# Analiza rizika u procesu razvoja informacijskih tehnologija

**Bekafigo, Antea**

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2018./ 2019.

Antea Bekafigo

# ANALIZA RIZIKA U PROCESU RAZVOJA INFORMACIJSKIH TEHNOLOGIJA

Diplomski rad

Mentor: dr.sc. Kristina Kocijan, doc.

Zagreb 2018.

# Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

# Sadržaj

Izjava o akademskoj čestitosti ..... 1
Sadržaj ..... 2
1. Uvod ..... 4
2. Rizik i analiza rizika ..... 6
2.1. Rizik ..... 6
2.2. Analiza rizika ..... 6
2.3. Metode analize rizika ..... 7
3. Komponente analize rizika ..... 9
3.1. Procjena rizika ..... 10
3.1.1. Identifikacija rizika ..... 11
3.1.2. Analiza relevantnih rizika ..... 11
3.1.3. Evaluacija rizika ..... 12
3.2. Upravljanje rizikom ..... 13
3.3. Komunikacija rizika ..... 14
3.4. Politika rizika ..... 14
3.5. Koristi od analize rizika ..... 14
4. Informacijske tehnologije i sustavi ..... 16
4.1. Povijest digitalne kulture ..... 16
4.1.1. Početci digitalne kulture ..... 16
4.1.2. Kibernetička era ..... 17
4.1.3. Digitalna avangarda ..... 19
4.1.4. Digitalna kontrakultura ..... 20
4.1.5. Digitalni otpori ..... 22
4.1.6. Digitalna kultura 21. stoljeća ..... 23
4.2. Definicija i povijesni razvoj informacijske tehnologije ..... 24
4.3. Informacijski sustav i povijesni razvoj informacijskih sustava ..... 28
4.4. Vrste informacijskih sustava ..... 30
4.5. Faze razvoja informacijskog sustava ..... 31
4.6. Zaštita informacijskog sustava ..... 33

5. Analiza rizika u procesu razvoja informacijskih sustava i tehnologija ..... 36
5.1. Analiza rizika u procesu razvoja informacijskih tehnologija ..... 36
5.2. Rizici koji se pojavljuju u razvoju informacijskih tehnologija ..... 37
5.3. Utjecaj razvoja informacijskih tehnologija na upravljanje rizikom ..... 39
5.4. Analiza rizika u procesu razvoja informacijskih sustava ..... 41
5.5. Rizici koji se pojavljuju pri izgradnji informacijskih sustava ..... 44
5.6. Proces upravljanja rizikom informacijskog sustava ..... 46
5.7. Suvremene informacijske tehnologije i analiza rizika ..... 48
6. Primjeri analize rizika ..... 50
6.1. Računarstvo u oblaku ..... 50
6.1.1. Nemogućnost prelaska kod drugog pružatelja usluga ..... 53
6.1.2. Gubitak vlasti ..... 54
6.1.3. Izazovi vezani uz sukladnost ..... 57
6.1.4. Neuspjeh izolacijskih mehanizama ..... 58
6.1.5. Zlonamjerni unutarnji suradnici ..... 59
6.1.6. Nesigurno ili nepotpuno brisanje podataka ..... 61
6.1.7. Kompromis u dizajnu upravljačkog sučelja ..... 62
6.1.8. Zaštita podataka ..... 63
6.1.9. Komparativna analiza ..... 64
6.1.10. Primjeri posljedica neprovedene analize rizika računarstva u oblaku ..... 65
6.2. Mrežno oglašavanje ..... 66
6.2.1. Namjerno otkrivanje tajnih informacija unutar platforme ..... 66
6.2.2. Limitiranje uloge korisnika ..... 69
6.2.3. Primjeri posljedica neprovedene analize rizika kod mrežnog oglašavanja ..... 70
7. Zaključak ..... 72
8. Literatura ..... 73
Sažetak ..... 76

# 1. Uvod

U samom početku razvoja informacijskih tehnologija, nije se pretjerano razmišljalo o rizicima koje će taj razvoj donijeti. Daljnji razvoj i dostupnost tehnologije široj masi ljudi doveli su i do intenzivnijeg razmatranja mogućnosti postojanja različitih rizika. U skladu s time bilo je potrebno razviti određene metode za identifikaciju rizika, kao i za njihovo rješavanje, kako bi se mogući rizici na vrijeme umanjili ili potpuno uklonili. Postoje različite vrste rizika koje na različite načine utječu na krajnji proizvod, a o nekima od njih će se govoriti i u ovome radu.

U današnje vrijeme informacijska se tehnologija razvija tolikom brzinom da se iz dana u dan pojavljuju sve sofisticiranija tehnološka rješenja. Budući da je tehnologija ovih dana dostupna gotovo svima, logično je da takav razvoj utječe na društvo u globalu, ali što je za ovu temu još važnije, utječe na proces samog razvoja i plasiranja svih informacijskih sustava i tehnologija. Prije no što se proizvod takve prirode ponudi krajnjem korisniku potrebno je da on, između ostalog, prođe i kroz proces analize rizika, kako bi do svoga cilja došao sa što manjom mogućnosti da tijekom njegova korištenja dođe do problema. Neke od suvremenih i rastućih tehnologija u kontekstu analize rizika biti će spomenute i u ovome radu.

Ova tematika je za današnje vrijeme jako važna upravo iz tog razloga što je tehnologija dostupna ogromnom broju korisnika. Prije nego što dođe do krajnjeg korisnika potrebno je minimizirati ili otkloniti što veći broj rizika koji se pojavljuju pri razvoju informacijskog sustava ili tehnologije.

Rad će biti podijeljen u tri glavna poglavlja. U prvom poglavlju opisat ću analizu rizika kao postupak koji ujedinjuje procese upravljanja rizikom i procjene rizika i objasniti važnost navedenog postupka u razvoju proizvoda. U drugom poglavlju govorit ću o informacijskim tehnologijama i informacijskim sustavima općenito, o njihovom razvoju i utjecaju na korisnike. Posebno ću se približiti nekima od aktualnijih informacijskih tehnologija i onima kojima se u svom poslovanju koristi veliki broj

korporacija, a to su računarstvo u oblaku i online oglašavanje. U trećem poglavlju detaljno ću se osvrnuti na objašnjenje analize rizika u procesu izrade informacijskih sustava i tehnologija općenito, a nakon toga ću isti postupak objasniti na primjerima gore navedenih suvremenih tehnologija.

# 2. Rizik i analiza rizika

## 2.1.Rizik

Prema definiciji rizika iz enciklopedije Leksikografskog zavoda Miroslav Krleža rizik označava, u širem smislu, mogućnost pogibelji, opasnosti, odnosno izloženost nezgodi, nesreći, propasti ili gubitku. Još općenitiju definiciju rizika daje Hrvatski jezični portal, a to je da je rizik opasnost koja se do određene mjere može predvidjeti i čiji je intenzitet moguće odrediti. Još jedna od definicija rizika, ona iz „Poslovnog riječnika“ (engl. *Business Dictionary*) kaže kako je rizik mogućnost ili prijetnja od određene štete, ozljede, gubitka ili bilo koje druge negativne pojave koja je uzrokovana vanjskim ili unutarnjim čimbenicima ranjivosti, a koju je moguće izbjeći preventivnim djelovanjem.

Sve tri definicije u suštini tvrde kako je rizik jedna vrsta opasnosti koja za posljedicu ima neku negativnu pojavu. Prve dvije definicije rizika su općenite i odnose se na sve situacije koje mogu proizvesti neku vrstu rizika, tj, moguće opasnosti. Budući da će se dalje govoriti o analizi rizika u procesu razvoja informacijskih tehnologija i sustava, najvažnija je posljednja definicija jer za razliku od ostalih spominje čimbenike ranjivosti, kao i preventivno djelovanje na rizik, a upravo su to pojmovi važni za navedenu temu i kasnije će biti pobliže objašnjeni.

## 2.2.Analiza rizika

Prema definiciji iz „Technopedije“ analiza rizika je pregled rizika povezanih s nekim događajem ili radnjom. Može biti primjenjena na raznim poslovnim projektima, informacijskim tehnologijama, problemima sa sigurnošću i svakoj drugoj aktivnosti u kojoj je rizike moguće analizirati na kvantitativnoj i kvalitativnoj razini. Analiza rizika predstavlja sastavni dio upravljanja rizikom.

Izvjesno je da su rizici dio svakog IT projekta i svakog poslovnog pothvata. Za sam proces analize rizika bilo bi poželjno da se tijekom vremena ponavlja i ažurira kako bi sama analiza bila u tijeku s novim potencijalnim prijetnjama.

U razvoju informacijske tehnologije ili informacijskog sustava analiza rizika jedan je od ključnih procesa kroz koje je potrebno proći kako bi krajnji rezultat bio zadovoljavajuć. Dobar i potpun pregled rizika znači da na putu razvoja informacijske tehnologije neće doći do neugodnih iznenađenja u obliku neidentificiranih rizika i samim time će sam proces razvoja proći neometano, a rizici će se tretirati u skladu s njihovom vrstom i količinom opasnosti koju predstavljaju.

## 2.3.Metode analize rizika

Moguće je da se analiza rizika zamjetno razlikuje kod različitih rizika, u svrsi analize, kao i u potrebnoj razini zaštite relevantnih informacija, podataka i resursa. Sama analiza može biti kvalitativna, polukvantitativna ili kvantitativna te kombinacija navedenih (ENISA, 2006).

Kod **kvalitativne analize**, utjecaj i vjerojatnost potencijalnih posljedica su vrlo detaljno predstavljeni i opisani. Skale koje se koriste za mjerenje mogu se oblikovati ili prilagoditi okolnostima pa se tako i različiti opisi mogu koristiti za razne rizike. Kvalitativnu analizu moguće je koristiti kao početnu procjenu kako bi se identificirali rizici koji će biti predmet daljnjih i detaljnijih analiza, potom tamo gdje je potrebno uzeti u obzir nevidljive aspekte rizika ali i tamo gdje nedostaju adekvatne informacije i brojčani podaci ili resursi koji su nužni za statistički relevantan kvantitativni pristup (ENISA, 2006).

Kod **polukvantitativne analize** cilj je dodijeliti vrijednosti skalama u kvalitativnoj procjeni. Te vrijednosti su u najviše slučajeva indikativne i nisu stvarne, što je zapravo preduvjet kvantitativnog pristupa. Zbog toga, budući da vrijednost dodijeljena svakoj ljestvici nije točan prikaz stvarne jačine utjecaja ili vjerojatnosti, upotrijebljeni brojevi moraju se kombinirati pomoću formule koja prepoznaje ograničenja ili pretpostavke iznesene u opisu korištenih skala. Potrebno je napomenuti i to da je moguće koristiti i

polukvantitativnu analizu različitih nedosljednosti zbog činjenice da postoji mogućnost da odabrani brojevi možda nisu ispravni i da ne prikazuju točno analogije među rizicima, najviše onda kada su u pitanju ekstremne posljedice ili vjerojatnosti (ENISA, 2006).

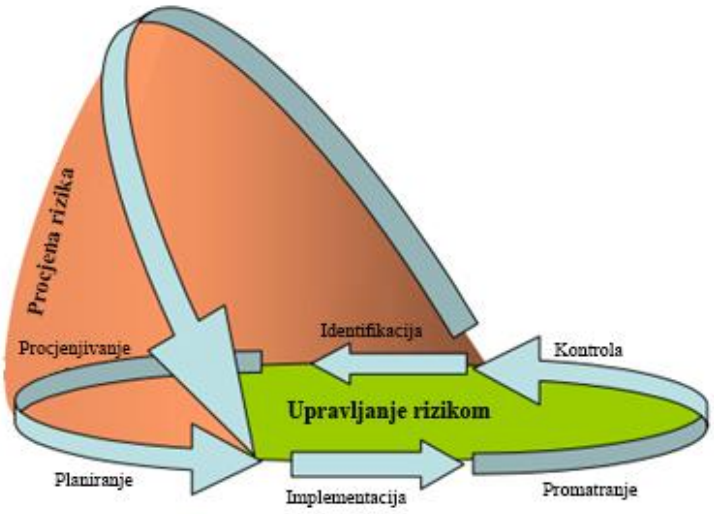
Kod **kvantitativne analize** numeričke se vrijednosti dodijeljuju i učinku i vjerojatnosti. Takve vrijednosti izvedene su iz različitih izvora. Kvaliteta cjelokupne analize ovisi o točnosti dodijeljenih vrijednosti i valjanosti statističkih podataka korištenih modela. Utjecaj se može odrediti vrednovanjem i obradom različitih rezultata ili ekstrakcijom iz eksperimentalnih studija ili prethodnih podataka. Posljedice mogu biti monetarne, tehničke, operativne i ljudske (ENISA, 2006), Nakon što je rizik kvantificiran, u skladu s dobivenim rezultatima, potrebno je osmisliti odgovarajuće opcije upravljanja rizikom. Zatim je moguće napraviti rizik-korist analizu (engl. *Risk-Benefit analysis*) ili trošak-korist analizu (engl. *Cost-Benefit analysis*), nakon ćega je moguće formulirati politike upravljanja rizikom i provoditi ih.

Glavni ciljevi postupka upravljanja rizicima su: smanjiti pojavu nezgoda smanjivanjem vjerojatnosti njihova pojavljivanja; smanjiti utjecaje nesreća koje je nemoguće kontrolirati (npr. na vrijeme se pripremiti za eventualne hitne slučajeve); i smanjenje rizika prijenosa (npr. putem osiguranja). Procjena vjerojatnosti, tj. učestalosti pojave opasnosti, uvelike ovisi o pouzdanosti komponenti sustava, sustava u cjelini i interakcije između čovjeka i sustava (Modarres, Kaminskiy & Krivtsov, 2002).

Jasno je da specifikacija razine rizika nije jedinstvena. Utjecaj i vjerojatnost mogu se izraziti ili kombinirati drugačije prema vrsti rizika i opsegu i cilju procesa upravljanja rizicima (ENISA, 2006).

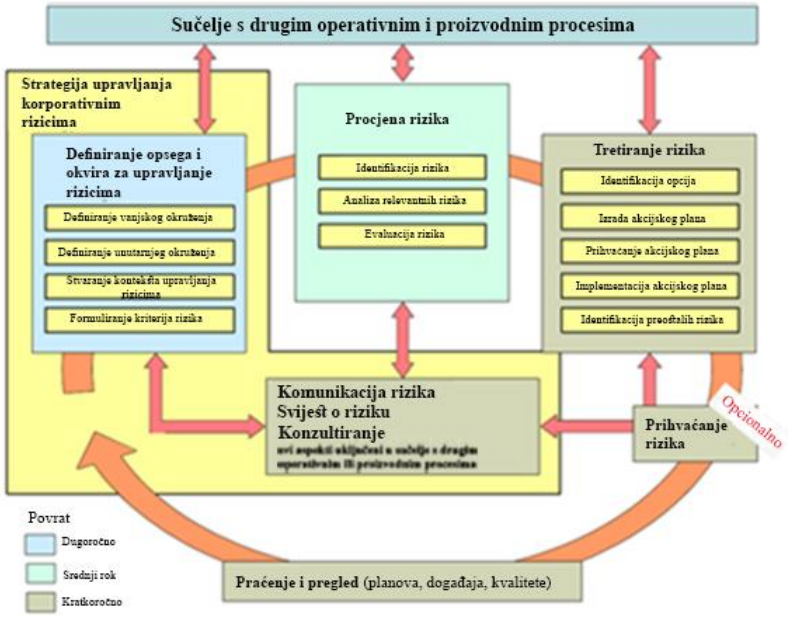
# 3. Komponente analize rizika

**Upravljanje rizikom** (engl. *risk management*) smatra se ponavljajućom aktivnošću koja se bavi analizom, planiranjem, provedbom, kontrolom i praćenjem provedenih mjerenja i provedene sigurnosne politike. Često se pojam upravljanja rizikom pojavljuje zajedno s pojmom **procjene rizika** (engl. *risk assesment*). Stručnjaci za informacijsku sigurnost prihvatili su da je procjena rizika dio procesa upravljanja rizicima. Procjena rizika provodi se u određenim vremenskim intervalima (npr. jednom godišnje; onda kad se procijeni da je to potrebno; kada stranka to zatraži) i, do obavljanja sljedeće procjene, daje privremeni uvid u procijenjene rizike i time postaje mjerni instrument cjelokupnog procesa upravljanja rizicima, a analiza rizika je jedan od procesa upravljanja rizicima. Na slici 1 je detaljnije prikazan odnos između upravljanja rizikom i procjene rizika.




*Slika 1.* poveznica između upravljanja rizikom i procjene rizika (prilagođeno prema (ENISA, 2006))

Upravljanje rizikom smatra se glavnim pojmom koji objedinjuje nekoliko procesa, odnosno aktivnosti, koji se dotiču identifikacije, ublažavanja, upravljanja i kontrole rizika, što se vidi na slici 2 (ENISA, 2006).




*Slika 2.* upravljanje rizikom (prilagođeno prema (ENISA, 2006))

Prema Byrdu i Cothernu (2005) procjena rizika, kao i upravljanje rizikom dvije su od tri komponente koje sačinjavaju proces analize rizika. Treća komponenta je **komunikacija rizika** (engl. *risk communication*). Pojavljuje se i četvrta, kako ju autori nazivaju „meta-tema“, (engl. *meta-topic*), **politika rizika** (engl. *risk policy*), no navedenu autori ne priznaju kao ravnopravnu komponentu analize rizika.

## 3.1.Procjena rizika

Procjena rizika predstavlja proces karakterizacije rizika. Navedeni proces uključuje procjenu vjerojatnosti, koja se najčešće izračunava matematički, i navođenje uvjeta koji prate rezultat procjene. Obično se u tome procesu objedinjuju opisni podatci i znanstvene teorije. Procjena rizika generalno služi za otkrivanje što sve može poći po zlu, kolika je vjerojatnost da će ishod biti loš, koliko će vremena biti potrebno da do lošeg ishoda

uopće dođe te ukoliko do njega i dođe, kolika će biti njegova važnost (Byrd; Cothern, 2005).

Procjena rizika, kao prema slici 2, sastoji se od tri faze: identifikacije rizika, analize relevantnih rizika i evaluacije rizika. Sve tri faze su jednako važne i svaku je potrebno temeljito odraditi kako bi se došlo do sljedeće faze, tretiranja rizika (ENISA, 2006).

### *3.1.1. Identifikacija rizika*

Identifikacija rizika prva je faza procjene rizika u kojoj se identificiraju prijetnje, ranjivosti i rizici povezani s tim istim prijetnjama i ranjivostima. Taj proces mora biti sustavan i sveobuhvatan kako bi se osiguralo to da nema propusta pri samoj identifikaciji jer bi takvi propusti kasnije mogli dovesti do loše odrađenog čitavog postupka procjene rizika. Od velike je važnosti da se tijekom ove faze identificiraju baš svi zabilježeni rizici, bez obzira na to što su neki od njih možda već poznati, a moguće već i pod nadzorom organizacije koja provodi identifikaciju (ENISA, 2006).

Postoji nekoliko različitih metoda identifikacije rizika koje se koriste, a to su: radionice za prepoznavanje rizika, konzultacije sa sudionicima, vrednovanje (engl. *benchmarking*), scenariji ili „što ako“ analiza, revizija i inspekcija, razne metode istraživanja (intervjui, ankete i sl.), uzročno-posljedični dijagrami. Identificirane rizike potrebno je prikazati u strukturiranom obliku, pritom koristeći tablicu kako bi se olakšao opis i procjena rizika (Harvey, 2008).

### *3.1.2. Analiza relevantnih rizika*

Analiza relevantnih rizika je proces u kojemu se procjenjuje razina rizika i priroda toga rizika. Upravo su te informacije prvi važan čimbenik pri donošenju odluke o tome trebaju li se rizici tretirati ili ne i, ako da, koji je najprikladniji i najisplativiji tretman koji će se koristiti pri tom postupku.

Sam proces analize relevantnih rizika uključuje nekoliko koraka, a to su: temeljito ispitivanje izvora rizika; evaluacija pozitivnih i negativnih posljedica koje rizik može

donijeti; izračunavanje stupnja vjerojatnosti da će se te posljedice uopće pojaviti te čimbenici koji utječu na njihovo moguće pojavljivanje; procjenu svih postojećih kontrola ili procesa za koje postoji mogućnost da će minimizirati negativne rizike ili povećati pozitivne rizike.

Sam stupanj rizika može se procijeniti kombiniranjem statističkih analiza i izračuna utjecaja i vjerojatnosti. Sve formule i metode za njihovo kombiniranje moraju biti dosljedne kriterijima koji su definirani pri uspostavljanju konteksta upravljanja rizicima. U slučaju da nisu dostupni pouzdani ili statistički pouzdani i relevantni prethodni podaci, mogu se napraviti i dodatne procjene.

