UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

OCENJEVANJE TVEGANJ V INFORMACIJSKIH SISTEMIH NA OSNOVI TEORIJE OMREŽIJ

Primož Žvanut

DIPLOMSKO DELO
NA UNIVERZITETNEM ŠTUDIJU

Mentor: izr. prof. dr. Denis Trček

Ljubljana, 2011

Zahvala

Zahvalil bi se mentorju izr. prof. dr. Denisu Trčku za pomoč in usmerjanje med izdelavo diplomskega dela.
Posebna zahvala pa gre tudi dr. Mini Žele, ki je s svojimi nasveti in idejami pripomogla h koncu diplomskega dela.

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01738/2011
Datum: 15.03.2011

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **PRIMOŽ ŽVANUT**

Naslov: **OCENJEVANJE TVEGANJ V INFORMACIJSKIH SISTEMIH NA OSNOVI TEORIJE OMREŽIJ**

INFORMATION SYSTEMS RISK MANAGEMENT BASED ON NETWORK THEORY

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Za namene učinkovitega upravljanja tveganj v informacijskih sistemih razvijte metodološko rešitev za sistematično analiziranje groženj, sredstev in ranljivosti sredstev glede na identificirane grožnje. Cilj je, da razvita rešitev (in prototipna programska implementacije le te) omogoča identifikacijo najbolj kritičnih tveganj. Rešitev naj omogoča tudi učinkovito filtriranje in agregiranje tveganj, kajti v praksi se pri tem delu srečujemo s težko preglednimi in obsežnimi količinami podatkov ter informacij. Pri doseganju cilja se oprite na teorijo omrežij (angl. network theory).

Mentor:

prof. dr. Denis Trček

Dekan:

prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Kazalo

Seznam uporabljenih kratic in simbolov

Oznaka	Opis
A	matrika
A_{ij}	element matrike
$n \times n$	dimenzija matrike
n	število vozlišč
$\deg(v)$	stopnja vozlišča
x	lastni vektor
x_i	element lastnega vektorja
λ	lastna vrednost
Geo_{ij}	normalizacijska mera
$\sigma(R_i)$	ocena ranljivosti
x_i^k	ocena vozlišča na k-tem koraku
$v(X_i, X_j)$	vrednost povezave med dvema vozliščema
δ	parameter vplivanja na vrednost povezave
$\sigma_1(X_i)$	vsota ocen ranljivosti pri vozlišču
$\sigma_2(X_i)$	normalizirana skupna ocena ranljivosti pri vozlišču
$\sigma_S(X_i)$	normalizirana subjektivna ocena
$\sigma_P(X_i)$	normalizirana ocena števila posledic
$K(X_i)$	reprezentativna ocena tveganja vozlišča
α, β, γ	parametri vplivanja posameznih ocen
$\sigma(.)$	končna ocena ranljivosti je vsota lastnih vektorjev

Povzetek

Učinkovito upravljanje s tveganji je pomembna komponenta vsakega uspešnega varnostnega programa. Glavni cilj upravljanja je omogočiti organizaciji, da lahko opravlja svoje poslanstvo. Upravljanje s tveganji je pomemben del organizacije kot celote, kar vključuje tudi vodstvo. Rezultat ocenjevanja tveganja je poročilo o tveganjih, ki ogrožajo organizacijo in priporočila (ukrepi), ki odpravljajo oz. zmanjšujejo možnosti uresničitve grožnje. Grožnja izkoristi neko ranljivost določenega sredstva v organizaciji. V svetu IT pravimo tem sredstvom informacijska sredstva in zajemajo strežnike, računalnike, prenosne računalnike, podatke, itd. Za sredstva se lahko šteje tudi karkoli v organizaciji, ki služi njenemu delovanju in vsebuje določeno stopnjo ranljivosti. Če za sredstvo obstaja ranljivost, za to ranljivost obstaja tudi grožnja, ki jo lahko izkoristi. Z ocenjevanjem tveganja bi radi ugotovili čimveč takih ranljivosti, jih ovrednotili in podali seznam ukrepov, da ugotovljene ali prepoznane grožnje ne bi izkoristile ranljivosti na sredstvu.

Prvotni namen orodja za ocenjevanje tvaganja oz. sistema za ocenjevanje tveganja, ki ga v nadaljevanju predstavljam, je bil predvsem pomoč strokovnjaku za varnost pri urejanju in obdelavi podatkov o ocenah tveganja. Končni namen je seveda identifikacija največjih tveganj v organizaciji, ki jih dobimo z enotno metodologijo. Težava, ki se pojavlja pri takem postopku, je ogromno podatkov, iz katerih se ne znajdemo zlahka. Dodatna težava je tudi prikazovanje dobljenih razultatov vodstvu, kjer je zaželen enostavno razviden prikaz. Zato naloga predlaga, da se problema loti s pomočjo predstavitve z omrežjem in z dosedanjim znanjem o mrežah sklepamo na določene zakonitosti, relacije med vozlišči omrežja, ki predstavljajo grožnje. Grožnje so povezane medseboj na podlagi skupnih ranljivosti. Mreža bi na koncu tudi služila za predstavitev rezultatov, saj bi posamezne skupine predstavil s povezanimi vozlišči.

Ključne besede: tveganje, ocenjevanje tveganja, omrežja, družabna omrežja

Abstract

Effective risk management is an important component of any successful security program. The main objective of risk managing is helping the organization to carry out its mission. Risk management is an important part of the organization as a whole, including the executives. The result of risk assessment is a report on the risks that threaten the organization and recommendations of actions that eliminate or reduce the realization of the threat. The threat takes advantage of a vulnerability of a particular asset in the organization. In the world of IT, assets are called information assets and include servers, computers, laptops, data, etc.. An asset is considered everything in the organization that serves its operation and contains a certain degree of vulnerability. If there is an asset, there is also asset's vulnerability and the threat that can exploit it. The purpose of risk assessment is to find as many such vulnerabilities as possible, evaluate them and present a list of actions which can prevent the realization of threats.

The primary purpose of this risk assessment tool was assistance for security experts in managing and processing data on risk assessments. The ultimate objective is identification of the greatest risks in the organization which are obtained with a uniform methodology. The problem that arises is that there is a lot of data which can not be handled easily. An additional problem is the presentation of obtained results to the executives, where they should be presented in easy and light way. The proposed solution to the problem is a network presentation. General knowledge of networks can assist with deducing certain rules and relationships between nodes of the network which represent the threats. Threats are related to each other based on common vulnerabilities. The network would also serve for the presentation of results.

Key words: risk, risk assessment, network, social networking

Poglavje 1

Uvod

Vsaka organizacija ima svoje poslanstvo in za delovanje uporablja tudi sisteme za informacijske tehnologije (v nadaljevanju IT) za procesiranje podatkov. Tu igra upravljanje s tveganji oz. analiza tveganja pomembno vlogo pri varovanju.

Učinkovito upravljanje s tveganji je pomembna komponenta vsakega uspešnega varnostnega programa. Glavni cilj upravljanja je organizaciji omogočiti, da lahko opravlja svoje poslanstvo. Upravljanje s tveganji se ne sme smatrati kot proces, ki se tiče le strokovnjakov IT, ampak je tudi pomemben del organizacije kot celote, kar vključuje tudi vodstvo (še posebno je od vodstva odvisna uspešnost opravljene analize tveganja). Rezultat ocenjevanja tveganja je poročilo o tveganjih, ki ogrožajo organizacijo in priporočila (ukrepi), ki odpravljajo oz. zmanjšujejo možnosti uresničitve grožnje. Grožnja izkoristi neko ranljivost, če obstaja na določenem sredstvu v organizaciji. V svetu IT pravimo tem sredstvom kar informacijska sredstva in zajemajo strežnike, računalnike, prenosne računalnike, podatke, itd. Seveda se za sredstva lahko šteje karkoli v organizaciji, ki služi njenemu delovanju in vsebuje določeno stopnjo ranljivosti. Če pa za sredstvo obstaja ranljivost, pa za to ranljivost obstaja tudi grožnja, ki jo lahko izkoristi. Z ocenjevanjem tveganja bi radi ugotovili čimveč takih ranljivosti, jih ovrednotili in podali seznam ukrepov, da ugotovljene ali prepoznane grožnje ne bi izkoristile ranljivosti na sredstvu.

Prvotni namen orodja za ocenjevanje tvaganja oz. sistema za ocenjevanje tveganja, ki ga v nadaljevanju predstavljam, je bil predvsem pomoč strokovnjaku za varnost pri urejanju in obdelavi podatkov o ocenah tveganja. Orodje torej služi vnašanju, urejanju in prikazovanju ocen tveganja na bolj strukturiran in organiziran način. Sistem se je nato dopolnjeval v skladu z željami strokovnjakov s področja varnosti in zajema vpeljavo ukrepov s kontrolami (po standardu), sledljivost oz. revizijske sledi, primerjave ocen tveganj, dodelitev različnih vlog izvajalcem, vodenje ukrepov in poročilni sistem.

Končni namen je seveda identifikacija največjih tveganj v organizaciji, ki jih dobimo z enotno metodologijo. Vodstvo dobi pregled nad vsemi informacijskimi tveganji v organizaciji in posredno vpliva na načrt za povečanje varnosti informacij oz. določitev načrta izboljšanja varovanja informacij (npr. z uvedbo ustreznih tehničnih varnostnih rešitev, z vpeljavo ustreznih postopkov in varnostnih politik).

Težava, ki se pojavlja pri takem postopku, je ogromno podatkov, iz katerih se ne znajdemo zlahka. Dodatna težava je tudi prikazovanje dobljenih razultatov vodstvu, kjer je zaželen enostavno razviden prikaz. V pomoč so sicer poročila v obliki tabel, kjer se do določene mere razvidijo glavna tveganja, grožnje in ranljivosti.

Iz neodvisnega zanimanja in proučevanja teorije družabnih mrež ter teorije grafov se mi je porodil izziv, da bi bilo mogoče omenjeno problematiko prevesti na problem mrež in morda na tak način poiskati nekatere zakonitosti in relacije. Zato predlagam, da se problema lotimo s pomočjo predstavitve z omrežjem in z dosedanjim znanjem o mrežah sklepamo na določene zakonitosti, relacije med vozlišči omrežja. V mreži bi povezali posamezne ocene, ki se medseboj povezujejo preko skupnih ranljivosti (in verjetno s posledicami). Vsaka ocena bi tako imela svojo specifično lastnost: ocena ranljivosti, posledice, ukrepi zoper ranljivosti in popravljena ocena (risk reduction). Med tako dobljenimi in zastavljenimi ocenami, povezanimi v omrežje, bi z iskanjem skupnosti oblikoval skupine ocen (združevanje ocen), ki si delijo skupne (strukturne) značilnosti – skupine podobnih ocen. Med takimi skupinami bi nato poiskal najbolj rizične, ki bi jih izpostavil.

Tveganje bi se ocenjevalo kot linearna kombinacija zgoraj naštetih lastnosti kot tudi vpliv na ostale ocene in vpliva ostalih na to oceno. Znotraj rizične skupine bi lahko nadaljevali z iskanjem najbolj rizične ocene. Ker velja, da vsaki oceni pripada par (grožnja, informacijsko sredstvo), bi na tak način lahko sklepali na najnevarnejše grožnje, pogoste ranljivosti in ukrepe, ki jih je treba izpeljati.

Mreža bi na koncu tudi služila za predstavitev rezultatov, saj bi posamezne skupine predstavil s povezanimi vozlišči, kjer bi bila velikost vozlišča (premer, vizualna velikost na grafu) odvisna od rizičnosti vozlišča (ki predstavlja bodisi posamezno oceno, torej grožnjo, bodisi združeno skupino več ocen in predstavlja množico groženj).

V nadaljevanju sledi kratka predstavitev problema ocenjevanja tveganja. Sledi teorija mrež oz. znanja, ki ga uporabim. Nato sledijo rezultati.

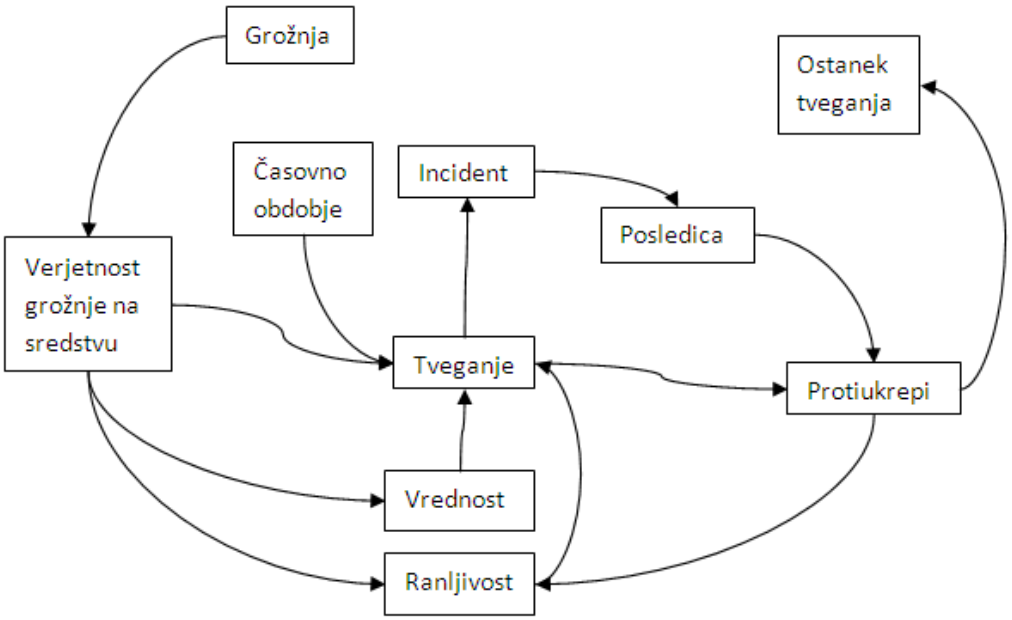
1.1 Namen

Tveganje lahko definiramo kot negativno posledico ob izrabi ranljivosti, če upoštevamo njeno verjetnost in obseg pojavitve. Upravljanje s tveganji je proces, v katerem identificiramo tveganja, ocenimo njihovo pomembnost in določimo ukrepe, ki jih zmanjšujejo na sprejemljivo raven.

Cilj upravljanja s tveganji je omogočiti organizacijam, da opravljajo svoje poslanstvo z izboljšano varnostjo IT sistemov, ki shranjujejo, procesirajo ali pošiljajo podatke, z ozaveščanjem vodstva organizacije, da sprejemajo odločitve, ki upoštevajo rezultate upravljanja s tveganji in na tak način lažje opravičijo stroške povezane z IT sredstvi, ter s pomočjo vodstvu organizacije pri odobritvi IT sistemov na osnovi dokumentacije, ki je nastala kot rezultat upravljanja s tveganji.

1.2 Upravljanje s tveganji

Pri upravljanju s tveganji se gibljemo v okviru sredstev in groženj [17]. Sredstvo predstavlja določeno vrednost organizaciji in grožnja pomeni vsak možen vzrok za incident. Tveganje je posledica interakcije med njima in pomeni možnost, da dana grožnja izkoristi ranljivost sredstva ter tako povzroči škodo. Ranljivost v tem primeru pomeni slabost, ki jo lahko izkoristi grožnja. Za zmanjšanje tveganja je potrebno ocenjevanje tveganja, kar pomeni identifikacijo tveganj, njihovo jakost in protiukrepe.



Slika 1.1: Osnovni elementi upravljanja s tveganji in njihove medsebojne povezave [17]. Grožnja vpliva z določeno verjetnostjo na sredstvo, izkoristi njeno ranljivost in zato

predstavlja določeno tveganje. Če se grožnja uresniči, pomeni to incident (dogodek), ki ima določene posledice. Za odpravo te ranljivosti in posledično grožnje, je potrebno uveljaviti pravilne protiukrepe. Po uveljavitvi protiukrepov še zmeraj ostane določeno tveganje (ostanek tveganja), ker ne moremo vedno 100 % odpraviti ranljivosti.

Upravljanje s tveganji obsega tri korake: ocenjevanje tveganja, ublažitev tveganja, stalno izvajanje procesa preverjanja in ocenjevanja. Ocenjevanje tveganja vključuje identifikacijo in oceno tveganja, posledice takega tveganja in priporočila za zmanjšanje tveganja. Ublažitev tveganja zajema določitev prioritete, implementiranje protiukrepov ali primernih kontrol za zmanjšanje tveganja, ki jih priporoča proces upravljanja s tveganji.
Upravljanje s tveganji je proces, ki omogoča upraviteljem sistemov IT, da pretehtajo med operativnimi in ekonomskimi stroški predlaganih varovalnih mer, ki z zaščito sistemov IT in podatkov izboljšujejo delovanje organizacije. Tako tehtanje odločitev ni vezano samo na informacijsko tehnologijo, ampak je prisotno v vsakodnevnem življenju, kot je npr. vgradnja alarma v stanovanjsko hišo, kjer lastnik pretehta korist plačevanja mesečnega varovanja v primerjavi s premoženjem, ki ga lahko morebiti izgubi ob neljubem dogodku.
Vodstvo organizacije mora zagotoviti varnost sredstev in virov, ki so potrebni za delovanje organizacije. To vključuje tudi varnost sistemov IT. Ponavadi je za varnost IT predviden skop proračun, tako da mora biti vsaka stroškovna zahteva skrbno preučena. Dobro strukturirana metodologija analize tveganja lahko vodstvu pomaga poiskati primerne kontrole, tudi v stroškovnem smislu, ki so nujne za varno delovanje.
Minimalna negativna posledica na organizacijo in potreba po tehtnih odločitvah sta temeljna razloga, da organizacije uvajajo upravljanje s tveganji v svoja IT okolja.

Upravljanje s tveganji je odgovornost vodstva oz. tistega, ki upravlja. Proces upravljanja s tveganji zajema osebje z različnimi vlogami v organizaciji:

- Vodstvo.
  Skrbi, da so zagotovljena potrebna sredstva in viri in da so učinkovito porazdeljeni. Poleg tega morajo pri svojih poslovnih odločitvah upoštevati tudi rezultate analize tveganja. Upravljanje s tveganji je lahko učinkovito le z vključitvijo vodstva v proces.
- Tehnični direktor za področje IT-ja.
  Direktor nosi odgovornost za načrtovanje sistemov IT, njihov proračun in varnostne komponente. Vse te odločitve morajo temeljiti na opravljeni analizi tveganja.
- Lastniki sredstev.

Lastniki sredstev so odgovorni za zagotavljanje primernih kontrol za zagotavljanje celovitosti, zaupnosti in razpoložljivosti njihovih sistemov IT ter podatkov, povezanih z njimi. Odobrijo spremembe na svojih sistemih in so tako vključeni v upravljanje s tveganji.

- Strokovnjaki za varnost IT.
  So odgovorni za uvedbo varnostnih zahtev v njihove sisteme IT. Ko se zgodijo spremembe v sistemih, morajo s pomočjo procesa za upravljanje s tveganji identificirati nova potencialna tveganja in uvesti nove kontrole za zmanjšanje le-teh.
- Ostali uporabniki in njihova ozaveščenost o IT varnosti.
  Osebje organizacije so uporabniki IT sistemov. Uporaba sistemov mora biti v skladu s politiko organizacije, pravili, kar je kritično za ublažitev tveganj in zaščito IT sredstev. Da minimiziramo tveganja na IT sredstvih, se moramo izobraziti na področju varnosti. Učitelji so strokovnjaki na področju varnosti, ki razumejo proces upravljanja s tveganji in vključujejo ocenjevanje tveganja v učni material.

1.3 Ocenjevanje tveganja

Ocenjevanje tveganja je prvi korak pri obvladovanju tveganj. Organizacije uporabljajo ocene za določitev obsega potencialnih groženj in tveganj, povezanih z IT sistemi. Rezultat tega procesa pomaga identificirati primerne kontrole za zmanjšanje ali odpravo tveganja.

Tveganje je verjetnost, da bo dana grožnja izkoristila posamezno ranljivost sredstva in imela negativne posledice na organizacijo.
Za določitev verjetnosti dogodka, morajo biti grožnje analizirane v zvezi s potencialnimi ranljivostmi in kontrolami. Posledica se nanaša na obseg škode, ki je lahko povzročena ob uresničitvi grožnje. Ocenjevanje tveganja zajema 9 korakov [5]:

1. karakterizacija sistema,
2. identifikacija groženj,
3. identifikacija ranljivosti,
4. analiza kontrol,
5. določitev verjetnosti,
6. analiza posledic,
7. ugotavljanje tveganja,
8. priporočene kontrole,
9. dokumentacija razultatov.

Koraki 2, 3, 4, 6 so lahko izpeljani vzporedno, ko je končan korak 1.

1.3.1 Karakterizacija sistema

Za karakterizacijo sistema potrebujemo podatke, ki se sistema tičejo. Identificiranje tveganj v IT sistemih zahteva poznavanje okolja sistema. Osebe, ki upravljajo tveganja, morajo zato najprej zbrati podatke o sistemu:

- strojna oprema,
- programska oprema,
- sistemski vmesniki,
- podatki in informacije,
- osebe, ki upravljajo in osebe, ki uporabljajo IT sisteme,
- procesi, ki jih izvajajo IT sistemi,
- kritičnost podatkov in sistema,
- občutljivost podatkov in sistema.

Poleg naštetih je potrebno zbrati še nekatere druge podatke glede operativnega okolja IT sistemov (npr. funkcionalne zahteve sistema IT, topologija omrežja).
Podatke dobimo s pomočjo različnih tehnik zbiranja informacij: vprašalniki, intervjuji, uporaba raznih orodij (npr. skeniranje omrežja vrne servise, ki tečejo na strežnikih), preučevanje obstoječih varnostnih politik, sistemskih dokumentacij in dokumentacije o že uporabljenih varnostnih mehanizmih v organizaciji.
Rezultat je slika okolja IT sistema in njegovih mej.

1.3.2 Identifikacija groženj

Grožnja pomeni možnost uspešne izrabe ranljivosti sredstva. Ranljivost je šibka točka nekega sistema, ki se jo lahko izkoristi namerno ali nenamerno. Vir grožnje predstavlja ali namero, da izkoristi ranljivost ali pa situacijo, ki nenamerno (ponesreči) sproži ranljivost. Vir grožnje je definiran kot katerakoli okoliščina ali dogodek, ki lahko povzroči škodo na sistemu IT. Najbolj pogosti so naravni (naravne grožnje, kot so poplave, potresi, nevihte), človeški (človeške grožnje: dogodki, ki jih sproži človek, nenamerna in namerna dejanja – napadi na omrežje, podtikanje programov za prisluškovanje, trojanski konji itd.) in okoljski viri (onesnaženje, izlitje nevarnih tekočin). Pri identifikaciji groženj je pomembno naštevanje vseh možnih virov groženj, ki lahko škodujejo sistemom IT. Grožnja, kjer ni ranljivosti, ne

predstavlja tveganja, ker se je ne da izkoristiti. Cilj tega koraka je identifikacija potencialnih groženj in sestava seznama groženj, ki bi lahko ogrozila obravnavan sistem IT.
Človeški viri groženj so še posebno nevarni, ker so lahko motivacijsko naravnani (v nasprotju z ostalimi viri). Tabela prikazuje nekatere današnje človeške grožnje in njihove motivacije ter akcije, ki se zgodijo ob nastopu grožnje.

