori, odnosno zaposlenici, koji svojim nemarom dovode Općinu u opasnost. To zaista može ugroziti sami rad lokalne samouprave, jer time će omogućiti upad vanjskih hakera na brz i jednostavan način. Možda to nije namjerno, ali sve to može uticati negativno po Općinu. Zbog toga smatram da svaki uposlenik mora proći edukaciju sigurnosti informacionog sistema kako bi uvidio njegovu bitnost.

Razgovorom sa IT uposlenicima dobila sam detaljne podatke o pokušajima napada. Postoje napadi. Svakodnevni prikaz na ruteru pokazuje im da postoje pokušaji ulaska u informacioni sistem Općine, ali da nisu realizovani do kraja. Tako da i oni smatraju da unutrašnji faktori više mogu da ugroze sigurnost. Namjerno ili ne namjerno, nije bitno. Bitno je samo da to može biti okidač vanjskim faktorima da pristupe informacijama koje nisu za njih.

Kako pristupiti predstavljanju sigurnosnih standarda uposlenicima lokalne samouprave?

Redovne obuke iz oblasti sigurnosti informacija su najbolji način da se naš kadar educira vezano za sigurnost standarda informacionih sistema, kao i uvođenje ISO 27000 norme uz pomoć koje svi uposlenici moraju proći obuku za njegovu primjenu. Na taj način će zaposlenici na najbolji način biti upoznati sa tim šta im standard sigurnosti nudi u njihovom poslovanju. Kroz razgovor sa deset intervuisanih zaposlenika i prezentacijom ISO 27000 kako bi im pobliže prikazala šta je ustvari standard sigurnosti, uvidjeli su kroz samo par minuta koliko je to nužno za naš rad. Onda zamislite kako bi prezentacija od sat vremena uticala na njihovo mišljenje. Standardi potiču ciklus poboljšanja našeg svakodnevnog rada, međutim, sam proces uvođenja nekih noviteta ili novih normi sigurnosti, je veoma spor. Razradom i planom, te detaljnom pripremom, kako bi svakodnevno poslovanje moglo nesmetano da funkcioniše.

4. ZAKLJUČAK

Najvažniji motiv za uspjeh svake kompanije je obezbjeđenje kontinuiteta u poslovanju. U današnjici taj kontinuitet poslovanja ovisi od više čimbenika koji na njega imaju uticaj. Jedan od njih se odnosi na informacionu sigurnost kompanije, tačnije bitnih informacija i podataka koji su ključni za obavljanje posla. Uvođenje standarda sigurnosti informacionog sistema gledamo kao jedan vid projekta kod kojeg se određuju ciljevi, vrijeme trajanja, troškovi, te stručni kadar koji će njegovu implementaciju dovesti do samog kraja procesa. Ovim uvođenjem kompanije omogućavaju nesmetano obavljanje posla, ali i kompanije tim postaju pouzdaniji partneri koji se u svakom momentu može suprotstaviti prijetnjama koje im se nađu na putu obavljanja posla. Njegova implementacija prilično je složena, gdje se zahtjeva konstantno ulaganje u ljudski rad i njegovo znanje, te konstantna finansijska sredstva. Sve ovo donosi određen rizik i dozu nesigurnosti za njegovu implementaciju. Što je rizik veći, implementacija će biti skuplja ali i informaciona sigurnost bolja.

Sagledam li cijeli rad od njegovog početka pa sve do kraja uviđam da je informacioni sistem od krucialne važnosti za obavljanje svakog posla. Bilo da se radi o lokalnoj samoupravi, ili pak nekoj drugoj kompaniji, cilj svake od njih je da obezbijede sigurnost na poslu. Standardi informacionih sistema su naša budućnost, te upravo zbog toga trebamo da istrajemo u njegovoj implementaciji. Ona će nam omogućiti sigurnost koju želimo da osjetimo u toku rada. Sigurnost koja ima veliki značaj ne samo za nas nego i za ljude, odnosno građane za koje obavljamo zahtjeve predate za njihovu realizaciju. Zbog, toga trebamo težiti ka njegovoj realizaciji jer ćemo samim time olakšati obavljanje posla, te stvoriti dozu sigurnosti koju želi osjetiti svaki radnik.