Informacije koje se koriste za procjenu utjecaja i vjerojatnosti pojave rizika obično dolaze od: prethodnog iskustva ili podataka i zapisa (npr. izvješća o incidentima); pouzdane prakse; međunarodnih standarda ili smjernica; istraživanja i analize tržišta; eksperimenata i prototipova; ekonomskih, inženjerskih ili drugih modela; stručnih savjeta.

Tehnike analize rizika uključuju intervjue sa stručnjacima iz toga područja interesa i upitnike, kao i korištenje postojećih modela i simulacija (ENISA, 2006).

### *3.1.3. Evaluacija rizika*

U fazi evaluacije rizika potrebno je donijeti odluke o tome koje je rizike potrebno tretirati, a koji od njih nisu prioritet. Potrebno je i usporediti razinu rizika utvrđenu tijekom procesa analize s kriterijima rizika uspostavljenima u kontekstu upravljanja rizicima (tj. u fazi identifikacije kriterija rizika). Isto tako, moguće je da će u nekim slučajevima procjena rizika dovesti do odluke za poduzimanje daljnjih analiza. Pri navedenom procesu također se moraju uzeti u obzir ciljevi organizacije, stavovi sudionika i opseg i cilj procesa upravljanja rizicima.

Uobičajena je praksa da se odluke donose na razini rizika, ali se istovremeno u njih mogu integrirati i posljedice, vjerojatnost događaja te sveukupni učinak niza događaja koji se mogu pojaviti istovremeno (ENISA, 2006).

## 3.2. Upravljanje rizikom

Upravljanje rizikom predstavlja proces odlučivanja o tome što će se točno učiniti vezano uz rizik koji se pojavio. Proučavaju se sve moguće opcije kako bi se pod kontrolom održali vjerojatnost gubitka, vrijeme koje je potrebno da do gubitka dođe i obujam gubitka. U tome procesu uvijek postoji nekoliko mogućnosti između kojih je moguće izabrati što će se dalje učiniti, a to su: da se ne učini ništa, da se uključi sudionike koji se inače bave upravljanjem rizikom, da se javno objavi postojeći rizik ili čekanje da se pojavi više informacija. Obično se donosi ona odluka za koju je najvjerojatnije da će pozitivno utjecati na smanjenje rizika.

Najčešće se postavlja pitanje što se sve može učiniti u vezi s rizikom i što će svaka od ponuđenih opcija donijeti? Uglavnom se proces upravljanja rizikom započinje utvrđivanjem svih mogućih opcija istovremeno evaluirajući širi raspon informacija, kao što su ekonomski troškovi, tehnička izvodljivost, društvena prihvatljivost, sukladnost sa zakonom, regulatorni ciljevi te provedivost. Nije jednostavno upravljati tolikom količinom informacija, pogotovo onda kada su te informacije nepouzdane ili nepotpune, što nije rijedak slučaj.

Za rješavanje toga nimalo lakog zadatka postoji mnoštvo alata koji mogu poslužiti u tu svrhu. Primjer jednoga od takvih alata je analiza odluka (engl. *decision analysis*), jedan od tradicionalnih postupaka primjene znanstvenih principa u poslovnom upravljanju što dovodi do osiguravanja kvantitativne osnove za složenije odluke. Uz pomoć spomenutog alata moguće je održavati u ravnoteži rizike više eventualnih opcija. Još jedan od iskoristivih alata je i analiza ekonomskih troškova i koristi svake od opcija, a upotrebljava se za odabir one opcije od koje će se imati najviše koristi s najmanjom mogućnošću rizika. Zapravo, u svrhu što jednostavnijeg dolaska do konačne odluke može se koristiti bilo koji od sljedećih pristupa: rizik-rizik, trošak-korist, rizik-korist. U praksi se može dogoditi da brojna ograničenja mogu smanjiti mogućnost potpunog istraživanja. Neka od takvih ograničenja su: manjak vremena, zakonska ograničenja te nedostatak podataka i financijskih mogućnosti (Byrd; Cothern, 2005).

## 3.3. Komunikacija rizika

Komunikacija rizika definirana je kao proces objašnjavanja rizika. Kako bi se informacija uspješno razmjenila, potrebno je da osoba zadužena za komuniciranje rizika, za početak, razumije prirodu rizika, procjenu i upravljanje rizikom. Ta osoba, isto tako, mora znati koga će angažirati u tom procesu, na koji način i kada, kao i koje je informacije potrebno razmijeniti i kako to učiniti. Najčešće je ciljani način komunikacije rizika otvoren i dvosmjeran kako bi se omogućilo i osobama koje nisu uključene u proces analize rizika da razumiju procjenu rizika i prihvate predložene odluke (Byrd; Cothern, 2005).

## 3.4. Politika rizika

Politika rizika, kao moguća četvrta komponenta analize rizika bavi se pitanjima poput smjernica za procjenu rizika, koje su često različite za različite tipove rizika. Byrd i Cothern (2005) navode kako se ne slažu s takvom podjelom već smatraju da je ta „četvrta komponenta“ sama po sebi ugrađena u prve tri komponente i da ju nije potrebno posebno izdvajati.

## 3.5. Koristi od analize rizika

Već je navedeno kako analiza rizika može na razne načine pomoći u poboljšavanju sigurnosti onoga za što uopće koristimo taj postupak. Ovisno o vrsti i opsegu analize rizika, njene rezultate moguće je upotrijebiti za pomoć u: identifikaciji, ocjenjivanju i usporedbi ukupnog utjecaja rizika na finalni produkt, u kontekstu financijskih i organizacijskih utjecaja; identifikaciji nedostataka u sigurnosti i određenju sljedećih koraka za uklanjanje slabosti i jačanje sigurnosti; poboljšanju komunikacije i procesa donošenja odluka u kontekstu sigurnosti informacija; poboljšanju sigurnosne politike i postupaka te razvoju financijski povoljne metode za provedbu tih politika i postupaka sigurnosti informacija; uspostavi sigurnosne kontrole za minimiziranje težih rizika;

povećanju svijesti sudionika o mjerama sigurnosti i rizicima uz pomoć isticanja najboljih i najučinkovitijih praksi tijekom procesa analize rizika; razumijevanju financijske štete koju mogu donijeti potencijalni sigurnosni rizici (Rouse, 2018).

# 4. Informacijske tehnologije i sustavi

Za razumijevanje suvremenih informacijskih tehnologija i sustava potrebno je razumjeti i digitalnu kulturu općenito, kao i poznavati početke te neke od prekretnica koje su obilježile pojedino razdoblje u povijesti digitalne kulture. Charlie Gere (2008) dijeli razvoj digitalne kulture na određene etape: početci digitalne kulture, kibernetička era, digitalna avangarda, digitalna kontrakultura, digitalni otpori i digitalna kultura 21. stoljeća. Neke od etapa se u vremenskom intervalu preklapaju, ali prikazuju različite karateristike istog vremenskog perioda, tj. promatra ih se iz različite perspektive.

## 4.1.Povijest digitalne kulture

### *4.1.1. Početci digitalne kulture*

Prema Gereu (2008) na najbližem tragu digitalnog doba bio je Alan Turing 1920-ih, 1930-ih i 1940-ih sa svojim strojem, koji je, iako je ostao samo u nacrtima, uvelike pridonijeo nastanku prvih modernih elektroničkih binarnih digitalnih računala. Najveća važnost Turingova stroja leži u time što je on u realizaciji trebao biti unverzalan stroj. Iako su se i prije njegove pojavljivale slične ideje (npr. diferencijalni stroj Charlesa Babbagea), on je ipak bio prvi koji je začeo ideju univerzalnog stroja na primjeru pisaće mašine, koja se pojavila krajem 19. stoljeća, kada je postojala ogromna potreba za mehanizacijom raznoraznih procesa koje su do tada mogli obavljati isključivo ljudi.

Za daljnji razvoj informacijske tehnologije, osnovu je postavio matematičar George Boole sa svojim formuliranjem simboličke logike. Njegova simbolička logika imala je izrazit utjecaj na kasniju generaciju logičara i matematičara, te je samim time neizravno pridonijela koncepciji modernog digitalnog računala. U direktnijem smislu, Booleova logika pridonijela je razvoju binarnih sustava za prebacivanje telefonskih centrala prije Drugog svjetskog rata, a nakon toga, i izgradnji logičkih sklopova. I izumi prije

Turingova, poput telegrafa, fotoaparata, stroja za tabeliranje, utjecali su na ono što će se uskoro nazvati digitalnim dobom, upravo zbog svoje sposobnosti prijenosa informacija jer je u to vrijeme zbog industrijalizacije to bilo prijeko potrebno.

1930-ih godina javljaju se prva digitalna i elektronička računala u Njemačkoj 1938. Z1 (Konrad Zuse), u Americi 1939. ABC (Atanasoff-Berry Computer) itd. Tijekom drugog svjetskog rata došlo je do razvoja kriptografije i kriptoanalize, no problem kod takvih sustava je bio taj što su sadržavali papir na kojemu su pisali podatci i svatko ih je mogao pročitati, a postojalo je htijenje da ti podatci budu pohranjeni unutar stroja. To je dovelo do pojave prvog digitalnog računala Manchester Mk1, koje je spremalo podatke pomoću katodnih cijevi. Godine 1945. Pojavljuje se elektroničko računalo ENIAC, ogromno, skupo, za pojmove onog vremena brzo, ali s gotovo nepostojećom memorijom. Gere (2008) tvrdi da je upravo pojava Manchestera Mk1 i ENIAC-a označila početak digitalnoga doba. To su prva računala u suvremenom smislu riječi: digitalni binarni strojevi sposobni pohraniti podatke i rješavati različite zadatke.

### *4.1.2. Kibernetička era*

Kibernetička era počinje otprilike krajem drugog svjetskog rata koji osim što je bio katalizator za izum modernog binarnog digitalnog elektroničkog računala, bio je to i za razvoj niza značajnih i utjecajnih smjerova, uključujući i kibernetiku, informacijsku teoriju, teoriju općih sustava, molekularnu biologiju, umjetnu inteligenciju i strukturalizam. Iako dolaze iz različitih konteksta, svi ti smjerovi bave se razvijanjem i implementacijom apstraktnih i formaliziranih sustava, kako bi se potpuno razumjele pojave s kojima se bave. U to vrijeme pojavljuje se sintagma „informacijska teorija“, a postavio ju je američki inženjer elektrotehnike Claude Shannon. Njemu i njegovim teorijama i koncepciji informacija dugujemo ideju informacijske tehnologije, a samim time i informacijskog društva.

Još jedan od tadašnjih ključnih znanstvenika bio je i Norbert Wiener, jedan od prvih postavljača opće teorijske osnove kibernetike. Kibernetika je donijela mnogo razmišljanja o informacijama, kao i elemente iz niza drugih disciplina i područja interesa. Gotovo

istovremeni razvoj kibernetike i teorije informacija također je potaknuo pojavu drugih sličnih ideja. Na dublji razvoj kibernetike utjecala su i otkrića u polju molekularne biologije, pogotovo u istraživanju DNK, koja su poslužila istraživačima iz polja kibernetike da razumiju informacijsku prirodu DNK operacija.

U međuvremenu računala su doprinijela razvoju novih spoznaja o svijesti i inteligenciji. 1948. godine Alan Turing objavio je izvještaj u kojem je sugerirao da će u ne tako dalekoj budućnosti računala posjedovati inteligenciju. Za dokazivanje inteligencije računala predložio je test kojim bi se utvrdilo je li računalo doista postiglo takvu inteligenciju. Taj test zove se "Turingov test", a uključuje osobu procjenitelja koja pomoću stroja komunicira prirodnim jezikom s jednim čovjekom i jednim strojem, a pri toj komunikaciji i čovjek i stroj predstavljaju se ljudima. Ako osoba procjenitelj ne može sa sigurnošću potvrditi koji je sugovornik stroj, tada se smatra da je stroj prošao test. Turingova ideja predstavlja konceptualnu osnovu onoga što je kasnije postalo poznato kao umjetna inteligencija (engl. *artificial intelligence*, akronim AI).

Znanstvenici Newell i Simon, zajedno s programerom Shawom, surađivali su na izgradnji programa za dokazivanje logičkih teorema, Newell-Simon-Shaw logičkog teoretičara (engl. *logic theorist*), koji je dovršen 1952. godine. Pojam umjetne inteligencije tada još nije postojao već je zapravo nastao 1956. godine kada je matematičar iz Dartmoutha, John McCarthy, organizirao konferenciju pod nazivom "Ljetni istraživački projekt o umjetnoj inteligenciji" (engl. *The Summer Research Project on Artificial Intelligence*). Danas se ta konferencija naziva "Dartmouthska konferencija" i smatra se početkom pojma umjetne inteligencije. Značajna je i zbog toga što je predstavljala zamjetan pomak od dotadašnjih razmišljanja o utjelovljenim, kibernetskim modelima strojnih misli, do bestjelesnih, logičkih, formaliziranih sustava.

Nakon drugog svjetskog rata nastavlja se „hladni rat“, a zahtjevi toga rata pružili su mnogo potpore istraživanju računalnih i informacijskih tehnologija, kao i idejama kao što su kibernetika i druge teorije sustava. Vrlo brzo počela se javljati i potreba za „mrežom“ koja će omogućiti brzi prijenos informacija. Šezdesetih godina 20. stoljeća radilo se na toj ideji, koja je izvorno bila ideja Paula Barana, s ciljem razmatranja izvedivosti izgradnje komunikacijskog sustava uz pomoć računala i uključivanja ideje „komutacije

paketa“ - slanja računalnih podataka u malim dijelovima koji će se ponovno sastaviti na njihovoj destinaciji. U jesen 1969. godine uspješno su povezana četiri računala, poznata kao procesori sučelja poruka (engl. *Interface Message Processors,* akronim IMP), na UCLA-u, Stanfordu, Sveučilištu u Kaliforniji Santa Barbara i Sveučilištu Utah. Ta mala mreža, nazvana ARPANET, predstavljala je osnovu za razvoj Interneta.

U 25 godina od završetka rata do 1970. godine računala su se razvila od ogromnih, glomaznih i skupih strojeva, koji zahtijevaju visoko specijalizirano znanje za upravljanje njima, do nečega što je blisko strojevima koje danas poznajemo. Razvoj grafičkih računalnih i digitalnih mreža, u velikoj mjeri potaknut potrebama Hladnog rata, u potpunosti je transformirao računalstvo i postavio temelje za budući razvoj.

### *4.1.3. Digitalna avangarda*

Digitalna avangarda je razdoblje gdje razni umjetnici, ponukani razvojem tehnologije, u realizaciji svoje umjetnosti žele koristiti spomenute novonastale tehnologije kako bi ponudili nešto suvremeno. Rad tih umjetnika odražavao je zabrinutost svijeta u kojemu su informacijska i komunikacijska tehnologija i srodni koncepti postajali sve važniji. To je uključivalo istraživanje pitanja interaktivnosti, multimedije, umrežavanja, telekomunikacija, informacija i apstrakcije, te korištenje kombinatornih i generativnih tehnika. Takav je rad bio od velike važnosti u poslijeratnoj umjetničkoj sceni i presudno je odredio ne samo oblik aktualne umjetničke prakse u odnosu na digitalnu tehnologiju, već i općeniti razvoj digitalnih medija.

U isto vrijeme kada su umjetnici počeli eksperimentirati s mogućnostima tehnologije, pisci poput Marshalla McLuhana razmatrali su njezine učinke i mogućnosti, McLuhan je specifično promatrao transformativnu moć medijskih tehnologija. Krajem 1960-ih računala su se također koristila u avangardnoj umjetničkoj praksi, najčešće kao vizualni medij. Neki projekti zahtijevali su razvoj grafičkih sučelja, a krajem 1950-ih mogućnosti računala kao vizualnog medija počele su se koristiti u različitim područjima. Godine 1957. u Nacionalnom birou za standarde (engl. *National Bureau of Standards*) proizvedena je prva obrađena fotografija, a 1958. godine John Whitney Sr. počeo je

koristiti analogno računalo za snimanje. Krajem pedesetih i početkom šezdesetih godina 20. stoljeća u Bell Labsu, Edward Zajac eksperimentirao je s računalno generiranim filmom kako bi vizualizirao podatke, a A. Michael Noll je počeo proizvoditi kompjuterski generirane Mondrianove slike, koristeći algoritamske metode za izradu slika. U međuvremenu, Charles Csuri izrađivao je svoja prva kompjuterski izrađena djela, koristeći slične tehnike.

Tijekom sljedećih nekoliko godina raširila se računalna umjetnost. Na kraju 1950-ih Ivan Sutherland proizveo je svoj softver Sketchpad. Godine 1960. William Fetter ustanovio je izraz "kompjuterska grafika". U ranim šezdesetima pojavljuje se prva video igra Spacewar, koju su razvili Steve Russell i njegovi kolege s MIT-a. Krajem šezdesetih godina započinje zatišje u širokoj primjeni kibernetike u suvremenoj umjetnosti, kao i za pokušaje korištenja računala kao umjetničkog medija, barem do 1990-ih, kada su Internet i World Wide Web ponudili nove mogućnosti za digitalnu umjetnost. To, dakako, ne znači da je umjetnost pod utjecajem kibernetike ili uz pomoć računala prestala postojati. Naprotiv, tijekom sedamdesetih i osamdesetih godina 20. stoljeća niz umjetnika nastavio je raditi u tom smjeru, koristeći video ili svakojake mogućnosti digitalne manipulacije.

Sedamdesetih i osamdesetih godina dvadesetog stoljeća dogodili su se izvanredni pomaci u širenju mogućnosti digitalne tehnologije. Do tog su razdoblja već u velikoj mjeri bili razvijeni umrežavanje, interaktivnost i multimedija. Velik dio toga razvoja bio je pod izravnim utjecajem umjetničke prakse. Na taj način kibernetičko razmišljanje i praksa postali su dio svakodnevnog života, putem video igara, kompjuterske multimedije, Interneta i, kasnije, World Wide Weba. Razvoj World Wide Weba devedesetih godina 20. stoljeća doveo je do cvjetanja umjetnosti i asimilaciji s novim medijima i tehnologijom. Lakoća izrade web stranica u kombinaciji s dostupnošću weba široj masi ljudi učinila ga je iznimno atraktivnim za umjetnike.

### *4.1.4. Digitalna kontrakultura*

Digitalna kontrakultura javlja se između kasnih 1960-ih i sredine 1970-ih godina kada se pomoću tehnoloških sredstava razvilo postindustrijsko informacijsko društvo,

ponajprije istovremenim pojavljivanjem miniračunala i umreženog računalstva, a nakon toga i pojavom i razvojem osobnog računala. Inženjer tvrtke Bell Labs William Shockley 1950. godine je u gradu Palo Alto osnovao tvrtku koja će iskoristiti izum tranzistora, koji je izumljen ubrzo nakon rata. Tranzistor je bio manjih dimenzija i trošio mnogo manje struje pa je ubrzo postao sastavni dio radija, televizora, a krajem 1950-ih i računala. Znanstvenici iz Silikonske doline u ovom su razdoblju nastavili raditi na smanjanju dimenzija računala s ciljem razvoja osobnog računala koje će biti dostupno svima. Istovremeno dok je društvo u globalu stvaralo svoju kontrakulturu, računalni svijet je razvio svoju. Ta kontrakultura poznata je kao „hakiranje“. Hakiranje se razvilo u računalnim laboratorijima na MIT-u.

Početkom 1975. godine tvrtka za elektroniku MITS, ponudila je u prodaju računalo na naslovnici časopisa „Popular Electronics“. Bila je riječ o stroju u dijelovima, kojega je bilo teško uopće sastaviti, a kada je sastavljen, nije bio od neke koristi. Mogao se programirati pomicanjem prekidača, ali budući da nije imao nikakav izlazni uređaj, jedini vidljivi dokaz operacije bio je niz svjetala koja trepere na prednjoj strani. To računalo zvalo se „Altair“, a iako nije imalo zamjetne performanse, sama ideja posjedovanja ikakvog računala zaintrigrala je velik broj računalnih entuzijasta.

1976. godine inženjer Steve Wozniak dizajnirao je prvo Apple računalo, imena Apple I, a promovirao ga je njegov prijatelj Steve Jobs. To računalo bila je ploča napunjena čipovima. No, zahvaljujući Wozniakovim programerskim i hardverskim vještinama, ta ploča prepoznata je kao vrhunski hardver, koji kada se priključi na tipkovnicu i TV monitor, dopušta korisniku da postigne ono što se do tada činilo nedostižnim, grafički prikaz. Sljedeće računalo, Apple II, bilo je daleko sofisticiranije, a uključivalo je i inačicu BASIC programskog jezika i mogućnost ispisa grafike u boji, sve u elegantnom kućištu. Iako je još uvijek moralo biti priključeno na televizor, to je očito bilo potpuno računalo koje funkcionira.