Vir grožnje	**Motivacija**	**Akcije grožnje**
heker	• izziv • ego • upornost	• socialni inženiring • vdori v sisteme
računalniški kriminalec	• izguba podatkov • dostop do zaupnih podatkov • neodobreno spreminjanje podatkov	• računalniški kriminal • goljufije • izsiljevanje z informacijami • »spoofing«
terorist	• izsiljevanje • uničenje • maščevanje	• bombni napad • napadi na sistem (DoS) • vmešavanje v delovanje sistema

Tabela 1.1: Nekatere grožnje, ki jih povzroči človek.

Te informacije so uporabne organizacijam za preučevanje človeških virov groženj na njihovo okolje. Poleg tega lahko s preučitvijo dokumentiranih preteklih vdorov, s poročili o kršitvah varnosti, poročilih o incidentih in intervjuji s sistemskimi administratorji zberemo informacije za lažje identificiranje človeških groženj, ki lahko škodujejo sistemom in podatkom ob prisotnosti ranljivosti.
Rezultat koraka je seznam groženj, ki lahko izrabijo sistemske ranljivosti.

1.3.3 Identifikacija ranljivosti

Analiza groženj na sistemu vključuje tudi analizo ranljivosti, ki se pojavljajo na sistemu. Cilj je seznam ranljivosti, ki bi jih lahko viri groženj izrabili. Ranljivost je pomankljivost ali šibka točka sistema ali določene varnostne procedure, zasnove, implementacije, rezultat tega se lahko pojavi kot kršitev varnostne politike.

Ranljivost	Vir grožnje	Realizacija grožnje
Požarni zid organizacije dopušča vhodno telnet povezavo na strežnik X, ki ima omogočen uporabniški račun.	Nepooblaščeni uporabniki (hekerji, bivši zaposleni, teroristi, itd.).	Uporaba telneta do strežnika X in brskanje po lokalnem disku strežnika s pomočjo uporabniškega računa.

Tabela 1.2: Primer ranljivosti in vir grožnje, ki izkoristi ranljivost.

Tipi ranljivosti so odvisni od narave sistema IT in od faze, v kateri se nahaja:

- Če sistem še ni zasnovan, je iskanje ranljivosti usmerjeno v preučevanje varnostne politike organizacije, načrtovane varnostne procedure in zahtevane sistemske lastnosti.
- Če je sistem sredi implementacije, so v identifikacijo ranljivosti vključujene bolj specifične informacije, kot so npr. načrtovane varnostne značilnosti, ki so opisane v dokumentaciji varnostnega načrta.
- Če je sistem operativen, proces identifikacije ranljivosti vključuje analizo varnostnih značilnosti IT sistema in varnostnih kontrol (tehničnih in proceduralnih), ki ščitijo sistem.

Metode, ki služijo za identificiranje ranljivosti sistemov:

- Avtomatizirana orodja za iskanje ranljivosti (npr. skeniranje gostiteljev na omrežju za iskanje znanih ranljivih storitev).
- Varnostni testi (vključujejo izvajanje testnega načrta, skripte, procedure z namenom testiranja učinkovitosti varnostnih kontrol sistema).
- Penetracijski testi (namen je testiranje sistema z vidika vira grožnje in identificiranje odpovedi sistemskih varnostnih shem in oceno zmožnosti upiranja sistema na namerne poskuse izognitve sistemske varnosti).

Rezultat koraka je seznam ranljivosti.

1.3.4 Analiza kontrol

Namen tega koraka je analiza kontrol, ki so bile implementirane, ali pa so načrtovane. Kontrole minimizirajo ali odpravijo možnost uresničitve grožnje.

Velja, da je verjetnost uresničitve grožnje ob dani ranljivosti majhna, če v sistemu obstajajo učinkovite varnostne kontrole, ki preprečujejo ali odpravljajo škodo. Kontrole obsegajo tehnične metode (metode, ki so vključene v strojno opremo, programsko opremo: mehanizem

nadzor dostopov, identifikacija in avtorizacija, metode kriptiranja, oprema za zaznavo vlomov) in ne-tehnične metode (operativne procedure, varnostne politike, fizična zaščita z osebjem).

Kontrole se ne glede na metode razvrščajo v dve skupini:

- Preventivne kontrole ovirajo poskuse kršitve varnostne politike in vključujejo kontrole preverjanja dostopa, enkripcije, avtentikacije.
- Kontrole detekcije opozarjajo na kršitve varnostne politike, kot npr. metode, ki zaznavajo vlome.

Rezultat je seznam trenutnih ali načrtovanih kontrol, ki bi zmanjšale ali morda odpravile verjetnost uresničitve grožnje.

1.3.5 Določitev verjetnosti

Za splošno oceno verjetnosti uresničitve grožnje ob dani ranljivosti morajo biti upoštevani naslednji faktorji:

- motivacija vira grožnje in njegovo znanje oz. sposobnost,
- narava ranljivosti,
- obstoj in učinkovitost trenutnih kontrol.

Verjetnost se lahko predstavi opisno npr. kot »visoka«, »srednja«, »nizka«.

Verjetnost	**Pomen**
Visoka	Vir grožnje je zelo motiviran in dovolj sposoben uresničitve grožnje ob dani ranljivosti. Poleg tega pa so kontrole, ki preprečujejo izrabo ranljivosti neučinkovite.
Srednja	Vir je motiviran in sposoben. Kontrole obstajajo in so na splošno dovolj uspešne.
Nizka	Vir grožnje ima ali premalo motivacije ali znanja ali pa so kontrole zelo uspešne pri preprečitvi izrabe ranljivosti.

Tabela 1.3: Primer kvalitativnega razvrščanja verjetnosti grožnje.

1.3.6 Analiza posledic

Naslednji korak pri ocenjevanju tveganja je določitev škodljivih posledic ob uresničitvi grožnje ob dani ranljivosti. Pri tem se opremo na procese, ki jih izvajajo IT sistemi, kritičnost

in občutljivost podatkov ter sistema. Podatke o teh najdemo v dokumentaciji, ki opisuje posledice na delovanje organizacije. Če pa ta dokumentacija ne obstaja, se opremo na specifikacijo zahtev, ki so potrebne, da vzdržujemo sistemsko in podatkovno celovitost, zaupnost ter razpoložljivost.

Pokaže se torej škodljiva posledica takega dogodka v zmanjšanju ene ali kombinacije treh varnostnih zahtev: celovitosti, zaupnosti in razpoložljivosti.

Nekatere posledice so lahko merljive kvantitativno kot npr. izpad dohodka, strošek popravila sistema ali potreben nivo napora, da popravimo posledice. Spet druge pa se ne morejo izraziti v enotah, tako da njihove vrednosti lahko opišemo kvalitativno kot »visoka«, »srednja«, »nizka« vrednost.

Rezultat je velikostni red posledic uresničitve grožnje ob dani ranljivosti.

1.3.7 Ugotavljanje tveganja

Namen tega koraka je ugotavljanje nivoja tveganja za sistem IT. Določitev tveganja dvojice grožnja/ranljivost je odvisna od:

- verjetnosti vira grožnje, da bo uresničil svojo namero ob dani ranljivosti,
- obsega učinka škode ob takem dogodku,
- primernosti obstoječih ali načrtovanih varnostnih kontrol za zmanjševanje tveganja takih dogodkov.

Za ocenjevanje tveganja grožnje na sredstvu se uporablja matrika tveganja. Končno tveganje se izračuna iz produkta verjetnosti grožnje in posledice grožnje. Velikost matrike je odvisna od števila vrednosti za verjetnost grožnje in posledice grožnje. Tako je primer (Slika 1.2) matrike velikosti 3 x 3 za verjetnost grožnje (visoka, srednja, nizka) in posledice grožnje (visoka, srednja, nizka).

Verjetnost grožnje	**Negativne posledice grožnje**		
	Nizka (10)	Srednja (50)	Visoka (100)
Visoka (1.0)	Nizka 10 x 1.0 = 10	Srednja 50 x 1.0 = 50	Visoka 100 x 1.0 = 100
Srednja (0.5)	Nizka 10 x 0.5 = 5	Srednja 50 x 0.5 = 25	Srednja 100 x 0.5 = 50

Nizka (0.1)	Nizka 10 x 0.1 = 1	Nizka 50 x 0.1 = 5	Nizka 100 x 0.1 = 10

Slika 1.2: Primer matrike velikosti 3 x 3, kjer verjetnosti grožnje pri 1.0 ustreza visok nivo, 0.5 srednjemu nivoju in 0.1 nizkemu nivoju. Vrednost posledic grožnje 100 ustreza visokemu nivoju, 50 srednjemu nivoju in 10 nizkemu nivoju. Tveganje: visoko (od 50 do 100), srednje (od 10 do 50), nizko (od 1 do 10).

Pomen nivojev tveganja, katerim je sistem IT podvržen:

Tveganje	**Opis tveganja in potrebne akcije**
Visoko	Visoka potreba po izboljšanju sistema.
Srednje	Potreba je po po izboljšavi sistema v doglednem času.
Nizko	Presodi se, če so izboljšave sploh potrebne.

Tabela 1.4: Opis tveganj.

1.3.8 Priporočene kontrole

V tem koraku se izbira med kontrolami, ki bi lahko zmanjšale ali odpravile identificirane ranljivosti in ki so v skladu z delovanjem organizacije. Cilj predlaganih kontrol je, da se zmanjša ogroženost sistema in podatkov na sprejemljiv nivo. Pri predlaganju kontrol se mora upoštevati naslednje faktorje:

- učinkovitost predlaganih možnosti,
- upoštevanje zakonodaje in uredb,
- politika znotraj organizacije,
- vpliv na delovanje,
- varnost in zanesljivost.

Implementirati se ne more vseh predlaganih kontrol, pred tem je potrebna še analiza stroškov posameznih kontrol.

Rezultat koraka je seznam predlaganih kontrol ali alternativnih rešitev za zmanjšanje tveganja.

1.3.9 Dokumentacija razultatov

Ko je opravljena analiza tveganja oz. urejanje s tveganji, je treba rezultate dokumentirati v obliki poročil. Taka poročila pomagajo vodstvu in ostalim odgovornim sprejemati odločitve glede varnostne politike in politike na splošno v organizaciji, proračunu, spremembah znotraj organizacije itd. Poročilo mora biti predstavljeno razumljivo, tako da vodstvo razume tveganja in lahko dodeli potrebne vire za zmanjšanje ali odpravo izgub.

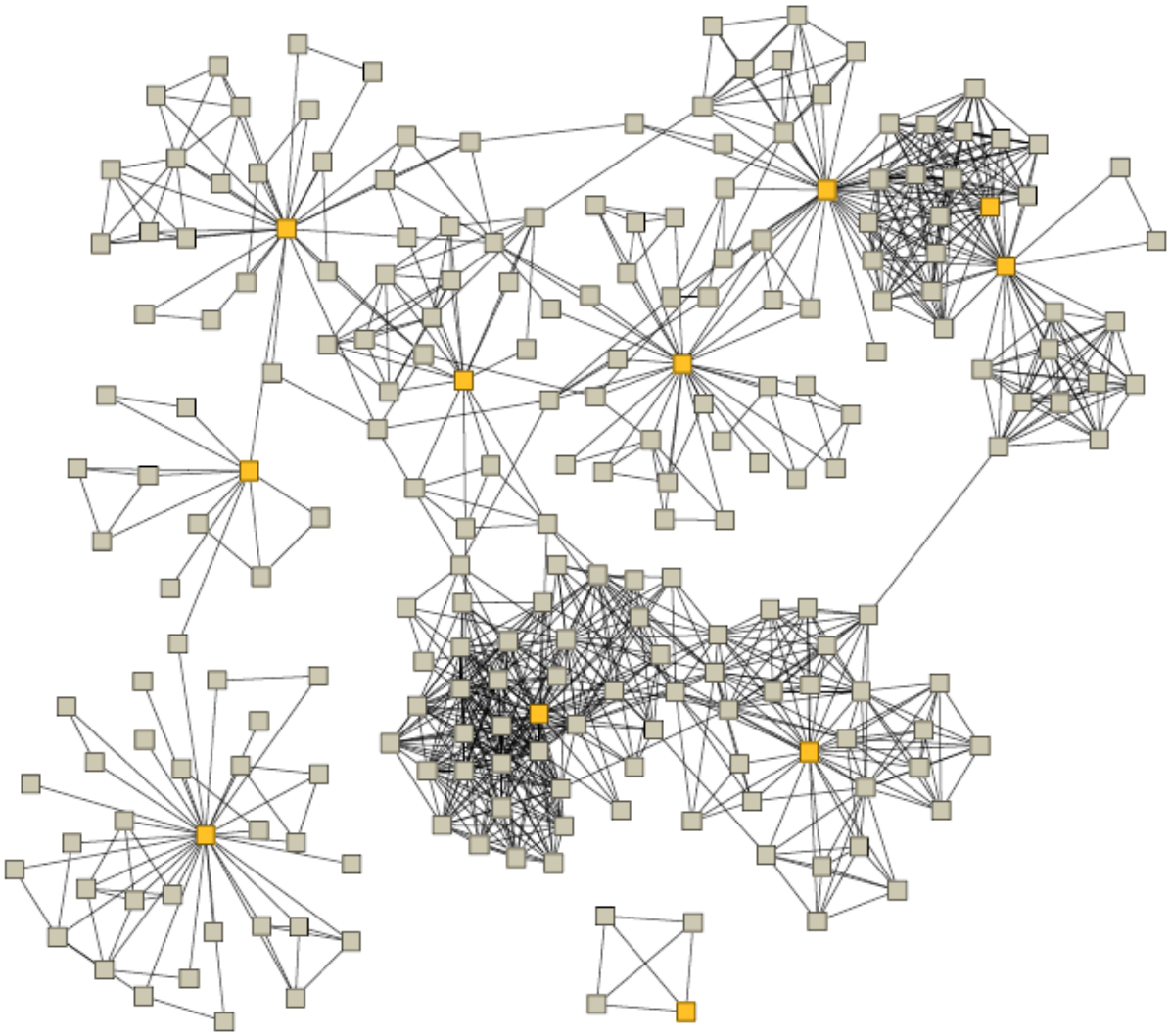
1.4 Osrednji prispevek diplomskega dela

V diplomski nalogi se bom osredotočil na točki 1.3.7 in 1.3.9, kjer bom poskušal z uporabo omrežij oz. grafov natančeje določiti tveganja in predstaviti tako dobljene rezultate vodstvenemu kadru organizacije.

Poglavje 2
Teoretična izhodišča

2.1 Predstavitev teorije mrež

Na splošno velja, da se trgovci med seboj sporazumevajo neposredno ali posredno. V resnici pa so stvari rahlo drugačne in različne komponente vplivajo na njihov izbor partnerjev, s katerimi komunicirajo ali trgujejo. Trgovci imajo na trgu raje trgovske partnerje že zaradi morebitnih preteklih izkušenj z njimi, poznanstev ali zaupanja. Kupci in prodajniki imajo raje določene dobavitelje in stranke. Končni uporabniki imajo rajši določene znamke. Večina posameznikov omejuje svoje delovanje, ekonomsko ali kakšno drugačno na izbran, zaključen krog partnerjev ali poznanstev. V večini primerov partnerji niso izbrani le na ekonomski postavki, ampak na socialni osnovi: posamezniki se nagibajo k sodelovanju (ali trgovanju ali poslovanju) s posamezniki, ki se gibljejo in razvijajo (intelektualno in kulturno) v enakih krogih, kot so oni sami. Vzorci povezav med agenti tvorijo družabno mrežo (Slika 2.1). Struktura takih omrežij vpliva na vzorce ekonomskih transakcij ali katerihkoli socialnih stikov med ljudmi. Katerakoli teorija medsebojnih stikov ali sodelovanja (povezav), ki ignorira taka omrežja, je nepopolna. Zato so raziskovalci v zadnjih desetletjih naredili obsežne raziskove omrežij v ekonomiji, matematiki in sociologiji, da bi doumeli njihov pomen.



Slika 2.1: Primer družabnega omrežja, kjer vozlišča predstavljajo ljudi, povezave pa njihove medsebojne socialne vezi.

Raziskava omrežja zajema tri glavne korake. Prvi korak je empiričen, s katerim sestavimo strukturo omrežja s pomočjo tehnik intervjujev, vprašalnikov, opazovanj, uporabe arhivskih podatkov. Cilj takih študij je sestavljanje celotne slike povezav med posamezniki (poslovne povezave, osebne povezave) ali entitetami. Študije morajo biti seveda prirejene področju opazovanja in merjenju povezav, ki nas zanimajo. Drugi korak nam govori o skupnosti, ki predstavlja omrežje z uporabo matematičnih in statističnih analiz. To je domena klasičnih analiz družabnih omrežij, ki se fokusirajo na vprašanja, kot so: kdo je najbolj središčen član omrežja in kdo obroben, kateri člani imajo največ vpliva, ali skupnost razpade na več manjših skupin in kakšne so, katere povezave so kritične za delovanje skupine. Tretji korak je spoznanje iz zbranih podatkov (prvi korak) in analiz (drugi korak). Tako lahko zgradimo model (matematični ali računalniški) procesov, ki se dogajajo v takšnih omrežnih sistemih.

Modeliranje nam omogoča napovedovanje obnašanja omrežja kot funkcija parametrov, ki vplivajo na sistem.

2.2 Omrežje

Omrežje ali mreža, ki ji v matematiki pravimo tudi graf, je sestavljena iz točk, imenovanih vozlišča, in povezav med točkami. Matematično gledano omrežje predstavimo z matriko sosednosti A. To je simetrična matrika velikosti $n \times n$, kjer je n število vseh vozlišč omrežja ali grafa. Matrika sosednosti ima torej elemente:

$$A_{ij} = \begin{cases} 1\,; & če\ obstaja\ povezava\ med\ i\ in\ j \\ 0\,; & sicer \end{cases} \tag{2.1}$$

Matrika je simetrična pri obstoju povezave med vozliščema i in j, velja tudi, da obstaja povezava med j in i. Torej je $A_{ij} = A_{ji}$.
V nekaterih omrežjih so povezave utežene, kar pomeni, da so nekatere povezave močnejše od preostalih povezav. V tem primeru neničelni elementi matrike sosednosti ustrezajo vrednostim, ki so manjše od 1, kar predstavljajo močnejše ali šibkejše povezave.

Varianta grafov so usmerjeni grafi, v katerih so povezave usmerjene, imajo začetno in končno vozlišče. Usmerjeni grafi so predstavljeni z asimetrično matriko sosednosti, v kateri $A_{ij} = 1$ predstavlja obstoj povezave, ki poteka v smeri od i do j.

Omrežja imajo lahko tudi več povezav med vozlišči, povratne povezave (vozlišče je povezano s samim seboj) in hiper povezave (povezave, ki povezujejo več kot dve vozlišči).

Analiza omrežnih podatkov se ponavadi prične pri ocenjevanju mer središčnosti, ki so tudi najbolj osnovne in najbolj pogosto uporabljene mere [1]. Mere središčnosti odgovarjajo na vprašanja tipa »Katero vozlišče je najbolj pomembno ali središčno v omrežju?«. Odgovorov je lahko več, odvisno od tega, kaj mislimo z »najbolj pomembno«.

2.3 Mere središčnosti

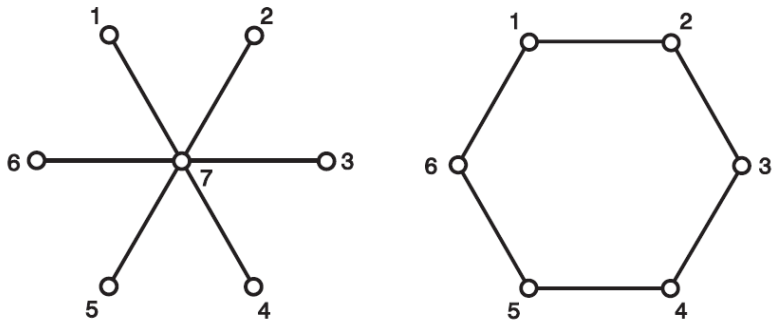
2.3.1 Stopnja vozlišča

Najenostavnejša mera središčnosti je stopnja vozlišča. Stopnja vozlišča v grafu je mišljena kot število povezav, ki so povezane s tem vozliščem. Matematično to označimo kot:

$$\deg(v) \tag{2.2}$$

Stopnja vozlišča je pogosto zelo učinkovita mera za merjenje vplivnosti ali pomembnosti vozlišča. V družabnem omrežju bi pomenilo, da je človek z velikim številom povezav tudi zelo vpliven. To je absolutna mera središčnosti glede na stopnjo. Absolutnih mer ne moremo uporabiti za primerjavo središčnosti po omrežjih z različnim številom točk, zato te mere ponavadi normaliziramo, tako da dobimo mero iz intervala [0,1]. To so relativne mere središčnosti.

$$C_D = \frac{\deg(v)}{n-1} \tag{2.3}$$



Slika 2.2: Primer omrežja zvezda in cikel. V prvem je vozlišče 7 najbolj središčno (s stopnjo 6), ostale pa so enako središčne. V drugem omrežju so si vsa vozlišča enako središčna s stopnjo 2.

2.3.2 Z lastnimi vektorji

Bolj zapletena varianta stopnje vozlišča je t.i. mera središčnosti z lastnimi vektorji. Tu pomeni stopnja vozlišča število povezav, ki jih ima vozlišče, pri čemer za mero središčnosti z lastnimi vektorji velja, da si niso vse povezave enake. V splošnem velja, da povezave z ljudmi, ki so vplivni, več pripomorejo k vplivnosti posamezne osebe kot povezave z manj vplivnimi. Torej je $A_{ij} = 1$, če je vozlišče i povezano z vozliščem j in $A_{ij} = 0$, če ni povezave. Bolj splošno velja, da so lahko elementi v matriki A realna števila, ki predstavlajo moč povezave.
Če označimo mero središčnosti vozlišča i z x_i, potem je mera središčnosti vozlišča i sorazmerna z vsoto mer središčnosti vozlišč, ki so povezane z vozliščem i.
Torej:

$$x_i = \frac{1}{\lambda}\sum_{j \in M(i)} x_j = \frac{1}{\lambda}\sum_{j=1}^{N} A_{ij}x_j, \tag{2.4}$$

kjer je λ je konstanta in N dimenzija matike A. Če definiramo mere središčnosti vozlišč v zaporedju, dobimo vektor mer središčnosti in lahko enačbo prepišemo v matrično obliko:

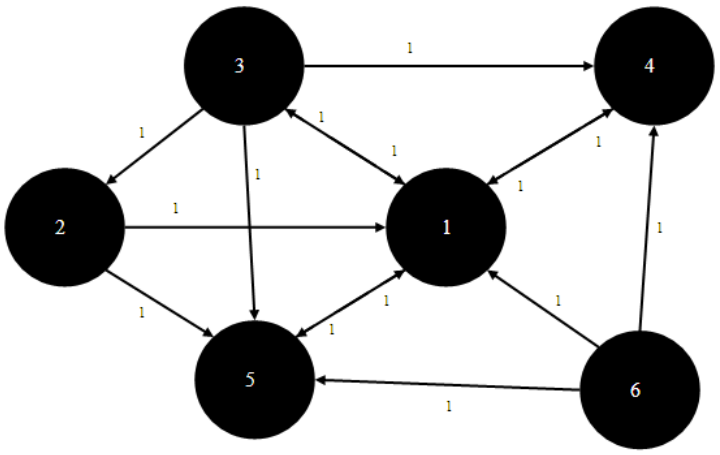
$$x = \frac{1}{\lambda} Ax \tag{2.5}$$

$$\lambda x = Ax \tag{2.6}$$

Vidimo, da je x lastni vektor matrike sosednosti A z lastno vrednostjo λ. Ker hočemo, da so mere središčnosti vse pozitivne vrednosti, po Perron–Frobenius teoremu [18] velja, da je λ največji lastni vektor matrike sosednosti s pozitivnimi vrednostmi in x ustrezni lastni vektor. i-ta komponenta lastnega vektorja poda želeno središčno mero vozlišča i v grafu. Perron–Frobenius teorem pravi, da ima kvadratna matrika s pozitivnimi realnimi elementi enolično največjo realno lastno vrednost in z ustreznim lastnim vektorjem s pozitivnimi komponentami. Taka mera središčnosti dodeli vsakemu vozlišču vrednost središčnosti, ki temelji na številu in kakovosti njegovih povezav: število povezav še vedno nekaj pomeni, vendar lahko vozlišče z manjšim številom zelo močnih povezav prednjači pred vozliščem z velikim številom povprečnih povezav. (Googlov algoritem PageRank za rangiranje spletnih strani je varianta mere središčnosti z lastnimi vektorji.)