Nažalost, Općina trenutno nema standard informacione sigurnosti koja bi njegovu sigurnost i obavljanje posla digla na veći nivo. Kroz razgovor sa zaposlenicima i prezentacijom ISO 27000 uvidjela sam veliku dozu zainteresovanosti kod njih. Zbog toga se nadam da će u budućem period doći do njegove realizacije. To bi bio dugotrajan proces, ali ne i nemoguć.

Dok god se vidi želja kod zaposlenika za napretkom i usavršavanjem treba se težiti ka uvođenju ovog standarda. Sa tako kvalitetnom i uspješnom tehnologijom poslovi unutar kompanija se mogu obaviti na izuzetan način, samo ukoliko mi to želimo i istrajemo u toj namjeri. Sigurnost je ključ svakog uspjeha u poslu zbog toga težimo ka tome da budemo što uspješniji u nečem što radimo.

Obzirom da postoji veoma mali broj istraživačkih i naučnih radova i članaka koji se odnose na uvođenje standarda informacionog sistema u organe lokalne samouprave, nadam se da će ovaj rad imati neki doprinos u realizaciji i obezbjeđenju sigurnosti informacionog sistema.

REFERENCE

1. Anon (2008). *Informatika 2*, oobo (Pristupljeno: 18.02.2024.)
2. Anon, (2008). *EMIS - Informacioni sistem u obrazovanju*, Scribd.(Pristupljeno: 30.03.2024.)
3. Anon (2010) *Edicija dokumenata iz područja informacijske sigurnosti.* (Pristupljeno: 12.03.2023)
4. Anon (2012). Uvod u poslovno odlučivanje i kompjuterski bazirane informacione sisteme, *Slideserve*. (Pristupljeno: 18.02.2024.)
5. Anon, (2020). *The CIA Triad — Confidentiality, Integrity, and Availability Explained* (Pristupljeno: 07.03.2024.)
6. Anon (2021). *Pojam informacionih sistema.* (Pristupljeno: 17.02.2024.)
7. Anon, (2022). *Šta je phishing (krađa identiteta)? 4 ključna pitanja,* (Pristupljeno: 10.03.2024.)
8. Anon, (2024). Malware and Ransomware, IT Connect. (Pristupljeno: 10.03.2024.)
9. Bača, M. (2004). *"Uvod u raučnalnu sigurnost"*, Narodne Novine d.d., Zagreb
10. Badžim, A. (2016). *Informacijska sigurnost u poslovnim organizacijama*, Split. (Pristupljeno: 07.04.2024.)
11. Bajgorić, N. (2003). *"Informacijska tehnologija - drugo izdanje"*, Univerzitetska knjiga, Mostar
12. Bajgorić, N. (2004). *"Operativni sistemi - drugo izdanje"*, Univerzitetska knjiga, Mostar
13. Barney, N. (2022). *Cryptojacking*, TechTarget. (Pristupljeno: 11.03.2024.)
14. Bečejski, V. (2008). (Pristupljeno: 24.02.2024.)
15. Bedi, I. (2020). *Rizici u poslovanju poduzeća*, Rada. (Pristupljeno: 06.03.2024.)
16. Bertina, A. (2009). *Implementacija Lean managementa u poduzećima*, Zagreb. (Pristupljeno: 25.02.2024.)
17. Bibović, A. (2013). *Revizija Informacionih Sistema*, Scribd. (Pristupljeno: 30.03.2024.)
18. Bijakšić, S., Markić, B., Bevanda, A. (2014). *Business intelligence and analysis of selling in retail Informatol.*
19. Boban, M., Babić, A. (2014). *Utjecaj internetskih tehnologija na gospodarski rast, poslovni rezultat i stopu rasta profita poduzeća u republici hrvatskoj*. Zbornik radova Veleučilišta u Šibeniku
20. Bogati, J. (2011). *Praktični menadžment*, Zagreb
21. Bogati, J. (2011). *Norme informacijske sigurnosti iso/iec 27k*, Zagreb
22. Braden, A. (2024). *What is software?*, Webopedia. (Pristupljeno: 17.02.2024.)
23. Brown, J. R. (2022). *6 Ways Cybercrime Impacts Business*, Investopedia. (Pristupljeno: 19.02.2024.)
24. Bušac, S. (2016). *Primjena norme ISO 27001*, Zagreb. (Pristupljeno: 07.04.2024.)
25. Carnet (n.d.). *Upravljanje sigurnošću informacionih sustava*, LS&S. (Pristupljeno: 21.02.2024.)
26. Casadesus-Masanell, R. & Ricart, J. (2010). *From strategy to business models and to tactics. Harvard Business School*