Uspjeh Applea poslužio je tvrtci IBM kao vjetar u leđa za razvoj njihovog osobnog računala, budući da je tvrtka Apple predstavljala prijetnju koja bi mogla srušiti njihovu dominaciju u računalnoj industriji. Godine 1981. proizveli su vlastito osobno računalo, IBM PC. Za to vrijeme u Apple-u se radilo na računalu koje će imati vlastito sučelje pa

su nakon Apple III i Lise napokon izbacili Macintosh koji je imao bitmap grafiku, grafičko korisničko sučelje, jednostavnu interakciju i elegantan izgled. Time je bio definiran oblik i izgled osobnog računala. Gotovo odmah nakon pojave Macintosha, Microsoft je proizveo novi operativni sustav Windows, koji je radio na većini IBM i osobnih računala kompatibilnih s IBM-om. Potencijal koji je ponudilo takvo sučelje, imena WIMP (prozori, ikone, miš, pokazivač) doveo je do infiltracije računala u mnoga nova ili nedovoljno istražena područja, uključujući grafički dizajn, tisak i izdavaštvo, proizvodnju zvuka, manipulaciju slikama i produkciju, kao i širenje tradicionalnog odnosa s poslovanjem. Isto tako to je sučelje približilo multimediju i hipertekst, tj. hipermediju komercijalnim programerima i javnosti. Tome je pripomogao i izum kompaktnog diska, koji je, iako je bio namijenjen pohrani glazbe, mogao jednako dobro pohraniti i druge vrste digitalnih podataka. Poznatiji kao CD-ROM, kompaktni disk postao je platforma na kojoj se mogu pohranjivati podatci i pristupiti igrama i drugoj multimediji.

Ono na čemu se dalje radilo je razvoj niza "protokola" za prijenos podataka preko mreža, počevši od "Ethernet-a", kojeg je razvio Bob Metcalfe 1974. godine. To je postao standardni protokol za povezivanje lokalnih mreža. Slijedio ga je „Transmission Control Protocol/Internet Protocol“ (TCP/IP), kojeg je razvio Bob Kahn, a koristio se za udaljene mreže te je univerzalno prihvaćen 1983. godine.

### *4.1.5. Digitalni otpori*

Ono što je za ovaj smjer razdoblja 1970-ih i 1980-ih karakteristično je korištenje novih tehnologija u svrhu stvaranja glazbe, pa je tako nastao žanr techno. Ono što je uzelo još većeg maha tada su video igrice. Nolan Bushnell, student inženjerstva pokušao je razviti vlastitu verziju arkadnih igrica. U tu svrhu pokrenuo je jednu od prvih tvrtki za izradu računalnih igara, Atari. Implementirao je igricu „Pong“, prvu računalnu igru koja je doživjela veliki prodajni uspjeh. Njezin je pozitivan prijem doveo do razvoja sličnih igara suparničkih tvrtki i započeo je razvoj industrije računalnih igara. Za ovaj aspekt navedenog razdoblja važno je spomenuti i to da je bavljenje tehnologijom u popularnoj

kulturi, umjetnosti, medijima i knjigama postalo potpuno uobičajeno. Sve to je dovelo do pojave „hakera“, u današnjem smislu te riječi, koji su zbog svojih djela bivali zakonski gonjeni pa se tako tijekom kasnih 1980-ih i 1990-ih vodila bitka između autoriteta i „hakera“.

### *4.1.6. Digitalna kultura 21. stoljeća*

Početak 21. stoljeća donio je blogove, čiju je pojavu medijski teoretičar Brian McNair opisao kao „kulturni kaos“. Za McNaira je činjenica da bilo tko, ili barem bilo tko s pristupom pravim tehnologijama, može pisati blogove znači kraj onoga što on opisuje kao „kontrolna paradigma“, u kojoj mediji pomažu održavanju društvenog poretka kroz širenje dominantnih ideja i vrijednosti istodobno služeći interesu onih koji kontroliraju. Na webu danas ima bezbroj blogova, ne samo zbog toga što je postavljanje jednog izrazito jednostavno, već je i uglavnom besplatno.

Blogovi se često navode kao jedan od glavnih fenomena „Web-a 2.0“, ime koje je dano koncepciji World Wide Weba kao prostora koji se koristi za suradnju i međusobnu komunikaciju. Toj skupini pripadaju i „društvene mreže“ kao što su Instagram, Snapchat, Facebook i Twitter; „peer-to-peer“ softveri kao što je BitTorrent za dijeljenje digitalnih glazbenih i video datoteka; tražilice, od kojih je najpoznatiji Google; sve oblike javne rasprave i samoizražavanja, poput blogova, podcasta, foruma i sl.; i oblike organiziranja i distribucije znanja, kao što je Wikipedija.

Transformacije medija koje donosi razvoj tehnologije mijenjaju način na koji ljudi razmišljaju o sebi. Ljudi više nisu isključivo pasivni potrošači medija, već su sve više i više aktivni producenti. Razvoj novih medija utječe na opstanak starijih medija, pa tako svakim danom neki mediji sve više zastarijevaju jer bivaju zamijenjeni novim i tehnološki naprednijim medijima.

Ono što se još pojavilo u prvome desetljeću 21. stoljeća je ideja da informacijske i komunikacijske tehnologije nude mogućnost neke vrste organizacije odozdo prema gore, koja može, barem djelomično, mijenjati hijerarhiju autoriteta. Najpoznatija takva tehnologija je Wiki. Wikiji su mjesta na webu koja korisnici mogu uređivati, a

Wikipedija je najpoznatiji primjer wikija, online enciklopedija u koju svatko može nešto dodati ili nešto urediti. Ideja da bi proces ove vrste trebao biti otvoren svima također se nalazi u jednom od najvažnijih koncepata koji su se pojavili iz pojave novih medija, a to je „otvoreni izvor“ (engl. *open source*). Kod „otvorenog izvora“ polazi se od ideje da je najučinkovitiji način da se proizvede dobra, učinkovita programska podrška (engl. *software*) taj da izvorni kod bude dostupan svima da ga nadopunjuju, uređuju i distribuiraju.

Pojavom RFID-a (engl. *Radio Frequency Identification*), tehnologije za automatsko slanje podataka iz objekata koji sadrže oznake, počelo se razmišljati i o „Internetu stvari“ (engl. *Internet of things*). „Internet stvari“ odnosi se na umrežene i međusobno povezane uređaje koji mogu komunicirati jedni s drugima i s drugim sustavima i entitetima.

Ono što se trenutno događa u digitalnoj kulturi su promjene koje utječu na svaki aspekt ljudskih života, a koje je sve teže i teže uočiti uočiti jer ih je sve lakše shvatiti pa čak i uzimati zdravo za gotovo jer polako sve postaje zamislivo i moguće. Čovječanstvo brzim korakom stiže do točke u kojoj digitalne tehnologije više nisu samo alati, već aktivni sudionici kulture čovječanstva. Ono o čemu se razmišlja, a potrebno je o tome i sve više razmišljati, su rizici koje takav način života već sad donosi, a i o tome koliko će ih još biti u budućnosti (Gere, 2008).

## 4.2.Definicija i povijesni razvoj informacijske tehnologije

Prema definiciji iz Technopedije **informacijska tehnologija** (IT) je poslovni sektor koji se bavi računalstvom, što pokriva hardver, softver, telekomunikacije i općenito sve ono što je uključeno u prijenos informacija ili sustava koji olakšavaju komunikaciju.

Informacijska tehnologija je širok pojam koji uključuje mnogo različitih stvari. Ako za primjer uzmemo IT odjel neke tvrtke, možemo vidjeti kako na tom mjestu postoji mnogo ljudi koji obavljaju velik broj raznih poslova i imaju različite odgovornosti. Te se odgovornosti kreću od nadzora i čuvanja sustava i podataka pa do održavanja mreže i njenog rada. U tom jednom odjelu postoje ljudi koji unose podatke, ljudi koji upravljaju bazama podataka i ljudi koji programiraju. Osim navedenih, tu su i donositelji odluka,

poput glavnih informatičara (CIO), koji, između ostalog, odlučuju kako će IT odjel raditi i funkcionirati te koje će komponente za nadogradnju biti kupljene i implementirane.

Informacijska tehnologija također uključuje upravljanje podacima, bilo u obliku teksta, glasa, slike, zvuka ili nekog drugog oblika. Može uključivati i stvari povezane s internetom, no to IT-u ipak daje potpuno novo značenje, budući da je Internet područje za sebe. Budući da IT uključuje prijenos podataka, ima smisla da Internet bude dio IT-a. Informacijske tehnologije su postale dio ljudskog svakodnevnog života i nastavljaju se širiti u nova područja (Technopedia).

Prema definiciji iz encklopedije Leksikografskog zavoda Miroslav Krleža **informacijska i komunikacijska tehnologija** se promatraju zajedno, a predstavljaju djelatnost i opremu koja čini tehničku bazu za sustavno prikupljanje, pohranjivanje, obradbu, širenje i razmjenu informacija koje se pojavljuju u različitim oblicima, npr. znakovnim, tekstualnim, zvukovnim i slikovnim.

Začetkom informacijske i komunikacijske tehnologije smatra se izum tiskarskoga stroja, no ipak se njezini pravi početci događaju otkrićem telegrafa, telefona, filma, radija i televizije u prvoj polovici 20. stoljeća. Svi ti mediji kompletno su promijenili način međuljudske komunikacije. Najveći procvat informacijske i komunikacijske tehnologije dogodio se nakon 2. svjetskog rata kada su u javnost izbačena računala koja su do tog trenutka bila čuvana vojna tajna. Sve to je početkom 1950-ih godina dovelo do pojave prvih računala na tržištu i u skladu s time do munjevitog razvoja računalstva. Otprilike u isto to vrijeme izumljen je i tranzistor. Jedno otkriće vodilo je drugome pa je daljnjim razvojem poluvodičke tehnologije nastala nova tehnička grana mikroelektronike. Ni razvoj područja telekomunikacija nije zaostajao za razvojem mikroelektronike i računalne tehnologije. U samome početku to su bile jednostavne telefonske centrale povezane žičnim vezama. Iz toga su se razvili današnji složeni sustavi za prijenos informacija. Svakim danom čovječanstvo svjedoči ekstremnom razvoju tehnologije pa stoga nije ni čudno da su donedavno izolirana računala danas uglavnom međusobno povezana u jedinstvenu računalnu mrežu, odnosno internet, preko koje se izrazito brzo mogu razmjenjivati informacije, tekst, slike, zvuk i ostalo. Za nastalu kombinaciju mikroelektronike, računalne tehnologije i telekomunikacija počeo se koristiti naziv

informacijska tehnologija (akronim IT), a u novije vrijeme naziv informacijska i komunikacijska tehnologija (engl. *Information and Communications Technology*, akronim ICT).

U današnje vrijeme informacijska i komunikacijska tehnologija nužna je za suvremeno funkcioniranje gotovo svake grane gospodarstva te se koristi u svim gospodarskim najvažnijim dijelovima, a to su razna istraživanja, razvoj, projektiranje, proizvodnja, administracija i marketing. Stupanj informatizacije, odnosno primjena informacijske i komunikacijske tehnologije, jedno je od najvažnijih mjerila razvijenosti zemalja. Sektor informacijske i komunikacijske tehnologije postao je jedna od glavnih gospodarskih grana gotovo svugdje u svijetu. Osim tehnološke revolucije, informacijska i komunikacijska tehnologija donijela je i promjene u društvu i životu svih njegovih sudionika (Enciklopedija Leksikografskog zavoda Miroslav Krleža).

Rastom interneta, čemu su ljudi svjedoci već i danas, a u budućnosti će biti još i više, mijenjat će se ljudsko shvaćanje većine životnih aspeketa. Rast i razvoj tehnologije nastaviti će uklanjati neke od starijih predrasuda i pepreka u ljudskoj komunikaciji i podići ljudski potencijal na neku novu razinu. Budući da se informacijske i komunikacijske tehnologije razvijaju gotovo nepojmljivom brzinom, danas gotovo većina svjetskog stanovništva ima pristup svim informacijama na svijetu pomoću jednog jedinog uređaja koji stane u dlan. Isto tako, smatra se da će do 2025. godine većina ljudi na Zemlji imati pristup internetu. Bežične internetske mreže će biti sveprisutne pa čak i u zemljama u razvoju u kojima ljudi dan danas ne posjeduju čak niti fiksne telefonske linije.

Jasno je da što više čovječanstvo usvaja nove tehnologije i alate, njihova se brzina i snaga povećavaju. To potkrepljuje i dobro poznati Mooreov zakon koji tvrdi da se brzina integriranih krugova za procesore udvostručuje svakih 18 mjeseci, što bi u praksi značilo da će računalo 2025. godine biti 64 puta brže nego što je bilo 2013. godine. Budući razvoj tehnologije predviđa raznorazne do prije nekog vremena nepojmljive pojmove kao što su automobili bez vozača, pokretanje i upravljanje robotima mislima, umjetnu inteligenciju i integriranu proširenu stvarnost, odnosno ljudsku trenutnu stvarnost prekrivenu slojem digitalnih informacija i sl.

Ono što se već događa u poslovnom svijetu zahvaljujući globalnom povezivanju, a nastavit će se događati i razvijati i dalje, je mijenjanje institucija iznutra i izvana. Već se rađaju pitanja zastarijevanja starih institucija i hijerarhija pa se planiraju strategije za njihovu prilagodbu novom tehnološkom dobu. Ono što će se nastaviti događati i razvijati je to da će ljudi sve češće komunicirati, povezivati se, surađivati, poslovati i razmjenjivati ideje s ljudima na drugim krajevima svijeta i iz potpuno različitih jezičnih skupina. Isto tako, globalno povezivanje dovest će organizacije i tvrtke do novih prilika i izazova. Nove razine odgovornosti koje se pojavljuju dovest će do prilagodbe planova budućnosti, što znači mijenjanje načina rada i predstavljanja javnosti. Sve veća uključenost u tehnologiju izjednačava pravo na informacije pa će doći i do otkrivanja novih konkurencija.

Još jedan tehnološki aspekt koji je u razvoju su virtualni identiteti koji su neizbježni za povezivanje putem interneta. Tragovi koje svaka osoba ostavlja na internetu tu ostaju zauvijek, a budući da sve objave, e-mailovi tekstualne poruke i bilo kakav način razmjene sadržaja putem interneta oblikuju identitete, ne samo osobe pošiljatelja, već i osobe primatelja, na snagu će u skorije vrijeme morati stupiti neki novi oblici zajedničke odgovornosti.

Izvjesno je da će računala i ljudi i u budućnosti surađivati i dijeliti zadatke. Ljudska inteligencija služit će za prosuđivanje, intuiciju, interakcije svojstvene samo ljudima. Računala će se upotrebljavati zbog svoje beskonačne memorije, beskrajno brzog procesiranja i postupaka koji su ograničeni ljudskim biološkim ustrojem. Nadalje, predviđa se da će virtualni svijet učiniti neke oblike ponašanja složenijima u smislu da će ljudima biti draži virtualni svijet, a državama stvarni, svakome onaj svijet u kojem ima veću kontrolu. Ta napetost će postojati sve dok postoji internet.

Iz toga proizlazi da će države morati provoditi dvije vanjske i dvije unutrašnje politike, odnosno po jednu za virtualni i stvarni svijet. Moglo bi doći i do toga da te politike budu naizgled proturječne, npr. predviđaju se kibernetički napadi od strane država na zemlje koje inače nikada ne bi napale vojnom silom. Na kraju, zbog širenja mobitela i povezanosti u svijetu, ljudi će imati više utjecaja nego ikada, međutim to će se odraziti na njihovu privatnost i sigurnost.

Ono o čemu je tu riječ je to da spomenuta tehnologija prikuplja i pohranjuje veliku količinu osobnih podataka koji bivaju pohranjeni na određeno vrijeme kako bi ih sustavi obrađivali. Pojavljuje se problem toga što do nedavno takvi podatci nikad nisu bili dostupni, a sada jesu i mogu biti upotrebljeni protiv osobe. Opasnost od objave takvih podataka raste i iako postoje tehnologije za zaštitu podataka, uvijek postoji mogućnost pogreške ili propusta, pa čak i puke ljudske zlobe. Daljnjim prolaskom vremena predviđa se da će biti sve teže sačuvati njihovu privatnost (Schmidt & Cohen, 2014).

## 4.3. Informacijski sustav i povijesni razvoj informacijskih sustava

Prema definiciji iz enciklopedije Leksikografskog zavoda Miroslav Krleža **informacijski sustav** je organizirani skup postupaka koji se koristi za prikupljanje, obradu, pohranu, pretraživanje i prikaz podataka i informacija koje su važne za neku organizaciju, ustanovu, društvo ili državu. Osnovne dijelove informacijskoga sustava čini osoblje obrazovano za rad u sustavu i, dakako, odgovarajuća oprema. Za izradu današnjih informacijskih sustava najčešće je potrebna pomoć suvremenih informacijskih i komunikacijskih tehnologija. Od većeg je značaja uporaba informacijskih sustava unutar poslovnih sustava, gdje se koriste za njihovo upravljanje i služe kao potpora izvođenju poslovnih procesa. Navedeni informacijski sustav ima i svoje osnovne komponente, a to su: sustav za obradbu transakcija, upravljački izvještajni sustav ili upravljački informacijski sustav, sustav za potporu odlučivanju i sustav uredskoga poslovanja. Podatci i informacije koji se nalaze unutar informacijskoga sustava u današnje se vrijeme uglavnom pohranjuju i čuvaju u bazama podataka.

Definicija **informacijskog sustava** koju nude Klasić i Klarin (2018) kaže kako je informacijski sustav dio svakog poslovnog sustava čiju funkciju čini neprekidna opskrba svih razina upravljanja, odlučivanja i svakodnevnog poslovanja potrebnim informacijama. Zbog toga što se informacijski sustav razvija za postojeći poslovni sustav, poslovni procesi toga sustava zapravo diktiraju modeliranje strukture informacijskog sustava. Sami zadatci informacijskog sustava su: prikupljanje, razvrstavanje, obrada, čuvanje, oblikovanje i raspoređivanje podataka svim radnim razinama poslovnog sustava.

Iako se u poduzećima danas uglavnom koriste računalni informacijski sustavi, za svrhu za koju oni zapravo služe, nije nužno da se oni koriste. Razvoj informacijskih sustava podijeljen je na četiri faze pa će se i tu primjetiti da itekako postoje informacijski sustavi za čije korištenje računalni sustavi nisu nužni.

Prva faza nosi naziv **faza ručne obrade podataka**, a njezine odlike su sporo obrađivanje podataka, korištenje ruku za taj proces, korištenje medija za pohranu podataka i dostupnih alata za pisanje po mediju za pohranu. Na ovakav način mogla se obraditi relativno mala količina podataka, a sam proces obrade nije bio pouzdan i nerijetko je bio upitne točnosti. Niža produktivnost zapravo se nadoknađivala većim brojem osoba koje su evidentirale podatke, a te osobe nazivaju se pisari. To zanimanje je bilo izrazito cijenjeno.

Faza koja je uslijedila je **mehanička faza obrade podataka** koja je nastala kao posljedica razvoja znanosti i tehnologije. Započela je sredinom 17. stoljeća nakon što su konstruirani prvi uređaji za pomoć u obradi podataka. Oni koji su najčešće izrađivali takve uređaje bili su uglavnom poznati matematičari i fizičari koji su živjeli i djelovali u tom vremenu (npr. Blaise Pascal i Gottfried Leibniz). Prvi mehanički pisaći stroj izumio je Henry Mill. Taj izum imao je zamjetan utjecaj i na razvoj informacijske znanosti, kao i na društvene odnose generalno. Za mehaničku fazu obrade podatake značajno je povećanje produktivnosti, količine obrađenih podataka i točnosti.

Sljedeća je faza **faza elektromehaničke obrade podataka**, a započinje u drugoj polovici 19. stoljeća nakon što je vlada SAD-a raspisala natječaj za konstrukciju uređaja koji bi bio zaslužan za obradu podataka popisa stanovništva u najkraćem mogućem vremenu. Na navedenom javnom natječaju pobjedio je Hermann Hollerith. On je predložio da nositelj podataka bude bušena kartica, a za obradu je sugerirao uporabu posebnog elektromehaničkog uređaja. To je omogućilo masovnu obradu velike količine podataka. Hermann Hollerith se u međuvremenu obogatio i osnovao vlastitu tvrtku, a iz njegove tvrtke se 1924. godine razvila tvrtha IBM (engl. *International Business Machines*).

**Faza elektroničke obrade podataka** posljednja je faza razvoja informacijskih sustava, a započinje 1944. godine kad je počeo razvoj ENIAC-a, prvog „pravog“

elektroničkog računala. Navedenu fazu karakterizira velika brzina obrade ogromne količine podataka s beznačajnom količinom pogrešaka. Pojava elektroničkog računala dovela je do mogućnosti trajne i privremene pohrane podataka, ali i do jednako važnoga povezivanja operacija nad podatcima. U operacije nad podatcima se ubrajaju obrada i prijenos podataka te integracija obrade teksta, slika, grafika i zvuka. U fazu elektroničke obrade podataka pripada i internet koji je najnoviji, ali zbog svojih nebrojenih funkcija, danas i sve raširenij način obrade podataka (Klasić & Klarin 2018).