Primer 1.1:

Začetni graf s povezavami in pripadajoča matrika sosednosti:



Slika 2.3: Začetni graf.

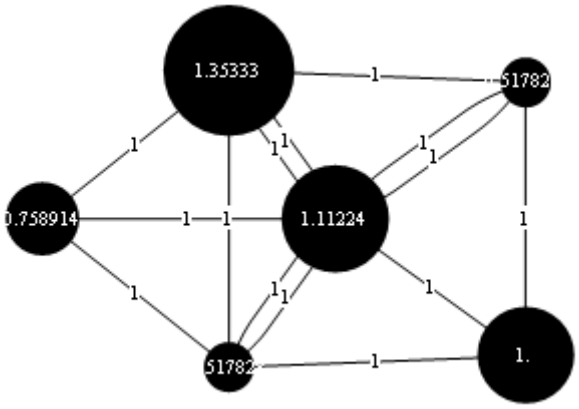
Matrika sosednosti zgornjega grafa:

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Izračunan in normaliziran lastni vektor matrike, ki ustreza vrednostim vozlišč:

$$\begin{bmatrix} 1.11224 \\ 0.758914 \\ 1.35333 \\ 0.517828 \\ 0.517828 \\ 1 \end{bmatrix}$$

Graf s Slike 2.3 ob upoštevanju lastnega vektorja matrike sosednosti. *i*-ta komponenta lastnega vektorja pripada *i*-temu vozlišču in predstavlja njegovo središčno mero. Graf na Sliki 2.4 upošteva te vrednosti tako, da je premer vozlišča odvisen od izračunane vrednosti *i*-te komponente lastnega vektorja.

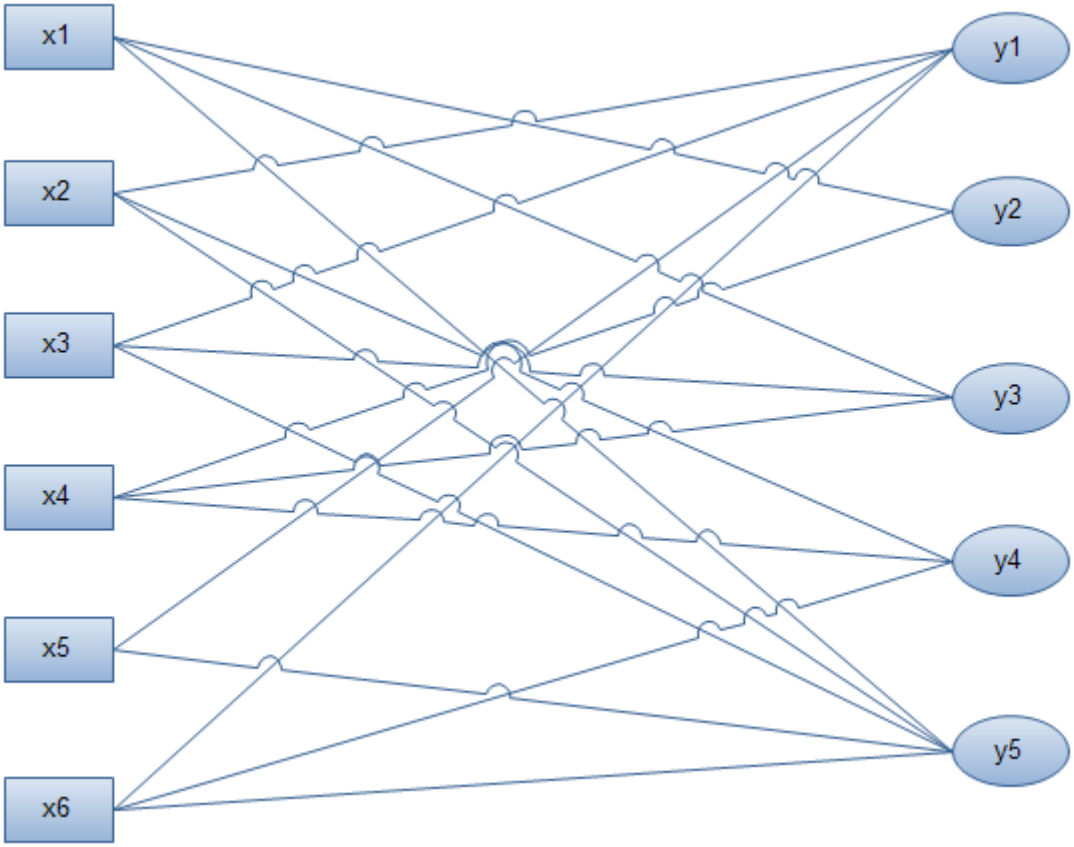


Slika 2.4: Dobljen graf omrežja iz primera.

2.4 Dvovrstna omrežja

Dvovrstno omrežje je sestavljeno iz dveh tipov entitet ali vozlišč (lahko so revije, bralci), relacija pa povezuje ti dve množici entitet, npr. bralci berejo revije. Primer takega omrežja je omrežje bralcev in revij, kjer bralec prebira revijo.

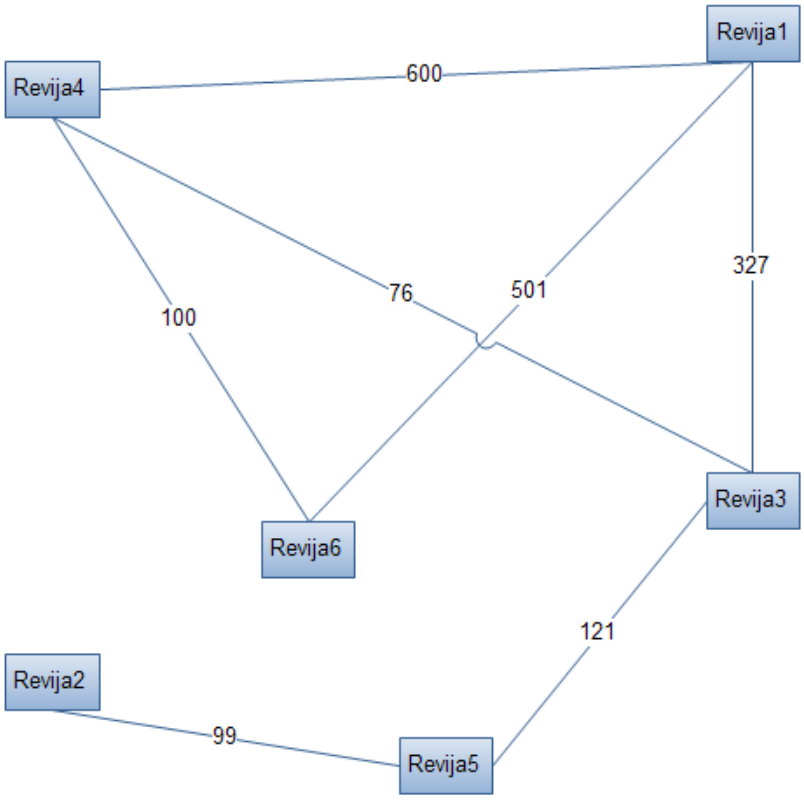
Graf, ki pripada omrežju, se imenuje dvodelen graf, povezave pa povezujejo točke ene množice entitet s točkami druge množice entitet [10]. Znotraj posamezne množice pa ni povezav.



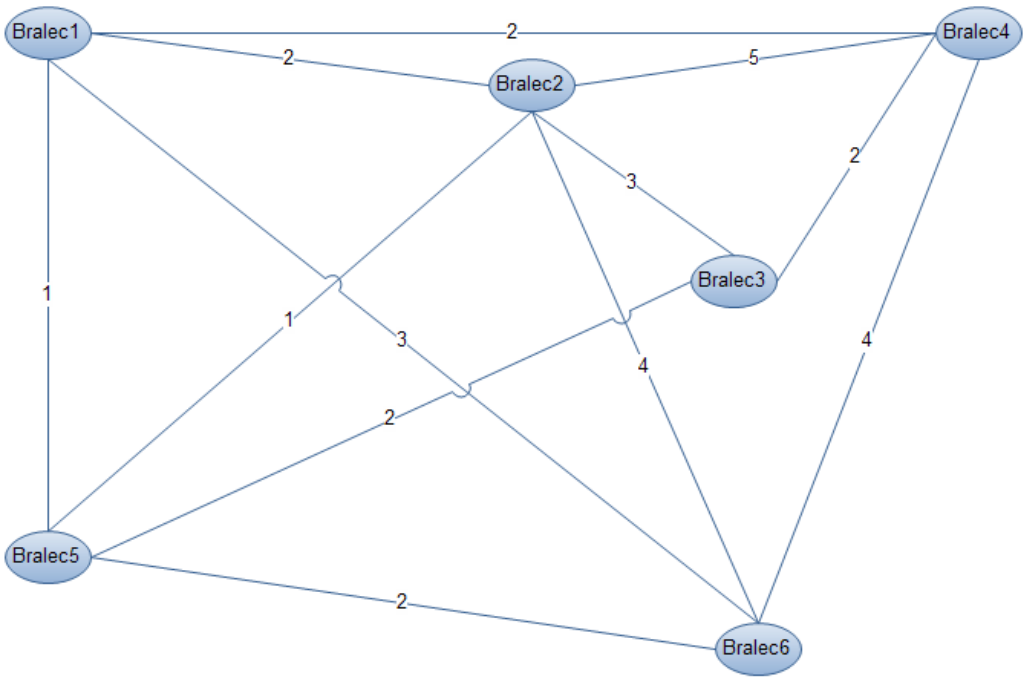
Slika 2.5: Primer dvodelnega grafa, kjer X predstavlja bralca, Y pa revijo. Povezava med X in Y pomeni, da bralec X bere revijo Y.

2.5 Pretvorba dvovrstnih omrežij v običajna omrežja z vrednostmi na povezavah

Dvovrstno omrežje lahko pretvorimo v običajno omrežje, kjer so vozlišča novega omrežja samo vozlišča iz prve ali iz druge množice entitet dvodelnega grafa [10]. Pretvorba dvovrstnega omrežja v običajno omrežje na primeru bralcev revij bi lahko bila dvojna. Vozlišča so lahko revije, relacije – povezave med vozlišči – revijami pa so bralci (bralci, ki berejo obe reviji, ki predstavljata vozlišči povezave). Povezava med revijama obstaja, če obstaja vsaj ena oseba, ki bere obe reviji. Vrednost na povezavi je torej število teh bralcev. Vrednost vozlišč pa je v tem primeru število vseh bralcev določene revije. Če pa pretvorimo v običajno omrežje, kjer so vozlišča bralci, potem so relacije – povezave med bralci njihove skupne revije. Povezava med bralcema obstaja, če bereta vsaj eno skupno revijo. Vrednost na povezavi je torej število skupnih revij in vrednost vozlišča je število revij, ki jih bralec bere.



Slika 2.6: Pretvorjeno dvovrstno omrežje v običajno omrežje, kjer so vozlišča revije, povezave pa število skupnih bralcev.



Slika 2.7: Omrežje bralcev s skupnim številom revij na povezavah.

Povezanost med revijami se lahko sklepa, če omrežje prej še normaliziramo. Obstaja več možnih smiselnih normalizacij [10]:

$$Geo_{ij} = \frac{a_{ij}}{\sqrt{a_{ii}a_{jj}}} \tag{2.7}$$

$$Min_{ij} = \frac{a_{ij}}{\min(a_{ii},a_{jj})} \tag{2.8}$$

$$MinDir_{ij} = \begin{cases} \frac{a_{ij}}{a_{ii}}\ ; & \check{c}e\ a_{ii} \leq a_{jj} \\ 0\ ; & sicer \end{cases} \tag{2.9}$$

a_{ij} je element matrike A, ki pripada i-ti vrstici in j-temu stolpcu. Matrika A je matrika sosednosti. Normalizacije so narejene tako, da vsak element v matriki delimo z ustreznim diagonalnim elementom ali ustreznima diagonalnima elementoma. Primer normalizacije je npr. *Geo*, *MinDir* in *Min* [10]. Pri normalizaciji *Geo* se vrednosti normalizirajo z geometrijsko sredino obeh diagonalnih elementov. Tako dobimo normalizacijo, ki meri povezanost oz. korelacijo med revijami. Pri normalizaciji *MinDir* vrednost na povezavi pove, kolikšen del bralcev, ki bere prvo revijo, bere tudi drugo. Pri normalizaciji *Min* se vrednosti normalizirajo z najmanjšim diagonalnim elementom.

Poglavje 3

Uporaba mrež pri analizi tveganja

3.1 O sistemu

Pri analizi tveganja neka grožnja lahko ogrozi določeno informacijsko sredstvo v organizaciji, kar predstavlja določeno tveganje, ki ga subjektivno oceni strokovnjak področja. Imamo torej opravka s tremi začetnimi entitetami sistema, in sicer ranljivost kot najbolj osnoven del, ki povezuje entiteti grožnjo in informacijsko sredstvo. Poznamo pa še dodatno entiteto sistema – ukrepe. Z ukrepi zmanjšamo ali popolnoma odpravimo ranljivosti določenega informacijskega sredstva, tako da se tveganje zmanjša ali izniči. Na osnovi podanega bi narisali graf ocen tveganja in povezav med njimi. Ocena tveganja ocenjuje tveganje grožnje za določeno informacijsko sredstvo oz. da bo grožnja izkoristila ranljivosti informacijskega sredstva. Ocena torej zajema kombinacijo grožnje in informacijskega sredstva ter jo bomo v nadaljevanju imenovali kar *dvojica*. Povezava med dvojicama obstaja, če obstaja vsaj ena skupna ranljivost. Ta graf imenujemo graf dvojic. Za potrebe ocenjevanja pomembnosti ranljivosti bomo uporabili še dva grafa, in sicer graf ranljivosti na osnovi ukrepov, ki povezuje ranljivosti na podlagi skupnih ukrepov, in graf ranljivosti na osnovi dvojic, ki povezuje ranljivosti na podlagi skupnih dvojic in je ravno obraten od prvega grafa, ki povezuje dvojice s skupnimi ranljivostmi (glej 2.4 in 2.5).

Ideja je, da bi iz obeh grafov sklepali na ocene pomembnosti posamezne ranljivosti, ki bi jih nato v naslednji stopnji uporabili za ocenjevanje tveganja dvojic v grafu dvojic. Ker vsaka dvojica v grafu dvojic predstavlja [grožnja, informacijsko sredstvo], v resnici dobimo tudi graf povezanih groženj.

Radi bi izvedeli, katere ranljivosti so najbolj nevarne, na katere moramo biti najbolj pazljivi in katere je treba posebej izpostaviti pri prikazovanju rezultatov analize tveganja vodstvu organizacije. Poleg tega bi bil tudi zaželen prikaz povezav ranljivosti med seboj. Ko bi določili t.i. oceno pomembnosti posameznih ranljivosti, bi v drugem delu z njihovimi

ocenami lažje določili tudi pomembnosti groženj na informacijskih sredstvih. Pri tem moramo upoštevati tudi ostale podatke, kot so npr. strokovnjakova subjektivna ocena tveganja posamezne grožnje na informacijskem sredstvu, število ranljivosti, število ukrepov, število posledic, morebiten vpliv dvojice grožnje na informacijskem sredstvu na ostale dvojice in morebiten vpliv ostalih dvojic na obravnavano.

3.2 Pomen dobljenih grafov

Graf dvojic bi koristil predvsem pri identifikaciji najbolj tvegane dvojice oz. grožnje informacijskemu sredstvu. Graf ranljivosti predstavi, katera ranljivost je najbolj razširjena, s tem že tudi podamo najbolj izpostavljeno ranljivost, ki bi jo bilo potrebno odpraviti, da se stanje sistema izboljša. Ker je taka ranljivost ponavadi tudi močno povezana z ostalimi, odprava take ranljivosti pomeni tudi širšo posledico, saj prizadane več groženj in informacijskih sredstev.

Po določitvi informacijskih sredstev in njihovih ranljivosti, groženj, tveganj ter ukrepov za odpravo ranljivosti, imamo na razpolago informacije za izgradnjo grafa ranljivosti. Kot zgoraj povedano, bomo generirali dva grafa:

- graf ranljivosti na podlagi skupnih ukrepov,
- graf ranljivosti na podlagi skupnih dvojic.

Oba grafa nam bosta služila za določitev ocene pomembnosti posamezne ranljivosti.

3.3 Graf ranljivosti

3.3.1 Graf ranljivosti na podlagi ukrepov

Ker so podane relacije ukrep–ranljivost (posamezno ranljivost odpravi določeno število ukrepov), lahko narišemo pripadajoči dvodelni graf z množico ukrepov na eni strani in množico ranljivosti na drugi strani. Povezav med elementi znotraj množice ni. Povezava med elementom iz prve množice in elementom iz druge množice obstaja, če se da določeno ranljivost odpraviti z ukrepom. Tako dobljen dvodelen graf nato pretvorimo v običajno omrežje, pri čemer predstavljajo vozlišča ranljivosti, povezave pa skupni ukrepi med ranljivostima. Povezava med ranljivostima torej obstaja, če imata obe ranljivosti vsaj en skupen ukrep.

Ocena ranljivosti je odvisna od tega, kako je ranljivost razširjena (koliko povezav z drugimi ranljivostmi obstaja). Ne smemo pa tudi zanemariti števila ukrepov, s katerimi se da posamezno ranljivost odpraviti, kar igra odločilno vlogo pri določanju ocene ranljivosti. Pri tako dobljenem grafu določimo jakost oz. moč povezanosti med ranljivostmi, tako da nadomestimo vrednost povezav z normalizacijsko mero Geo (2.7). Geo torej normalizira število skupnih ukrepov dveh ranljivosti z geometrijsko sredino števila ukrepov pri posamezni ranljivosti.

Oceno ranljivosti bi torej radi dobili na podlagi povezanosti z ostalimi ranljivostmi in ob upoštevanju števila ukrepov, s katerimi se odpravi ranljivost, ker očitno velja, da bi morala imeti ranljivost, ki ima veliko število ukrepov, tudi visoko oceno pomembnosti. Ranljivost, ki ima veliko povezav z drugimi ranljivostmi, se smatra kot zelo razširjena ranljivost in kot taka običajno pomeni visoko tveganje, tako da bi morala tudi ta dobiti visoko oceno. Slednjo bi lahko na najbolj enostaven način izračunali s pomočjo stopnje vozlišč, vendar bi imele ob skoraj polno povezanem grafu ranljivosti približno enake ocene, poleg tega pa obravnavamo vse povezave enako. Iz podobnega razloga glede na dostopnost in vmesnost nista primerni tudi središčni meri. Radi bi dosegli tudi to, da ocena ranljivosti ni odvisna samo od njene stopnje vozlišča oz. števila njenih povezav do drugih ranljivosti, ampak da se pri določanju njene ocene upošteva tudi njena okolica, torej tudi ocene ranljivosti, s katerimi je obravnavana ranljivost povezana. Za vsako ranljivost pa je dana ranljivost povezana z določeno močjo, ki smo jo izračunali z Geo normalizacijo. Ocena ranljivosti je torej odvisna od »jakosti« povezav na njene sosede (povezane ranljivosti) in tudi od ocene sosed (povezane ranljivosti).

Potrebujemo torej metodo, ki bi ocenila vozlišče na osnovi njenih povezav, jakosti njenih povezav in pri tem upoštevala tudi ocene sosedov. Enostavna rešitev, ki se ponuja, je uporaba utežene linearne kombinacije ocen vseh sosedov. Ocene sosedov utežimo z vrednostjo povezave na sosedo in nato seštejemo vse produkte. Ideja je omejena na lokalno ocenjevanje, ker v tem primeru upoštevamo samo neposredne sosede, torej je dolžina koraka 1 ($k = 1$). Če povečujemo korak $k + 1$, obiščemo širšo okolico danega vozlišča, njegove posredne sosede. Pri tem ustrezno oceno posrednega vozlišča pomnožimo še z uteženo vrednostjo koraka. V najbolj enostavnem primeru bi bila utež $\frac{1}{k}$. Velja, da bolj oddaljeni posredni sosedi šibkeje vplivajo kot bližnji sosedi. Pri tem pa nastopi nov problem, ki se pojavi, in sicer kako določiti število korakov oz. konstanto k. Ne vemo torej, kako daleč od prvotnega vozlišča naj se sprehodimo in obiščemo njegove posredne sosede za izračun njegove ocene. Verjetno dolžina koraka 2 ($k = 2$) zadostuje in pokrije dovolj veliko okolico vpliva, ker imajo bolj oddaljeni sosedi prešibek vpliv. Boljša kot fiksiranje konstante k, bi bila iterativna metoda, pri kateri sproti računamo, kako daleč oz. koliko korakov od prvotnega vozlišča se še splača obiskati posredna vozlišča pri izračunu ocene vozlišča. Če je razlika med novo izračunano vrednostjo in prej izračunano vrednostjo manjša od v naprej določene konstante ε (ki je poljubno majhna), končamo s povečevanjem korakov in se zadovoljimo z izračunano vrednostjo oz. oceno vozlišča. Naslednja podobna rešitev pri ocenjevanju vozlišča prav tako zajema linearno kombinacijo ocen vozlišč z vrednostjo povezav med njimi. Podobno kot prej, bi z iterativno metodo iskali končne ocene vozlišč, in sicer:

1. Na začetku ($k = 1$) inicializiramo ocene vsakega vozlišča na začetno vrednost. To je lahko npr. neka začetna lastnost vozlišča. V našem primeru je to število ukrepov na ranljivosti.

$$\forall i: x_i^1 = \frac{število\ ukrepov\ proti\ ranljivosti\ i}{število\ vseh\ ukrepov} \tag{3.1}$$

2. Nato povečujemo korak $k \leftarrow k + 1$:

$$\forall i: x_i^{k+1} = \sum_{j \in M(i)} v(i,j) x_j^k, \tag{3.2}$$

kjer je $v(i,j)$ vrednost povezave med vozliščema i in j, x_j^k, pa je ocena vozlišča iz prejšnje iteracije. Korake povečujemo, dokler se ne zadosti v naprej postavljenemu

pogoju, npr. da se nova ocena v koraku $k+1$ ne razlikuje bistveno od ocene v prejšnjem koraku k:

$$\left(x_i^{k+1} - x_i^k\right) < \varepsilon. \tag{3.3}$$

Na ta način v prvi iteraciji zajamemo vse neposredne sosede, njihove začetne ocene, ki jih nato zmnožimo z vrednostmi povezav. V naslednji iteraciji ponovimo isto, vendar bo sedaj ocena neposrednega vozlišča zajemala širšo okolico kot v prejšnji iteraciji, kar se pozna na popravljeni oceni sosednih vozlišč.