27. Castagna, R. i Bigelow, S. J. (n.d.). *Information technology* (IT), TechTarget. (Pristupljeno: 23.02.2024.)
28. Christino, C. (2023). ISO 27001: *Complete 10-step implementation guide*, SoftExpert Blog. (Pristupljeno: 22.03.2024.)
29. Cingula, M (2019). *Pojam sigurnosti i temeljni srodni pojmovi*. (Pristupljeno: 27.03.2023)
30. Corrons, L. (2023). *What is antivirus? Definition, types, and benefits*, Norton. (Pristupljeno: 15.03.2024.)
31. Custer, C. (2023). *What is fault tolerance, and how to build fault-tolerant systems*? Cockroach Labs. (Pristupljeno: 12.03.2024.)
32. Cvjetković, M. (2014). *Uloga znanja u kreiranju konkurentske prednosti*, Beograd. (Pristupljeno: 22.02.2024.)
33. Čakovec (2021). *Što je zapravo digitalna transformacija i kakve nas promjene očekuju?*, Europe direct. (Pristupljeno: 18.02.2024.)
34. Ćurić, F. (2017). *Projektiranje i zaštita informacijsko - komunikacijskih sustava u bankarskim institucijama*, Zagreb. (Pristupljeno: 28.02.2024.)
35. Dube, R. (2019). *What Is Antivirus?*, Lifewire. (Pristupljeno: 15.03.2024.)
36. Đelmo, I. (2020). *Informacija, definicija i osobine,* Zenica. (Pristupljeno: 22.02.2024.)
37. Đapić M., Lukić. Lj. (2007). *Standardi serije iso/iec 27000 najbolja poslovna praksa za sigurnost informacija*, Kragujevac. (Pristupljeno: 28.02.2024.)
38. Ellö, R. (2022). *Model baze podataka za evidenciju radnog vremena*, Osijek. (Pristupljeno: 18.02.2024.)
39. Essex, D. (2024). *Material requirements planning* (MRP), TechTarget. (Pristupljeno: 25.02.2024.)
40. Faraguna, K. (2015). *Korištenje strateških računovodstvenih Informacija u hrvatskom gospodarstvu*, Pula. (Pristupljeno: 18.02.2024.)
41. Fernando, J. (2024). *Supply Chain Management (SCM): How It Works & Why It's Important,* Investopedioa. (Pristupljeno: 26.02.2024.)
42. Fortinet (2023). *What is Hacking?* (Pristupljeno: 12.03.2024.)
43. Gilman, R. (2012). *Introduction to Management Information Systems. Academy of Management Review*
44. Giones, F., Brem, A. (2017). *Digital technology entrepreneurship: a definition and research agenda.* Technology Innovation Management Review
45. Glamoslija, K. (n.d.). *Što je Phishing? Jednostavan vodič sa primjerima*, SafetyDetectives. (Pristupljeno: 10.03.2024.)
46. Glaser, (2001). P*erspektiva utemeljene teorije: Konceptualizacija u suprotnosti s opisom,* Sociology Press. (Pristupljeno: 18.02.2024.)
47. Glaser (2007). Sve su podaci, *Grounded Theory Review: An International Journal.* (Pristupljeno: 18.02.2024.)
48. Golob, B. (2012). *Inovacija poslovnih modela*, Rijeka
49. Gredelj, E. (2020). *Informacija kao čimbenik konkurentskog razvoja logističkog poduzeća*, Osijek. (Pristupljeno: 18.02.2024.)