## 4.4. Vrste informacijskih sustava

Postoji nekoliko kriterija za podjelu informacijskih sustava pa samim time postoje i različite podjele. Podjela koja je ovdje važna je **podjela prema primjeni informacijske tehnologije** jer ta primjena nije jednako značajna za različite poslovne sustave, čak i onda kada imaju implementirane sve informacijske podsustave. U skladu s time informacijski sustavi dijele se na četiri osnovna tipa: operativni, potporni, strateški i izgledni.

**Operativni informacijski sustavi** su sustavi koji su odgovorni za uspješnost tekućeg poslovanja. U navedenom slučaju samo funkcioniranje poduzeća izrazito ovisi o korištenoj informacijskoj tehnologiji zbog same namjene infomacijskog sustava, a ta namjena je potpora svakodnevnom poslu.

Drugi tip su **potporni informacijski sustavi** koji su korisni, ali nisu od kritične važnosti za poslovni uspjeh poduzeća. Kod navedenih sustava mala je razina ovisnosti funkcioniranja poduzeća o informacijskoj tehnologiji.

Sljedeći su tip **strateški informacijski sustavi** koji su od velike važnosti za buduće poslovne strategije i zbog toga moraju omogućiti pohranu i brzu obradu velike količine podataka. Kod strateškog informacijskog sustava za funkcioniranje poduzeća i poslovni rezultat poduzeća neophodno je korištenje informacijske tehnologije.

**Izgledni informacijski sustavi** su oni koji bi mogli utjecati na budući uspjeh u poslovanju. Ovisnost funkcioniranja poduzeća o informacijskoj tehnologiji nije velika, no utjecaj informatike na poslovni rezultat je velik.

Neovisno o tipu informacijskog sustava koji se koristi, u njemu se čuvaju podatci koji su nužni za daljnju obradu. Kvaliteta samog informacijskog sustava ovisi o kvaliteti tih podataka. Ipak, informacijski sustav dio je poslovnog sustava pa iz toga ishodi da o njegovoj kvaliteti ovisi čitavo poslovanje tvrtke. Iz toga slijedi da bez dobro definiranih podataka informacijski sustav ne može biti kvalitetan i dobro strukturiran, a samim time ne dolazi do rasta i razvoja poduzeća.

Postoje osnovna načela koja bi bilo potrebno da zadovoljava kvalitetan informacijski sustav, a ta načela su: informacijski sustav predstavlja model poslovne tehnologije organizacijskog sustava; resurs poslovnog sustava su podatci; poslovni procesi grade temelj razmatranja prilikom određivanja podsustava budući da su poslovni procesi nepromjenjivi dio svake poslovne tehnologije; informacijski sustav izgrađuje se integracijom podsustava, a osnova su zajednički podatci; za izvođenje informacija za upravljanje i odlučivanje temelj su zbivanja na razini izvođenja. Informacijski sustavi izgrađeni na navedenim načelima slika su poslovne tehnologije određenog poduzeća i u potpunosti zadovoljavaju svoju zadaću koja je prikupljanje, obrada, pohrana i distribucija podataka svakome kome je potrebno. Cilj je, naravno, unapređenje poslovanja i ostvarenje pozitivnih poslovnih rezultata (Klasić & Klarin 2018).

## 4.5.Faze razvoja informacijskog sustava

Podlogu za organizacijski razvoj poduzeća čini tehnološka razina informacijskog sustava, a istovremeno taj organizacijski razvoj utječe na tehnološku razinu informacijskog sustava. U nekim fazama informatika prethodi promjenama u organizaciji, a u drugima pak zaostaje za organizacijom. Kvalitetan informacijski sustav najviše će doći do izražaja ukoliko je komunikacijska razina poduzeća na razini. Postoji i druga strana, ako situacija nije takva, čak ni najbolja tehnička oprema, niti jedinstveni informacijski sustav, neće učiniti zamjetnu promjenu na bolje, a djelovat će kao opterećenje za poduzeće.

Informacijska razina poduzeća koja se tiče uporabe informacijske tehnologije definira se Nolanovom podjelom koja opisuje šest faza razvoja informacijskog sustava:

uvođenje (engl. *Initiation*), proširenje (engl. *Contagion*), upravljanje (engl. *Control*), povezivanje (engl. *Integration*), sređivanje (engl. *Data Administration*) i zrelost (engl. *Maturity*). Značajke svake od faza vidljive su u tablici 1.

*Tablica 1. Značajke pojedinih faza Nolanove podjele (Preuzeto iz: Klasić & Klarin, 2009:15)*

| FAZA | SKUP APLIKACIJA | ORGANIZACIJA OBRADE PODATAKA | PLANIRANJE I KONTROLA PODATAKA | ULOGA KORISNIKA |
|---|---|---|---|---|
| 1. Faza **Uvođenje** | Ograničene, pojedinačne aplikacije po poslovnim područjima | Učenje tehnologije obrade podataka | Slaba | Nema interesa |
| 2. Faza **Proširenje** | Nagli porast broja aplikacija | Korisnički orijentirani programi | Vrlo slaba | Površan interes |
| 3. Faza **Upravljanje** | Sređivanje dokumentacije i restrukturiranje postojećih aplikacija | Srednja razina upravljanja | Formalizacija planiranja i kontrole podataka | Neprihvaćanje odgovornosti za podatke |
| 4. Faza **Povezivanje** | Prilagodba postojećih aplikacija uporabom tehnologije baza podataka | Afirmiranje korisnosti računala i uvođenje korisnika u timove | Povezano planiranje i kontrola sustava | Odgovornost za podatke ovisi o pojedincu odnosno korisniku |
| 5. Faza **Sređivanje** | Organizacijska integracija aplikacija | Administracija podataka | Dijeljeni podaci i zajednički sustavi | Efektivna odgovornost korisnika |
| 6. Faza **Zrelost** | Integriranje informacijskih tokova kroz aplikacije | Upravljanje resursima podataka | Strategijsko planiranje resursa podataka | Prihvaćanje korištenja zajedničkih podataka i odgovornosti za njih |

Pretpostavka je da svaka faza obavezno slijedi iz prethodne. Preskakanje faza nije dozvoljeno budući da će samo poduzeće s prijašnjim iskustvom biti spremno iz prethodne faze prijeći na sljedeću. Isto tako, ukoliko nema eksperimentiranja, neće biti niti korisnika koji će potaknuti fazu proširenja informacijskog sustava. Iako slijed faza predstavlja svojevrsno ograničenje, faze je ipak moguće planirati, koordinirati ih i upravljati s njima u svrhu dobivanja što boljih rezultata.

Korištenje opisanog modela omogućuje i utvrđivanje organizacijske razine poduzeća koje za poslovanje koristi računalo. Utvrđivanje je vrlo jednostavno: što je viša faza razvoja informacijske tehnologije koja se koristi, viša je i sama organizacijska razina poduzeća. Kada su te informacije dostupne lakše je i planiranje daljnjeg razvoja

poduzeća. Navedene faze odnose se na idealan slučaj, bez utjecaja vanjskih čimbenika (npr. promjena generacije računala) (Klasić & Klarin 2018).

## 4.6. Zaštita informacijskog sustava

U informatičko/internetskoj tehnologiji rizikom se smatra opasnost da će se njezinim korištenjem pokrenuti šteta unutar organizacijskog sustava ili šteta u njegovoj okolini. Najčešće postoje dva razloga zbog kojih dolazi do zloupotrebljavanja tehnologije. Prvi razlog je realiziranje neopravdanih, neetičnih ili protupravnih koristi od strane pojedninca ili organizirane skupine. Drugi razlog je namjerno nanošenje materijalne ili nematerijalne štete pojedincu, skupini ili zajednici. Mađu najugroženije od ovakvih napada spadaju informacijski sustavi koji imaju pristup internetu budući da je i internet sam po sebi jako ugrožen.

Rizik od zloupotrebe je nemoguće u potpunosti ukloniti, no moguće ga je učiniti minimalnim. To se radi tako da se poduzmu opće preventivne mjere, kao što su zaštita podataka koji su pohranjeni na računalnim memorijskim medijima, zaštita privatnosti osobe, zaštita od prevara u poslu, zaštita od dobivanja velkog broja neželjenih poruka, zaštita tajnosti enkripcijskih i identifikacijskih ključeva i sl. Neophodne su redovite provjere programa koji se obrađuju, ne bi li se naišlo na računalni virus ili crv, a potrebno je i raditi na razvijanju sigurnosnih politika unutar tvrtki i obučiti djelatnike kako da se pridržavaju te politike.

Osim navedenih mjera prevencije potrebno je provoditi i fizičku zaštitu samog sustava, a ona se sastoji od: kontrole namjernog i nenamjernog ugrožavanja fizičke imovine informacijskog sustava, računala i druge opreme; kontrole zlonamjernog ugrožavanja logičke imovine informacijskog sustava (diskova, medija, podataka pohranjenih na računalu); provođenja mjera zaštite pristupa informacijskom sustavu kroz identifikaciju korisnika putem lozinke i provjeru autorizacije korisnika.

Definirane su tri razine organizacije sigurnosti i zaštite informacijskog sustava. Na prvoj razini uklanjaju se fizički rizici pomoću postupaka: kontrole fizičkog pristupa opremi i računalnim prostorijama; zaštite opreme i podataka od prirodnih nepogoda

(požari, potresi, poplave); osiguranja napajanja računala električnom energijom; zaštite od prljavštine, prašine i elektrostatičkog naboja; redovite izrade sigurnosnih kopija podataka.

Na drugoj razini uklanjaju se rizici zloupotrebe informacijskog sustava ili neovlaštenog pristupa podatcima. Takva vrsta zaštite oslanja se na fizičku i logičku identifikaciju korisnika (ključevi, lozinke i sl.) i dodatnim provjerama ovlasti u koracima obrade podataka. Zaštita podataka koji se čuvaju na računalnom magnetnom mediju provodi se na više načina, a ovisi o djelatnicima i načinu organizacije podataka. Spomenuti načini su: zaštita od neovlaštenog pristupa podatcima, njihova umnožavanja i krađe, a mogući napadač je zaposlenik tvrtke ili haker koji napada putem interneta (računalo nije dopušteno iznositi iz tvrtke bez da su prije s njega izbrisani poslovni podatci; prijenosne magnetne medije ne smije se prenositi bez da je prije provedena odgovarajuća zaštita pohranjenih podataka; potrebno je zaštititi i podatke koji se prenose komunikacijskim linijama); zaštita od neovlaštenog mijenjanja sadržaja podataka (korištenjem aplikacijskog programa zbog greške programera ili namjerno napravljenog zlćudnog koda; uporabom jezika baze podataka za izravno mijenjanje sadržaja baze); zaštita od neovlaštenog pristupa podatkovnim arhivama koji su locirani na magnetnom mediju (odlaganjem u vlastitoj arhivi, no to je često nepouzdano; odlaganjem u podzemnim bunkerima, zakopavanjem zapečaćenih kontejnera, odlaganjem u čuvanim prostorima u vodootpornim ormarima, što je također nepouzdano; brisanjem informacija jakim magnetnim poljem); zaštita od gubitka podataka ukoliko dođe do uništenja magnetnog medija (redovnom izradom sigurnosnih kopija podataka; izradom i redovnim ažuriranjem procedura za rekonstrukciju i oporavak podataka iz sačuvanih sigurnosnih kopija).

Treća razina najviše se odnosi na iznimno važne i podatke i informacije u sustavu koji su od velike vrijednosti. Usredotočena je na očuvanje njihove tajnosti i sigurnosti, a utemeljana je na kriptografskim metodama.

Planiranje zaštite informacijskog sustava dio je aktivnosti koje su vezane uz primjenu informacijske tehnologije u poslovnom sustavu. Prema tome, ISO organizacija organizirala je potkomitet broj 27 preko kojega nastaju norme za sigurnost

informacijskog sustava. Kroz vrijeme su se norma mijenjale, a danas su na snazi ISO 27001 i ISO 27002. Svrha tih normi je uspostavljanje organizacijske kontrole i upravljanja zaštitom i sigurnošću informacijskog sustava u sklopu poslovnog sustava. Uzimajući u obzir to da je svaki sustav specifičan, navedene norme nude preporuke, kao i neophodne elemente koje bi bilo poželjno slijediti kada se izrađuje i primjenjuje vlastiti model upravljanja sigurnošću. Isto tako, trebalo bi poštivati i standarde za uspostavu, primjenu, održavanje i unaprijeđivanje sustava upravljanja sigurnošću informacija (Klasić & Klarin 2018).

# 5. Analiza rizika u procesu razvoja informacijskih sustava i tehnologija

## 5.1. Analiza rizika u procesu razvoja informacijskih tehnologija

Za projekte unutar informacijske tehnologije (IT) poznato je da imaju visoku stopu neuspjeha. Upravljanje rizikom bitan je proces za uspješnu isporuku takvih projekata. Rizici u navedenim projektima mogu se definirati kao vjerojatnost da će se pojaviti događaj koji će imati negativan utjecaj na projekt, a mjeri se u odnosu vjerojatnosti i posljedica. Upravljanje rizicima u spomenutom slučaju sastoji se od sljedećih procesa: utvrđivanje konteksta, identifikacija rizika, analiza rizika, evaluacija rizika, tretiranje rizika, praćenje i preispitivanje rizika te praćenje i konzultacija rizika.

Samo tretiranje rizika zahtijeva korištenje prikladnih strategija koje su u skladu s preprekom koja se pojavljuje. Baccarini, Salm i Love (2004) tvrde da prema Zhiju (1994) postoje četiri najvažnije strategije za savladavanje rizika u IT projektima. Prva strategija je **izbjegavanje** (engl. *avoidance*), odnosno neodgovaranje na rizik koji se pojavljuje, tj. ne poduzima se nikakva aktivnost u vezi s rizikom. Sljedeća strategija je **ublažavanje** (engl. *reduction*), a podrazumijeva smanjenje vjerojatnosti pojave rizičnog događaja te samim time i utjecaja koji bi taj događaj mogao imati. Ublažavanje je najčešća strategija koja se koristi u tretiranju rizika. Treća strategija je **prijenos** (engl. *transfer*) što označava prijenos rizika u potpunosti ili djelomično na drugu stranku. Posljednja strategija je **zadržavanje** (engl. *retention*), tj. prihvaćanje rizika i njegovih posljedica.

Ono zbog čega projekti često bivaju neuspješni je slabo davanje pažnje rizicima unutar pojedinačnih projekata i narazumijevanje toga da je za različite projekte potrebno imati i različite tipove upravljanja rizikom. Tako je moguće da upravljanje rizikom unutar razvoja informacijskih tehnologija bude loše izvedeno, a moguće je i da se rizik previdi. Razlog tome je mogućnost negativnog tumačenja usredotočenosti na problem. Uglavnom, menadžerski tim najčešće želi usaditi pozitivan stav prema implementaciji

novih informacijskih tehnologija budući da one predstavljaju gibanje prema naprijed i unapređivanje poslovanja unutar organizacije (Baccarini, Salm & Love, 2004).

## 5.2.Rizici koji se pojavljuju u razvoju informacijskih tehnologija

Najčešće je identifikacija rizika zahtjevan izazov za menadžere organizacije, a tome je tako najviše zbog brojnih načina na koje može biti kategorizirana i opisana. Rizici se razlikuju po svojoj prirodi, ozbiljnosti i posljedicama koje donose. Najvažnije je prepoznati, razumjeti i tretirati one za koje se smatra da su visokorizični. Najčešći rizici mogu se svrstati u nekoliko kategorija.

Prva kategorija su **trgovinski i pravni odnosi**. U toj kategoriji rizici su: neodgovarajuća izvedba treće strane (odabrani poduzetnik nije adekvatna osoba za ispunjavanje svrhe projekta i ne može pružiti rješenje koje zadovoljava uvjete vremena, troškova, kvalitete i ciljeve izvedbe), spor o zaštiti intelektualnog vlasništva (neodgovarajuća zaštita programske podrške od početka projekta rezultirat će mogućnošću da će konkurencija kopirati projekt, a rezultat će biti vođenje skupih sudskih sporova i gubitak tržišnih potencijala), nesuglasice između klijenata i izvođača projekta (može postojati osobno neprijateljstvo između klijenata i onih koji izrađuju programsku podršku, a rezultat je nesporazuma, iznenadne izmjene ugovora, kašnjenje isporuke i sličnih razloga).

Drugu kategoriju rizika čine **ekonomske prilike**. Rizici koji ovdje pripadaju su: promjena tržišnih uvjeta (poslovnu dobit pri investiranju u informacijske tehnologije može ugroziti promjena potrošačkih i tržišnih uvjeta ili tehnološki napredak), štetne natjecateljske akcije (moguće je da konkurenti izrade brže rješenje programske podrške, s boljim funkcionalnostima i manjim financijskim troškovima te brzo plasiraju finalni produkt na isto tržište), programska podrška postaje nepotrebna (korištenje programske podrške prekida se prije no što je vrijeme za to zbog toga što njezina vrijednost ili utjecaj premašuje mogućnosti menadžmenta).

Sljedeća kategorija je **ljudsko ponašanje**, a u nju spadaju: nedostatak osoblja, nekvalitetno osoblje (zbog nedostatka spodobnosti, prakse, motivacije ili iskustva).

Sljedeća, četvrta kategorija, su **političke okolnosti**. Tu spadaju sljedeći rizici: kad korporativna kultura ne predstavlja podršku (korporativna kultura može biti nepovoljna zahvaljujući skrivenim namjerama, frakcijama unutar tvrtke, organizacijska kultura koja se stalno mijenja ili stalno postoji mogućnost promjene, a to sve rezultira slabom menadžerskom podrškom iz čega slijedi i neispunjavanje cilja), izostanak izvršne podrške (projekt ne doseže cilj zbog neusklađenosti menadžmenta), politički motivirana zbirka nepovezanih zahtjeva (zbog političkih motiva unutar organizacije, veliki broj nepovezanih zahtjeva grupira se u sveobuhvatni projekt s kojim je iznimno teško upravljati i postaviti mu ciljeve).

Petu kategoiju rizika čine **tehnološki i tehnički problemi**. Oni su: neodgovarajuća identifikacija korisnika, aplicirana programska podrška neprikladna je za ono čemu je namijenjena (korisnici ju mogu percipirati kao da im ne pomaže dovoljno u izvršavanju zadataka i samim time korisnici su nezadovoljni), slaba učinkovitost proizvodnog sustava (platforma programske podrške ne zadovoljava svrhu kojoj je namijenjena što rezultira time da se u proizvodnju stavlja sustav koji je odveć spor ili ima veće operacijske probleme), dosegnuta su ili premašena tehnička ograničenja (u razvoju programske podrške česta je pojava tehničkih ograničenja što rezultira vremenskim odgodama u projektu dok se ne pronađe rješenje, a može se dogoditi čak i to da se rješenje uopće ne pronađe, što na kraju rezultira otkazivanjem cijelog projekta ili započinjanjem ispočetka s održivijim tehničkim rješenjem), nepotpuni zahtjevi (dobivene nepotpune informacije u fazi analize rezultiraju konstrukcijom rješenja koja se ne podudaraju s projektnim ciljevima), neprikladno korisničko sučelje (razvijeno ili izabrano sučelje ne udovoljava zahtjevima korisnika).

Sljedeća, šesta kategorija su **aktivnosti upravljanja i kontrole**. U nju spadaju: nerazuman raspored i budžet projekta (nemoguće je doći do realizacije ciljeva projekta ako postoje nerealna ograničenja u budžetu, rasporedu, kvaliteti ili razini izvedbe), konstantne promjene zahtjeva klijenata (sudionici, uključujući korisnike, kroz proces razvoja pojekta stalno mijenjaju funkcionalnosti programske podrške), izostanak pristanka korisnika na testiranja (završetak projekta može biti odgođen zahvaljujući nejasnoćama u tome što bi trebala sadržavati finalna isporuka rješenja projekta),

izostanak pregleda dnevnog napretka (menadžer ne bilježi dnevni napredak isporuke što rezultira zastojima u razvoju projekta), izostanak jedinstvene točke odgovornosti (tipično je da veliki projekti razvoja programske podrške imaju više vođa timova, ali ne i jednu osobu odgovornu za isporuku, a rezultat toga su teškoće u ispunjavanju ciljeva projekta), loše vodstvo (projektni menadžer i/ili upravni odbor nije posvećen rješavanju problema i usmjeravanu projektnog tima), razvoj krive funkcionalnosti programske podrške (dizajn i konstrukcija programske podrške ne poklapa se sa svrhom za koju je namijenjena), izostanak formalnog procesa upravljanja promjenama (napredak projekta ometaju naprečac donesene promjene u specifikacijama sustava bez formalnog pregleda utjecaja na projekt).