Sorodna rešitev in rešitev, ki smo jo tudi uporabili, zajema uporabo mere središčnosti z lastnimi vektorji. Kot povedano, moramo v ta namen sestaviti matriko sosednosti, kjer vrednosti elementov matrike predstavljajo jakosti oz. moči povezave dveh vozlišč. Oceno x_i posameznega vozlišča i ocenjujemo z linearno kombinacijo ocen njegovih sosedov, ki so pomnožene z vrednostjo elementa matrike sosednosti.

$$x_i = A_{i1}x_1 + A_{i2}x_2 + A_{i3}x_3 + \ldots = \sum_{j \in M(i)} A_{ij}x_j \tag{3.4}$$

$$x_j = \sum_{k \in M(j)} A_{jk}x_k \tag{3.5}$$

$M(i)$ je množica sosednih vozlišč vozlišča i in zajema tudi vozlišče j, pri čemer x_j označuje njegovo izračunano oceno. Kar pa pomeni, da so v oceni x_j že zajete ocene okoliških vozlišč vozlišča j in je ni potrebno ponovno računati pri ocenjevanju vozlišča i.
V zgornji izraz vpeljemo konstanto λ in ga zapišemo v obliki:

$$x_i = \frac{1}{\lambda} \sum_{j \,\epsilon\, M(i)} A_{ij}x_j \tag{3.6}$$

Tako dobimo že znano obliko, ki jo ob upoštevanju vseh vrednosti ocen lahko nadaljnjo zapišemo v vektorsko in matrično obliko:

$$x = \frac{1}{\lambda} Ax \tag{3.7}$$

V ta namen moramo iz grafa ranljivosti na podlagi ukrepov sestaviti pripadajočo matriko sosednosti, kjer pa povezavo med ranljivostima izrazimo z Geo.

Na ta način rešimo prvi del problema, ki zadeva razširjenost ranljivosti in povezljivost z ostalimi ranljivostmi. Za rešitev drugega problema, ki se nanaša na število ukrepov posamezne ranljivosti, s katerimi se jo da odpraviti in je nekakšna začetna ocena vozlišča, pa se zatečemo k enemu od dveh načinov. V prvem primeru lahko elemente matrike sosednosti zmnožimo z normalizirano vrednostjo števila ukrepov pripadajoče ranljivosti (to je nekakšna ocena števila ukrepov na posamezni ranljivosti, kar bo razloženo kasneje). Vrednosti matrike množimo tako, da bi za obravnavano ranljivost vsako vrednost povezave zmnožili z normalizirano vrednostjo števila ukrepov (y_j') na ranljivosti, s katero je obravnavana ranljivost povezana. Matrika sosednosti je torej:

$$\begin{bmatrix} 0 & a_{12}y_2' & a_{13}y_3' & \cdots & a_{1n}y_n' \\ a_{21}y_1' & 0 & a_{23}y_3' & & a_{2n}y_n' \\ & \vdots & & \ddots & \vdots \\ a_{n1}y_1' & a_{n2}y_2' & a_{n3}y_3' & \cdots & 0 \end{bmatrix} \tag{3.8}$$

Vrednost posamezne ranljivosti je vsota produktov jakosti povezave in normalizirana vrednost števila ukrepov ranljivosti, s katero je povezana.

V drugem primeru bomo raje izkoristili mero središčnosti z lastnimi vektorji. Ker je to vsota produktov pripadajočega elementa matrike in ocena sosedne povezane ranljivosti, lahko v to oceno vključimo tudi začetno število ukrepov na ranljivosti. Kar pomeni, da diagonala matrike sosednosti ne bo več ničelna, ampak sestavljena iz normaliziranih vrednosti števila ukrepov na ranljivosti. Sestavimo torej vektor števila ukrepov, ga normaliziramo glede na najmanjši element v vektorju in ga zapišemo v diagonalo. Najmanjši element vektorja bo imel po normalizaciji vrednost 1 (ker je element najmanj v relaciji s samim seboj).

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_k \\ \vdots \\ y_n \end{bmatrix} = y_k \begin{bmatrix} y_1' \\ y_2' \\ y_3' \\ \vdots \\ 1 \\ \vdots \\ y_n' \end{bmatrix} \tag{3.9}$$

Vektor $[y_1, y_2, y_3, \dots, y_n]$ vsebuje razpoložljiva števila ukrepov za posamezno ranljivost (za ranljivost R_1 je na voljo y_1 ukrepov, za ranljivost R_2 je na voljo y_2 ukrepov, itd.). Torej y_1 predstavlja število ukrepov za ranljivosti R_1. Naj bo y_k najmanjši element vektorja, vsi ostali elementi pa so deljeni z njim. Torej dobimo normalizacijo $y_1' = \frac{y_1}{y_k}$.

V vektor uvedemo še t.i. konstanto vpliva (α), ki uravnava vpliv števila ukrepov na ocenjevanje ranljivosti. Pri $\alpha = 0$ bi na ocenjevanje ranljivosti vplivala samo okolica s povezavami. Na tak način dobimo končni vektor:

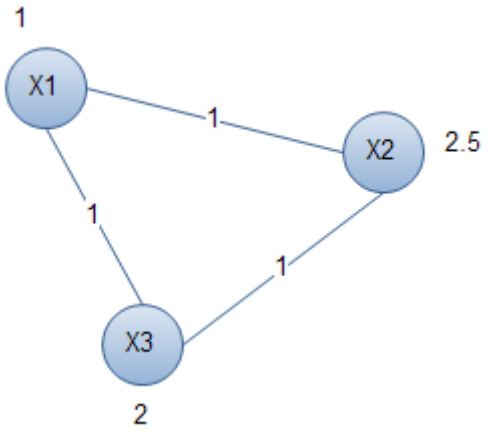
$$\alpha \begin{bmatrix} y_1' \\ y_2' \\ y_3' \\ \vdots \\ 1 \\ \vdots \\ y_n' \end{bmatrix} \tag{3.10}$$

Tako bo imela matrika sosednosti obliko, v kateri namesto diagonale nastopa zgoraj podani vektor:

$$\begin{bmatrix} \alpha y_1' & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & \alpha y_2' & a_{23} & & a_{2n} \\ & \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & \alpha y_n' \end{bmatrix} \tag{3.11}$$

Primer 3.1:

Primer s tremi vozlišči X_1, X_2, X_3, ki so polno povezana (vsako vozlišče z vsakim) z jakostjo. 1. Naj vektor $[1, 2.5, 2]$ opisuje njihove začetne vrednosti vozlišč (3.10).



Slika 3.1: Začetni graf primera 3.1.

Matrika sosednosti (3.11) vsebuje začetni vektor vrednosti (3.10) na svoji diagonali:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2.5 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

Pri čemer je $\alpha = 1$.
Lastni vektor pri največji lastni vrednosti $\lambda_{max} = 3.95$ je:

$$\begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} 0.43 \\ 0.69 \\ 0.58 \end{bmatrix}$$

Velja, da vozlišču X_1 ustreza izračunana ocena 0.43, X_2 ustreza ocena 0.69 in X_3 ustreza ocena 0.58.

Po normalizaciji glede na najmanjši element v vektorju dobimo:

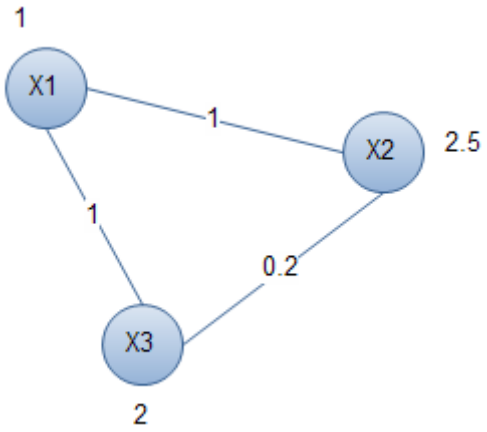
$$\begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix} = 0.43 \begin{bmatrix} 1 \\ 1.60 \\ 1.35 \end{bmatrix}$$

Vrstni red pomembnosti vozlišč, ki ustreza lastnemu vektorju, je potem X_2, X_3, X_1. Glede na povezanost in jakost povezav so si vozlišča enakovredna, zato o pomembnosti vozlišč

odločajo začetne vrednosti posameznih vozlišč. V tem primeru prevladuje vozlišče X_2, ki mu sledi vozlišče X_3 in na koncu še vozlišče X_1.

Primer 3.2:

V drugem primeru 3.2 naj velja, da je povezava med X_2 in X_3 šibkejša:



Slika 3.2: Začetni graf primera 3.2.

Matrika sosednosti:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2.5 & 0.2 \\ 1 & 0.2 & 2 \end{bmatrix}$$

Lastni vektor pri največji lastni vrednosti $\lambda_{max} = 3.34$ je:

$$\begin{bmatrix} X_1 \\ X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} 0.51 \\ 0.71 \\ 0.48 \end{bmatrix} = 0.48 \begin{bmatrix} 1.06 \\ 1.48 \\ 1 \end{bmatrix}$$

Vrstni red pomembnosti vozlišč, ki ustreza lastnemu vektorju, je sedaj nekoliko drugačen: X_2, X_1, X_3. Vozlišče X_2 je še zmeraj najpomembnejše zaradi svoje visoke začetne vrednosti, poleg tega je tudi močno povezano z drugim najpomembnejšim vozliščem X_1, ki pa dobi višjo oceno kot X_3 zaradi svojih močnih povezanosti z drugima vozliščema, sploh pa z najpomembnejšim vozliščem X_2.

3.3.2 Graf ranljivosti na podlagi dvojic

Ker so podane relacije dvojica–ranljivosti oz. posamezna dvojica vsebuje določeno število ranljivosti, ki so navedene (dvojico predstavlja par [grožnja, informacijsko sredstvo]), lahko narišemo pripadajoči dvodelni graf z množico dvojic na eni strani in množico ranljivosti na drugi strani. Povezav med elementi znotraj množice ni. Povezava med elementom iz prve množice in elementom iz druge množice obstaja, če določena ranljivost nastopa v posamezni dvojici oz. nastopa v grožnji na določenem informacijskem sredstvu. Tako dobljen dvodelen graf nato pretvorimo v običajno omrežje, pri čemer predstavljajo vozlišča ranljivosti, povezave pa skupne dvojice med ranljivostima. Povezava med ranljivostima torej obstaja, če obe ranljivosti nastopata v vsaj eni isti dvojici.

Tudi tu je ocena ranljivosti odvisna od tega, kako je ranljivost razširjena (koliko povezav z drugimi ranljivostmi obstaja). Ne smemo pa tudi zanemariti števila dvojic, v katerih je posamezna ranljivost vsebovana, ki igra odločilno vlogo pri določanju ocene ranljivosti. Pri tako dobljenem grafu določimo korelacijo med ranljivostmi, tako da nadomestimo vrednost povezav z normalizacijsko mero Geo. Geo torej normalizira število skupnih dvojic dveh ranljivosti z geometrijsko sredino števila dvojic pri posamezni ranljivosti.

Oceno ranljivosti bi radi dobili na podlagi povezanosti z ostalimi ranljivostmi in ob upoštevanju števila dvojic, v katerih nastopa, ker očitno velja, da bi morala imeti ranljivost, ki nastopa v velikem številu dvojic, tudi visoko oceno pomembnosti. Ranljivost, ki ima veliko povezav z drugimi ranljivostmi, se pojmuje kot zelo razširjena ranljivost in kot taka običajno pomeni visoko tveganje, tako da bi morala tudi ta dobiti visoko oceno. Podobno kot smo naredili pri ocenjevanju ranljivosti na podlagi ukrepov, tudi pri grafu ranljivosti na podlagi dvojic uporabimo mero središčnosti z lastnimi vektorji in s to metodo ocenimo pomembnost ranljivosti.

3.4 Ocena ranljivosti

Pomembnost ranljivosti oz. njeno oceno smo ocenili na dva načina, in sicer s pomočjo 3.3.1 in 3.3.2. Radi bi imeli enotno oceno ranljivosti, zato uvedemo pojem *skupne ocene ranljivosti*. Skupna ocena ranljivosti je sestavljena iz obeh ocen ranljivosti na podlagi ukrepov (3.3.1) in na podlagi dvojic (3.3.2). Zajema oceno razširjenosti ranljivosti med ukrepi, oceno števila ukrepov, oceno razširjenosti ranljivosti med dvojicami in oceno števila le-teh. Obe oceni zaradi medsebojne primerljivosti še normaliziramo glede na najmanjša elementa v obeh vektorjih.
Skupna ocena ranljivosti R_i je tako:

$$\sigma(R_i) = \sigma_u(R_i) + \sigma_o(R_i), \tag{3.12}$$

kjer pomeni $\sigma(R_i)$ skupno oceno ranljivosti R_i, ki je sestavljena iz ocene grafa ranljivosti na podlagi skupnih ukrepov ($\sigma_u(R_i)$) in grafa ranljivosti na podlagi skupnih dvojic ($\sigma_o(R_i)$), kjer sta $\sigma_u(R_i)$ in $\sigma_o(R_i)$ vrednosti i-te komponente dveh lastnih vektorjev obeh grafov. Seveda bi se lahko tudi odločili na podlagi samo enega grafa, npr. $\sigma(R_i) = \sigma_u(R_i)$ ali $\sigma(R_i) = \sigma_o(R_i)$, vendar se tu odločimo upoštevati oba grafa. Z utežitvijo posameznih ocen vplivamo na to, kako resno naj se jemlje oceno določenega grafa. V našem primeru predpostavimo, da sta si enakovredna.

3.5 Ocenjevanje dvojic grožnja, informacijsko sredstvo

Ocene ranljivosti služijo za ocenjevanje pomembnosti končnih groženj oz. ocenjevanje tveganih groženj. V ta namen uporabimo graf oz. omrežje ocen dvojic, ki so medseboj povezane na podlagi ranljivosti. Tak graf tudi predstavi korelacijo med grožnjami. Ker je graf sestavljen iz vozlišč, kjer posamezno vozlišče predstavlja dvojica [grožnja, informacijsko sredstvo] in zajema tudi oceno, v resnici predstavlja povezanost ocen medseboj, glede na grožnje in informacijska sredstva.

Tako dvojico imenujemo ocena tveganja in se nanaša na grožnjo ter informacijsko sredstvo. Pove, katera grožnja ogroža določeno informacijsko sredstvo, katere ranljivosti jo povzročajo, in s kakšno oceno tveganja, ki je subjektivno določena s strani strokovnjaka ob pomoči v naprej uporabljene metodologije ocenjevanja tveganja.

Vsaka dvojica po končanem vnašanju podatkov vsebuje v analizi tveganja specifične atribute, ki povedo nekaj o njej sami. Ti atributi so:

- subjektivna ocena tveganja ki jo opredeli strokovnjak ob uporabi predpostavljene metodologije,
- posledice grožnje,
- ranljivosti, zaradi katerih se grožnja uresniči,
- ukrepi zoper te ranljivosti.

Linearna kombinacija atributnih vrednosti oz. njihovih ocen poda skupno oceno tveganja za posamezno dvojico. V splošnem se iz take analize upoštevajo kot končne in predstavljive ocene samo subjektivne ocene strokovnjaka, zato poskušamo z metodo oceniti, če se morda da iz grafov povezanosti sklepati še kaj več. Intuitivno bi predpostavili, da kombinacija visoke subjektivne ocene, velikega števila ranljivosti, ukrepov in posledic pomeni visoko tvegano oceno ter bi se morali takemu primeru posvetiti prioritetno. Ponavadi pa subjektivna ocena že zajema vse to.

Zastavljeni cilj torej dosežemo s pomočjo vsote uteženih atributnih vrednosti. Vrednost atributov ranljivosti in ukrepov pokrijemo z ocenjevanjem ranljivosti, ki v svojem izračunu ocene ranljivosti upošteva število ranljivosti na posamezni dvojici in tudi ukrepe (graf ranljivosti na podlagi ukrepov). Pri tem se je treba vprašati, če ne obstaja taka ranljivost, ki bi lahko imela različne ukrepe pri različnih situacijah. Izkaže se, da ista ranljivost vedno pokriva iste ukrepe.

Podobno kot pri ocenjevanju ranljivosti sestavimo matriko sosednosti. Velja, da sta si dvojici sosedni, če obstaja med njima vsaj ena skupna ranljivost. V grafu ovrednotimo povezave na način:

$$v(X_i, X_j) = \delta \frac{\sum_{R_k \in R(X_i \cap X_j)} \sigma(R_k)}{\sum_{k=1}^{M(X_j)} \sigma(R_k)} \tag{3.13}$$

Vrednost povezave je vsota ocen ranljivosti, ki so skupne dvojici X_i in X_j, deljeno z vsoto ocen vseh ranljivosti pri dvojici X_j ($\left|M(X_j)\right|$ je število ranljivosti pri dvojici X_j). Dvojica X_i ima skupno $|M(X_i)|$ ranljivosti s skupno oceno $\sum_{k=1}^{M(X_i)} \sigma(R_k)$. Nekaj od teh ranljivosti se deli z dvojico X_j, kar pomeni, da od vseh svojih ranljivosti z nekaj vpliva na X_j in predstavlja nek

delež ranljivosti v X_j. Delež tega vpliva je vrednost njene povezave do dvojice X_j ($v(X_i, X_j)$). Obratno vpliva X_j na X_i z $v(X_j, X_i)$. δ označuje moč povezave in jo lahko na začetku nastavimo na $\delta = 1$.

Vsaka dvojica X_i ima *skupno oceno ranljivosti* enako vsoti posameznih ocen ranljivosti pri tej dvojici:

$$\sigma_1(X_i) = vsota\ ocen\ ranljivosti\ pri\ dvojici\ X_i = \sum_{k=1}^{M(X_i)} \sigma(R_k) \tag{3.14}$$

Oceno še normaliziramo z vsoto ocen vseh ranljivosti:

$$\sigma_2(X_i) = \frac{vsota\ ocen\ ranljivosti\ pri\ dvojici\ X_i}{vsota\ ocen\ vseh\ ranljivosti} = \frac{\sigma_1(X_i)}{\sum_{k=1}^{N} \sigma(R_k)} = \frac{\sum_{k=1}^{M(X_i)} \sigma(R_k)}{\sum_{k=1}^{N} \sigma(R_k)} \tag{3.15}$$

Primer:

Naj ima dvojica X_1 ranljivosti in njihovo skupno oceno $\sigma_1(X_1) = 2.71$, X_2 pa $\sigma_1(X_2) = 4.25$. X_1 in X_2 si delita skupne ranljivosti, ki imajo skupno oceno $\sigma_1(X_1 \cap X_2) = 1.03$. Skupna ocena vseh ranljivosti v sistemu je $\sigma_1(X_1 \cup X_2 \cup ... \cup X_n) = 10.83$. Torej je $\sigma_2(X_1) = 0.25$ in $\sigma_2(X_1) = 0.39$, $v(X_1, X_2) = 0.24$ ter $v(X_2, X_1) = 0.38$.

X_1 ima 25 % vseh ranljivosti v sistemu. Od teh 25 % je 38 % ranljivosti, ki si jih deli z X_2 in predstavlja 24 % ranljivosti X_2, torej vpliva s 24 % na X_2. Lahko si razlagamo tudi tako, če se zgodi X_1, potem se zgodi tudi 24 % X_2.

Pri ocenjevanju tveganja posameznih dvojic [grožnja, informacijsko sredstvo] želimo upoštevati še ostale atributne vrednosti, ki pa jih moramo zapisati tako, da jih lahko med seboj primerjamo. Ob upoštevanju tega naštejemo vse atributne vrednosti za dvojico X_i:

- subjektivno oceno normaliziramo, tako da dobimo mero iz intervala [0,1]:

$$\sigma_S(X_i) = \frac{subjektivna\ ocena\ tveganja\ pri\ dvojici\ X_i}{največja\ subjektivna\ ocena\ tveganja} \tag{3.16}$$

- število posledic normaliziramo, tako da dobimo mero iz intervala [0,1]:

$$\sigma_P(X_i) = \frac{število\ posledic\ pri\ dvojici\ X_i}{število\ vseh\ posledic} \tag{3.17}$$

- ranljivosti in ukrepe na dvojici X_i zajamemo s skupno oceno ranljivosti: $\sigma_2(X_i)$.

Pridobljene vrednosti nato uporabimo v linerani kombinaciji, da dobimo *reprezentativno oceno* tveganja posamezne dvojice. Tako oceno dobimo kot:

$$K(X_i) = \alpha\sigma_S(X_i) + \beta\sigma_P(X_i) + \gamma\sigma_2(X_i) \tag{3.18}$$

Od uteženih faktorjev α, β, γ je odvisno, katera vrednost se bo najbolj upoštevala. Ker hočemo v matriki sosednosti na diagonali najmanjšo vrednost 1 (ker je element s samim seboj 100 % v povezavi), zložimo vrednosti $K(X_1)$, $K(X_2)$, ..., $K(X_n)$ v vektor in ga normaliziramo z najmanjšim elementom vektorja, drugi pa so ovrednoteni glede na njegovo vrednost. Tak vektor nato zapišemo v diagonalo matrike. Ostale vrednosti matrike so enake $v(X_i, X_j)$ (3.13). Vektor vrednosti $K(X_i)$ (3.18) in normalizirani vektor:

$$\begin{bmatrix} K(X_1) \\ K(X_2) \\ K(X_3) \\ \vdots \\ K(X_k) \\ \vdots \\ K(X_n) \end{bmatrix} = K(X_k) \begin{bmatrix} K'(X_1) \\ K'(X_2) \\ K'(X_3) \\ \vdots \\ 1 \\ \vdots \\ K'(X_n) \end{bmatrix} \tag{3.19}$$

Matrika sosednosti ima končno obliko:

$$\begin{bmatrix} K'(X_1) & v(X_1, X_2) & v(X_1, X_3) & \cdots & v(X_1, X_n) \\ v(X_2, X_1) & K'(X_2) & v(X_2, X_3) & & v(X_2, X_n) \\ & \vdots & & \ddots & \vdots \\ v(X_n, X_1) & v(X_n, X_2) & v(X_n, X_3) & \cdots & K'(X_n) \end{bmatrix} \tag{3.20}$$

Iz pridobljene matrike sosednosti izračunamo lastni vektor ocen tveganja dvojic. i-ta komponenta izračunanega lastnega vektorja ustreza oceni tveganja dvojice X_i.

Poglavje 4

Eksperimentalni rezultati

Za testni primer smo vzeli analizo tveganja za izmišljeno organizacijo, kjer smo ocenili oceno tveganja na podlagi uporabljene metodologije in matrike ocene stopnje tveganja, ki je predstavljena v nadaljevanju. Rezultati so dobljeni ob pogovoru kvalificiranega strokovnjaka za standard ISO9001 in ISO27001.