50. Grgić, K. (2019). R*evizija financijskih izvještaja u okruženju suvremenih informacijsko - komunikacijskih tehnologija*, Pula. (Pristupljeno: 06.04.2024.)
51. Gregurić, B. (2021). *Sustavi upravljanja kvalitetom na primjeru poduzeću podravka* d.d., Karlovac. (Pristupljeno: 07.04.2024.)
52. Hamidović, H. (2010). *Standardi informacijske sigurnosti*, Zagreb, Info Press
53. Hamidović, H. (2006). *Standardi informacijske sigurnosti*, Zagreb
54. Hečimović, I. (2023). *Spam vs. Phishing: u čemu je razlika između ovih dviju vrsta neželjenih poruka?* (Pristupljeno: 10.03.2024.)
55. Huđek, D. (2015). *Primjena biometrijske zaštite u inteligentnim transportnim sustavima,* Zagreb. (Pristupljeno: 09.03.2024.)
56. Igrec, A. (2018). *Digitalna transformacija,* Varaždin. (Pristupljeno: 18.02.2024.)
57. Ivanov, Š. (n.d). *Poslovni informacioni sistemi,* Požarevac (Pristupljeno: 24.02.2024.)
58. Ivković, I. (2019). *Održavanje informacijskih sustava,* Šibenik. (Pristupljeno: 17.02.2024.)
59. Jadrić M., Ćukušić, M. (2015). *Informacijsko-komunikacijske tehnologije u cjeloživotnom učenju,* Split. (Pristupljeno: 09.03.2024.)
60. Jokanović, B. et,al. (2019). *Uticaj informacione tehnologije na organizacionu komunikaciju,* Sremska Kamenica. (Pristupljeno: 23.02.2024.)
61. Jones, D. (2018). *Everything is Information, and Information is Everything,* Washington, DC. (Pristupljeno: 19.02.2024.)
62. Kaić, A. (2019). *Općenito o standardima i normama*
63. Kanade, V. (2024). *What Is an Information Security Management System (ISMS)? Meaning, Working, Benefits, and Best Practices*. (Pristupljeno: 14.03.2024.)
64. Kantor, I. (2021). ISO 27001: *Implementation guide for IT Companies*, Siterasec. (Pristupljeno: 22.03.2024.)
65. Kardašić, M. (2020). *Revizija informacijskih sustava,* Pula. (Pristupljeno: 30.03.2024.)
66. Kelly, C., Jiwon M. A. (2024). *Enterprise Resource Planning (ERP): Meaning, Components, and Examples,* Investopedia. (Pristupljeno: 25.02.2024.)
67. Kirvan, P. (2023). ISACA, TechTarget. (Pristupljeno: 30.03.2024.)
68. Kopal, R., Korkut, D. (2012). *TEORIJA IGARA Praktična primjena u poslovanju,* Društvena istraživanja, Zagreb
69. Kos, G. (2017). *Implementacija kontrolinga u poduzeće iz sektora prehrambene industrije*, Zagreb. (Pristupljeno: 07.04.2024.)
70. Kosutic, D. (n.d). *Jednostavan uvod u osnovne podatke,* Advisera. (Pristupljeno: 07.04.2024.)
71. Kovačević, D. (2008). *Sigurnosna politika,* Zagreb. (Pristupljeno: 21.02.2024.)
72. Krmek, I. (2022). *Procjena rizika – kako je izraditi?,* Centar za zaštitu na radu. (Pristupljeno: 12.03.2024.)
73. Kujundžić, M. (2022). R*azmjena povjerljivih podataka putem interneta sigurnosnim protokolima i način spajanja s interneta na intranet*, Zaprešić. (Pristupljeno: 07.04.2024.)
74. Kujović, S., Dulović, D. (2011). *CRM u telekomunikacionoj kompaniji,* Jahorina. (Pristupljeno: 27.02.2024.)