Posljednju kategoriju rizika čine **individualne aktivnosti**, a to su: preveliko specificiranje (tim je usredotočen na analizu i generiranje velike količine detalja i time se odmiču od uspostavljenih ciljeva projekta), nerealna očekivanja (stavke koje su obećane da će se isporučiti mogu biti prodane za cijenu manju od njihove realne vrijednosti) (Baccarini, Salm & Love, 2004).

Budući da se u razvoju informacijske tehnologije može pojaviti više vrsta rizika, potrebno je njihovo pozicioniranje, odnosno rangiranje. To se radi tako da je, ukoliko se pojave, jednostavnije njima upravljati. Potrebno je definirati opcije tretiranja rizika kako bi se menadžeri lakše nosili s rizikom i kako on ne bi ugrozio performanse projekta. Postoje dva procesa unutar projekta, a to su: proces upravljanja projektom i proizvodni proces (Fadlallah, 2018).

## 5.3. Utjecaj razvoja informacijskih tehnologija na upravljanje rizikom

Evolucija informacijske tehnologije utjecala je na svaku domenu ljudskoga života, kao što su učenje, marketing, poslovanje, zabava i politika. Upravljanje rizikom jedna je od domena koja se našla pod snažnim utjecajem ove evolucije jer se uglavnom temelji na podatcima. Informacijska tehnologija iz dana u dan olakšava automatizaciju procesa, počevši od identifikacije rizika pa do završetka kontroliranja. Nove tehnologije koje se koriste, kao što su veliki podatci (engl. *Big Data*), analitika, mobilne aplikacije,

računarstvo u oblaku (engl. *cloud computing*), planiranje resursa poduzeća (engl. *enterprise resource planning*, akronim ERP) i sustavi upravljanja (engl. *governance*), rizika (engl. *risk*) i usklađenosti (engl. *compliance*) (akronim GRC), jako su važni u procesu upravljanja rizicima (Fadlallah, 2018).

Promjene u načinu pružanja i upravljanja uslugama koje pružaju suvremene informacijske tehnologije rezultirale su i značajnim promjenama u načinu na koji ljudi komuniciraju i koriste tehnologiju. Mogu ju upotrebljavati kao poslovni ljudi, kao potrošači i kao korisnici. Kako se visokorizične aktivnosti sve češće javljaju izvan granica djelovanja tradicionalnih kontrolnih okruženja, te će promjene dovesti do zastarijevanja pravilnika o načinima na koje uspješna poduzeća identificiraju rizike i upravljaju njima. Usklađenost sa standardima u funkciji informacijskih tehnologija možda više neće biti dovoljna za upravljanje rizicima u uslugama koje nude informacijske tehnologije, a postavlja se pitanje jesu li to uopće ikada i bili (Fraser, 2010).

Prema Fraser (2010) postoji nekoliko segmenata koje bi se trebalo uzeti u obzir kada se razmišlja o rizicima u današnjem tehnološkom i informacijskom okruženju. Prvo je to da tvrtke odgovaraju na potrebu za čuvanjem i upravljanjem brzorastućim količinama podataka tako da prepuštaju upravljanje podacima vanjskim suradnicima (engl. *outsourcing*), odnosno trećoj strani. Ipak, mora se pratiti koliko je kontrolirano upravljanje podacima koje obavlja dotična treća strana, pa čak i na onim mjestima na kojima su vanjski suradnici akreditirani, kao i količina razumijevanja koja postoji nad sigurnošću koju ta akreditacija eventualno pruža.

Drugo, budući da poduzeća sve više i više sudjeluju u zajedničkim ulaganjima i partnerstvima, proporcionalno raste i potreba za dijeljenjem i širenjem komercijalno osjetljivih podataka. Unatoč tome, mnoge organizacije trenutno ne uspijevaju identificirati i upravljati svojim osjetljivim podacima na odgovarajući način pa se postavlja pitanje, uzimajući navedeno u obzir, mogu li očekivati od svojih partnera da će to činiti.

Sljedeće se odnosi na interakciju ljudi s tehnologijom dok vanjske radnje nerijetko predstavljaju područje koje se uglavnom ne uzima u obzir kad se rizici registriraju. Na

primjer, to može biti rizik da će osoblje dijeliti osobne i potencijalno osjetljive informacije o tvrtki putem društvenih mreža. To, primjerice, može uključivati informacije na korisničkim računima mreže poduzeća koje se mogu upotrijebiti za ugrožavanje sigurnosti (kao npr. datum rođenja, ime supružnika, adresa stanovanja, datumi rođenja članova obitelji i sl.). Dilema koja se pojavljuje u navedenom primjeru postavlja pitanje kako upravljati kršenjima sigurnosti koja se odvijaju izvan radnog mjesta.

I posljednje, postoje enormne količine podataka koje se kroz vrijeme grade u korporativnim sustavima, a trenutno su na snazi i ogromne sposobnosti i mogućnosti poduzeća za iskorištavanjem navedenih podataka. Kvaliteta podataka je gotovo jednako važna kao i kvaliteta proizvoda. Trenutno je izvjesno da se neadekvatno iskorištavanje komercijalnih podataka tretira kao rizik.

Događa se to da ona poduzeća koja se bave razvojem informacijskih tehnologija, a mogu efikasno upravljati svojim rizicima, iz temelja premašuju ona poduzeća koja se ne mogu nositi s nabrojanim izazovima. Poduzeća u kojima razvoj informacijskih tehnologija ima utjecaj na komercijalno donošenje odluka, samim time dokazujući kako se poslovnom osposobljenošću može učinkovito upravljati tehnološkim rizicima, napredovat će velikom brzinom, za razliku od onih poduzeća u kojima ih nepoznavanje ili strah od novih ili područja tehnološkog rizika podložnih promjenana sprječava da se prošire u nova područja ili rezultira neuspjehom onda kada to pokušaju (Fraser, 2010).

## 5.4.Analiza rizika u procesu razvoja informacijskih sustava

Razvoj informacijske i komunikacijske tehnologije mnogim je organizacijama pružio priliku za izravnu poslovnu korist u vidu povezivanja s klijentima. Uspjeh navedene interakcije ovisi o učinkovitosti informacijskog sustava koji se pritom koristi. Bilo kakva smetnja ili prekid u odnosu između kupca i dobavljača usluga može dovesti do naknadnog gubitka posla. Ključno vrijeme u tom odnosu je onda kada davatelj usluga odluči nadograditi svoje informacijske sustave. Tvrtka koja razvija sustav nada se besprijekornoj implementaciji koja će proći nesmetano, a kupac ima očekivanja kako neće doći do prekida u poslovnim transakcijama. No, ipak postoje mnoge mogućnosti da

će stvari krenuti u krivom smjeru tijekom razvoja novog informacijskog sustava, a organizacije poduzimaju brojne rizike prilikom započinjanja ovog postupka.

Većina informacijskih sustava implementira se s očekivanjem da će implementacija proći uspješno. Unatoč tome, postoji sve veći broj slučajeva i primjera u kojima sustavi na prvu funkcioniraju, a kasnije se tek primjete negativne posljedice koje imaju za one ljude koji ih koriste. To može biti puno izraženije kada se sustavi implementiraju u područjima koja imaju izravan utjecaj na poslovni uspjeh.

Mnoge organizacije razvijaju svoje informacijske sustave sa sviješću da je mogućnost pojave rizika izvjesna. Zapravo, one djeluju bez obzira na poslovne rizike. Većina autora iz područja informacijskih sustava, rizike doživljava kao nešto što se treba riješiti onda kada se sustav digne i pokrene. To se poklapa s fokusom koji su usvojile mnoge aktualne metodologije upravljanja rizikom.

Značajno povećanje broja distribuiranih sustava u okruženju, gdje gotovo svaki zaposlenik ima pristup sustavima, učinilo je pitanje sigurnosti kritičnijim. Oni koji revidiraju sustave mogu biti zainteresirani za zaštitu imovine, integritet podataka, učinkovitost sustava i učinkovitost općenito. Pogrešna je pretpostavka da je samo zato što je moguće provesti procjenu rizika, moguće i kontrolirati istu.

Ipak, postoje brojni čimbenici rizika koje valja razmotriti prije nego što se pokrene informacijski sustav. Izvjesno je i to da je proces implementacije informacijskih sustava podjednako važan za uspješnost informacijskog sustava kao i gotovi informacijski sustav. Postoji dosta pogrešaka koje se mogu dogoditi tijekom procesa razvoja sustava, a posao organizacije je da istovremeno treba pokušati smanjiti rizik i povećati sigurnost tijekom implementacije sustava. Integritet organizacijskih informacijskih sustava treba se smatrati visokim prioritetom. Također će se u jednom trenutku pojaviti pitanje jesu li trenutne metodologije upravljanja rizikom relevantne za širi proces.

Procjenu rizika treba napraviti na samom početku projekta, ili barem prije dizajniranja samog sustava odrediti razinu rizika i napraviti planove za smanjenje tog rizika. Nužno je osigurati organizaciju projekta tako da on bude završen u zadanim vremenskim i financijskim ograničenjima. Sigurnost projekta tek tada može osigurati upravljački odbor koji se bavi računalnim sustavom. Oni imaju ovlasti uspostave općeg

usmjerenja informacijskih sustava organizacije. Nakon svega toga može se implementirati tehnologija. Tim postupkom izbjegava se nepotrebni rizik.

Međutim, mjerenje potencijalne računalne prijetnje često može ovisiti o informacijama o prethodnim prijetnjama, za koje je moguće da uopće ne postoje ili da nisu sačuvane. U razvoju informacijskih sustava uz pomoć novih računalnih platformi mogu postojati veliki problemi s neizvjesnošću, usprkos poznatim mjernim podatcima. Isto tako, ključno je da projektni tim uopće prizna da postoji rizik u određenim područjima.

Dodatni pritisak na informacijske resurse sustava često čine analizu rizika opsežnim i rizičnim postupkom. Mnoge organizacije posjeduju potpuno integrirane sustave koji se istovremeno povezuju s kupcima i dobavljačima. Financijske posljedice koje donosi neuspjeh sustava zahtijevaju jaku vezu između analize rizika i analize troškova i koristi. To predstavlja jedan od ključnih dijelova procesa strateškog planiranja. U tom slučaju bi se rizik mogao procijeniti na različite načine: rizici povezani s novom tehnologijom; rizici povezani s veličinom projekta; opasnost od neuspjeha, tj. šteta koja može biti načinjena tvrtci ukoliko projekt ne uspije.

Proporcionalno povećanje rizika od neuspjeha moguće je ako je projekt ambiciozan, kao npr. projekt redizajniranja poslovnih procesa (engl. *business process re-engineering*, ankronim BPR). Uspjeh razvoja sustava često može ovisiti o sposobnosti upravljanja promjenama unutar organizacije. Ukoliko je moguće da konkurenti brzo kopiraju sustav, postoji opasnost od financijskih rizika pri prevelikim ulaganjima u novi projekt. U nekima od poslovnih sektora može biti iznimno zahtjevno zadržati čak i kratkoročnu konkurentsku prednost. Isto tako, može biti teško uspješno implementirati i održavati profitabilne informacijske sustave. No, bez inovacija u sustavima, moguće je da organizacija pretrpi nedostatak strategija. Ono što treba prethoditi ulaganju u novi informacijski sustav je procjena položaja tvrtke u odnosu na novčana sredstva, tehnološku sofisticiranost i organizacijsku fleksibilnost.

Prije upuštanja u sam projekt potrebno je postaviti nekoliko osnovnih pitanja. Ima li tvrtka dovoljno financijskih sredstava za finalizaciju projekta izgradnje informacijskih sustava? U odnosu na tehnološke inovacije, je li tvrtka vođa ili sljedbenik? Ima li tvrtka

sposobnost brze reakcije na promjene u okolišu? Informacijski sustavi unutar organizacije mogu zahtijevati stalnu i kontinuiranu inovaciju. Moguće je i da uspjeh ili neuspjeh uvođenja informacijskog sustava tvrtke ovisi o razumijevanju složenosti njegovih unutarnjih i vanjskih okruženja.

Razvoj informacijskih sustava trebalo bi promatrati kao organizacijski sustav kojim je potrebno upravljati. Menadžment bi trebao težiti što boljem razumijevanju čimbenika koji utječu na uspješnost provedbe. Postoji potreba za dugoročnijim, strateškim pogledom na rizik i sigurnost. Ono što je karakteristično za pojavu rizika u izgradnji informacijskih sustava je to da: veliki projekti nose veći rizik od manjih projekata; sustavi u kojima se zahtjevi lako ispunjavaju i visoko su strukturirani biti će manje rizični od onih u kojima su zahtjevi neuredni, loše strukturirani, loše definirani ili podložni prosudbi pojedinca; razvoj sustava koji koristi uobičajenu, odnosno standardnu tehnologiju bit će manje rizičan od onoga koji koristi novu ili nestandardnu tehnologiju; projekt će biti manje rizičan kada je korisnička skupina upoznata s procesom razvoja sustava i područjem primjene (Maguire, 2004).

Često razvoj sustava može biti samo jedna od nekoliko različitih inicijativa koje bi trebale biti prioritetne. Dio tog procesa biti će pokušaj procjene vjerojatnosti uspješnosti projekta. Taj bi dio mogao ovisiti o količini prijetnje koju predstavlja konkurencija. Osnovni rizik u razvoju novog informacijskog sustava može biti korištenje još uvijek nedokazane tehnologije ili potrebe od strane osoblja koje radi na izgradnji informacijskih sustava da ovladaju novom tehnologijom. Maguire (2004) u svome članku citira Warda i Griffithsa (1996) koji identificiraju šest širih kategorija za identificiranje rizika unutar projekta. Razina utjecaja rizika ovisit će o prirodi sustava koji se razvija pa se pritom uzima u obzir: veličina projekta, složenost projekta, problemi vezani uz ljudski faktor, kontrola projekta, noviteti i stabilnost zahtjeva.

## 5.5.Rizici koji se pojavljuju pri izgradnji informacijskih sustava

Bez obzira bila riječ o malom ili velikom projektu izgradnje informacijskog sustava taj je projekt uvijek vrlo složen. Gotovo uvijek postoje događaji koji se ne mogu

predvidjeti, a povezani su s projektom. Ti događaji mogu negativno utjecati na financijske troškove, trajanje, kvalitetu i druge aspekte razvoja informacijskih sustava. Rizik unutar projekta predstavlja subjektivnu procjenu postavljenu na temelju vjerojatnosti neostvarivanja postavljenog cilja u okviru datog vremena, financija i drugih resursa. Dakako, rizik projekta predstavlja vjerojatnost pojave gubitaka tijekom životnog ciklusa projekta. Negativni događaj može se realizirati na početku, tijekom razvojne faze, tijekom završne faze i faze održavanja. Vjerojatnost ostvarivanja rizika može se mjeriti, a koristi se ljestvica mjerenja od 0 (nemoguće) do 1 (sigurna realizacija negativnog događaja).

Svaki projekt razvoja informacijskog sustava okuplja neke specifične vrste rizika, no, poneke kategorije rizika su uobičajene za sve vrste projekata, bez obzira na to koliko je složeno njima upravljati. Đuraković i Raković (2009) u svome članku koriste Heldmanovu podjelu gdje se rizici mogu svrstati u tri kategorije: poznati rizici s poznatim posljedicama (događaji poznati projektnom timu; vjerojatnost njihova pojavljivanja je visoka), poznati rizici s nepoznatim posljedicama (poznati su projektnom timu, ali je nepoznat njhov utjecaj na projekt) i nepoznati rizici (ne mogu se identificirati pa nema ni načina da se predvide njihove posljedice, niti da se napravi plan aktivnosti u slučaju pojave takvih događaja). Rizici mogu potjecati iz unutarnjih i vanjskih izvora. Interni rizici, koji potječu iz unutarnjih izvora, ovise o samoj prirodi projekta, organizacijskim pitanjima, osoblju, dostupnosti resursa itd. Vanjskim rizicima pripadaju politička, pravna i ostala pitanja.

Postoji nekoliko općenitih rizika koji se mogu javiti pri razvoju informacijskih sustava. Prvi su rizici koji se odnose na sukladnost s projektnim ciljevima između voditelja projekta, članova tima i naručitelja projekta. Ako ciljevi projekta nisu jasno definirani u početku projekta, biti će vrlo teško postići željene rezultate. Sljedeći su rizici koji se odnose na definiranje veličine projekta. Loše definirana veličina može rezultirati pogrešnim smjerom razvoja projekta što opet vodi do različitih posljedica, kao što su manjak vremena, trajne promjene u veličini projekta, povećanje troškova i sl. Nadalje, rizici koji se odnose na definiranje plana projekta slični su prethodnoj kategoriji i mogu imati identične posljedice.

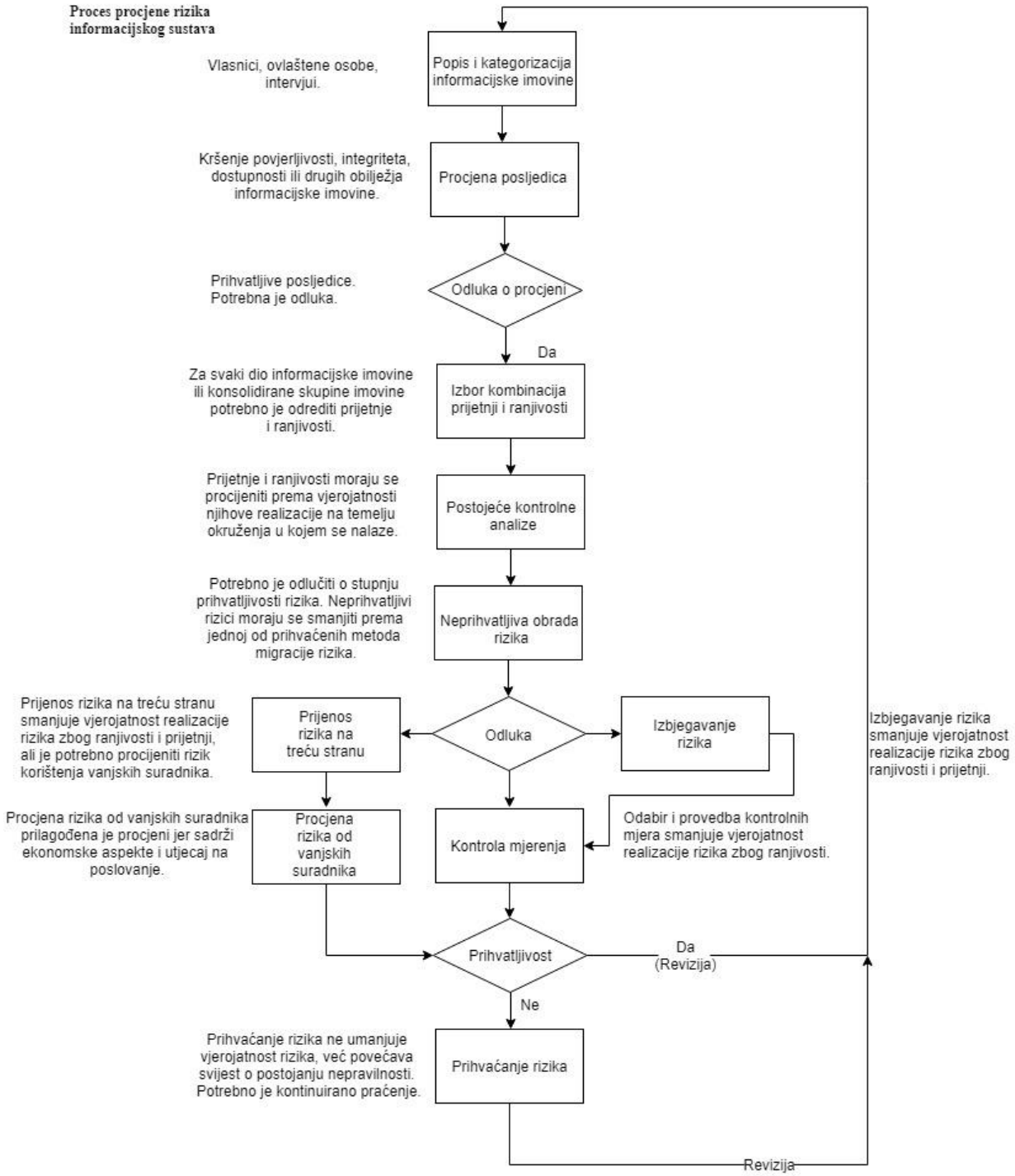
Vanjski rizici u razvoju informacijskih sustava su rizici koji su van kontrole projektnog tima i organizacije. Također, tehnički problemi, u slučaju da se projekt oslanja na novu tehnologiju koja još nije dovršena, kao i finalni izgled nove tehnologije, mogu predstavljati potencijalni rizik. Ako dođe do pojave takvoga događaja potrebno je provesti nova alternativna rješenja. Osim navedenih, i složenost projekta predstavlja rizik u slučaju da je projektni tim prihvatio projekt određene veličine i složenosti. Ako to nije slučaj, to predstavlja rizik koji se može ostvariti u obliku potrebe za dodatnim vremenom, dodatnom obukom i savjetodavnim uslugama članovima tima. Razvoj informacijskih sustava koji zahtijevaju korištenje alata programske podrške i programskih jezika koji su nepoznati članovima tima, također predstavljaju rizik. Iskustvo projektnog tima također predstavlja jedan od oblika rizika jer praksa pokazuje da iskustvo starijih članova tima može u velikoj mjeri pomoći u smanjenju rizika od neuspjeha projekta.