4.1 Zasnova analize tveganja

Za primer smo vzeli sklop groženj pod imenom »Okoljski vplivi«, ki zajema naslednje grožnje:

- razkritje dokumentov/podatkov,
- socialni inženiring,
- vdori v notranje omrežje – z interneta,
- razkritje gesla,
- kraja prenosne opreme.

Analiza tveganja pokriva en proces, ki vsebuje naslednja informacijska sredstva:

- informacije v elektronski obliki,
- programska oprema,
- strežniki.

4.2 Metodologija

Metodologija ocenjevanja je sestavljena iz elementov in njihovih vrednosti:

- Verjetnost grožnje:
    - majhna

- srednja
- velika

- Stopnja posledic grožnje:
  - majhna
  - srednja
  - velika
- Stopnja ranljivosti:
  - nizka
  - srednja
  - visoka
- Učinkovitost protiukrepov:
  - nična
  - nizka
  - srednja
  - visoka

Matrika ocene stopnje tveganja je ob upoštevanju elementov metodologije in njihovih vrednosti torej:

				Verjetnost grožnje								
				majhna			srednja			visoka		
				Stopnja posledic grožnje								
				majhna	srednja	visoka	majhna	srednja	visoka	majhna	srednja	visoka
Stopnja ranljivosti	nizka	Učinkovitost protiukrepov	nična	1	2	4	3	4	5	4	5	5
			nizka	1	1	3	2	3	4	3	5	5
			srednja	1	1	1	1	2	3	2	4	5
			visoka	1	1	1	1	1	1	1	2	2
	srednja		nična	2	3	4	4	5	5	5	5	5
			nizka	2	2	4	3	4	5	4	5	5
			srednja	1	1	2	2	3	4	3	5	5
			visoka	1	1	1	1	2	2	1	2	2
	visoka		nična	3	4	5	4	5	5	5	5	5
			nizka	3	3	4	4	5	5	5	5	5
			srednja	2	2	3	3	4	5	4	5	5
			visoka	1	1	2	1	2	3	2	3	3

Slika 4.1: Matrika ocene stopnje tveganja.

Matrika ocene stopnje tveganja je sestavljena iz štirih elementov (vsak s svojim naborom vrednosti), ki tako definirajo 4 dimenzije. S Slike 4.1 je razvidna metodologija, ki določi končno oceno tveganja s pomočjo kombinacije vrednosti vseh štirih elementov. Barva igra vlogo lažje predstave, kjer zelena pomeni manjše tveganje za oceni 1 in 2, oranžna srednje in rdeča, kamor spadata obe oceni 4 in 5, ki ponazarja največje tveganje.

4.3 Rezultat metodologije

	Procesi / Informacijska sredstva		
	Privzeti proces		
Grožnja	Informacije v elektronski obliki	Programska oprema	Strežniki
1. Okoljski vplivi			
1.1 Razkritje dokumentov/podatkov	**5** Ukrep 1.1.1 Ukrep 1.1.2 Ukrep 1.1.3 Ukrep 1.1.4 Ukrep 1.1.5		
1.2 Socialni inženiring	**3** Ukrep 1.2.1 (1.1.1) Ukrep 1.2.2 Ukrep 1.2.3	**3** Ukrep 1.2.1 (1.1.1) Ukrep 1.2.2 Ukrep 1.2.3	**3** Ukrep 1.2.1 (1.1.1) Ukrep 1.2.2 Ukrep 1.2.3
1.3 Vdori v notranje omrežje - iz interneta	**5** Ukrep 1.3.1 (1.2.1) Ukrep 1.3.2 (1.2.3) Ukrep 1.3.3 Ukrep 1.3.4 Ukrep 1.3.5	**5** Ukrep 1.3.1 (1.2.1) Ukrep 1.3.2 (1.2.3) Ukrep 1.3.3 Ukrep 1.3.4 Ukrep 1.3.5	**5** Ukrep 1.3.1 (1.2.1) Ukrep 1.3.2 (1.2.3) Ukrep 1.3.3 Ukrep 1.3.4 Ukrep 1.3.5
1.4 Razkritje gesla	**5** Ukrep 1.4.1 (1.1.1) Ukrep 1.4.2 Ukrep 1.4.3	**5** Ukrep 1.4.1 (1.1.1) Ukrep 1.4.2 Ukrep 1.4.3	**5** Ukrep 1.4.1 (1.1.1) Ukrep 1.4.2 Ukrep 1.4.3
1.5 Kraja prenosne opreme	**2** Ukrep 1.5.1 (1.2.3) Ukrep 1.5.2 (1.4.1)	**2** Ukrep 1.5.1 (1.2.3) Ukrep 1.5.2 (1.4.1)	

Slika 4.2: Prikaz grafičnega rezultata analize tveganja po strokovnjakovi interpretaciji.

Kratka razlaga določanja in ocenjevanja tveganja za vsako od zgornjih celic oz. dvojic informacijsko sredstvo – grožnja. Razloženo je, katera grožnja ogroža informacijsko sredstvo v organizaciji, katere morebitne ranljivosti pri tem povzroči, kakšne so lahko posledice, podana je subjektivna ocena tveganja na podlagi matrike ocene stopnje tveganja in predlagani ukrepi za odpravo ali zmanjšanje ranljivosti za dano dvojico. Številka (tveganje) v celici in barva celice sovpadata z metodologijo, ki je predstavljena na Sliki 4.1. Slika 4.2 prikazuje

tudi ukrepe v skrčeni obliki oz. v obliki, kjer so samo našteti s svojo vrstno številko. Podroben opis ukrepov je podan v nadaljevanju.

Na podlagi tako opravljene analize nato sestavimo grafe, ki bi nam lahko pomagali pri določanju pomembnosti ranljivosti in groženj.

Iz slike je razvidno, da razkritje dokumentov oz. podatkov nima posebnega vpliva na programsko opremo kot samo in tudi ne na fizične strežnike. Prav tako kraja prenosne opreme nima vpliva na fizične strežnike.

4.4 Podatki

Informacije v elektronski obliki/razkritje dokumentov ali podatkov

Razkritje dokumentov ali drugih podatkov ogroža informacije v elektronski obliki in lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nenadzorovano delo zunanjega ali čistilnega osebja, neprimerna ali neprevidna uporaba fizičnega nadzora dostopa v stavbo in sobe, neustrezen nadzor obiskovalcev, neustrezen postopek preklica pravic dostopa, neustrezna razvrstitev sredstev glede na zaupnost, neustrezno upravljanje šifriranja, nezadovoljen zaposleni, nezaščitena hramba, nezaščitene točke dostopa, pomanjkanje politike prazne mize in čistega zaslona, zaposleni se ne odjavijo, ko zapustijo delovno mesto.

Subjektivna ocena tveganja tako zastavljene nastavke v organizaciji:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Nizka
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje na informacijskem sredstvu:

- Visoke posledice: izguba ugleda organizacije, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.1.1 Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezadostno usposabljanje na področju varnosti.
    - Neprimerna ali neprevidna uporaba fizičnega nadzora dostopa v stavbo in sobe.
    - Neustrezen nadzor obiskovalcev.
    - Pomanjkanje politika prazne mize in čistega zaslona.
    - Zaposleni se ne odjavijo, ko zapustijo delovno postajo.
- 1.1.2 Izvajalci storitev čistilnega servisa podpišejo izjavo o varovanju informacij. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nenadzorovano delo zunanjega ali čistilnega osebja.
- 1.1.3 Uvesti pravilo zaklepanja sob po odhodu z delovnega mesta. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neprimerna ali neprevidna uporaba fizičnega nadzora dostopa v stavbo in sobe.
    - Neustrezen nadzor obiskovalcev.
    - Nezaščitena hramba.
- 1.1.4 Izdelava varnostne politike nadzora dostopa, ki opredeljuje postopek preklica pravic dostopov. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neustrezen postopek preklica pravic dostopa.
- 1.1.5 Izdelati in izvajati politiko razvrstitve informacij glede na zaupnost. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neustrezna razvrstitev sredstev glede na zaupnost.

Informacije v elektronski obliki/Socialni inženiring

Grožnja socialnega inženiringa ogroža informacije v elektronski obliki in lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezadovoljen zaposleni, osebne okoliščine, pomanjkljive politike/standardi/postopki, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Nizka
Učinkovitost protiukrepov	Srednja

Ocena po matriki	3

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.2.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Nezadostno usposabljanje na področju varnosti.
  - Osebne okoliščine.
  - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
- 1.2.2 Izvajanje motivacijskih treningov za zaposlene. Vpliva na ranljivosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Nezadovoljen zaposleni.
  - Osebne okoliščine.
- 1.2.3 Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Pomanjkljive politike/standardi/postopki.

Informacije v elektronski obliki/Vdori v notranje omrežje - iz interneta

Če informacije v elektronski obliki ogroža grožnja vdorov v notranje omrežje – z interneta, lahko povzroči naslednje ranljivosti: nepravilna nastavitev parametrov, neprimerno upravljanje omrežja, neustrezen nadzor dela na daljavo, neustrezen postopek preklica pravic dostopa, nezaščitene točke dostopa, omogočene nepotrebne storitve, pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme, pomanjkljive politike/standardi/postopki, pomanjkljivi nadzorni mehanizmi, pomanjkljivo specifično

izobraževanje delavcev, ki svoje delo opravljajo na daljavo, slabo upravljanje z gesli programske opreme, znane pomanjkljivosti programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Nizka
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.3.1 (kopija ukrepa 1.2.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
  - Slabo upravljanje z gesli programske opreme.
- 1.3.2 (kopija ukrepa 1.2.3) Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Pomanjkljive politike/standardi/postopki.
- 1.3.3 Postavitev požarnih pregrad. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Nepravilna nastavitev parametrov.
  - Neprimerno upravljanje omrežja.
  - Neustrezen nadzor dela na daljavo.
  - Nezaščitene točke dostopa.
  - Omogočene nepotrebne storitve.

    - Pomanjkljivi nadzorni mehanizmi.
- 1.3.4 Namestitev protivirusne zaščite na vseh strežnikih, delovnih postajah in prenosnikih ter redno osveževanje popravkov. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme.
    - Znane pomanjkljivosti programske opreme.
- 1.3.5 Izvajanje zunanjih varnostnih pregledov omrežja. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neustrezen nadzor dela na daljavo.
    - Neustrezen postopek preklica pravic dostopa.
    - Nezaščitene točke dostopa.
    - Omogočene nepotrebne storitve.
    - Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme.
    - Pomanjkljive politike/standardi/postopki.
    - Slabo upravljanje z gesli programske opreme.
    - Znane pomanjkljivosti programske opreme.

Informacije v elektronski obliki/Razkritje gesla

Če informacije v elektronski obliki ogroža grožnja razkritja gesel, lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezaščitene tabele gesel, osebne okoliščine, pomanjkanje ali neustrezna določila glede varovanja informacij v pogodbah o zaposlitvi, pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta, pomanjkanje varnostne ozaveščenosti, pomanjkljive politike/standardi/postopki, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo, slabo upravljanje gesel, slabo upravljanje z gesli programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Srednja
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.4.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezadostno usposabljanje na področju varnosti.
    - Osebne okoliščine.
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
    - Slabo upravljanje gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.2 Izdelava in vpeljava politike upravljanja z gesli. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi.
    - Pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta.
    - Pomanjkljive politike/standardi/postopki.
    - Slabo upravljanje gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.3 Hramba gesel v šifrirani obliki. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezaščitene tabele gesel.

Informacije v elektronski obliki/Kraja prenosne opreme

Če informacije v elektronski obliki ogroža grožnja kraje prenosne opreme, lahko povzroči naslednje ranljivosti: osebne okoliščine, pomanjkanje nadzora nad opremo izven prostorov organizacije, pomanjkanje politike uporabe prenosne računalniške opreme, pomanjkanje

varnostne ozaveščenosti, pomanjkljive politike/standardi/postopki, pomanjkljivi nadzorni mehanizmi.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Srednja
Stopnja ranljivosti	Srednja
Učinkovitost protiukrepov	Visoka (Organizacija že uporablja šifriranje diskov v prenosnih računalnikih.)
Ocena po matriki	2

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, razkritje zaupnih podatkov.
- Srednje posledice: ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.5.1 (kopija ukrepa 1.2.3) Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkanje politike uporabe prenosne računalniške opreme.
    - Pomanjkljive politike/standardi/postopki.
- 1.5.2 (kopija ukrepa 1.4.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Osebne okoliščine.
    - Pomanjkanje nadzora nad opremo izven prostorov organizacije.
    - Pomanjkanje varnostne ozaveščenosti.

Programska oprema/Socialni inženiring

Če programsko opremo ogroža grožnja socialnega inženiringa, lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezadovoljen zaposleni, osebne okoliščine, pomanjkljive politike/standardi/postopki, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Nizka
Učinkovitost protiukrepov	Srednja
Ocena po matriki	3

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.2.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Nezadostno usposabljanje na področju varnosti.
  - Osebne okoliščine.
  - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
- 1.2.2 Izvajanje motivacijskih treningov za zaposlene. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Nezadovoljen zaposleni.
  - Osebne okoliščine.
- 1.2.3 Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
  - Pomanjkljive politike/standardi/postopki.

Programska oprema/Vdori v notranje omrežje – z interneta

Če programsko opremo ogroža grožnja vdora v notranje omrežje z interneta, lahko povzroči naslednje ranljivosti: nepravilna nastavitev parametrov, neprimerno upravljanje omrežja, neustrezen nadzor dela na daljavo, neustrezen postopek preklica pravic dostopa, nezaščitene točke dostopa, omogočene nepotrebne storitve, pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme, pomanjkljive politike/standardi/postopki, pomanjkljivi nadzorni mehanizmi, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo, slabo upravljanje z gesli programske opreme, znane pomanjkljivosti programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Nizka
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.3.1 (kopija ukrepa 1.2.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
    - Slabo upravljanje z gesli programske opreme.

- 1.3.2 (kopija ukrepa 1.2.3) Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljive politike/standardi/postopki.
- 1.3.3 Postavitev požarnih pregrad. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nepravilna nastavitev parametrov.
    - Neprimerno upravljanje omrežja.
    - Neustrezen nadzor dela na daljavo.
    - Nezaščitene točke dostopa.
    - Omogočene nepotrebne storitve.
    - Pomanjkljivi nadzorni mehanizmi.
- 1.3.4 Namestitev protivirusne zaščite na vseh strežnikih, delovnih postajah in prenosnikih ter redno osveževanje popravkov. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme.
    - Znane pomanjkljivosti programske opreme.
- 1.3.5 Izvajanje zunanjih varnostnih pregledov omrežja. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neustrezen nadzor dela na daljavo.
    - Neustrezen postopek preklica pravic dostopa.
    - Nezaščitene točke dostopa.
    - Omogočene nepotrebne storitve.
    - Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme.
    - Pomanjkljive politike/standardi/postopki.
    - Slabo upravljanje z gesli programske opreme.
    - Znane pomanjkljivosti programske opreme.

Programska oprema/Razkritje gesla

Če programsko opremo ogroža grožnja razkritja gesla, lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezaščitene tabele gesel, osebne okoliščine, pomanjkanje ali neustrezna določila glede varovanja informacij v pogodbah o zaposlitvi, pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta, pomanjkanje varnostne ozaveščenosti, pomanjkljive politike/standardi/postopki, pomanjkljivo

specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo, slabo upravljane gesel, slabo upravljanje z gesli programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Srednja
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.4.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezadostno usposabljanje na področju varnosti.
    - Osebne okoliščine.
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
    - Slabo upravljanje gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.2 Izdelava in vpeljava politike upravljanja z gesli. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi.

    - Pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta.
    - Pomanjkljive politike/standardi/postopki.
    - Slabo upravljane gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.3 Hramba gesel v šifrirani obliki. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezaščitene tabele gesel.

Programska oprema/Kraja prenosne opreme

Če programsko opremo ogroža grožnja kraje prenosne opreme, lahko povzroči naslednje ranljivosti: osebne okoliščine, pomanjkanje nadzora nad opremo izven prostorov organizacije, pomanjkanje politike uporabe prenosne računalniške opreme, pomanjkanje varnostne ozaveščenosti, pomanjkljive politike/standardi/postopki, pomanjkljivi nadzorni mehanizmi.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Srednja
Stopnja ranljivosti	Srednja
Učinkovitost protiukrepov	Visoka
Ocena po matriki	2

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, razkritje zaupnih podatkov.
- Srednje posledice: ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.5.1 (kopija ukrepa 1.2.3) Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkanje politike uporabe prenosne računalniške opreme.
    - Pomanjkljive politike/standardi/postopki.

- 1.5.2 (kopija ukrepa 1.4.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Osebne okoliščine.
    - Pomanjkanje nadzora nad opremo izven prostorov organizacije.
    - Pomanjkanje varnostne ozaveščenosti.

Strežniki/Socialni inženiring

Če strežnike ogroža grožnja socialnega inženiringa, lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezadovoljen zaposleni, osebne okoliščine, pomanjkljive politike/standardi/postopki, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Nizka
Učinkovitost protiukrepov	Srednja
Ocena po matriki	3

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.2.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:

    - Nezadostno usposabljanje na področju varnosti.
    - Osebne okoliščine.
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
- 1.2.2 Izvajanje motivacijskih treningov za zaposlene. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezadovoljen zaposleni.
    - Osebne okoliščine.
- 1.2.3 Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljive politike/standardi/postopki.

Strežniki/Vdori v notranje omrežje – z interneta

Če strežnike ogroža grožnja vdora v notranje omrežje z interneta, lahko povzroči naslednje ranljivosti: nepravilna nastavitev parametrov, neprimerno upravljanje omrežja, neustrezen nadzor dela na daljavo, neustrezen postopek preklica pravic dostopa, nezaščitene točke dostopa, omogočene nepotrebne storitve, pomanjkljive politike/standardi/postopki, pomanjkljivi nadzorni mehanizmi, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo, znane pomanjkljivosti programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Nizka
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izguba ugleda organizacije, izpad procesa/storitve za več, kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.

- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, ogrožanje ugleda organizacije, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.3.1 (kopija ukrepa 1.2.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.
- 1.3.2 (kopija ukrepa 1.2.3) Izdelava in izvajanje varnostne politike. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkljive politike/standardi/postopki.
- 1.3.3 Postavitev požarnih pregrad. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nepravilna nastavitev parametrov.
    - Neprimerno upravljanje omrežja.
    - Neustrezen nadzor dela na daljavo.
    - Nezaščitene točke dostopa.
    - Omogočene nepotrebne storitve.
    - Pomanjkljivi nadzorni mehanizmi.
- 1.3.4 Namestitev protivirusne zaščite na vseh strežnikih, delovnih postajah in prenosnikih ter redno osveževanje popravkov. Ukrep zmanjšuje ranljivosti:
    - Znane pomanjkljivosti programske opreme.
- 1.3.5 Izvajanje zunanjih varnostnih pregledov omrežja. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Neustrezen nadzor dela na daljavo.
    - Neustrezen postopek preklica pravic dostopa.
    - Nezaščitene točke dostopa.
    - Omogočene nepotrebne storitve.
    - Pomanjkljive politike/standardi/postopki.
    - Znane pomanjkljivosti programske opreme.
    - Pomanjkljivi nadzorni mehanizmi.

Strežniki/Razkritje gesla

Če strežnike ogroža grožnja razkritja gesla, lahko povzroči naslednje ranljivosti: nezadostno usposabljanje na področju varnosti, nezaščitene tabele gesel, osebne okoliščine, pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi, pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta, pomanjkanje varnostne ozaveščenosti, pomanjkljive politike/standardi/postopki, pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo, slabo upravljane gesel, slabo upravljanje z gesli programske opreme.

Subjektivna ocena tveganja:

Element matrike	Vrednost
Verjetnost grožnje	Srednja
Stopnja posledic grožnje	Visoka
Stopnja ranljivosti	Visoka
Učinkovitost protiukrepov	Nizka
Ocena po matriki	5

Predvidene posledice, ki jih prinese uresničitev grožnje:

- Visoke posledice: izguba celovitosti finančnih podatkov, izguba celovitosti osebnih podatkov, izguba podatkov, ki si jih izmenjujejo stranke oziroma partnerji, izpad procesa/storitve za več kot je toleriran čas izpada, kršitev zakonodaje, razkritje ali uničenje podatkov strank oziroma partnerjev, razkritje zaupnih podatkov.
- Srednje posledice: izpad procesa/storitve za toleriran čas izpada, razkritje internih informacij.
- Majhne posledice: izpad procesa/storitve za manj, kot je toleriran čas izpada, prestrezanje/razkritje šifriranih podatkov.

Za zmanjšanje ali odpravo ranljivosti bi morali izvesti naslednje ukrepe:

- 1.4.1 (kopija ukrepa 1.1.1) Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezadostno usposabljanje na področju varnosti.
    - Osebne okoliščine.
    - Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo.

    - Slabo upravljane gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.2 Izdelava in vpeljava politike upravljanja z gesli. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi.
    - Pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta.
    - Pomanjkljive politike/standardi/postopki.
    - Slabo upravljane gesel.
    - Slabo upravljanje z gesli programske opreme.
- 1.4.3 Hramba gesel v šifrirani obliki. Ukrep odpravlja ali zmanjšuje ranljivosti:
    - Nezaščitene tabele gesel.

4.5 Rezultati

4.5.1 Graf ranljivosti na podlagi skupnih ukrepov

Iz danega primera analize tveganja zberem oziroma pogrupiram ukrepe, ki odpravljajo ali zmanjšujejo ranljivosti. V seznamu so zbrane ranljivosti in s katerimi ukrepi se jih lahko odpravi oz. zmanjša njihov vpliv. Poleg tekstovnega opisa so podani še njihovi ID-ji za lažje razpoznavo v matriki sosednosti. Z njihovo pomočjo nato sestavim graf ranljivosti, ki temelji na podlagi skupnih ukrepov.