75. Lagumdžija, Z. et al. (2007). *Izvještaj o kompetitivnosti Bosne i Hercegovine 2007-2008, World economic forum,* MIT Centar Ekonomskog fakulteta u Sarajevu
76. Lagumdžija, Z., Zaimović, T., Šabić, T., Kačapor, K., Grabovica, E. (2008). *Menadžment informacioni sistemi: kompetitivnost i informacione tehnologije,* Ekonomski fakultet Sarajevo
77. Lagumdžija, Z., Zaimović, T., Turulja, L., Grabovica, E., Kapo, A., Kačapor, K. (2021). *Menadžment informacioni sistemi*, Ekonomski fakultet Sarajevo
78. Laudon and Travel (2007). "E-*commerce", 3rd edition*, Prentice Hall
79. Laudon, K. C. & Laudon, J. P. (2012). *Management information systems: managing the digital fir. Pearson Education Inc.*
80. Laudon, K. C. & Laudon, J. P. (2016). *Management Information Systems Managing the Digital Firm, 14. edt. Harlow: Pearson Education Limited*.
81. Lemeš, S., Hamidović, H. (2023). *"Uvod u informacione tehnologije",* Zenica
82. Lemeš, B. (n.d.). *Sigurnost informacijskih sustava.* (Pristupljeno: 09.03.2024)
83. Lerotić, M. (2015). *ERP sustavi - primjer SAP*, Pula. (Pristupljeno: 25.02.2024.)
84. Luić, Lj. (2009). *Informacijski sustavi*, Veleučilište u Karlovcu, Karlovac
85. Lukić, S. (2022). *Informacijske tehnologije u malorpodaj*, Osijek. (Pristupljeno: 25.02.2024.)
86. Ly-Huong T. Pham et. al, (n.d.). *Identifying the Components of Information Systems,* Libretexts. (Pristupljeno: 17.02.2024.)
87. Maček, M. (2019). *Uvođenje sustava poslovne inteligencije u proizvodnom poduzeću*, Zagreb.
88. Marijanović, I. (2006). *Upravljanje sigurnošću informacija*, Zagreb. (Pristupljeno: 09.03.2024.)
89. Markgraf, B. (2019). *Importance of Information Systems in an Organization*, Chron. (Pristupljeno: 19.02.2024.)
90. Mel (2021). *Sigurnost informacionih sistema – broj jedan u poslovanju!* (Pristupljeno: 28.02.2024.)
91. Mijić, B. (2019). *Informacijska sigurnost u Bosni i Hercegovini*, Sarajevo. (Pristupljeno: 28.02.2024.)
92. Milanović, N. (2022). *Šta je CRM i kako ga efektivno koristiti?*, Pit.ba. (Pristupljeno: 28.02.2024.)
93. Mitchell, B. (2020). *Introduction to Information Technology*, Lifewire. (Pristupljeno: 23.02.2024.)
94. Mudželet, A. (n.d.). *MIS DL*, Scribd. (Pristupljeno: 18.02.2024.)
95. Mujakić, M. I. (2016). *Lokalna samouprava u Bosni i Hercegovini,* Sarajevo. (Pristupljeno: 18.03.2024.)
96. Mukherjee, S. (2022). *What is Information System? Definition, Examples, & Facts*, Emeritus. (Pristupljeno: 17.02.2024.)
97. Muris, J. (2020). *Upotreba statistike i informatike u naučnim istraživanjima. Valjanost varijabli , oblikovanje uzorka i skupina,* Sarajevo. (Pristupljeno: 18.02.2024.)
98. Mustapić, M. (2022). *Izvori konkurentske prednosti u nabavnom lancu*, Zagreb. (Pristupljeno: 26.02.2024.)