Sve u svemu, rizici u razvojnim projektima su brojni i prema tome, potrebno je identificirati rizike koji se odnose na ključne čimbenike uspješnosti projekta. Uklanjanje ili ublažavanje negativnih utjecaja rizika koji utječu na ključne čimbenike uspješnosti razvoja informacijskih sustava, u velikoj mjeri poboljšava priliku za uspjeh projekta (Đurković & Raković, 2009).

## 5.6.Proces upravljanja rizikom informacijskog sustava

Definicija procesa upravljanja rizikom informacijskog sustava kaže kako je to kontinuirano ponavljanje identifikacije, procjene i određivanja prioriteta rizika. Cijeli proces pobliže opisuje slika 3.

Slijedeći specifične prioritete za određene rizike određuju se mjere za smanjenje rizika na razinu prihvatljivosti ili potpunog uklanjanja rizika. Mjere za smanjenje rizika, kao i kod informacijskih tehnologija, dijele se na: provedbe sigurnosnih mjera, prijenos rizika na treću osobu, izbjegavanje i prihvaćanje rizika. Odabirom nekih od opcija za smanjenje rizika, stupanj ranjivosti se smanjuje, odnosno smanjuje se vjerojatnost da će zabilježena prijetnja iskoristiti ranjivost sustava.




*Slika 3.* Proces upravljanja rizikom informacijskog sustava (prilagođeno iz Očevčić et al., 2019:43)

Smanjenje procijenjene opasnosti moguće je prijenosom rizika na treću osobu ili izbjegavanjem rizika, ali samo u posebnim slučajevima. Ako se rizik ne može smanjiti

gore navedenim metodama, odabire se prihvaćanje rizika kao metoda naglašavanja postojećih slabosti. Prihvaćeni rizici se kontinuirano prate i promatraju, a sami su uključeni i u proces procjene prijetnji i ranjivosti (Očevčić, Nenadić & Šolić, 2019).

## 5.7.Suvremene informacijske tehnologije i analiza rizika

Informacijska tehnologija danas je potpuno prihvaćen i sastavni dio gotovo svakog poslovnog plana. U svim korporacijama, od multinacionalnih pa do malih tvrtki koje posjeduju po jedno računalo, koriste se informacijske tehnologije (MacKechnie, 2019). Već je spomenuto da informacijske tehnologije potiču inovacije u poslovanju. Inovacije za rezultat imaju pametnije aplikacije, bolju pohranu podataka, bržu obradu te širenje informacija. Istovremeno one čine poduzeće učinkovitijim, povećavaju vrijednost, poboljšavaju kvalitetu i povećavaju produktivnost. Inovacije u poslovanju nastale zbog uvođenja informacijske tehnologije dovele su do sljedećih većih promjena u poslovanju: online kupnja postala je učinkovitija od kupovine u trgovini, digitalni marketing zastupljeniji je od oglašavanja u novinama, putem televizije i radija, društveno umrežavanje zastupljenije je od odlaska u klubove, VoiP komunikacija zastupljenija je od telefonske, računarstvo u oblaku zastupljenije je od privatne računalne mreže i sl. Tvrtke koje su prihvatile tehnološku inovaciju imaju sljedeće karakteristike: točnije poslovno planiranje, učinkovitiji marketing, veću globalnu prodaju, sustavnije upravljanje, koriste nadzor u stvarnom vremenu, nude trenutnu dostupnost korisničke podrške itd.

Tehnološka revolucija pozitivno je utjecala na poslovanje 21. stoljeća na pet osnovnih načina. Prvi način na koji je informacijska tehnologija poboljšala poslovanje je taj da je omogućila tvrtkama alate za rješavanje složenih problema. Tu pripadaju poboljšani hardver, s više memorije, bržim procesorima, oštrijim vizualnim prikazima itd., i pametnije aplikacije (npr. programske podrške mentalnih mapa, kolaborativne programske podrške, razni organizatori i sl). Sve je to učinilo jednostavnijim istraživanje i analizu podataka. Dostupno je mnogo alata koji služe za rješavanje različitih složenih problema.

Sljedeće je to da informacijska tehnologija tvrtkama omogućuje donošenje boljih odluka. Inače je osnova dobrih odluka u poslovanju temeljito istraživanje tržišta. To se može činiti kroz angažiranje timova putem video konferencija, pregledom javnog mišljenja na društvenim medijima i forumima i korištenjem online anketa kako bi se dobile povratne informacija od korisnika.

Treći način je poboljšanje marketinga uz pomoć informacijskih tehnologija. Internet marketing koristi razne metode online oglašavanja (npr. oglasi na društvenim mrežama). Korištenjem tih metoda puno je lakše pronaći i doprijeti do ciljane publike nego tradicionalnim marketinškim kanalima. Jednostavnije je otkriti potrebe kupaca, kao sama izgradnja marketinške kampanje. Puno je lakše doći do podatka o tome koliko je ljudi kliknulo na mrežnu reklamu nego do toga koliko je ljudi čitalo novinski oglas.

Sljedeći način na koji je informacijska tehnologija pozitivno utjecala na poslovanje je poboljšanje korisničke podrške. Korisnici mogu dobiti podršku s više kanala, preko e-pošte, društvenih medija, webinara itd. Osim navedenoga, postoje i sustavi upravljanja odnosima s klijentima koji pomažu tvrtkama u razumijevanju ponašanja kupaca.

Posljednji, peti, način je taj da je informacijska tehnologija poboljšala upravljanje resursima. Računarstvo u oblaku omogućuje zaposlenicima poduzeća da koriste bilo koji uređaj bilo gdje u svijetu za pristup programskoj podršci na razini poduzeća (BusinessVibes, 2015).

Kao što je već prije objašnjeno, u razvoju informacijskih tehnologija i sustava proces analize rizika igra veliku ulogu. Na primjeru dviju suvremenih tehnologija koje se koriste u poslovanju, a to je računarstvo u oblaku i mrežno oglašavanje biti će objašnjen proces analize rizika.

# 6. Primjeri analize rizika

Za potpuno razumijevanje važnosti analize rizika u razvoju informacijskih tehnologija, pogotovo u pooslovnom svijetu, potrebno se približiti nekima od aktualnijih informacijskih tehnologija, odnosno onima kojima se u svom poslovanju koristi veliki broj korporacija, a to su računarstvo u oblaku i online oglašavanje. Korištenje svake od navedenih informacijskih tehnologija nosi određene rizike koje je potrebno identificirati i analizirati kako bi ih se uspješno minimiziralo, ili potpuno eliminiralo.

## 6.1. Računarstvo u oblaku

Računarstvo u oblaku (engl. *cloud computing*) naziv je za korištenje raznih usluga, kao što su platforme za razvoj programske podrške, poslužitelji, pohrana putem interneta. Često se naziva samo „oblak“. Općenito, postoje tri značajke računarstva u oblaku koje su uobičajene, bez obzira na to tko je omogućio tu uslugu: krajnjim rezultatom aplikacije (osobito hardvera) upravlja pružatelj usluge oblaka, korisnik plaća samo za korištene usluge (memorija, vrijeme obrade i sl.), usluge su skalabilne. Uobičajeno je kategorizirati usluge računalstva u oblaku kao **infrastrukturu kao uslugu** (engl. *infrastructure as a service*, akronim IaaS), **platformu kao uslugu** (engl. *platorm as a service*, akronim PaaS) ili **softver kao uslugu** (engl. *software as a service*, akronim SaaS) (Technopedia).

Oblak može biti privatan ili javni. Javni oblak prodaje usluge svima na internetu, tj. dostupan je svima na korištenje. Trenutno je *Amazon Web Services* najveći pružatelj usluga u javnom oblaku. Privatni oblak je vlasnička mreža ili podatkovni centar koji ugostiteljskim uslugama opskrbljuje ograničen broj ljudi. Bio oblak privatni ili javni, cilj računalstva u oblaku je osigurati jednostavan, skalabilan pristup računalnim resursima i uslugama informacijskih tehnologija.

Isporuka usluga privatnog oblaka odvija se iz poslovnog podatkovnog centra internim korisnicima. Ovakav model nudi svestranost i praktičnost oblaka, uz očuvanje

zajedničkog upravljanja, kontrole i sigurnosti lokalnih podatkovnih centara. Interni korisnici mogu ili ne moraju platiti usluge privatnog oblaka. Najpoznatiji pružatelji usluga privatnog oblaka su VMware i OpenStack.

Kod modela javnog oblaka, pružatelj usluga u oblaku je treća strana i isporučuje uslugu oblaka putem interneta. Javne usluge prodaju se na zahtjev, a obično se naplaćuju po minuti ili satima, ali dostupne su i dugoročne opcije za mnoge usluge. U ovom slučaju kupci plaćaju samo za količinu memorije ili propusnost koju troše. Vodeći pružatelji usluga javnog oblaka su *Amazon Web Services, Microsoft Azure, IBM* i *Google Cloud Platform*.

Hibridni oblak je kombinacija javnog oblaka i lokalnog privatnog oblaka, između njih je omogućena suradnja i automatizacija. Korporacije mogu pokretati kritična radna opterećenja ili osjetljive aplikacije na privatnom oblaku i koristiti javni oblak za obradu opterećenja i povećanja potražnje. Javna infrastruktura oblaka može pružiti, a istovremeno i zadržati kontrolu nad kritičnim podacima.

Organizacije sve više prihvaćaju model više oblaka (engl. *multicloud*), tj. korištenje višestrukih infrastrukturnih pružatelja usluga. To omogućuje aplikacijama da se prebacuju između različitih pružatelja usluga u oblaku, kao i da istovremeno djeluju na dva ili više pružatelja usluga u oblaku. Organizacije prihvaćaju ovakav način iz različitih razloga. Jedan od razloga je smanjenje rizika od prekida rada ili gubitka usluga u oblaku ili kako bi iskoristili konkurentnije cijene određenog pružatelja usluga. Implementacija i razvoj aplikacija kod ovakvog načina mogu predstavljati izazov zbog razlika između pružatelja usluga u oblaku i sučelja aplikacijskih programa. Ipak, višestruka implementacija trebala bi biti lakša jer se usluge i sučelja aplikacijskih programa pružatelja usluga međusobno približavaju.

Osnovna briga za poduzeća koje razmišljaju o korištenju oblaka je sigurnost. To se najviše očituje kod korištenja javnog oblaka budući da javni pružatelji usluga u oblaku dijele svoju temeljnu hardversku infrastrukturu između brojnih kupaca. Takvo okruženje zahtjeva obilnu izolaciju između logičkih računalnih resursa. Isto tako, za pristup oblaku i računalnim resursima potrebna je prijava na račun i lozinka.

Mnoge organizacije koje su ograničene složenim regulatornim obvezama i standardima upravljanja još uvijek oklijevaju stavljati podatke u javni oblak zbog straha od prekida rada, gubitka ili krađe. Međutim, ovaj otpor blijedi, jer se logička izolacija pokazala pouzdanom, a dodavanje enkripcije podataka i različitih alata za upravljanje identitetom i pristupom poboljšalo je razinu sigurnosti unutar javnog oblaka. (Rouse, 2019)

Najčešći rizici koji se vezuju uz **računarstvo u oblaku** prema ENISA-i[1] (akronim *European Network and Information Security Agency*) su: gubitak vlasti (engl. *loss of governance*), nemogućnost prelaska kod drugog pružatelja usluga (engl. *lock-in*), neuspjeh izolacijskih mehanizama (engl. *isolation failure*), izazovi vezani uz sukladnost (engl. *compliance challenges*), kompromis u dizajnu upravljačkog sučelja (engl. *management interface compromise*), zaštita podataka (engl. *data protection*), nesigurno ili nepotpuno brisanje podataka (engl. *insecure or incomplete data deletion*), zlonamjerni upućeni unutarnji suradnici (engl. *malicious insider*). Svaki će od navedenih rizika biti prikazan u tablicama koje uključuju: razinu vjerojatnosti, razinu učinka, upućivanje na ranjivosti, upućivanje na utjecaj na imovinu i razinu rizika. Također, u prikazu rizika, na mjestima gdje je to značajno, dodana je i usporedna vjerojatnost i usporedna vjerojatnost utjecaja kako bi se usporedili rizici računarstva u oblaku s rizicima u standardnim IT pristupima.

Rizici se dijele u tri kategorije. U prvoj su **politički i organizacijski rizici**, a tu spadaju: nemogućnost prelaska kod drugog pružatelja usluga, gubitak vlasti, izazovi vezani uz sukladnost. Slijede ih **tehnološki rizici**: neuspjeh izolacijskih mehanizama, zlonamjerni unutarnji suradnici, nesigurno ili nepotpuno brisanje podataka i kompromis u dizajnu upravljačkog sučelja. Posljednji su **pravni rizici** i od najčešćih rizika njima pripadaju rizici vezani uz zaštitu podataka.

[1] European Network and Information Security Agency, akronim ENISA agencija je Europske unije čija je osnovna djelatnost rješavanje pitanja sigurnosti informacija i informacijskih mreža.

### *6.1.1. Nemogućnost prelaska kod drugog pružatelja usluga*

Nemogućnost prelaska kod drugog pružatelja usluga javlja se iz razloga što trenutno u ponudi postoji mali broj alata, postupaka i standardnih formata podataka ili sučelja usluge koji mogu garantirati podatke, aplikaciju i uslugu prenosivosti. To može otežati kupcu da se prebaci s jednog na drugog davatelja usluga ili da premjesti podatke i usluge natrag u interno informacijsko-tehnološko okruženje. Rezultat je ovisnost o određenom pružatelju usluge u oblaku, osobito u slučaju kad prenosivost podataka, jedan od temeljnih aspekata, nije omogućena.

U tablici 2 vide se faktori analize navedenog rizika: vjerojatnost pojave rizika, koja je u ovom slučaju visoka; utjecaj, koji je srednji, ranjivosti i utjecaj na imovinu. Ranjivosti obuhvaćaju: manjak standardnih tehnologija i rješenja (podatci mogu biti „zaključani“ kod pružatelja usluge što za ishod ima ograničenje korištenja sigurnosnih usluga i vanjskih sigurnosnih tehnologija), loš izbor pružatelja usluga, nedostatak pružatelja usluga i nepotpunost i nerazumljivost uvjeta korištenja.

***Tablica 2:*** *Analiza rizika nemogućnosti prelaska kod drugog pružatelja usluga (prilagođeno od ENISA, 2009:25)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Visoka | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Srednji | **Stupanj usporedbe**: jednak |
| **RANJIVOSTI** | • Manjak standardnih tehnologija i rješenja<br>• Loš izbor pružatelja usluga<br>• Nedostatak pružatelja usluga<br>• Nepotpunost i nerazumljivost uvjeta korištenja | |
| **UTJECAJ NA IMOVINU** | • Reputacija kompanije<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga | |
| **RIZIK** | **VISOK** | |

Aspekti imovine na koje navedeni rizik može utjecati su: reputacija kompanije (utjecaj rizika na reputaciju kompanije je vrlo visok), osjetljivi osobni podatci (vrlo visok utjecaj rizika jer uključuje podatke o onome tko koristi sustav), osobni podatci (utjecaj rizika može biti srednji ili visok ovisno o tome jesu li podatci u potpunosti izbrisani ili se na njih utjecalo na drugi način), kritični osobni podatci (klasificirani su kritičnima ili ih organizacija takvima smatra; utjecaj rizika također može biti srednji ili visok), isporuka usluga u stvarnom vremenu (sve one usluge za koje je kritični faktor vrijeme i potreban je visok stupanj dostupnosti; utjecaj rizika je visok), isporuka usluga (utjecaj rizika je srednji) (ENISA, 2009).

### *6.1.2. Gubitak vlasti*

Korištenjem infrastrukture u oblaku, klijent prepušta kontrolu pitanja koja mogu utjecati na sigurnost pružatelju usluge. Štoviše, mogući su sukobi između procedura pridobivanja kupaca i okruženja u oblaku.

S druge strane, ugovori o razini usluge ne smiju nuditi obvezu pružanja takvih usluga čime se ostavlja praznina u sigurnosnoj obrani. Tim više, davatelj usluga u oblaku može ili koristiti treću stranu za davanje usluga ili unajmiti treću stranu (nepoznatog davatelja usluga), koja ne nudi ista jamstva (npr. pružanje usluga na zakonit način) kao originalni davatelj usluga. Kako se kontrola nad pružateljem usluga u oblaku mijenja, tako se mogu mijenjati i uvjeti i odredbe.

Gubitak upravljanja i kontrole mogao bi imati ozbiljan utjecaj na strategiju organizacije, a samim time i na sposobnosti organizacije da ispuni svoje ciljeve. To može dovesti i do nemogućnosti ispunjavanja sigurnosnih zahtjeva, nedostatka povjerenja, cjelovitosti i dostupnosti podataka, kao i pogoršanja izvedbe i kvalitete usluga.

U tablici 3 detaljnije se vidi proces analize rizika i što on nosi. Kao i u prethodnoj tablici prikazani su faktori analize navedenog rizika: vjerojatnost pojave rizika, koja je jako visoka; utjecaj, koji je jako visok, ranjivosti i utjecaj na imovinu. Ranjivosti obuhvaćaju: nejasne uloge i odgovornosti (neadekvatno pripisivanje uloga i odgovornosti davatelja usluga u oblaku), slaba provedba definicija uloga (kod pružatelja usluga u

oblaku, loše definiranje uloga može dovesti do pretjerano povlaštenih uloga što velike sustave može učiniti ranjivim pa se tako nikome osobi ne bi trebao omogućiti pristup podatcima o cijelom oblaku), usklađivanje odgovornosti ili ugovornih obveza izvan oblaka (kupci usluga u oblaku često nisu svjesni odgovornosti koje su im dodijeljene unutar uvjeta pružanja usluge), klauzule ugovora o razini usluge sa suprotstavljenim obećanjima različitim sudionicima (klauzule ugovora o razini usuge mogu nositi previše poslovnog rizika za pružatelja usluga, s obzirom na stvarni rizik od tehničkih kvarova), revizija ili certifikacija nisu dostupne korisnicima (pružatelj usluge u oblaku ne može pružiti jamstvo klijentu putem ovjere revizije), aplikacije u oblaku stvaraju skrivenu ovisnost (skrivene zavisnosti postoje u opskrbnom lancu usluga, a arhitektura pružatelja usluga u oblaku ne podržava nastavak rada iz oblaka kada je uključena treća strana, dakle podizvođač ili tvrtka kupca moraju biti odvojeni od usluge i obrnuto), manjak standardnih tehnologija i rješenja, čuvanje podataka u više nadležnosti i nedostatak informacija o tome (pohranjivanje podataka bez informacija koje su dostupne klijentu, o tome gdje se podaci pohranjuju, predstavlja razinu ranjivosti; tvrtke mogu nesvjesno kršiti propise, osobito ako se ne daju jasne informacije o skladištenju podataka), nema izvornog ugovora koji čuva treća strana, a važeći je onda kada je ispunjen određeni uvjet (ako pružatelj usluga u oblaku bankrotira, njegovi kupci nisu zaštićeni), nema kontrole na procesom procjene ranjivosti (ograničenja u testiranju ranjivosti predstavljaju ozbiljan rizik), sheme certificiranja nisu prilagođene infrastrukturi oblaka (nema kontrole specifične za oblak, što znači da će vjerojatno biti sigurnosnih propusta), nedostatak informacija o nadležnima (podatci se mogu pohranjivati i obrađivati u visokorizičnim jurisdikcijama koje su podložne prisilnim ulascima i ako ta informacija nije dostupna klijentu, on ne može poduzeti korake kako bi ih izbjegao opasnost), nepotpunost i nerazumljivost uvjeta korištenja, nejasno vlasništvo nad imovinom. Aspekti imovine na koje navedeni rizik može utjecati su: reputacija kompanije, povjerenje kupaca (vrlo visok utjecaj rizika), odanost i iskustvo zaposlenih (visok rizik), osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, isporuka usluga u stvarnom vremenu, isporuka usluga (ENISA, 2009).