Ranljivost [ranljivost ID]	Ukrep [ukrep ID]
Nezaščitene tabele gesel [149]	• Hramba gesel v šifrirani obliki. [158]
Neustrezna razvrstitev sredstev glede na zaupnost [109]	• Izdelati in izvajati politiko razvrstitve informacij glede na zaupnost. [146]
Pomanjkljive politike/standardi/postopki [30]	• Izdelava in izvajanje varnostne politike. [150] • Izdelava in vpeljava politike upravljanja z gesli. [157] • Izvajanje zunanjih varnostnih pregledov omrežja. [155]

Pomanjkanje politike uporabe prenosne računalniške opreme [203]	• Izdelava in izvajanje varnostne politike. [150]
Pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi [201]	• Izdelava in vpeljava politike upravljanja z gesli. [157]
Pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta [202]	• Izdelava in vpeljava politike upravljanja z gesli. [157]
Slabo upravljane gesel [150]	• Izdelava in vpeljava politike upravljanja z gesli. [157] • Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Slabo upravljanje z gesli programske opreme [72]	• Izdelava in vpeljava politike upravljanja z gesli. [157] • Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Neustrezen postopek preklica pravic dostopa [33]	• Izdelava varnostne politike nadzora dostopa, ki opredeljuje postopek preklica pravic dostopov. [145] • Izvajanje zunanjih varnostnih pregledov omrežja. [155]
Nenadzorovano delo zunanjega ali čistilnega osebja [175]	• Izvajalci storitev čistilnega servisa podpišejo izjavo o varovanju informacij. [143]
Nezadovoljen zaposleni [36]	• Izvajanje motivacijskih treningov za zaposlene. [149]
Osebne okoliščine [31]	• Izvajanje motivacijskih treningov za zaposlene. [149] • Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Neustrezen nadzor dela na daljavo [117]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Postavitev požarnih pregrad. [153]
Nezaščitene točke dostopa [102]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Postavitev požarnih pregrad. [153]

Omogočene nepotrebne storitve [151]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Postavitev požarnih pregrad. [153]
Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme [84]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Namestitev protivirusne zaščite na vseh strežnikih, delovnih postajah in prenosnikih ter redno osveževanje popravkov. [154]
Pomanjkljivi nadzorni mehanizmi [29]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Postavitev požarnih pregrad. [153]
Znane pomanjkljivosti programske opreme [138]	• Izvajanje zunanjih varnostnih pregledov omrežja. [155] • Namestitev protivirusne zaščite na vseh strežnikih, delovnih postajah in prenosnikih ter redno osveževanje popravkov. [154]
Neprimerna ali neprevidna uporaba fizičnega nadzora dostopa v stavbo in sobe [177]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142] • Uvesti pravilo zaklepanja sob po odhodu z delovnega mesta. [144]
Neustrezen nadzor obiskovalcev [119]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142] • Uvesti pravilo zaklepanja sob po odhodu z delovnega mesta. [144]
Nezadostno usposabljanje na področju varnosti [171]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Pomanjkanje politika prazne mize in čistega zaslona [206]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo [41]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Zaposleni se ne odjavijo, ko zapustijo delovno postajo [139]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Pomanjkanje nadzora nad opremo izven prostorov organizacije [204]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]

Pomanjkanje varnostne ozaveščenosti [173]	• Izvajati redno izobraževanje zaposlenih na področju informacijske varnosti. [142]
Nepravilna nastavitev parametrov [146]	• Postavitev požarnih pregrad. [153]
Neprimerno upravljanje omrežja [167]	• Postavitev požarnih pregrad. [153]
Nezaščitena hramba [134]	• Uvesti pravilo zaklepanja sob po odhodu z delovnega mesta. [144]

Tabela 4.1: Razpredelnica ukrepov in pripadajoče ranljivosti, ki jih zmanjšuje oz. odpravlja.

Pripadajoča matrika sosednosti je navadena v Prilogi 1.1. Matrika sosednosti po normalizaciji z normalizacijsko mero Geo je navedena v Prilogi 1.2. Lastni vektor pomembnosti ranljivosti je iz tako izračunane matrike podan spodaj. V nadaljevanju je lastni vektor predstavljen z IDji ranljivosti na levi strani in njihovimi pripadajočimi vrednostmi, ki so bile izračunane iz matrike sosednosti, na desni strani. Ta podatek bomo predvsem potrebovali kasneje pri izrisovanju grafa.

$$\sigma_u(.) = \begin{bmatrix} 149 \\ 109 \\ 30 \\ 203 \\ 201 \\ 202 \\ 150 \\ 72 \\ 33 \\ 175 \\ 36 \\ 31 \\ 117 \\ 102 \\ 151 \\ 84 \\ 29 \\ 138 \\ 177 \\ 119 \\ 171 \\ 206 \\ 41 \\ 139 \\ 204 \\ 173 \\ 146 \\ 167 \\ 134 \end{bmatrix} = \begin{bmatrix} 0.0 \\ 0.0 \\ 0.05838 \\ 0.00439 \\ 0.05477 \\ 0.05477 \\ 0.27019 \\ 0.24504 \\ 0.03139 \\ 0.0 \\ 0.02278 \\ 0.24755 \\ 0.04217 \\ 0.04217 \\ 0.04217 \\ 0.03342 \\ 0.04217 \\ 0.03342 \\ 0.26600 \\ 0.26600 \\ 0.32681 \\ 0.32681 \\ 0.32681 \\ 0.32681 \\ 0.32681 \\ 0.32681 \\ 0.01783 \\ 0.01783 \\ 0.04896 \end{bmatrix}$$

Najmanjši element v vektorju ima vrednost 0.0, zato normalizacija z najmanjšim elementom ni mogoča.

4.5.2 Graf ranljivosti na podlagi skupnih dvojic

Podobno kot v prejšnjem primeru sestavimo graf ranljivosti na podlagi skupnih dvojic informacijsko sredstvo – grožnja. Tudi tu pogrupiramo ranljivosti, ki nastopajo v istih dvojicah. Seznam vsebuje ranljivosti, ki nastopajo v posameznih dvojicah, opremljene z njihovimi ID-ji za lažje razpoznavo v matriki sosednosti.

Ranljivost [ranljivost ID]	Dvojice (informacijsko sredstvo, grožnja) [ocena ID]
Osebne okoliščine [31]	• (Informacije v elektronski obliki, Socialni inženiring) [95] • (Programska oprema, Socialni inženiring) [96] • (Strežniki, Socialni inženiring) [97] • (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103] • (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Pomanjkanje nadzora nad opremo izven prostorov organizacije [204]	• (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Pomanjkanje politike uporabe prenosne računalniške opreme [203]	• (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Pomanjkanje varnostne ozaveščenosti [173]	• (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103] • (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Pomanjkljive	• (Informacije v elektronski obliki, Socialni inženiring)

politike/standardi/postopki [30]	[95] • (Programska oprema, Socialni inženiring) [96] • (Strežniki, Socialni inženiring) [97] • (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - iz interneta) [100] • (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103] • (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Pomanjkljivi nadzorni mehanizmi [29]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100] • (Informacije v elektronski obliki, Kraja prenosne opreme) [104] • (Programska oprema, Kraja prenosne opreme) [105]
Nezadostno usposabljanje na področju varnosti [171]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94] • (Informacije v elektronski obliki, Socialni inženiring) [95] • (Programska oprema, Socialni inženiring) [96] • (Strežniki, Socialni inženiring) [97] • (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Nezadovoljen zaposleni [36]	• (Informacije v elektronski obliki, Razkritje

	dokumentov/podatkov) [94] • (Informacije v elektronski obliki, Socialni inženiring) [95] • (Programska oprema, Socialni inženiring) [96] • (Strežniki, Socialni inženiring) [97]
Pomanjkljivo specifično izobraževanje delavcev, ki svoje delo opravljajo na daljavo [41]	• (Informacije v elektronski obliki, Socialni inženiring) [95] • (Programska oprema, Socialni inženiring) [96] • (Strežniki, Socialni inženiring) [97] • (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100] • (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Nezaščitene tabele gesel [149]	• (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Pomanjkanje ali neustrezna določila glede varovanje informacij v pogodbah o zaposlitvi [201]	• (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Pomanjkanje opredelitve disciplinskega postopka v primeru varnostnega incidenta [202]	• (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Slabo upravljane gesel [150]	• (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Slabo upravljanje z gesli programske	• (Informacije v elektronski obliki, Vdori v notranje

opreme [72]	omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Informacije v elektronski obliki, Razkritje gesla) [101] • (Programska oprema, Razkritje gesla) [102] • (Strežniki, Razkritje gesla) [103]
Nenadzorovano delo zunanjega ali čistilnega osebja [175]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Neprimerna ali neprevidna uporaba fizičnega nadzora dostopa v stavbo in sobe [177]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Neustrezen nadzor obiskovalcev [119]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Neustrezen postopek preklica pravic dostopa [33]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94] • (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Neustrezna razvrstitev sredstev glede na zaupnost [109]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Neustrezno upravljanje šifriranja [80]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Nezaščitena hramba [134]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Nezaščitene točke dostopa [102]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94] • (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Pomanjkanje politika prazne mize in	• (Informacije v elektronski obliki, Razkritje

čistega zaslona [206]	dokumentov/podatkov) [94]
Zaposleni se ne odjavijo, ko zapustijo delovno postajo [139]	• (Informacije v elektronski obliki, Razkritje dokumentov/podatkov) [94]
Nepravilna nastavitev parametrov [146]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Neprimerno upravljanje omrežja [167]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Neustrezen nadzor dela na daljavo [117]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Omogočene nepotrebne storitve [151]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]
Pomanjkljiva zaščita pred virusi in zlonamernimi programi programske opreme [84]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99]
Znane pomanjkljivosti programske opreme [138]	• (Informacije v elektronski obliki, Vdori v notranje omrežje - z interneta) [98] • (Programska oprema, Vdori v notranje omrežje - z interneta) [99] • (Strežniki, Vdori v notranje omrežje - z interneta) [100]

Tabela 4.2: Razpredelnica ranljivosti in dvojic, v katerih se pojavljajo.

Pripadajoča matrika sosednosti je navadena v Prilogi 2.1. Matrika sosednosti po normalizaciji z normalizacijsko mero Geo je navedena v Prilogi 2.2. Lastni vektor pomembnosti ranljivosti je iz tako izračunane matrike enak (na desni strani so ID-ji ranljivosti, na levi pa pripadajoče vrednosti lastnega vektorja):

$$\sigma_o(.) = \begin{bmatrix} 31 \\ 204 \\ 203 \\ 173 \\ 30 \\ 29 \\ 171 \\ 36 \\ 41 \\ 149 \\ 201 \\ 202 \\ 150 \\ 72 \\ 175 \\ 177 \\ 119 \\ 33 \\ 109 \\ 80 \\ 134 \\ 102 \\ 206 \\ 139 \\ 146 \\ 167 \\ 117 \\ 151 \\ 84 \\ 138 \end{bmatrix} = \begin{bmatrix} 0.114600 \\ 0.040692 \\ 0.040692 \\ 0.105243 \\ 0.213403 \\ 0.197679 \\ 0.166970 \\ 0.131434 \\ 0.218171 \\ 0.102661 \\ 0.102661 \\ 0.102661 \\ 0.102661 \\ 0.201596 \\ 0.174082 \\ 0.174082 \\ 0.174082 \\ 0.280462 \\ 0.174082 \\ 0.174082 \\ 0.174082 \\ 0.280462 \\ 0.174082 \\ 0.174082 \\ 0.223045 \\ 0.223045 \\ 0.223045 \\ 0.223045 \\ 0.192705 \\ 0.276450 \end{bmatrix}$$

4.5.3 Ocena ranljivosti

Končna ocena ranljivosti je vsota lastnih vektorjev, pridobljenih iz zadnjih dveh grafov na podlagi enačbe (3.12):

$$\sigma(.) = \sigma_u(.) + \sigma_o(.)$$

Ocene ranljivosti torej služijo za ocenjevanje pomembnosti groženj, zato v ta namen zgradimo graf oz. omrežje ocen – dvojic, ki so med seboj povezane na podlagi skupnih ranljivosti.

4.5.4 Graf dvojic

Priloga 3.1 prikazuje matriko ocen po skupnih ranljivostih. V diagonali so predstavljene ranljivosti, ki jih vsebujejo posamezne dvojice, v nediagonalnih elementih pa so preseki ranljivosti med dvema dvojicama. Matrika sosednosti (3.20) je prikazana v Prilogi 3.2.
Diagonalni vektor in njegov normaliziran vektor (3.19) je:

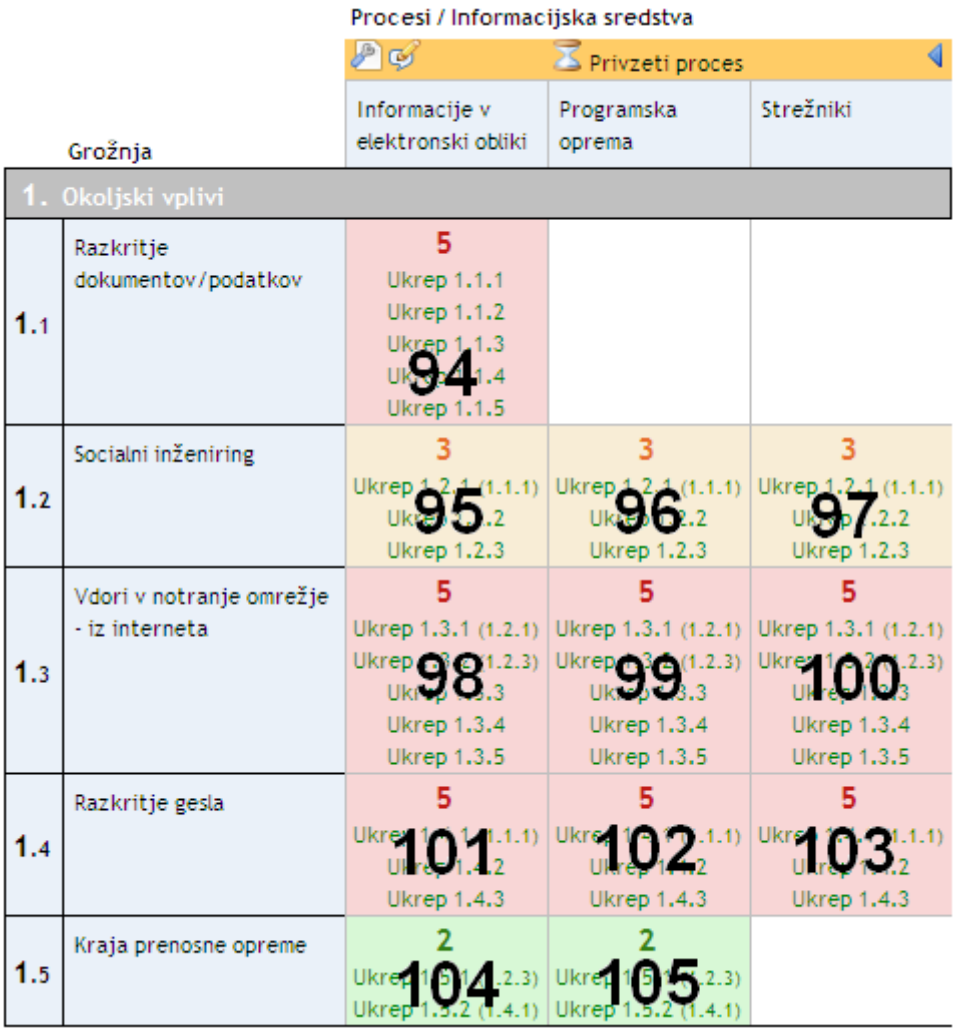
$$\begin{bmatrix} 0.63 \\ 0.90 \\ 1.46 \\ 1.49 \\ 1.51 \\ 0.63 \\ 0.90 \\ 1.46 \\ 1.51 \\ 0.90 \\ 1.46 \\ 1.44 \end{bmatrix} = 0.63 \begin{bmatrix} 1.00 \\ 1.42 \\ 2.28 \\ 2.34 \\ 2.37 \\ 1.00 \\ 1.42 \\ 2.28 \\ 2.37 \\ 1.42 \\ 2.28 \\ 2.25 \end{bmatrix}$$

Normalizirana matrika dvojic je prikazana v Prilogi 3.3.
Na diagonali mora biti najmanjša vrednost 1, ker je dvojica sama s sabo povezana in se tako lahko primerja z ostalimi dvojicami (glede na normalizirano oceno 1).
Iz tako pridobljene matrike sosednosti in ob upoštevanju uteži $\alpha = \beta = \gamma = 1$ iz (3.18) in uteži $\delta = 0.5$ iz (3.13) izračunam končni normalizirani lastni vektor dvojic, ki je:

$$\begin{bmatrix}104\\95\\101\\94\\98\\105\\96\\102\\99\\97\\103\\100\end{bmatrix} = \begin{bmatrix}0.63384\\1.00000\\0.87701\\0.23567\\0.59598\\0.63384\\1.00000\\0.87701\\0.59598\\1.00000\\0.87701\\0.60452\end{bmatrix}$$

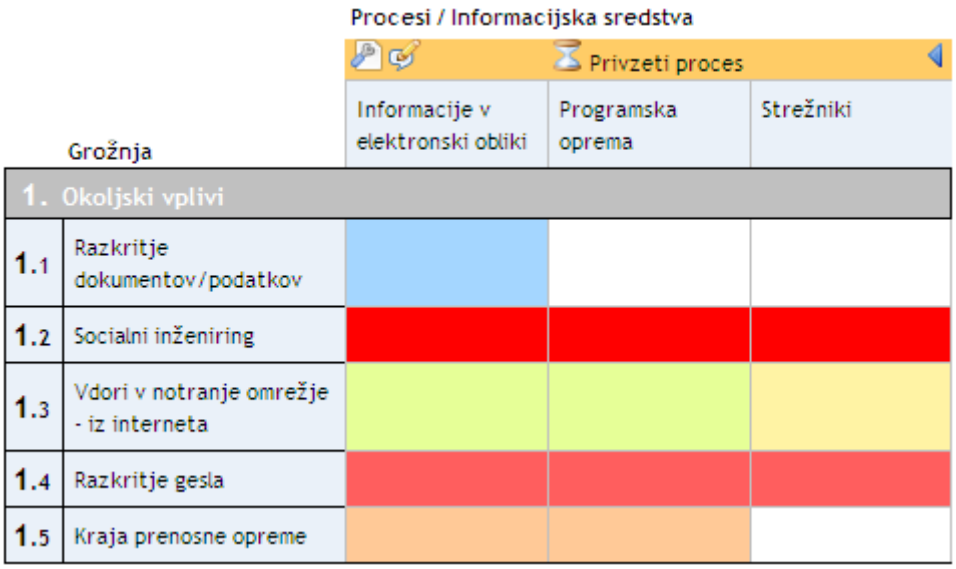
Rezultate smo izračunali s pomočjo odprto kodnega produkta Octave, ki ga uporabljamo v PHP kodi aplikacije.

Za lažjo predstavo smo dvojice na sliki dopolnili z ID-ji posameznih dvojic. To služi predvsem za preglednejši prikaz kasneje v grafu.



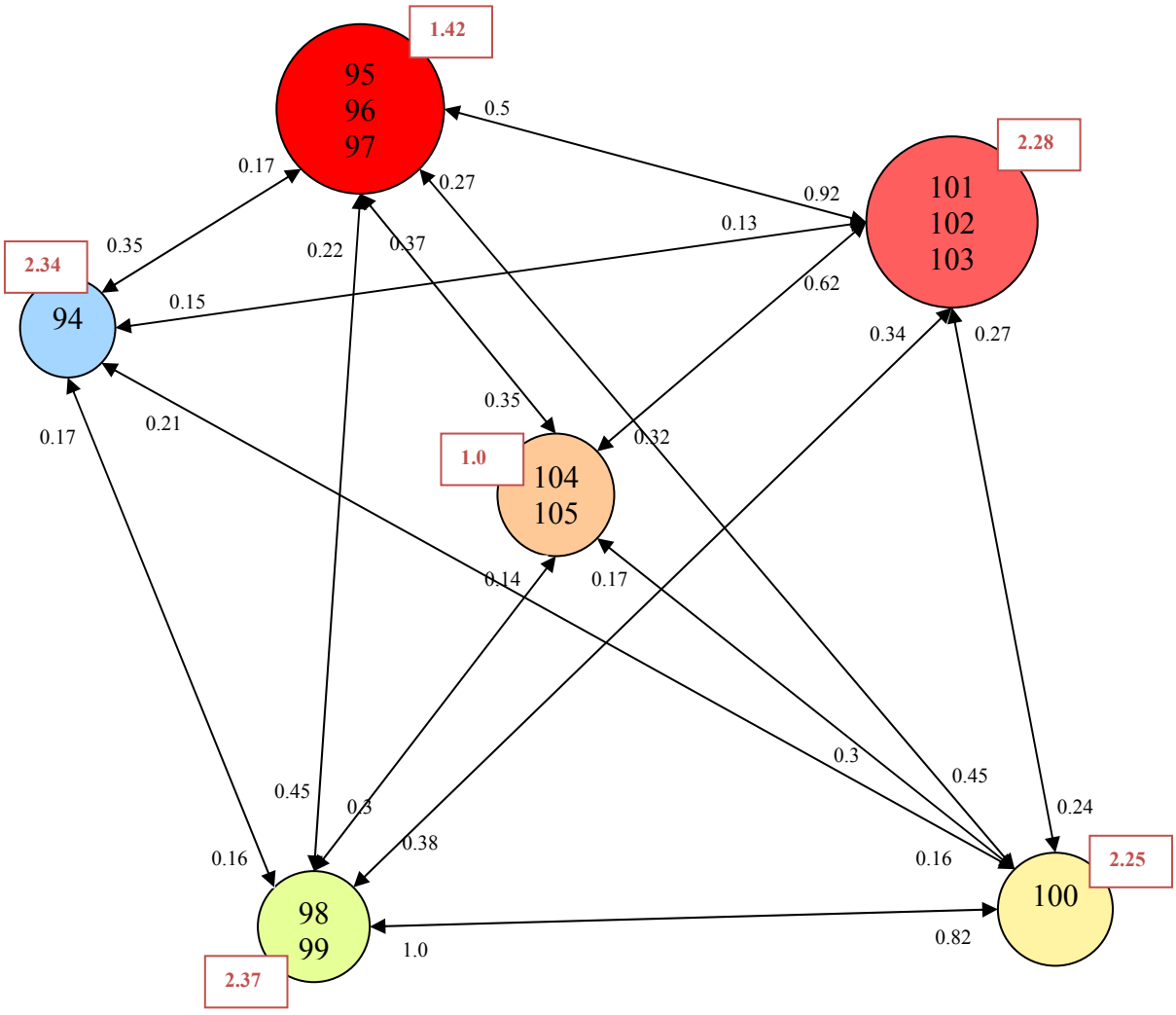
Slika 4.3: Prikaz ID-jev posameznih dvojic informacijskih sredstev – groženj. ID je s črno barvo napisana številka v posamezni celici.

Ob upoštevanju normaliziranega lastnega vektorja dvojic sestavim podobno sliko, kjer vrednostim, ki jih dobim iz vektorja, določim svojo barvo. Ker dvojicam [Socialni inženiring, Informacije v elektronski obliki], [Socialni inženiring, Programska oprema], [Socialni inženiring, Strežniki] v vektorju pripadajo največje ocene oz. vrednosti, so zato obarvane z rdečo barvo. Sledijo jim dvojice [Razkritje gesla, Informacije v elektronski obliki], [Razkritje gesla, Programska oprema], [Razkritje gesla, Strežniki], ki so obarvane v vijolično barvo. Na podoben način določim barve vsem ostalim dvojicam, kjer pomembnost pada od rdeče proti modri barvi. Dvojica z modro barvo je ocenjena kot najmanj pomembna.



Slika 4.4: Prikaz najbolj tveganih dvojic v barvah, kjer rdeča pomeni največje tveganje, modra pa najmanjše. Izkaže se, da je socialni inženiring za organizacijo najnevarnejša grožnja, ki učinkuje na prav vsa informacijska sredstva, kjer so dobili največjo možnjo oceno. Sledi razkritje gesla.

K razumevanju rezultatov pripomore tudi slika grafa, dobljena iz matrike sosednosti, kjer so definirane povezave, smer povezav in njihove jakosti med posameznimi dvojicami. Podaja pa tudi oceno posameznih dvojic. To oceno smo imenovali reprezentativna ocena. Z združevanjem posameznih dvojic dobimo tudi sliko odvisnosti posameznih groženj med seboj.



Slika 4.5: Graf dvojic po razvrstitvi pomembnosti.