99. Nibis (n.d.). *Business Information System "NIBIS"*. (Pristupljeno: 01.04.2024.)
100. Objašnjeno (2020). Što je osjetljivost na informacije? (Pristupljeno: 22.02.2024.)
101. Oskoruš, M. (2018). *Digitalna transformacija poslovanja*, Mentorica.biz. (Pristupljeno: 18.02.2024.)
102. Oštrić, D. I. (2015). *Sigurnosni aspekti i metode zaštite informacijskih sustava*, Zagreb. (Pristupljeno: 09.03.2024.)
103. Patrizio, A. (n.d.). *Malware vs. ransomware: What's the difference?*, TechTarget. (Pristupljeno: 10.03.2024.)
104. Pavković, V. (2020). *Povezanost kvalitete erp sustava i poslovnih performansi poduzeća,* Split. (Pristupljeno: 25.02.2024.)
105. Pit (2020). *Šta je ERP – značaj ERP rješenja u poslovanju preduzeća?* (Pristupljeno: 25.02.2024.)
106. Plojović, S. (2009). *Menadžment informacioni sistemi*, Novi Pazar. (Pristupljeno: 23.02.2024.)
107. Pokorni, M. (2019). *Standardi i okviri upravljanja sigurnošću informacijskih sustava*, Pula. (Pristupljeno: 13.02.2024.)
108. Ponjević, E. (2010). *Sigurnost informacija,* General security. (Pristupljeno: 05.03.2024.)
109. Profozić, M. V. (2018). *Informacijska sigurnost u poslovanju*, Karlovac. (Pristupljeno: 12.02.2024.)
110. Radinić, Z. (2019). *Procjena rizika na radu*, Karlovac. (Pristupljeno: 09.03.2024.)
111. Radivojević, D., Radivojević, M. (2017). *Menadžment informacionih sistema*, Banja Luka.
112. Rainer, R. K., & Casey, G. C. (2013). *Introduction to Information Systems*. Singapore: John Wiley and Sons.
113. Rasure, E., Jackson, A. (2023). *Cryptojacking: What It Is, How It Works*, Investopedia. (Pristupljeno: 11.03.2024.)
114. Raza, M. (2019). *Introduction to Information Security Management Systems* (ISMS), BMC. (Pristupljeno: 14.03.2024.)
115. Rebrača, I. (2018). Procena ugroženosti od elementarnih nepogoda i drugih nesreća, *Security SEE*. (Pristupljeno: 12.03.2024.)
116. Redžibašić i Jašarević, (2021). (Pristupljeno: 28.02.2024.)
117. Ristić, M. (2017). *Šta je ERP – kako ERP sistemi utiču na poslovanje preduzeća*?, Beleške. (Pristupljeno: 25.02.2024.)
118. Robinson, S., Diann, D. (2024). *Supply chain management* (SCM),TechTarget. (Pristupljeno: 26.02.2024.)
119. Rušev, P. (2017). *Analiza načina kontrole zaliha*, Zagreb. (Pristupljeno: 25.02.2024.)
120. Samaržija, D. (2019). *Troškovi radne snage*, Zaprešić. (Pristupljeno: 25.02.2024.)
121. Savic, N., Ograjensek, I. & Buhovac, A. (2016). *The Drivers of Success in Business Model Transformation*
122. Schulze, J. (2024). *What is Information Technology?* Coursera. (Pristupljeno: 23.02.2024.)

123. Sharma, P. (n.d.). *Business Information System: Meaning, Features and Components*. (Pristupljeno: 24.02.2024.)
124. Sheps, A. (2023). *Cryptojacking*, Cloud native wiki. (Pristupljeno: 11.03.2024.)
125. Simplilearn (2023). W*hat Is Data: Types of Data, and How to Analyze Data?*, Simplinearn. (Pristupljeno: 18.02.2024.)
126. Skolait, (2021). *Pojam informacionih sistema*. (Pristupljeno: 24.02.2024.)
127. Službeni glasnik (2017). *Odluku o usvajanju politike upravljanja informacionom sigurnošću u institucijama Bosne i Hercegovine, za period 2017 - 2022. godine*, Bosna i Hercegovina. (Pristupljeno: 21.02.2024.)
128. Smiljčić, I., Livaja I., Acalin J. (2017). *"ICT u obrazovanju"*, Šibenik
129. Sonnenberg, A. (2022). *How to Use Meta Business Suite*, SocialMedia Examiner. (Pristupljeno: 24.02.2024.)
130. Spilker, J. (2023). *Data vs Information vs Knowledge: What Are The Differences?*, Tettra. (Pristupljeno: 19.02.2024.)
131. Spremić, M. (2007). *Metode provedbe revizije informacijskih sustava*, Zagreb.
132. Spremić, M. (2017). *Digitalna transformacija poslovanja*, Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet
133. Spremić M. (2020). *Sigurnost I Revizija Is-A U Okruzenju Digitalne Ekonomije*, Zagreb
134. Staff, C. (2023). *What Is the CIA Triad?*, Coursera. (Pristupljeno: 06.03.2024.)
135. Stanišić, M. (2014). *Revizija kontrola informacionih sistema*, Srbija. (Pristupljeno: 07.03.2024.)
136. Strauss, L. (2022). *What is information systems? Definition, uses, and examples*, Zapier. (Pristupljeno: 17.02.2024.)
137. Strilic, S. (2021). *Metoda uzorka u reviziji financijskih izvještaja*, Pula. (Pristupljeno: 06.04.2024.)
138. Sundgren, B. (2005). *What is a public information system?*, Sweden. (Pristupljeno: 21.02.2024.)
139. Šabić, Z. (2008). *"Metodološki okvir za simultani razvoj informacionih sistema"*, doktorska disertacija, Univerzitet u Sarajevu
140. Šafar, N. (2022). *Analiza odniosa podataka, informacije, znanja i mudrosti*, Osijek.
141. Šehić, DŽ. (2001). *"Strateški Menadžment"*
142. Šumić, Z., Petrović, J. (2008). *HACCP sistem 15 – Utvrđivanje korektivnih mera*, Enciklopedija. (Pristupljeno: 07.03.2024.)
143. Tanović, E. (2012). *Standardizacija*, Sarajevo. (Pristupljeno: 07.04.2024.)
144. TechTarget Contributor (2023). *Information systems (IS)*. (Pristupljeno: 17.02.2024.)
145. Turban, E., King, D., McKay, J., Marshall, P., Lee, J., Viehland, D. (2008). *"Electronic Commerce, A Managerial Perspective"*
146. Turban, R., & Volonino, L. (2012), *Information technology for management*. John Wiley and Sons.
147. UAGC-a, (2023). *What Is Business Information Systems?*, Global Campus. (Pristupljeno: 24.02.2024.)
148. Vasiljev, S., Milovac, N. (2010). *Upravljanje odnosima sa potrošačima (crm) iz perspektive marketinga i informatičkih tehnologija.* (Pristupljeno: 28.02.2024.)