***Tablica 3:*** *Analiza rizika gubitka vlasti (prilagođeno od ENISA, 2009:28)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Jako visoka | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Jako visok (ovisi o organizaciji) | **Stupanj usporedbe**: jednak |
| **RANJIVOSTI** | • Nejasne uloge i odgovornosti<br>• Slaba provedba definicija uloga<br>• Usklađivanje odgovornosti ili ugovornih obveza izvan oblaka<br>• Klauzule ugovora o razini usluge sa suprotstavljenim obećanjima različitim sudionicima<br>• Revizija ili certifikacija nisu dostupne korisnicima<br>• Aplikacije u oblaku stvaraju skrivenu ovisnost<br>• Manjak standardnih tehnologija i rješenja<br>• Čuvanje podataka u više nadležnosti i nedostatak informacija o tome<br>• Nema izvornog ugovora koji čuva treća strana, a važeći je onda kada je ispunjen određeni uvjet<br>• Nema kontrole na procesom procjene ranjivosti<br>• Sheme certificiranja nisu prilagođene infrastrukturi oblaka<br>• Nedostatak informacija o nadležnima<br>• Nepotpunost i nerazumljivost uvjeta korištenja<br>• Nejasno vlasništvo nad imovinom | |
| **UTJECAJ NA IMOVINU** | • Reputacija kompanije<br>• Povjerenje kupaca<br>• Odanost i iskustvo zaposlenih<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga | |
| **RIZIK** | **VISOK** | |

### *6.1.3. Izazovi vezani uz sukladnost*

Određene organizacije koje koriste oblak uložile su znatna sredstva u postizanje certifikacije ili zbog prednosti pred konkurencijom ili zbog zadovoljavanja industrijskih standarda ili propisa. Navedeno ulaganje može biti ugroženo prebacivanjem poslovanja u oblak: ako pružatelj usluge ne može pružiti dokaze usklađenosti s relevantnim zahtjevima ili ako pružatelj usluge ne dopušta reviziju od strane korisnika oblaka.

U tablici 4 vide se mogući rizici koje nose izazovi vezani uz sukladnost i utjecaj kojeg imaju. Faktori analize rizika su: vjerojatnost pojave rizika, koja je jako visoka; utjecaj, koji je visok, ranjivosti i utjecaj na imovinu. Ranjivosti ovoga puta obuhvaćaju: revizija ili certifikacija nisu dostupne korisnicima, manjak standardnih tehnologija i rješenja, čuvanje podataka u više nadležnosti i nedostatak informacija o tome, sheme certificiranja nisu prilagođene infrastrukturi oblaka, nedostatak informacija o nadležnima. Aspekt imovine na koje navedeni rizik može utjecati je certifikacija i takav je rizik, ukoliko se pojavi, visok (ENISA, 2009).

***Tablica 4:*** *Analiza rizika izazova vezanih uz sukladnost (prilagođeno od ENISA, 2009:29)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Jako visoka | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Visok | **Stupanj usporedbe**: jednak |
| **RANJIVOSTI** | • Revizija ili certifikacija nisu dostupne korisnicima<br>• Manjak standardnih tehnologija i rješenja<br>• Čuvanje podataka u više nadležnosti i nedostatak informacija o tome<br>• Sheme certificiranja nisu prilagođene infrastrukturi oblaka<br>• Nedostatak informacija o nadležnima<br>• Nepotpunost i nerazumljivost uvjeta korištenja | |
| **UTJECAJ NA IMOVINU** | • Certifikacija | |
| **RIZIK** | **VISOK** | |

### *6.1.4. Neuspjeh izolacijskih mehanizama*

Višestruki zakup i zajednički resursi dva su najvažnija obilježja računarstva u oblaku. Računalni kapacitet, pohranu i mrežu dijeli veći broj korisnika. Ova klasa rizika uključuje neuspjeh mehanizama koji odvajaju pohranu, memoriju, usmjeravanje i ugled različitih korisnika zajedničke infrastrukture.

Vjerojatnost navedenog scenarija ovisi o modelu oblaka, pa će rizik biti manji za privatne oblake. Zbog toga postoji razina izračunatog rizika kod dodjeljivanja svih usluga u oblaku budući da se sredstva dodjeljuju prema statističkim izračunima. Utjecaj ove skupine rizika može biti gubitak vrijednih ili osjetljivih podataka, narušavanje ugleda i prekid pružene usluge.

Tablica 5 prikazuje rizike koje nosi neuspjeh izolacijskih mehanizama. Faktori analize rizika su: vjerojatnost pojave rizika, koja je niska za privatni oblak, a srednja za javni oblak; utjecaj, koji je jako visok, ranjivosti i utjecaj na imovinu.

***Tablica 5:*** *Analiza rizika vezana uz neuspjeh izolacijskih mehanizama (prilagođeno od ENISA, 2009:35)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Niska (privatni oblak)<br>Srednja (javni oblak) | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Jako visok | **Stupanj usporedbe**: viši |
| **RANJIVOSTI** | • Hipervizorske ranjivosti<br>• Manjak izolacije izvora<br>• Manjak reputacijske izolacije<br>• Moguće je da će doći do internog sondiranja mreže<br>• Mogućnost provjere zajedničkog boravka | |
| **UTJECAJ NA IMOVINU** | • Reputacija kompanije<br>• Povjerenje kupaca<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga | |
| **RIZIK** | **VISOK** | |

Ranjivosti su: hipervizorske ranjivosti (napadi na hipervizorski sloj vrlo su atraktivni: hipervizor zapravo u potpunosti kontrolira fizičke resurse i rad virtualnih mašina, tako da

je svaka ranjivost u ovom sloju iznimno kritična), manjak izolacije izvora (korištenje resursa od strane jednog korisnika može utjecati na korištenje resursa od strane drugog korisnika), manjak reputacijske izolacije (aktivnosti jednog korisnika imaju učinak na ugled drugog korisnika), moguće je da će doći do internog sondiranja mreže (klijenti usluga u oblaku mogu izvršiti skeniranje portova i druge testove na drugim korisnicima unutar mreža), mogućnost provjere zajedničkog boravka (Napadi iskorištavaju nedostatak izolacije resursa i omogućuju napadačima da odrede koji resursi se dijele klijentima). Aspekti imovine na koje navedeni rizik može utjecati su: reputacija kompanije, povjerenje kupaca, osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, isporuka usluga u stvarnom vremenu, isporuka usluga (ENISA, 2009).

### *6.1.5. Zlonamjerni unutarnji suradnici*

Zlonamjerne aktivnosti unutarnjih suradnika korporacije, odnosno aktivnosti kojima ti suradnici svjesno i namjerno zaobilaze poštivanje privatnosti korisnika i njihovih podataka, mogu potencijalno utjecati na: povjerljivost, integritet i dostupnost svih podataka, internetskog protokola, svih vrsta usluga, a samim time i neizravno utjecati ne ugled organizacije, povjerenje klijenata i iskustva zaposlenika. To se pogotovo uzima u obzir u slučaju računarstva u oblaku zbog činjenice da arhitekture u oblaku zahtijevaju određene akcije koje nose veće rizike. Povećanjem upotrebe oblaka, pružatelji usluga u oblaku sve više postaju mete za kriminalne bande.

Ovakvi rizici su rizici visoke razine i pobliže su opisani u tablici 6. Faktori analize rizika su: vjerojatnost pojave rizika, koja je srednja; utjecaj, koji je visok, ranjivosti i utjecaj na imovinu. Ranjivosti su: nejasne uloge i odgovornosti, loša provedba definiranja uloga, ne primjenjuje se načelo potrebe za znanjem (strankama se ne smije dati nepotreban pristup podacima, a ako se to ipak učini onda to predstavlja nepotreban rizik), ranjivosti autentifikacijskog, autorizacijskog i računovodstvenog servera (slab sustav provjere autentičnosti, autorizacije i računovodstva može olakšati neovlašteni pristup resursima, eskalaciju privilegija, nemogućnost praćenja zlouporabe resursa i sigurnosnih incidenata uopće), ranjivosti sustava ili operacijskog sustava, neodgovarajuće provođenje

fizičke sigurnosti (uključuje nedostatak fizičkih kontrola perimetra, kao što je autentifikacija kartice pri ulasku, i nedostatak elektromagnetske zaštite za kritična sredstva podložna prisluškivanju), nemogućnost obrade podataka u šifriranom obliku (šifriranje podataka u mirovanju nije teško, ali zahvaljujući napretcima u homomorfnom šifriranju, malo je izglednu da bilo koji komercijalni sustav može održavati ovu enkripciju tijekom obrada), ranjivosti aplikacija ili loše upravljanje nadogradnjama (bugovi u aplikacijskom kodu, proturječne procedure nadogradnji između davatelja usluga i korisnika, primjena netestiranih nadogradnji, ranjivosti u preglednicima itd.). Aspekti imovine na koje navedeni rizik može utjecati su: reputacija kompanije, povjerenje kupaca, odanost i iskustvo zaposlenih (visoki rizik), intelektualno vlasništvo (visok rizik), osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, podatci o ljudskim resursima, isporuka usluga u stvarnom vremenu, isporuka usluga (ENISA, 2009).

***Tablica 6:*** *Analiza rizika vezana uz zlonamjerne upućene unutarnje suradnike (prilagođeno od ENISA, 2009:36)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Srednja<br>(manja nego kod tradicionalnog) | **Stupanj usporedbe**: manji |
| **UTJECAJ** | Jako visok<br>(viši nego kod tradicionalnog) | **Stupanj usporedbe**:<br>viši (za velik broj kupaca)<br>**Stupanj usporedbe**: isti (za jednog kupca) |
| **RANJIVOSTI** | • Nejasne uloge i odgovornosti<br>• Loša provedba definiranja uloga<br>• Ne primjenjuje se načelo potrebe za znanjem<br>• Ranjivosti autentifikacijskog, autorizacijskog i računovodstvenog servera<br>• Ranjivosti sustava ili operacijskog sustava<br>• Neodgovarajuće provođenje fizičke sigurnosti<br>• Nemogućnost obrade podataka u šifriranom obliku<br>• Ranjivosti aplikacija ili loše upravljanje nadogradnjama | |
| | • Reputacija kompanije<br>• Povjerenje kupaca | |

| | |
|---|---|
| **UTJECAJ NA IMOVINU** | • Odanost i iskustvo zaposlenih<br>• Intelektualno vlasništvo<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Podatci o ljudskim resursima<br>• Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga |
| **RIZIK** | **VISOK** |

### *6.1.6. Nesigurno ili nepotpuno brisanje podataka*

Kada se pojavi zahtjev za brisanjem resursa u oblaku, kao što to biva u slučaju većine operacijskih sustava, to ne razultira istinskim brisanjem podataka. Potpuno brisanje podataka nije moguće ili zbog toga što postoji više kopija podataka koji se pohranjuju, ali te kopije nisu dostupne, ili zato što medij koji bi trebalo uništiti pohranjuje podatke i od drugih klijenata.

Navedeni rizici prikazani su u tablici 7. Faktori analize rizika su: vjerojatnost pojave rizika, koja je srednja; utjecaj, koji je jako visok, ranjivosti i utjecaj na imovinu.

***Tablica 7:*** *Analiza rizika vezana uz nesigurno ili nepotpuno brisanje podataka (prilagođeno od ENISA, 2009:39)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Srednja | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Jako visok | **Stupanj usporedbe**: viši |
| **RANJIVOSTI** | • Osjetljive sanacije medija | |
| **UTJECAJ NA IMOVINU** | • Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Akreditiranje | |
| **RIZIK** | **SREDNJI** | |

Ranjivost je osjetljiva sanacija medija (zajednički zakup fizičkih resursa za pohranu znači da osjetljivi podaci mogu procuriti zbog politike uništavanja podataka koje se primjenjuju na kraju životnog ciklusa, a može ih biti nemoguće provesti jer se, na primjer, medij ne može fizički uništiti, jer disk još uvijek koristi drugi korisnik ili se ne može locirati i sl.). Aspekti imovine na koje navedeni rizik može utjecati su: osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, akreditiranje (osoblja koje ima pristup sustavu; jako visok rizik) (ENISA, 2009).

### *6.1.7. Kompromis u dizajnu upravljačkog sučelja*

Korisnička upravljačka sučelja pružatelja usluga javnog oblaka dostupna su putem interneta i posreduju u pristupu većim skupovima resursa (više od tradicionalnih pružatelja usluga) i samim time predstavljaju povećani rizik, posebno u kombinaciji s udaljenim pristupom i ranjivosti web-preglednika.

Sve se to detaljnije vidi u tablici 8. Faktori analize rizika su: vjerojatnost pojave rizika, koja je srednja; utjecaj, koji je jako visok, ranjivosti i utjecaj na imovinu.

***Tablica 8:*** *Analiza rizika u dizajnu upravljačkog sučelja (prilagođeno od ENISA, 2009:37)*

| | | |
|---|---|---|
| **VJEROJATNOST** | Srednja | **Stupanj usporedbe**: viši |
| **UTJECAJ** | Jako visok | **Stupanj usporedbe**: viši |
| **RANJIVOSTI** | • Ranjivosti autentifikacijskog, autorizacijskog i računovodstvenog servera<br>• Daljinski pristup sučelju za upravljanje<br>• Pogrešna konfiguracija<br>• Ranjivosti sustava ili operacijskog sustava<br>• Ranjivosti aplikacija ili loše upravljanje nadogradnjom | |
| **UTJECAJ NA IMOVINU** | • Reputacija kompanije<br>• Povjerenje kupaca<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci | |

| | |
|---|---|
| | • Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga<br>• Sučelje za upravljanje uslugama oblaka |
| **RIZIK** | **SREDNJI** |

Ranjivosti obuhvaćaju: ranjivosti autentifikacijskog, autorizacijskog i računovodstvenog servera, daljinski pristup sučelju za upravljanje (omogućuje propuste u završnom stadiju i kompromitira se infrastruktura oblaka, npr. kroz slabu autentifikaciju odgovora i zahtjeva), pogrešna konfiguracija, ranjivosti sustava ili operacijskog sustava, ranjivosti aplikacija ili loše upravljanje nadogradnjom. Aspekti imovine na koje dotični rizik ima utjecaj su: reputacija kompanije, povjerenje kupaca, osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, isporuka usluga u stvarnom vremenu, isporuka usluga, sučelje za upravljanje uslugama oblaka (Ovo je upravljačko sučelje koje upravlja svim uslugama oblaka; rizik je jako visok) (ENISA, 2009).

### *6.1.8. Zaštita podataka*

Računarstvo u oblaku predstavlja nekoliko rizika za zaštitu podataka za korisnike u oblaku i pružatelje usluga u oblaku. U nekim slučajevima korisniku oblaka (u ulozi kontrolora podataka) može biti teško učinkovito provjeravati postupke rukovanja podatcima davatelja usluga u oblaku i time biti sigurni da se podatci tretiraju na zakonit način. Moguće je pogoršanje navedenog problema, najviše u slučajevima višestrukih prijenosa podataka. S druge strane, neki pružatelji usluga u oblaku pružaju informacije o načinu na koji postupaju s podatcima. Isto tako, neki također nude sažetke certifikata o obradi podataka i podatcima sigurnosne aktivnosti te kontrole podataka.

Analiza rizika vezana uz zaštitu podataka, ranjivosti i njihov utjecaj pobliže se opisuju u tablici 9. Faktori analize rizika su: vjerojatnost pojave rizika, koja je visoka; utjecaj, koji je visok, ranjivosti i utjecaj na imovinu. Ranjivosti uključuju: nedostatak informacija o nadležnima, čuvanje podataka u više nadležnosti i nedostatak informacija o tome. Aspekti imovine na koje rizik ima utjecaj su: reputacija kompanije, povjerenje

kupaca, osjetljivi osobni podatci, osobni podatci, kritični osobni podatci, isporuka usluga u stvarnom vremenu, isporuka usluga (ENISA, 2009).

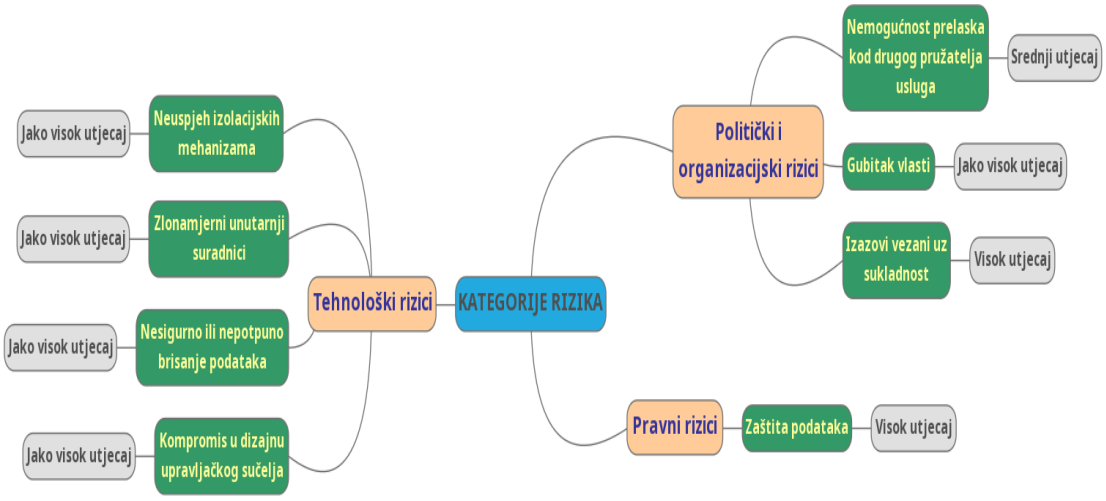
***Tablica 9:*** *Analiza rizika vezanih uz zaštitu podataka (prilagođeno od ENISA, 2009:46)*

| | |
|---|---|
| **VJEROJATNOST** | Visoka |
| **UTJECAJ** | Visok |
| **RANJIVOSTI** | • Nedostatak informacija o nadležnima<br>• Čuvanje podataka u više nadležnosti i nedostatak informacija o tome |
| **UTJECAJ NA IMOVINU** | • Reputacija kompanije<br>• Povjerenje kupaca<br>• Osjetljivi osobni podatci<br>• Osobni podatci<br>• Kritični osobni podatci<br>• Isporuka usluga u stvarnom vremenu<br>• Isporuka usluga |
| **RIZIK** | **VISOK** |

### *6.1.9. Komparativna analiza*

Kao što je već spomenuto, postoje tri kategorije rizika (politički i organizacijski rizici, tehnološki rizici, pravni rizici), od kojih svaka sadrži nekoliko podkategorija. U slici 3 uspoređene su sve gore navedene podkategorije kako bi se moglo vidjeti i usporediti koliki utjecaj na imovinu koji rizik ima. Iz slike možemo pročitati da svi tehnlološki rizici (neuspjeh izolacijskih mehanizama, zlonamjerni unutarnji suradnici, nesigurno ili nepotpuno brisanje podataka, kompromis u dizajnu upravljačkog sučelja) imaju jako visok utjecaj. Politički i organizacijski rizici razlikuju se po utjecaju na imovinu pa tako nemogućnost prelaska kod drugog pružatelja usluge ima srednji utjecaj, gubitak vlasti ima jako visok utjecaj, a izazovi vezani uz sukladnost imaju visok utjecaj. Među pravnim rizicima, najčešći rizik je zaštita podataka i ima visok utjecaj na imovinu.

***Slika 3**: Utjecaj rizika kod najčešćih rizika prema kategorijama (prilagođeno od ENISA)*




### *6.1.10. Primjeri posljedica neprovedene analize rizika računarstva u oblaku*

Neprovedena ili loše provedene analiza rizika kod računarstva u oblaku može imati razne loše posljedice po korisnike oblaka, kao i po davatelje usluga u oblaku. U nastavku slijedi dva primjera slučajeva koji su se dogodili pri korištenju usluga u oblaku kada se nije provela adekvatna analiza rizika. Navedeno se možda moglo izbjeći da je provedena sveobuhvatna analiza rizika.

Navedeni propust se dogodio CloudFlare-u, jednome od dobavljača usluga u oblaku, 2013. godine. Tvrtka CloudFlare jedan je od pružatelja usluga u oblaku koji nude alate Software-as-a-Service (SaaS) namijenjene osiguravanju mrežne prisutnosti klijenta i poboljšanju rada web-mjesta. Ponekad se događa da SaaS oblak koji bi trebao pomoći u poboljšavanju vremena neprekidnog rada ima suprotan učinak. Točno se to dogodilo kada su CloudFlare-ovi rubni usmjerivači istovremeno nadograđivani, što je uzrokovalo rušenje svih usmjerivača odjednom. Rezultat toga je bila nedostupnost oko 785.000 web-lokacija korisnika usluga u oblaku u vremenskom periodu od sat vremena (Froehlich, 2015).

Propust se dogodio i u Microsoftovom oblaku 2010. godine. Hotmailovi poslužitelji imali su problema s uravnoteženjem opterećenja, što je rezultiralo gubitkom svih

podataka sa preko 17.000 računa e-pošte. Microsoftu je trebalo tri dana za vraćanje podataka (Leonhard, 2011).