Graf dvojic prikazuje vozlišča dvojic, ki so združena glede na svojo oceno in povezave ter vrednosti povezav na druga vozlišča. Dvosmernost povezav nakazuje vsebovanost ranljivosti enega vozlišča v drugem vozlišču (vozlišče za dvojico 94 vpliva z 0.16 na vozlišče dvojice 100 – če se zgodi 94, potem se z 0.16 zgodi lahko tudi 100 – ta pa nazaj na 94 z 0.21). Ocena (tj. reprezentativna ocena tveganja dvojice) vozlišča oz. dvojic je prikazana v temno rdečem kvadratku (pripadajoča vrednost na diagonali normalizirane matrike dvojic).

Iz grafa je razvidno, katere dvojice so po reprezentativnih ocenah tveganja najpomembnejše in se jih lahko izpostavi, to sta npr. dvojici 98, 99, ki imata oceno 2.37, nato sledi dvojica 94 z oceno 2.34 itd. Reprezentativno oceno dobimo iz normalizirane uteženе vsote $K(X_i) = \alpha\sigma_S(X_i) + \beta\sigma_P(X_i) + \gamma\sigma_2(X_i)$ (3.18), kjer so $\alpha = \beta = \gamma = 1$. Torej so v oceni zajete normalizirana subjektivna ocena strokovnjaka po metodologiji, normalizirano število posledic in skupna ocena ranljivosti na izbrani dvojici. Po tem kriteriju prednjačita dvojici 98, 99, ki

jima sledi dvojica 94. Dvojici 98, 99 imata največjo subjektivno oceno po metodologiji, največ posledic in največjo skupno oceno ranljivosti.

Ko se upošteva še povezave (kontekst) in jakost povezav v omrežju, dobimo popolnoma drugačne rezultate, ki se jih da razložiti. Ko se upošteva kontekst, v katerem je dvojica, preidejo v ospredje dvojice 95, 96, 97, čeprav imajo skoraj najmanjšo reprezentativno oceno tveganja. Izkaže se, da si dane dvojice delijo veliko ranljivosti z dvojicami 101, 102, 103, v katerih predstavlja kar 92 % njihovih ocen ranljivosti. Obratno velja, da ranljivosti v 101, 102, 103 predstavlja 50 % ocen ranljivosti v dvojicah 95, 96, 97. Iz grafa se hitro vidi, da so dvojice 95, 96, 97 dobro jakostno povezane z ostalimi dvojicami, in sicer so najmočneje povezane ravno z ostalimi dvojicami, ki so visoko ocenjene. Tudi iz logičnega stališča bi se sklepalo, da bi morala biti grožnja »Razkritje gesla« ocenjena relativno visoko, ker lahko povzroči večino ostalih groženj. Ker pa si lahko razlagamo tudi tako, da »Razkritje gesel« povzročimo z grožnjo »Socialni inženiring«, je le-ta ocenjena še višje. »Vdor v notranje omrežje z interneta« povzroči ranljivosti, ki vplivajo na strežnike in posledično tudi na programsko opremo ter informacije v elektronski obliki.

V primeru, da uteži nastavim še vedno na $\alpha = \beta = \gamma = 1$ iz (3.18), vendar utež iz (3.13) spremenim na $\delta = 0.5$ (povezave oz. kontekst dvojic ima samo polovično moč), se rezultati in izgled grafa spremenijo. Normalizirana matrika dvojic je prikazana v Prilogi 3.4. Iz tako pridobljene matrike sosednosti izračunamo končni normalizirani lastni vektor dvojic, ki je:

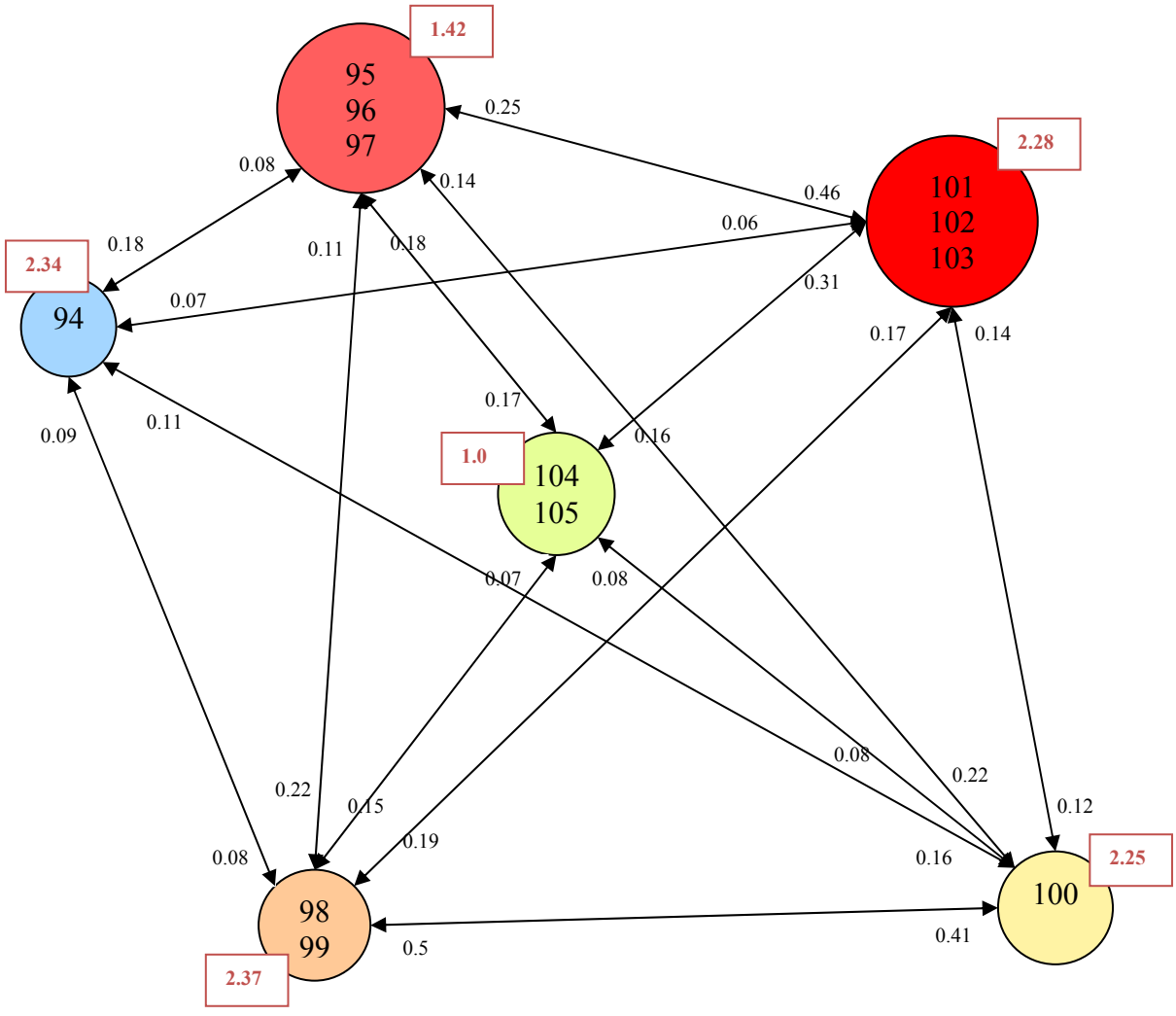
$$\begin{bmatrix} 104 \\ 95 \\ 101 \\ 94 \\ 98 \\ 105 \\ 96 \\ 102 \\ 99 \\ 97 \\ 103 \\ 100 \end{bmatrix} = \begin{bmatrix} 2.2052 \\ 3.7109 \\ 3.8082 \\ 1.0000 \\ 2.7497 \\ 2.2052 \\ 3.7109 \\ 3.8082 \\ 2.7497 \\ 3.7109 \\ 3.8082 \\ 2.7398 \end{bmatrix}$$

Procesi / Informacijska sredstva

Privzeti proces

Grožnja		Informacije v elektronski obliki	Programska oprema	Strežniki
1. Okoljski vplivi				
1.1	Razkritje dokumentov/podatkov			
1.2	Socialni inženiring			
1.3	Vdori v notranje omrežje - iz interneta			
1.4	Razkritje gesla			
1.5	Kraja prenosne opreme			

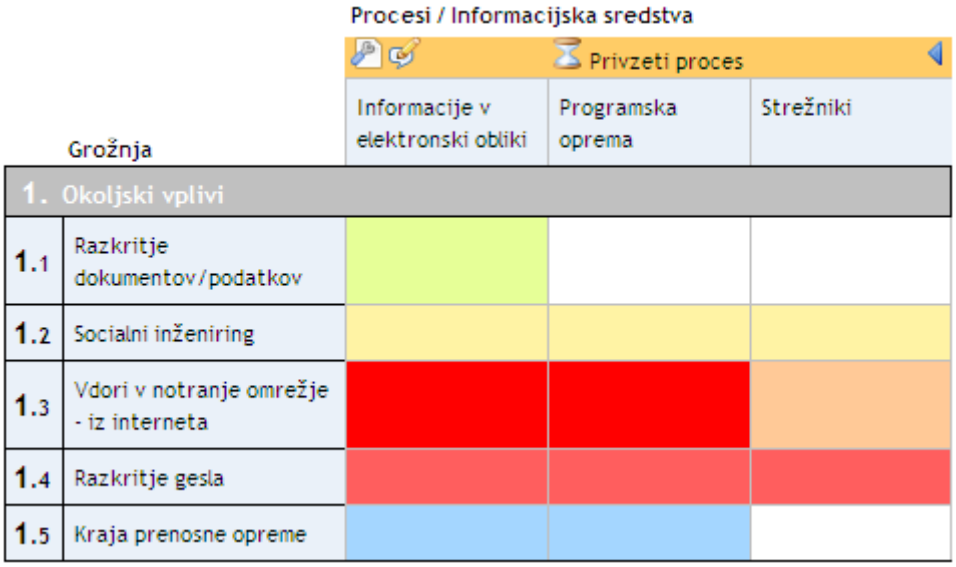
Slika 4.6: Prikaz najbolj tveganih dvojic v barvah, kjer rdeča pomeni največje tveganje, modra pa najmanjše. Izkaže se, da je razkritje gesla za organizacijo najnevarnejša grožnja, ki učinkuje na prav vsa informacijska sredstva, kjer so dobili največjo možno oceno. Sledi socialni inženiring.



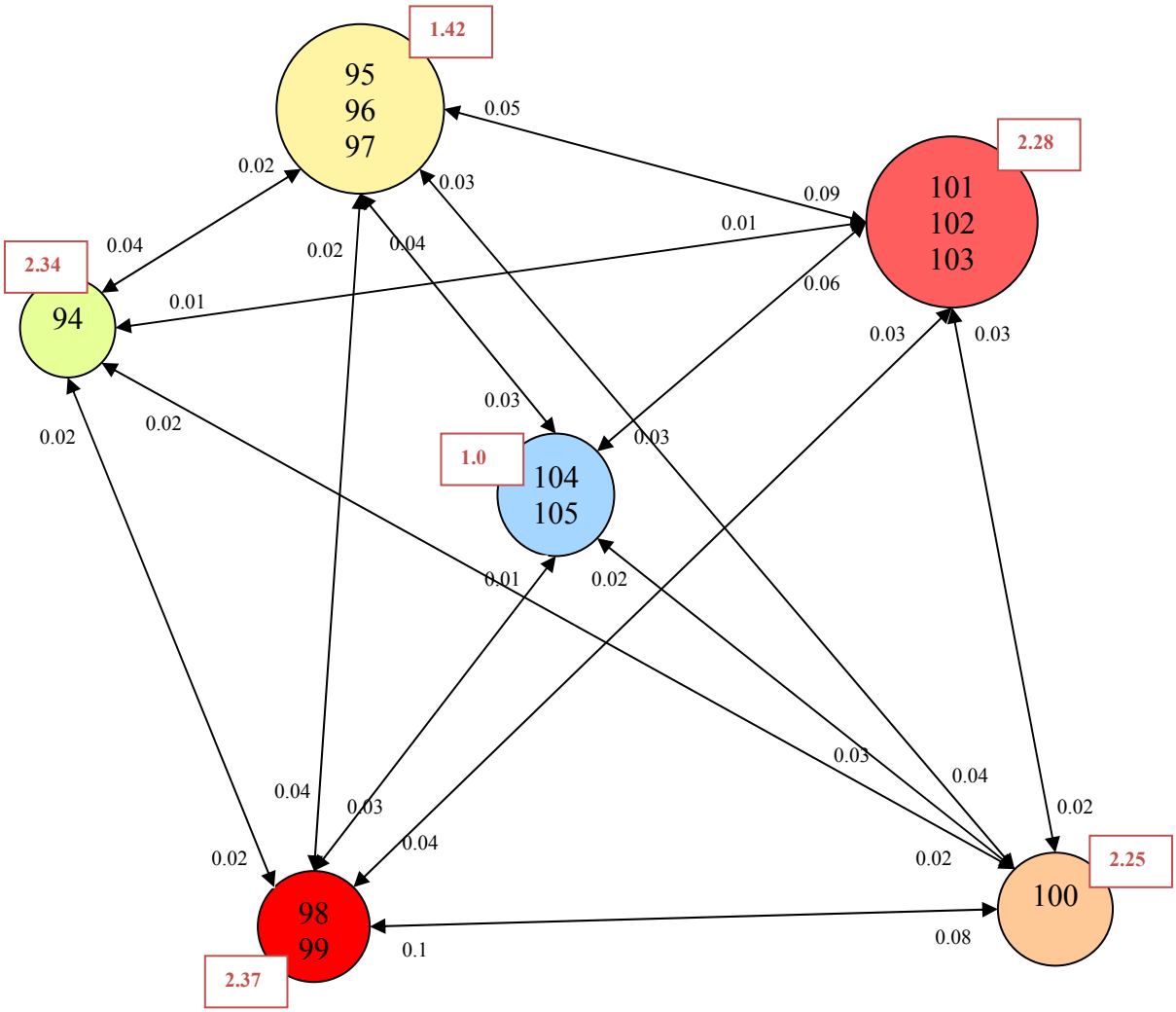
Slika 4.7: Graf dvojic po razvrstitvi pomembnosti.

V primeru, da so parametri še vedno $\alpha = \beta = \gamma = 1$, vendar je $\delta = 0.1$ (povezave oz. kontekst ima moč samo 0.1), prevladujejo reprezentativne ocene tveganja. Normalizirana matrika dvojic je prikazana v Prilogi 3.5. Iz tako pridobljene matrike sosednosti izračunamo končni normalizirani lastni vektor dvojic, ki je:

$$\begin{bmatrix} 104 \\ 95 \\ 101 \\ 94 \\ 98 \\ 105 \\ 96 \\ 102 \\ 99 \\ 97 \\ 103 \\ 100 \end{bmatrix} = \begin{bmatrix} 1.0000 \\ 1.9668 \\ 4.9205 \\ 1.7559 \\ 5.1255 \\ 1.0000 \\ 1.9668 \\ 4.9205 \\ 5.1255 \\ 1.9668 \\ 4.9205 \\ 4.2339 \end{bmatrix}$$



Slika 4.8: Prikaz najbolj tveganih dvojic v barvah, kjer rdeča pomeni največje tveganje, modra pa najmanjše. Izkaže se, da so vdori v notranje omrežje z interneta za organizacijo najnevarnejša grožnja, ki učinkuje na informacije v elektronski obliki in programsko opremo, kjer so dobili največjo možnjo oceno. Sledi razkritje gesla. Vdor v notranje omrežje naj ne bi imel prevelikega vpliva na same fizične strežnike, zato so tudi dobili nižjo oceno pomembnosti.



Slika 4.9: Graf dvojic po razvrstitvi pomembnosti.

Iz primerov je razvidno, kako različne rezultate dobimo pri različnih utežeh δ. Z zmanjševanjem uteži δ zmanjšujemo tudi pomen jakosti povezav oz. konteksta, v katerem se nahajajo grožnje. Zato slika postaja z zmanjševanjem uteži δ čedalje bolj podobna izhodiščni, ki jo je imel v glavi strokovnjak ob uporabi primerne metodologije. Verjetno bi se strokovnjak najbolj strinjal s sliko ob najmanjšem δ, saj se približa njegovi predstavi rezultatov. Pri uteži $\delta = 0.1$ je to dovolj vidno, saj se najbolj tvegane ocene groženj že močneje skladajo z izhodiščno sliko. Pri tem je grožnja vdorov v notranje omrežje z interneta ocenjena kot najvišja oz. med višjimi. Prav tako grožnja razkritja gesla in socialnega inženiringa. Pozna pa se še vpliv algoritma pri grožnji razkritij dokumentov oz. podatkov, ki ga še zmeraj uvrsti med manj pomembne grožnje v nasprotju s strokovnjakovim prepričanjem.

Poglavje 5
Zaključek

V diplomski nalogi predstavim sistem za dodatno odkrivanje pomembnosti groženj pri procesu ocenjevanja tveganja. Izhodišče je ocenitev pomembnosti posameznih ranljivosti, ki jih grožnja povzroči in na podlagi teh ocen nato zgradim graf dvojic groženj ter informacijskih sredstev. Iz tako dobljenega grafa sestavim matriko sosednosti po podanem postopku in lastni vektor te matrike, ki ustreza največji lastni vrednosti, ki pove pomembnost posameznih dvojic. Rezultati so podani v pregledni predstavitvi v obliki spremenjene začetne tabele ocen in mreže medsebojno povezanih dvojic. Sistem torej izkorišča nekatera znanja s področja mrež in mer središčnosti, saj problem ocenjevanja tveganja poskušamo prevesti v domeno mrež, kjer lahko računamo pomembnosti posameznih vozlišč omrežja. Sistem v končni fazi torej predstavi rezultate dovolj jasno strokovnjaku področja, ki jih nato še pregleda oz. nadaljno analizira in mu služijo v morebitno pomoč.

Z nastavljanjem parametrov se obnašanje sistema lahko prilagodi zahtevam strokovnjaka področja. Tako lahko s parametri vplivamo na odločitve sistema, v kolikšni meri naj se upošteva subjektivna ocena strokovnjaka po zastavljeni metodologiji, v kolikšni meri naj se upoštevajo posledice uresničitve grožnje, ali poudarek na kontekstu, v katerem leži dvojica v relaciji z ostalimi dvojicami.

Sistem bi lahko izboljšali tako, da bi upoštevali tudi »risk reduction« analizo. To pomeni, da bi merili učinkovitost posameznih ukrepov (kontrol), da se določena ranljivost zmanjša ali odpravi in koliko ostane še preostalega tveganja po izvedbi ukrepa (»residual risk«). Torej bi lahko sistem predlagal tudi pomembnost ukrepov, katere bi se najbolj izplačalo uvesti takoj, ki bi tudi najbolj učinkovali (»residual risk«) in zadostovali (pokrije oz. zmanjša čimveč ranljivosti).

Zanimiva bi bila tudi stroškovna analiza tveganj oz. »cost-benefit«. Ker je vsaki organizaciji denarna postavka pomembna, bi bila taka analiza še kako zaželena. V analizo bi tako vključili

tudi škodo, merjeno v denarnih enotah, ki jo določena grožnja ob izrabi ranljivosti povzroči in stroškovna cena ukrepa, ki bi ga bilo potrebno izvesti.

Verjetno bi bilo tudi smiselno preučiti uvedbo strojnega učenja parametrov sistema, pri katerem bi strokovnjakova izbira parametrov večih ocen tveganj služila kot učni primer. Poleg tega sistem poenostavlja ocenjevanje tveganja, saj ne ločuje tveganj, ki vplivajo na celovitost, integriteto in zaupnost in jih jemlje kot enakovredne.

Dodatek A

1.1 Pripadajoča matrika sosednosti.

	149	109	300	203	201	202	150	72	333	175	36	311	117	102	151	84	29	138	177	119	171	206	41	139	204	173	146	167	134
149	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
109	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
300	0	0	3	1	1	1	1	2	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
203	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
201	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
202	0	0	1	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
150	0	0	1	0	1	1	2	2	0	0	0	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
72	0	0	2	0	1	1	2	3	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
333	0	0	1	0	0	0	0	1	2	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
175	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
311	0	0	0	0	0	0	1	1	0	0	1	2	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
117	0	0	1	0	0	0	0	1	1	0	0	0	2	2	2	1	2	1	0	0	0	0	0	0	0	0	1	1	0
102	0	0	1	0	0	0	0	1	1	0	0	0	2	2	2	1	2	1	0	0	0	0	0	0	0	0	1	1	0
151	0	0	1	0	0	0	0	1	1	0	0	0	2	2	2	1	2	1	0	0	0	0	0	0	0	0	1	1	0
84	0	0	1	0	0	0	0	1	1	0	0	0	1	1	1	2	1	2	0	0	0	0	0	0	0	0	0	0	0
29	0	0	1	0	0	0	0	1	1	0	0	0	2	2	2	1	2	1	0	0	0	0	0	0	0	0	1	1	0
138	0	0	1	0	0	0	0	1	1	0	0	0	1	1	1	2	1	2	0	0	0	0	0	0	0	0	0	0	0
177	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	2	2	1	1	1	1	1	1	0	0	1

711																														
1199	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	2	2	1	1	1	1	1	1	0	0	1
1711	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
2006	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
4141	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
1399	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
2044	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
1733	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0
1466	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0
1677	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0
1344	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	1

1.2 Matrika sosednosti po normalizicaiji z normalizacijsko mero Geo.

	149	109	30	203	201	202	150	72	33	175	36	31	117	102	151	84	29	138	177	119	171	206	41	139	204	173	146	167	134
149	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
109	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	5	5	5	4	6	4	0	0	0	4	4	4	4	4	4	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	8	8	8	1	7	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
203	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
201	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	5	0	0	0	7	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	8	0	0	0	1	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
202	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	5	0	0	0	7	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	8	0	0	0	1	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
150	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	7	7	0	8	0	0	0	5	0	0	0	0	0	0	5	5	7	7	7	7	7	7	0	0	0
	0	0	1	0	1	1	0	2	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
72	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	6	0	5	5	8	0	4	0	0	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	0	0	0
	0	0	7	0	8	8	2	0	1	0	0	1	1	1	1	1	1	1	1	1	1	8	8	8	8	8	0	0	0
33	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

	0	0	4	0	0	0	0	4	0	0	0	0	5	5	5	5	5	5	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
175	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	5	4	0	0	7	0	0	0	0	0	0	0	0	5	5	7	7	7	7	7	7	0	0	0
	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
117	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	0	0	0	5	0	5	0	0	0	0	0	0	0	0	7	7	0	
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	
102	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	0	0	0	5	0	5	0	0	0	0	0	0	0	0	7	7	0	
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	
151	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	0	0	0	5	0	5	0	0	0	0	0	0	0	0	7	7	0	
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	
84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	5	5	5	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	0	0	0	5	0	5	0	0	0	0	0	0	0	0	7	7	0	
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	
138	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	4	0	0	0	0	4	5	0	0	0	5	5	5	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
177	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	5	4	0	0	0	5	0	0	0	0	0	0	0	0	0	7	7	7	7	7	7	0	0	7
	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	1
119	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	5	4	0	0	0	5	0	0	0	0	0	0	0	0	0	7	7	7	7	7	7	0	0	7
	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	1
171	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
206	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
139	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
204	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
173	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	7	5	0	0	0	7	0	0	0	0	0	0	0	7	7	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	1	8	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
146	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	0	7	7	7	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
167	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	0	0	0	0	0	0	7	7	7	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0