149. Višnjić, M. (2021). *Provedba revizije informacijskih sustava primjenom različitih metodologija*, Zagreb.
150. Vuković, A., Džambas, I., Blažević, D. (2007). *Razvoj erp-koncepta i erp-sustava development of erp concept and erp system.* (Pristupljeno: 25.02.2024.)
151. Yasar, K. (2022). *Information security management system (ISMS)*, TechTarget. (Pristupljeno: 14.03.2024.)
152. Yasar, K., Rosencrance, L. (2023). *Antivirus software (antivirus program)*, TechTarget.

PRILOZI

Prilog 1. Pitanja za intervju zaposlenika

1. Koliko je važno imati siguran informacioni sistem za rad u lokalnoj samoupravi?

   Potpitanje: Koji vi informacioni sistem koristite?

2. Kako informacioni sistem utiče na efikasnost rada lokalne samouprave?

3. Koliko često imamo prijetnje sigurnosti informacionog sistema i baze podataka, te da li su napadi uspješni ili ne?

   Potpitanje: Kako se nositi s incidentima sigurnosti informacijskih sistema?

4. Koje su najčešće prijetnje i izazovi u području sigurnosti informacija?

   Potpitanje: Prema Vašem stručnom mišljenju, da li veću prijetnju stvaraju vanjski (hakeri) ili unutrašnji faktor (stručni kadar)?

5. Koje tehničke mjere preventivno koristi Općina za zaštitu informacija (npr., firewall, antivirusni programi, enkripcija)?

   Potpitanje: Kako se provodi preventivna zaštita informacijskih sistema i informacija u Općinama?

   Potpitanje: Postoji li sistem za praćenje i detekciju neovlaštenog pristupa sistemu?

6. Tehnologije poput umjetne inteligencije (AI) i analitike podataka doprinose li poboljšanju ili ugrožavaju sigurnost informacija?

7. Kako se educiraju uposlenici za uvođenje standarda/normi informacijskih sistema?

   Potpitanje: Kako lokalna samouprava može unaprijediti svijest o sigurnosti informacija među svojim zaposlenicima?

8. Možete li objasniti važnost uvođenja standarda sigurnosti informacijskih sistema u organizacijama, te kako će ono uticati na svakodnevne radne zadatke?