## 6.2. Mrežno oglašavanje

Jedna od osnovnih prednosti korištenja informacijske tehnologije u poslovanju jest sposobnost tvrtki u različitim industrijama da oglašavaju svoje proizvode i usluge putem interneta. Gotovo svako web-mjesto sadrži oglase, naravno uz primarni sadržaj web-lokacije. Uglavnom su takvi oglasi veze s kojih, jednim klikom miša ili dodirom zaslona, korisnici mogu pronaći informacije o proizvodima ili uslugama tvrtke čiji su oglas otvorili.

Na taj način tvrtke koje oglašavaju čine informacije lako dostupnima i samim time će vjerojatno imati koristi od mnogo veće posjećenosti svojih web stranica. Tako će također uvelike povećati šanse da netko zamijeti i iskoristi njihovu robu ili usluge. Preko online oglašavanja tvrtke čak mogu i komunicirati s ljudima iz cijelog svijeta ili doprijeti do njih. Na taj način povećava se izloženost njihovim oglasima bez plaćanja prekomjernih dodatnih troškova oglašavanja. (Miley, 2018)

Rast online oglašavanja na internetu i sveprisutna potreba za oglasnim platformama i drugim posrednicima za prikupljanje podataka o korisnicima dovode do ozbiljnije zabrinutosti u vezi s privatnošću korisnika. Najveća zabrinutost proizlazi iz rizika od zloupotrebe ogromne količine korisničkih podataka koje se održavaju na platformama za oglašavanje.

Dakle, rizici koji se javljaju pri online oglašavanju najčešće su rizici privatnosti, koje se dalje unutar sebe dijele na namjerno otkrivanje tajnih informacija unutar platforme i limitiranje uloge korisnika. (Estrada-Jiménez et al., 2017)

### *6.2.1. Namjerno otkrivanje tajnih informacija unutar platforme*

Glavni uzroci prijetnja privatnosti mrežnom oglašavanju čvrsto su povezani s infrastrukturom i mogućnostima oglasnih platformi. Prvo, unutar infrastrukture mrežnog

oglašavanja omogućen je zadani mehanizam praćenja i ne postoji zadana opcija koja onemogućuje praćenje korisnika ili prikazivanje oglasa. Drugo, ova je infrastruktura iznimno pretrpana subjektima koji se izravno ili neizravno opskrbljuju korisničkim podacima.

Isto tako, očito je da se poslovni model mrežnog oglašavanja, pa tako i njegove infrastrukture, temelji na prikupljanju što više informacija o korisnicima. Kada govorimo o mogućnostima platformi za mrežno oglašavanje, one provode prakse koje podržavaju napredne razine traženja ciljanih korisnika, a pritom zanemaruju privatnost i čak podržavaju curenje osobnih podataka. Podjela takvih prijetnji detaljnije je prikazana u tablici 11 (Estrada-Jiménez et al., 2017).

Praćenje prve strane (engl. *first-party tracking*) prva je prijetnja koja se pojavljuje, a obuhvaća aktivnosti koje obavljaju protivnici prve strane (najčešće izdavači) za prikupljanje i analiziranje korisničkih podataka. Takve aktivnosti uključuju posluživanje kolačića korisnicima i dobavljanje informacija iz prve ruke koje su im dostavljene na zahtjev. Ovisno o razini interakcije izdavača s korisnicima, oni mogu izravno prikupiti osobne podatke (spol, ocjene, društvene interakcije, preferencije, navike kupovine, zdravstveno stanje).

Sljedeća je prijetnja, odnosno rizik, praćenje treće strane *(*engl. *third-party tracking)*. Gradi se na neizravnim, i najčešće neprimjerenim, interakcijama između posrednika za oglašavanje i korisnika. Takve interakcije generiraju sadržaj ugrađen u web-lokacije prve strane koje su informacije o korisniku također dostavile trećim stranama. Širi opseg i viša hijerarhija subjekata koji obavljaju praćenje trećih strana olakšavaju masovno agregiranje osobnih podataka. Međutim, praćenje treće strane ne koristi se samo putem kolačića, već i putem dodataka (engl. *plug-ins*) koji također mogu otkriti podatke o pregledavanju korisnika na društvenim mrežama. Mehanizmi za zaštitu korisnika od rizika privatnosti online oglašavanja najčešće su blokiranje veza trećih strana nakon što ih klasificiraju kao neželjene.

Dalje, podudaranje kolačića (engl. *cookie matching)* tehnologija je koja podržava dijeljenje korisničkih podataka. Koristi i prvoj i trećoj strani. Koriste se kolačići kao osnovna tehnologija praćenja koja se koristi u online oglašavanju. Prvo se koriste kolačići

za pohranu osobnih podatka (npr. adresa e-pošte), a zatim i kao identifikatori za prepoznavanje korisnika u budućim posjetima. Kao drugo, omogućuju masovno dijeljenje osobnih podataka. Korisnički kolačići zatim se mapiraju i dijele između razmjenjivača oglasa i oglašivača.

Četvrta je prijetnja uzimanje otisaka prstiju (engl. *fingerprinting*). Ona se ne bazira na kolačićima. Sastoji se od otkrivanja niza uređaja ili aplikacija korisnika. Dakle, ako korisnik ne obriše kolačiće, uvijek ih se može mrežno pratiti putem niza posrednika. Uobičajeno je korištenje varijacije otisaka prstiju da bi se ponovno izdali kolačići nakon što ih je korisnik izbrisao.

Instant kolačići (engl. *flash cookies*) predstavljaju alternativnu tehnologiju praćenja za oglašivačke subjekte koji su suočeni s pojavom mehanizama za blokiranje tradicionalnog praćenja. Instant kolačići učinkovitiji su u praćenju korisnika od običnih kolačića. Zapravo, čak se smatraju i boljima zbog svojih karakteristika postojanosti, tj. više skladišnog kapaciteta i prostora za pohranu neovisnog o pregledniku.

Sljedeći je rizik uzimanje otisaka prstiju na platnu (engl. *canvas fingerprinting*). To je tehnologija mrežnog praćenja koju trenutno koriste neki agenti mrežnih oglašavanja, osobito agregatori podataka. Otisak prstiju na platnu olakšava praćenje generiranjem otiska prsta korisnika pomoću preglednika iz elementa HTML5 platna. Takav element protivnik može koristiti za dinamički prikaz, pa čak i nevidljivi prikaz te prikaz teksta ili slike u pregledniku korisnika.

Posljednja je prijetnja lokalno HTML5 spremište (engl. *HTML5 local storage*). To je profinjenija tehnologija praćenja na temelju kolačića, razvijena kao dio HTML5 mrežnog jezika. Lokalno pohranjivanje omogućuje univerzalnije praćenje korisnika koje ne ovisi o pregledniku koji koristi i nudi još više prostora za pohranu. Takva značajka može dopustiti pohranjivanje podataka prve ili treće strane koji se ne mogu izbrisati čak ni nakon brisanja kolačića preglednika. Međutim, takvo agresivno praćenje efikasno rješavaju mehanizmi za zaštitu (Estrada-Jiménez et al., 2017).

***Tablica 11:*** *Podjela namjernog otkrivanja tajnih informacija unutar platforme (prilagođeno od Estrada-Jiménez et al., 2017:8)*

| **PRIJETNJA** | **KRATKI OPIS** |
|---|---|

| **PRIVATNOSTI** | |
|---|---|
| ***Praćenje prve strane*** | informacije o korisniku cure izravno od strane korisnika do izdavača |
| ***Praćenje treće strane*** | korisničke informacije cure iz interakcija između posrednika za oglašavanje i korisnika |
| ***Podudaranje kolačića*** | korisnički kolačići mapiraju se i dijele između razmjenjivača oglasa i oglašivača |
| ***Uzimanje otisaka prstiju*** | niz agenta za identifikaciju izveden je od strane prvih i trećih strana iz određenih specifičnih karakteristika korisničkih aplikacija i uređaja |
| ***Instant kolaćići*** | intruzivna i trajna tehnologija kolačića koju omogućavaju web-lokacije temeljene na Flashu |
| ***Uzimanje otisaka prstiju na platnu*** | omogućuje praćenje korisnika na temelju otiska prsta stvorenog prikazivanjem HTML5 elementa na platnu |
| ***Lokalno HTML5 spremište*** | dugotrajna tehnologija praćenja koja se temelji na kolačićima razvijena je kao dio jezika HTML5 |

### *6.2.2. Limitiranje uloge korisnika*

Mogućnosti korisnika su, prema zadanim postavkama, poprilično ograničene na mreži. Korisnici uglavnom nisu svjesni transakcija koje se događaju u pozadini oglasa koji se poslužuje, što umanjuje njihove šanse da se zaštite. Ovakav nedostatak kontrole korisnika plodno su tlo za prijetnje privatnosti, posebno u sustavima mrežnog oglašavanja, gdje su usluge oglašavanja nerazdvojive od web pregledavanja. Takvi rizici i njihov opis pikazani su u tablici 12 (Estrada-Jiménez et al., 2017).

Prvi rizik je nedostatak svijesti (engl. *lack of awarness*). Povijesno gledano, privatnost na mreži oduvijek je predstavljala brigu korisnicima. Međutim, kada su korisnici suočeni s apstraktnim kontekstom u kojemu curenje osobnih podataka nije očito, brige korisnika su zamjetno manje. Takav odnos korisnika prema njihovoj privatnosti pokazuje da se oni više srame neugodnih oglasa, nego što ih je strah toga da se prati njihova aktivnost. U skladu s navedenim nedostatkom svijesti, korisnici jedva primjećuju relativnu vrijednost svojih podataka unutar komercijalnog konteksta.

Sljedeći je rizik nedostatak kontrole (engl. *lack of control*). U neizvjesnom scenariju mrežnog oglašavanja korisnici najčešće ne mogu adekvatno zaštititi svoju privatnost. Oni predstavljaju samo pasivne entitete unutar mrežnog oglašavanja.

Posljednja je prijetnja u ovoj kategoriji ograničeno tehničko znanje. Korisnici se suočavaju s važnom kognitivnom barijerom koja ozbiljno ograničava njihove mogućnosti upravljanja zaštitom od prijetnji privatnosti u mrežnom oglašavanju. Čak i ako su svjesni rizika koji se, te čak možda i imaju kontrolu nad nekima od njih, većina njih ne posjeduje tehničko znanje da bi se zaštitili u takvome scenariju (Estrada-Jiménez et al., 2017).

***Tablica 12:*** *Rizici kod limitiranja uloge korisnika (prilagođeno od Estrada-Jiménez et al., 2017:8)*

| **LIMITIRANJE ULOGE KORISNIKA** | **KRATKI OPIS** |
|---|---|
| ***Nedostatak svijesti*** | prilikom mrežog oglašavanja curenje osobnih podataka nije vidljivo korisnicima |
| ***Nedostatak kontrole*** | korisničke postavke i problemi nisu tehnički nametnuti prema zadanim postavkama u mrežnom oglašavanju |
| ***Ograničeno tehničko znanje*** | korisnici imaju slabo tehničko znanje za razumijevanje i učinkovito korištenje zaštitnih alata |

### *6.2.3. Primjeri posljedica neprovedene analize rizika kod mrežnog oglašavanja*

Mrežno je oglašavanje najčešći način oglašavanja kompanija i samim time potrebno je provesti analizu mogućih rizika po tvrtku ili korisnika. U nastavku slijedi primjer slučaja kada je mrežno oglašavanje na neki način zakazalo, opet najvjerojatnije zbog propusta u analizi rizika.

Facebook je do 2009. godine posjedovao mrežnu podršku zaduženu za oglašavanje, koja je automatski ažurirala profile korisnika svaki put kada bi stupili u interakciju sa partnerskim web-lokacijama (Encyclopedia). Isto tako, usluga Facebook Beacon korisnicima Facebooka omogućavala je da dijele svoje kupnje sa partnerskih internetskih tvrtki, kao što su knjige, filmovi i darovi, sa svojim prijateljima na

Facebooku. Problem je bio taj što, kada je usluga prvi put ponuđena, sudjelovanje nije bilo opcionalno, dakle sve kupnje su se na profilima prikazivale automatski. Uskoro su se mnogi korisnici razbjesnjeli i pokrenuli mrežnu peticiju koja je ubrzo dobila više od 50.000 potpisa. Korisnici su Facebook čak okrivili za "uništavanje Božića" jer je Beacon sustav oglašavanja korisnicima omogućio da vide kupovinu od prijatelja i obitelji. Ubrzo nakon toga, Facebook je promijenio uslugu tako da se ona može uključiti isključivo ako to korisnici dopuštaju prije objavljivanja kupnji (Conti, 2009).

# 7. Zaključak

Cilj ovoga rada bio je postaviti proces analize rizika u kontekst razvoja informacijskih tehnologija i informacijskih sustava, pokazati važnost toga procesa i moguće posljedice ukoliko se analiza rizika ne provede ili loše provede.

Rizike je prvo potrebno identificirati, a zatim na njih primijeniti analizu rizika koja se može napraviti na kvantitativnoj i kvalitativnoj razini. Sama analiza rizika sastoji se od tri glavne komponente, a to su: procjena rizika, upravljanje rizikom i komunikacija rizika. Rezultati provedene analize, ovisno o vrsti i opsegu, upotrebljajvaju se za pomoć u različitim aspektima procesa plasiranja novog proizvoda na tržište.

Za razumijevanje suvremenih informacijskih tehnologija i sustava neophodno je i razumijevanje digitalne kulture u globalu, kao i poznavanje važnih događaja koji su obilježili svako pojedino doba. Informacijske tehnologije i informacijski sustavi danas su neizostavan dio gotovo svake tvrtke ili organizacije.

Kod projekata unutar informacijske tehnologije (IT) nije neobično da imaju visoku stopu neuspjeha. Proces analize rizika vrlo je važan za uspješnu isporuku takvih projekata. Za suočavanje s identificiranim rizicima koriste se četiri strategije: izbjegavanje, ublažavanje, prijenos i zadržavanje. Ovisno o vrsti rizika i njegovom utjecaju primjenjuje se jedna od navedenih strategija. Na primjeru dviju suvremenih tehnologija koje se koriste u poslovanju, a to je računarstvo u oblaku i mrežno oglašavanje objašnjen je proces analize rizika i navedeni su primjeri posljedica do kojih može doći ako se ne provede adekvatna analiza rizika.

Analiza rizika, pogotovo u današnje vrijeme informacijskih previranja, neophodan je proces koji treba proći ukoliko tvrtke ili organizacije krajnjem korisniku žele ponuditi dobar i potpun proizvod. Potrebno je detaljno i s pažnjom pristupiti riziku koji se pojavljuje i na adekvatan ga način razriješiti kako ne bi došlo do nepoželjnih posljedica.

# 8. Literatura

1. Baccarini, David; Salm, Geoff; Love, Peter E.D. Management of risks in information technology projects. // Industrial Management and Data Systems 104, 4(2004), str. 286-295.
2. BusinessVibes. The Importance of Information Technology in Business Today, 2015. URL: https://www.business2community.com/tech-gadgets/importance-information-technology-business-today-01393380 (10.4.2019.)
3. Conti, Greg. Advertising and Embedded Content, 2009. URL: http://www.informit.com/articles/article.aspx?p=1250497&seqNum=4 (29.4.2019.)
4. Đurković, Ozren; Raković, Lazar. Risks in Information Systems Development Projects. // Management Information Systems 4, 1(2009), str. 13-20.
5. ENISA. Cloud Computing Risk Assesment, 2009. URL: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment (12.4.2019.)
6. Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. Online advertising: Analysis of privacy threats and protection approaches. Computer Communications, 100 (2017), str. 32–51.
7. Facebook Beacon. // Encyclopedia. URL: https://www.pcmag.com/encyclopedia/term/58518/facebook-beacon (29.4.2019.)
8. Fadllalah, Hadi. How information technologies influenced Risk Management?, 2018. URL: https://medium.com/@hadi.fadlullah/how-information-technologies-influenced-risk-management-7eb3a38d253 ( 20.3.2019.)
9. Fraser, Nicol. The impact of technological change on risk management, 2010. URL: https://www.computerweekly.com/opinion/The-impact-of-technological-change-on-risk-management (20.3.2019.)

10. Froehlich, Andrew. 9 Spectacular Cloud Computing Fails, 2015. URL: https://www.informationweek.com/cloud/9-spectacular-cloud-computing-fails/d/d-id/1321305?image_number=4 (29.4.2019.)
11. Gere, Charlie. Digital Culture. Expanded second edition. London: Reaktion Books, 2008.
12. Harvey, Jasmin. Introduction to managing risk. // Risk Management 28, (2008), str. 1-12. Str. 6
13. Informacijska i komunikacijska tehnologija. // Leksikografski zavod Miroslav Krleža. URL: http://www.enciklopedija.hr/natuknica.aspx?id=27406 (31.03.2019.)
14. Informacijski sustav. // Leksikografski zavod Miroslav Krleža. URL: http://www.enciklopedija.hr/natuknica.aspx?id=27410 (3.4.2019.)
15. Information Technology (IT) // Technopedia. URL: https://www.techopedia.com/definition/626/information-technology-it (31.03.2018.)
16. Klasić, Ksenija; Klarin, Karmen. Informacijski sustavi: načela i praksa. Zagreb: Intus, 2009.
17. Leonhard, Woody. Hotmail fail: Microsoft lays an egg in the cloud, 2011. URL: https://www.infoworld.com/article/2624887/hotmail-fail--microsoft-lays-an-egg-in-the-cloud.html (29.4.2019.)
18. MacKechnie, Chris. Information Technology and Its Role in the Modern Organization, 2019. URL: https://smallbusiness.chron.com/information-technology-its-role-modern-organization-1800.html (10.4.2019.)
19. Maguire, Stuart. Identifying risks during information system development: managing the process. // Information Management & Computer Security 10, 3(2004), str. 126-134.
20. M. Byrd, Daniel; Cothern, C. Richard. Introduction to Risk Analysis: A Systematic Approach to Science-Based Decision Making. Toronto: Government institutes, 2005. Str. 4-7

21. Miley, Erik. Uses of Information Technology in Business, 2018. URL: https://bizfluent.com/list-6496451-uses-information-technology-business.html (16.4.2019.)
22. Modarres, Mohammad; Kaminskiy, Mark; Krivtsov, Vasily. Reliability Engineering and Risk Analysis: Marcel Dekker, Inc., 2002. Str. 461;
23. Očevčić, Hrvoje; Nenadić, Krešimir; Šolić, Krešimir; Keser, Tomislav. The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents. // International journal of electrical and computer engineering systems 8, 2(2019), str. 41-46.
24. Risk. // Business Dictionary. URL: http://www.businessdictionary.com/definition/risk.html (14.01.2019.)
25. Rizik. // Hrvatski jezični portal. URL: http://hjp.znanje.hr/index.php?show=search (14.01.2019.)
26. Rizik. // Leksikografski zavod Miroslav Krleža. URL: http://enciklopedija.lzmk.hr/clanak.aspx?id=34325 (14.01.2019.)
27. Rouse, Margaret. What is Cloud Computing?, 2019. URL: https://searchcloudcomputing.techtarget.com/definition/cloud-computing (11.4.2019.)
28. Rouse, Margaret. What is risk analysis?, 2018. URL: https://searchsecurity.techtarget.com/definition/risk-analysis(24.2.2019.)
29. Schmidt, Eric; Cohen, Jared. Novo digitalno doba. Zagreb: Profil, 2014.
30. Technical Department of ENISA, Section Risk Management. Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006. Str. 6; 12-15;19-23
31. What is Cloud Computing? // Technopedia. URL: https://www.techopedia.com/definition/2/cloud-computing (11.4.2019.)
32. What is Risk Analysis?// Technopedia. URL: https://www.techopedia.com/definition/16522/risk-analysis (14.01.2018.)

## Sažetak

U svrhu razumijevanja analize rizika u kontekstu razvoja informacijskih tehnologija i informacijskih sustava, ovaj rad donosi detaljan opis rizika, procesa analize rizika i njezinih komponenti. Autor rada nas vodi kroz povijest digitalne kulture, od njezinih samih početaka pa do digitalne kulture 21. stoljeća, a i pretpostavke o tome što nosi budućnost. Zbog boljeg razumijevanja teme opisane su i informacijske tehnologije i informacijski sustavi, kao i njihov razvoj. U radu se potom analiziraju mogući rizici u razvoju informacijskih tehnologija i sustava općenito, a na kraju se donose i stvarni primjeri analize rizika.

**Ključne riječi:** *rizik, analiza rizika, informacijske tehnologije, informacijski sustavi, računarstvo u oblaku, mrežno oglašavanje*

# Risk analysis in the process of information technology development

## Abstract

For the purpose of understanding the risk analysis in the context of the development of information technology and information systems, this paper provides a detailed description of the risk, the risk analysis process and its components. The author's work leads us through the history of digital culture, from its very beginnings to the digital culture of the 21st century, and the assumptions about what the future holds. Due to a better understanding of the topic, information technology and information systems, as well as their development, have been described. The paper then analyses possible risks in the development of information technology and systems in general, and in the end, actual examples of risk analysis are also presented.

**Key words:** *risk, risk analysis, information technologies, information systems, cloud computing, online advertising*