134	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.71	0.71	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

2.1 Matrika sosednosti.

	31	**204**	**203**	**173**	**30**	**29**	**171**	**36**	**41**	**149**	**201**	**202**	**150**	**72**	**175**	**177**	**119**	**33**	**109**	**80**	**134**	**102**	**206**	**139**	**146**	**167**	**117**	**151**	**84**	**136**
31	8	2	2	5	8	2	6	3	6	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
204	2	2	2	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
203	2	2	2	2	2	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
173	5	2	2	5	5	2	3	0	3	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	8	2	2	5	11	5	6	3	9	3	3	3	3	5	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
29	2	2	2	2	5	5	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
171	6	0	0	3	6	0	7	4	6	3	3	3	3	3	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
36	3	0	0	0	3	0	4	4	3	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
41	6	0	0	3	9	3	6	3	9	3	3	3	3	5	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
149	3	0	0	3	3	0	3	0	3	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
201	3	0	0	3	3	0	3	0	3	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
202	3	0	0	3	3	0	3	0	3	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
150	3	0	0	3	3	0	3	0	3	3	3	3	3	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	3	0	0	3	5	2	3	0	5	3	3	3	3	5	0	0	0	2	0	0	0	2	0	0	2	2	2	2	2	2
175	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
177	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
119	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
33	0	0	0	0	3	3	1	1	3	0	0	0	0	2	1	1	1	4	1	1	1	4	1	1	3	3	3	3	2	3
109	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
80	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
134	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
102	0	0	0	0	3	3	1	1	3	0	0	0	0	2	1	1	1	4	1	1	1	4	1	1	3	3	3	3	2	3
22	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

06																													
139	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
146	0	0	0	0	3	3	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
167	0	0	0	0	3	3	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
117	0	0	0	0	3	3	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
1511	0	0	0	0	3	3	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3
84	0	0	0	0	2	2	0	0	2	0	0	0	0	2	0	0	0	2	0	0	0	2	0	0	2	2	2	2	2	2
136	0	0	0	0	3	3	0	0	3	0	0	0	0	2	0	0	0	3	0	0	0	3	0	0	3	3	3	3	2	3

2.2 Matrika sosednosti po normalizicaiji z normalizacijsko mero Geo.

	31	**204**	**203**	**173**	**30**	**29**	**171**	**36**	**41**	**149**	**201**	**202**	**150**	**72**	**175**	**177**	**119**	**33**	**109**	**80**	**134**	**102**	**206**	**139**	**146**	**167**	**117**	**151**	**84**	**136**
31	1.000	0.505	0.557	0.785	0.853	0.323	0.800	0.538	0.711	0.616	0.616	0.616	0.616	0.470	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
204	0.500	1.000	0.000	0.634	0.433	0.463	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
203	0.500	0.000	1.000	0.634	0.433	0.463	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
173	0.079	0.634	0.634	1.000	0.067	0.401	0.451	0.045	0.777	0.777	0.777	0.777	0.777	0.600	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
30	0.853	0.433	0.433	0.067	1.000	0.067	0.681	0.045	0.902	0.522	0.522	0.522	0.522	0.670	0.000	0.000	0.000	0.455	0.000	0.000	0.000	0.455	0.000	0.000	0.522	0.522	0.522	0.522	0.433	0.522
29	0.323	0.463	0.463	0.401	0.067	1.000	0.000	0.045	0.402	0.000	0.000	0.000	0.000	0.402	0.000	0.000	0.000	0.677	0.000	0.000	0.000	0.677	0.000	0.000	0.777	0.777	0.777	0.777	0.634	0.777
171	0.800	0.000	0.000	0.451	0.681	0.000	1.000	0.076	0.765	0.655	0.655	0.655	0.655	0.518	0.388	0.388	0.388	0.199	0.388	0.388	0.388	0.199	0.388	0.388	0.000	0.000	0.000	0.000	0.000	0.000
36	0.538	0.000	0.000	0.045	0.045	0.045	0.076	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.555	0.555	0.555	0.255	0.555	0.555	0.555	0.255	0.555	0.555	0.000	0.000	0.000	0.000	0.000	0.000
41	0.711	0.000	0.000	0.777	0.902	0.402	0.765	0.000	1.000	0.000	0.000	0.000	0.000	0.750	0.000	0.000	0.000	0.500	0.000	0.000	0.000	0.500	0.000	0.000	0.588	0.588	0.588	0.588	0.477	0.588
149	0.616	0.000	0.000	0.777	0.522	0.000	0.655	0.000	0.000	1.000	1.000	1.000	1.000	0.777	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
201	0.616	0.000	0.000	0.777	0.522	0.000	0.655	0.000	0.000	1.000	1.000	1.000	1.000	0.777	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
202	0.616	0.000	0.000	0.777	0.522	0.000	0.655	0.000	0.000	1.000	1.000	1.000	1.000	0.777	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
150	0.616	0.000	0.000	0.777	0.522	0.000	0.655	0.000	0.000	1.000	1.000	1.000	1.000	0.777	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
72	0.470	0.000	0.000	0.600	0.670	0.402	0.518	0.000	0.750	0.777	0.777	0.777	0.777	1.000	0.000	0.000	0.000	0.500	0.000	0.000	0.000	0.500	0.000	0.000	0.588	0.588	0.588	0.588	0.477	0.588
175	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
177	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
119	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
33	0.000	0.000	0.000	0.000	0.000	0.000	0.199	0.255	0.000	0.000	0.000	0.000	0.000	0.000	0.255	0.255	0.255	1.000	0.255	0.255	0.255	1.000	0.255	0.255	0.000	0.000	0.000	0.000	0.000	0.000
109	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
80	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
134	0.000	0.000	0.000	0.000	0.000	0.000	0.199	0.255	0.000	0.000	0.000	0.000	0.000	0.000	0.255	0.255	0.255	1.000	0.255	0.255	0.255	1.000	0.255	0.255	0.000	0.000	0.000	0.000	0.000	0.000
102	0.000	0.000	0.000	0.000	0.455	0.677	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.500	0.255	0.255	0.255	0.255	0.255	0.255	0.255	0.255	0.255	0.255	0.000	0.000	0.000	0.000	0.000	0.000
206	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
139	0.000	0.000	0.000	0.000	0.000	0.000	0.199	0.255	0.000	0.000	0.000	0.000	0.000	0.000	0.255	0.255	0.255	1.000	0.255	0.255	0.255	1.000	0.255	0.255	0.000	0.000	0.000	0.000	0.000	0.000
146	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
167	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
117	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
151	0.000	0.000	0.000	0.000	0.000	0.000	0.388	0.555	0.000	0.000	0.000	0.000	0.000	0.000	1.000	1.000	1.000	0.255	1.000	1.000	1.000	0.255	1.000	1.000	0.000	0.000	0.000	0.000	0.000	0.000
84	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
136	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

	1	0	0	7	2	0	5	0	8	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
200	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
202	6	0	0	7	5	0	6	0	5	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	7	2	0	5	0	8	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
150	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
150	6	0	0	7	5	0	6	0	5	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	7	2	0	5	0	8	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	4	0	0	6	6	4	5	0	7	7	7	7	7	0	0	0	0	4	0	0	0	4	0	0	5	5	5	5	6	5
	7	0	0	0	7	0	1	0	5	7	7	7	7	0	0	0	0	5	0	0	0	5	0	0	2	2	2	2	3	2
175	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
175	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
177	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
177	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
119	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
119	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	4	6	1	2	5	0	0	0	0	4	5	5	5	0	5	5	5	0	5	5	8	8	8	8	7	8
	0	0	0	0	5	7	9	5	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	7	7	7	7	1	7
109	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
109	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
134	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
134	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
102	0	0	0	0	4	6	1	2	5	0	0	0	0	4	5	5	5	0	5	5	5	0	5	5	8	8	8	8	7	8
	0	0	0	0	5	7	9	5	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	7	7	7	7	1	7
206	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
206	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
139	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
139	0	0	0	0	0	0	3	5	0	0	0	0	0	0	0	0	0	5	0	0	0	5	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
146	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
146	0	0	0	0	5	7	0	0	5	0	0	0	0	5	0	0	0	8	0	0	0	8	0	0	0	0	0	0	8	0
	0	0	0	0	2	7	0	0	8	0	0	0	0	2	0	0	0	7	0	0	0	7	0	0	0	0	0	0	2	0
167	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
167	0	0	0	0	5	7	0	0	5	0	0	0	0	5	0	0	0	8	0	0	0	8	0	0	0	0	0	0	8	0
	0	0	0	0	2	7	0	0	8	0	0	0	0	2	0	0	0	7	0	0	0	7	0	0	0	0	0	0	2	0
117	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
117	0	0	0	0	5	7	0	0	5	0	0	0	0	5	0	0	0	8	0	0	0	8	0	0	0	0	0	0	8	0
	0	0	0	0	2	7	0	0	8	0	0	0	0	2	0	0	0	7	0	0	0	7	0	0	0	0	0	0	2	0
151	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
151	0	0	0	0	5	7	0	0	5	0	0	0	0	5	0	0	0	8	0	0	0	8	0	0	0	0	0	0	8	0
	0	0	0	0	2	7	0	0	8	0	0	0	0	2	0	0	0	7	0	0	0	7	0	0	0	0	0	0	2	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	
	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
	0	0	0	0	4	6	0	0	4	0	0	0	0	6	0	0	0	7	0	0	0	7	0	0	8	8	8	8	0	8	
	0	0	0	0	3	3	0	0	7	0	0	0	0	3	0	0	0	1	0	0	0	1	0	0	2	2	2	2	0	2	

	0.000	0.000	0.000	0.000	0.052	0.077	0.000	0.000	0.058	0.000	0.000	0.000	0.000	0.052	0.000	0.000	0.000	0.087	0.000	0.000	0.000	0.087	0.000	0.000	1.000	1.000	1.000	1.000	0.082	1.000

3.1 Matrika dvojic po skupnih ranljivostih. V glavi matrike so ID-ji dvojic, v celicah pa ID-ji ranljivosti.

	104	**95**	**101**	**94**	**98**	**105**	**96**	**102**	**99**	**97**	**103**	**100**
104	31,204,203,173,30,29	31,30	31,173,30		30,29	31,204,203,173,30,29	31,30	31,173,30	30,29	31,30	31,173,30	30,29
95	31,30	171,36,31,30,41	171,31,30,41	171,36	30,41	31,30	171,36,31,30,41	171,31,30,41	30,41	171,36,31,30,41	171,31,30,41	30,41
101	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	171	30,41,72	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41,72	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41
94		171,36	171	171,175,177,119,33,109,80,36,134,102,206,139	33,102		171,36	171	33,102	171,36	171	33,102
98	30,29	30,41	30,41,72	33,102	146,167,117,33,102,151,84,30,29,41,72,138	30,29	30,41	30,41,72	146,167,117,33,102,151,84,30,29,41,72,138	30,41	30,41,72	146,167,117,33,102,151,30,29,41,138
105	31,204,203,173,30,29	31,30	31,173,30		30,29	31,204,203,173,30,29	31,30	31,173,30	30,29	31,30	31,173,30	30,29
96	31,30	171,36,31,30,41	171,31,30,41	171,36	30,41	31,30	171,36,31,30,41	171,31,30,41	30,41	171,36,31,30,41	171,31,30,41	30,41
102	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	171	30,41,72	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41,72	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41
99	30,29	30,41	30,41,72	33,102	146,167,117,33,102,151,84,30,29,41,72,138	30,29	30,41	30,41,72	146,167,117,33,102,151,84,30,29,41,72,138	30,41	30,41,72	146,167,117,33,102,151,30,29,41,138
97	31,30	171,36,31,30,41	171,31,30,41	171,36	30,41	31,30	171,36,31,30,41	171,31,30,41	30,41	171,36,31,30,41	171,31,30,41	30,41
103	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	171	30,41,72	31,173,30	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41,72	171,31,30,41	171,149,31,201,202,173,30,41,150,72	30,41
100	30,29	30,41	30,41	33,102	146,167,117,33,102,151,30,29,41,138	30,29	30,41	30,41	146,167,117,33,102,151,30,29,41,138	30,41	30,41	146,167,117,33,102,151,30,29,41,138

3.2 Matrika sosednosti dvojic.

	104	95	101	94	98	105	96	102	99	97	103	100
1	0.6379	0.3689	0.6203	0	0.2977	1	0.3689	0.6203	0.2977	0.3689	0.6203	0.2977
0	78097	04789	29500		34138		04789	29500	34138	04789	29500	34138
4	61051	8097	54672		18167		8097	54672	18167	8097	54672	18167
9	0.3469	0.9039	0.9155	0.3546	0.4470	0.3469	1	0.9155	0.4470	1	0.9155	0.4470
5	97768	34697	87429	94379	74510	97768		87429	74510		87429	74510
	9079	87066	68995	79362	59386	9079		68995	59386		68995	59386
1	0.3189	0.5005	1.4576	0.1477	0.3780	0.3189	0.5005	1	0.3780	0.5005	1	0.2444
0	89681	43277	50153	60594	64592	89681	43277		64592	43277		11547
1	1767	08448	8277	20239	96711	1767	08448		96711	08448		57812
9	0	0.1657	0.1262	1.4902	0.1622	0	0.1657	0.1262	0.1622	0.1657	0.1262	0.1622
4		39488	95683	81017	83993		39488	95683	83993	39488	95683	83993
		8731	00904	2058	15142		8731	00904	15142	8731	00904	15142
9	0.1388	0.2215	0.3427	0.1721	1.5114	0.1388	0.2215	0.3427	1	0.2215	0.3427	0.8174
8	07588	90989	64930	37774	51772	07588	90989	64930		90989	64930	77538
	25234	24878	64938	46426	2617	25234	24878	64938		24878	64938	77742
1	1	0.3689	0.6203	0	0.2977	0.6379	0.3689	0.6203	0.2977	0.3689	0.6203	0.2977
0		04789	29500		34138	78097	04789	29500	34138	04789	29500	34138
5		8097	54672		18167	61051	8097	54672	18167	8097	54672	18167
9	0.3469	1	0.9155	0.3546	0.4470	0.3469	0.9039	0.9155	0.4470	1	0.9155	0.4470
6	97768		87429	94379	74510	97768	34697	87429	74510		87429	74510
	9079		68995	79362	59386	9079	87066	68995	59386		68995	59386
1	0.3189	0.5005	1	0.1477	0.3780	0.3189	0.5005	1.4576	0.3780	0.5005	1	0.2444
0	89681	43277		60594	64592	89681	43277	50153	64592	43277		11547
2	1767	08448		20239	96711	1767	08448	8277	96711	08448		57812
9	0.1388	0.2215	0.3427	0.1721	1	0.1388	0.2215	0.3427	1.5114	0.2215	0.3427	0.8174
9	07588	90989	64930	37774		07588	90989	64930	51772	90989	64930	77538
	25234	24878	64938	46426		25234	24878	64938	2617	24878	64938	77742
9	0.3469	1	0.9155	0.3546	0.4470	0.3469	1	0.9155	0.4470	0.9039	0.9155	0.4470
7	97768		87429	94379	74510	97768		87429	74510	34697	87429	74510
	9079		68995	79362	59386	9079		68995	59386	87066	68995	59386
1	0.3189	0.5005	1	0.1477	0.3780	0.3189	0.5005	1	0.3780	0.5005	1.4576	0.2444
0	89681	43277		60594	64592	89681	43277		64592	43277	50153	11547
3	1767	08448		20239	96711	1767	08448		96711	08448	8277	57812
1	0.1697	0.2710	0.2710	0.2105	1	0.1697	0.2710	0.2710	1	0.2710	0.2710	1.4363
0	99880	66761	66761	71870		99880	66761	66761		66761	66761	52582
0	32446	76104	76104	53934		32446	76104	76104		76104	76104	1141

3.3 Normalizirana matrika dvojic za parametre $\alpha = \beta = \gamma = 1, \delta = 1.0$.

	104	95	101	94	98	105	96	102	99	97	103	100
104	1.00	0.37	0.62	0.00	0.30	1.00	0.37	0.62	0.30	0.37	0.62	0.30
95	0.35	1.42	0.92	0.35	0.45	0.35	1.00	0.92	0.45	1.00	0.92	0.45
101	0.32	0.50	2.28	0.15	0.38	0.32	0.50	1.00	0.38	0.50	1.00	0.24
94	0.00	0.17	0.13	2.34	0.16	0.00	0.17	0.13	0.16	0.17	0.13	0.16
98	0.14	0.22	0.34	0.17	2.37	0.14	0.22	0.34	1.00	0.22	0.34	0.82
105	1.00	0.37	0.62	0.00	0.30	1.00	0.37	0.62	0.30	0.37	0.62	0.30
96	0.35	1.00	0.92	0.35	0.45	0.35	1.42	0.92	0.45	1.00	0.92	0.45
102	0.32	0.50	1.00	0.15	0.38	0.32	0.50	2.28	0.38	0.50	1.00	0.24
99	0.14	0.22	0.34	0.17	1.00	0.14	0.22	0.34	2.37	0.22	0.34	0.82
97	0.35	1.00	0.92	0.35	0.45	0.35	1.00	0.92	0.45	1.42	0.92	0.45
103	0.32	0.50	1.00	0.15	0.38	0.32	0.50	1.00	0.38	0.50	2.28	0.24
100	0.17	0.27	0.27	0.21	1.00	0.17	0.27	0.27	1.00	0.27	0.27	2.25

3.4 Normalizirana matrika dvojic za parametre $\alpha = \beta = \gamma = 1, \delta = 0.5$.

	104	95	101	94	98	105	96	102	99	97	103	100
104	1.00	0.18	0.31	0.00	0.15	0.50	0.18	0.31	0.15	0.18	0.31	0.15
95	0.17	1.42	0.46	0.18	0.22	0.17	0.50	0.46	0.22	0.50	0.46	0.22
101	0.16	0.25	2.28	0.07	0.19	0.16	0.25	0.50	0.19	0.25	0.50	0.12
94	0.00	0.08	0.06	2.34	0.08	0.00	0.08	0.06	0.08	0.08	0.06	0.08
98	0.07	0.11	0.17	0.09	2.37	0.07	0.11	0.17	0.50	0.11	0.17	0.41
105	0.50	0.18	0.31	0.00	0.15	1.00	0.18	0.31	0.15	0.18	0.31	0.15
96	0.17	0.50	0.46	0.18	0.22	0.17	1.42	0.46	0.22	0.50	0.46	0.22
102	0.16	0.25	0.50	0.07	0.19	0.16	0.25	2.28	0.19	0.25	0.50	0.12
99	0.07	0.11	0.17	0.09	0.50	0.07	0.11	0.17	2.37	0.11	0.17	0.41

97	0.17	0.50	0.46	0.18	0.22	0.17	0.50	0.46	0.22	1.42	0.46	0.22
103	0.16	0.25	0.50	0.07	0.19	0.16	0.25	0.50	0.19	0.25	2.28	0.12
100	0.08	0.14	0.14	0.11	0.50	0.08	0.14	0.14	0.50	0.14	0.14	2.25

3.5 Normalizirana matrika dvojic za parametre $\alpha = \beta = \gamma = 1$, $\delta = 0.1$.

	104	**95**	**101**	**94**	**98**	**105**	**96**	**102**	**99**	**97**	**103**	**100**
104	1.00	0.04	0.06	0.00	0.03	0.10	0.04	0.06	0.03	0.04	0.06	0.03
95	0.03	1.42	0.09	0.04	0.04	0.03	0.10	0.09	0.04	0.10	0.09	0.04
101	0.03	0.05	2.28	0.01	0.04	0.03	0.05	0.10	0.04	0.05	0.10	0.02
94	0.00	0.02	0.01	2.34	0.02	0.00	0.02	0.01	0.02	0.02	0.01	0.02
98	0.01	0.02	0.03	0.02	2.37	0.01	0.02	0.03	0.10	0.02	0.03	0.08
105	0.10	0.04	0.06	0.00	0.03	1.00	0.04	0.06	0.03	0.04	0.06	0.03
96	0.03	0.10	0.09	0.04	0.04	0.03	1.42	0.09	0.04	0.10	0.09	0.04
102	0.03	0.05	0.10	0.01	0.04	0.03	0.05	2.28	0.04	0.05	0.10	0.02
99	0.01	0.02	0.03	0.02	0.10	0.01	0.02	0.03	2.37	0.02	0.03	0.08
97	0.03	0.10	0.09	0.04	0.04	0.03	0.10	0.09	0.04	1.42	0.09	0.04
103	0.03	0.05	0.10	0.01	0.04	0.03	0.05	0.10	0.04	0.05	2.28	0.02
100	0.02	0.03	0.03	0.02	0.10	0.02	0.03	0.03	0.10	0.03	0.03	2.25

Seznam slik

Seznam tabel

Literatura

[1] M. E. J. Newman, *The mathematics of networks*, Center for the Study of Complex Systems, University of Michigan.

[2] P.J.G. Long, *Introduction to Octave*, Department of Engineering, University of Cambridge, 2005.

[3] George Karypis, *Mining Scientific Data Sets: Challenges and Opportunities*, Department of Computer Science & Engineering, University of Minnesota.

[4] Anjali Koppal, *Properties of Networks*, Columbia University, 2008.

[5] Gary Stoneburner, Alice Goguen, Alexis Feringa, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology, Technology Administration and U.S. Department of Commerce, 2002.

[6] Risk assessment. Dostopno na http://en.wikipedia.org/wiki/Risk_assessment, uporabljeno: februar 2010.

[7] Data mining. Dostopno na http://en.wikipedia.org/wiki/Data_mining, uporabljeno: februar 2010.

[8] Network Centrality Using Eigenvectors. Dostopno na http://demonstrations.wolfram.com/NetworkCentralityUsingEigenvectors/, uporabljeno: marec 2010.

[9] Tommy DiRaimondo, Rob Carr, Marc Palmer, Matt Pickvet , *Eigenvalues Eigenvectors*, dostopno na http://controls.engin.umich.edu/wiki/index.php/EigenvaluesEigenvectors, 2006.

[10] Andrej Mrvar: Analiza omrežij s programom Pajek.

[11] Centrality. Dostopno na http://en.wikipedia.org/wiki/Centrality, uporabljeno: februar 2010.

[12] Perron–Frobenius theorem. Dostopno na http://en.wikipedia.org/wiki/Perron%E2%80%93Frobenius_theorem, uporabljeno: februar 2010.

[13] Adjacency matrix. Dostopno na http://en.wikipedia.org/wiki/Adjacency_matrix, uporabljeno: februar 2010.

[14] Google PageRank. Dostopno na http://en.wikipedia.org/wiki/PageRank, uporabljeno: februar 2010.

[15] Tomaž Kuralt, *Avtonomen sistem za združevanje podatkovnih omrežij*, diplomsko delo na univerzitetnem študiju, 2009.

[16] Lovro Šubelj, *Odkrivanje goljufij na osnovi analize socialnih mrež*, diplomsko delo na univerzitetnem študiju, 2008.

[17] Denis Trček, Managing *information systems security and privacy*, Berlin, Heidelberg, New York: Springer, 2006, pogl. 2

[18] Perron Frobenius teorem. Dostopno na http://en.wikipedia.org/wiki/Perron%E2%80%93Frobenius_theorem, uporabljeno: februar 2010.