9. Koliko je uvođenje sigurnosnih normi nužno za potrebe lokalne samouprave?

10. Kako Općina potiče i informiše građane o planiranim izmjenama?

11. Koji su planovi za poboljšanje informacijske sigurnosti u budućnosti?

Prilog 2. Molba za odobrenje obavljanja intervjua

Općina XXX
Ul. XXX
71000 Sarajevo
n/r Općinskom načelniku

Hana Zeković
Porodice Ribar XX
71000 Sarajevo
+387 62 XXX XXX

PREDMET: Molba za odobrenje obavljanja intervjua, *dostavlja se*
VEZA: Magistarski rad na Ekonomskom fakultetu

Poštovani Načelniče,

ljubazno Vas molim da mi izađete u susret i odobrite obavljanje intervjua sa 12 do 15 uposlenika Općine u svrhu pisanja magistarskog rada na Ekonomskom fakultetu Univerziteta u Sarajevu, na temu: ***„Uspostavljanje standarda sigurnosti informacijskih sistema u organima lokalne samouprave: Studija slučaja općina“***. Intervju mi je potreban kako bih dobila potrebne informacije o informacionim sistemim u našoj općini, te iste iskoristila za pisanja master teze. Informacije neće biti korištene ni u jednu drugu svrhu.

Zaposlenica sam Općine u Službi za obrazovanje, kulturu i sport, te iskreno vjerujem da ćete pozitivno razmotriti moju molbu. Ukoliko nije problem da me o Vašem odgovoru obavijestite pismeno, odnosno da mi akt o odobrenju bude dostavljen u Službu za obrazovanje, kulturu i sport.

U nadi da ćete razmotriti i odobriti moju molbu unaprijed Vam se zahvaljujem.

S poštovanjem,

Sarajevo, 12.02.2024. _____

Hana Zeković

PRILOG: pitanja zaposlenicima
1. Pitanja zaposlenicima

DOSTAVITI:
1. Naslovu
2. a/a

Prilog 3. Saglasnost o učešću

SAGLASNOST

Tema: *„Uspostavljanje standarda sigurnosti informacijskih sistema u organima lokalne samouprave: Studija slučaja općina“*

Poštovani učesniče,

vašim potpisom saglasni ste za učešće u istraživanju pisanja master teze kandidatkinje Hane Zeković, pod mentorstvom doc. dr. Kemala Kačapora. Saglasnost je napisana u svrhu Vašeg informisanja o navedenoj temi kako bi Vi dali dozvolu za doprinos o učešću u daljem istraživanju. Cilj samog rada je istražiti uspostavljanje standarda sigurnosti informacionih sistema u Općini, te njegova kvalitetna primjena i unapređenje u budućnosti. Informacioni sistemi su mnogo važni za sam rad Općine. Bez njih nijedan organ lokalne samouprave ne bi mogao funkcionisati niti se odbraniti od štetnih stvari unutra i izvan same lokalne zajednice. Štete sa kojima se radnici susreću bit će predočene kroz intervju iz kojeg ću ja kao istraživač donijeti konačne zaključke na kraju samog ispitivanja. Rad će biti napisan kao studij slučaja gdje će podaci biti prikupljeni od strane uposlenika Općine XXX iz različitih Službi koje koriste informacione sisteme za obavljanje svog rada. Obuhvaćena će biti muška i ženska populacija različite životne skupine. Uposlenici će biti snimani sa urađenom transkripcijom nakon intervjuisanja.

Vi, kao ispitanici možete u svakom momentu istraživanja navedene teme povući Vašu saglasnost. Posljedica prilikom odustajanja za davanje doprinosa o učešću po Vas neće biti. Samo Vas molim da to uradite u što kraćem roku kako bih ja kao istraživač mogla pronaći drugog ispitanika. Ukoliko u toku istraživanja budete imali bilo kakva pitanja ili dilemu, budite slobodni da mi se obratite kako bih razriješila Vaše nedoumice. Također budite uvjereni da Vaše ime i prezime neću koristiti niti povezati sa podacima koje ste dali u toku istraživanja.

Vašim potpisom dajete saglasnost o učešću istraživanja master teze, te meni kao istraživaču pružate mogućnost da Vaše informacije koristim u svrhu pisanja magistarskog rada. Unaprijed Vam se zahvaljujem što mi dajete potporu kao i mogućnost da Vaše informacije iskoristim u daljem procesu.

_____ _____ (potpis)

Hana Zeković (istraživačica)