Univerzitet Singidunum

Fakultet za informatiku i računarstvo

ZNAČAJ OCJENE RIZIKA KOD UMREŽENIH INFORMACIJSKIH SISTEMA

Doktorski rad

Mentor:

Prof. dr. Milan Milosavljević

Kandidat:

Mr. sc. Zdenko Adelsberger

KATALOGIZACIJA

Komisija:

1. Prof. dr. Mladen Veinović, predsjednik komisije
2. Prof. dr. Branko Kovačević, član
3. Prof. dr. Milan Milosavljević, član i mentor

Koristim ovi priliku da se zahvalim prof. dr. Milanu Milosavljević, koji mi je pružio nesebičnu podršku u realizaciji ovog rada.

Također bi želio izraziti svoju zahvalnost doc. dr. Gojku Grubor koji mi je svojim savjetima i pomoći omogućio da rad realiziram u formi kakav je u konačnici.

Posebno bi se zahvalio kolegi i prijatelju dr. Nenadu Injac koji mi je s neizmjernom podrškom, razumijevanjem, savjetima i verifikacijom rezultata bitno pomogao da rad završim u formi i sadržaju kakav je.

Želim se zahvaliti i sinu Dejanu Adelsberger koji mi je pomogao oko tehničke obrade rada, kao i drugima članovima moje porodice koja mi je stalno pružala podršku pri izradi rada.

Sažetak

U radu se obrađuje mogućnost obrade i upravljanja rizicima sistema u području informacijskih sistema. Istražene su sve do sada ponuđene metode u okvirima postojećih saznanja iz literature, međunarodnih standarda i najbolje prakse. Postavljene su hipoteze koje se odnose na mogućnost upravljanja rizicima promjenom veza elemenata unutar strukture i davanjem različitih vrijednosti opterećenja pojedinih elemenata ili cijelih grupa. Razvijen je poseban model koji istražuje strukturu uz pomoć latinske kompozicije i u potpunosti je realiziran izradom odgovarajućeg programa. Konačno se daje novi niz teorema koje dokazuju potpuno novu mogućnost upravljanja informacijskim i drugim sistemima uz pomoć promjene njihove strukture i izmjenom parametara elemenata od kojih se sastoje.

Ključne riječi: informacijski sistem, rizici, upravljanje rizicima, ISMS, struktura sistema, latinska kompozicija

Abstract

This article discusses the possibility of processing and risk management systems in the field of information systems. All until now offered methods within the framework of existing knowledge from literature, international standards and best practices have been investigated.

The hypotheses have been set related to the ability to manage risks by changing the relationships of elements within the structure and giving different load values of individual elements or entire groups. A special model has been developed that examines the structure with the help of Latin composition, and is fully realized by creating the appropriate software.

Finally, a new set of theorems that prove the possibility of a completely new information management and other systems by changing their structure and changing the parameters of the elements that they are made of has been provided.

Keywords: information system, risk, risk management, ISMS, system structure, Latin composition

PREGLED SLIKA

Slika 2.1.	Ilustracija odnosa signala, podatka i informacije	6
Slika 2.2.	Pojednostavljena blok shema informacijskog sistema	9
Slika 2.3.	Funkcionalna shema informacijskog sistema	11
Slika 2.4.	PDCA krug i utjecaj na kvalitetu performansi sistema	12
Slika 2.5.	Blok shema poslovnog procesa	14
Slika 2.6.	Mapiranje poslovnih procesa po hijerarhijskim nivoima	15
Slika 2.7.	Blok shema primjera mapiranja složenog poslovnog procesa	15
Slika 2.8.	Vrste poslovnih procesa u organizaciji	17
Slika 3.1.	Shema informacijskog sistema s obzirom na vrste imovine koje ulaze u sastav informacijskog sistema	20
Slika 3.2	„Klasični“ pogled na hijerarhiju informacijskih sistema	20
Slika 3.3.	Primjer strukture složenog informacijskog sistema	23
Slika 4.1.	Odnos informacijskog sistema i značajki informacija	24
Slika 4.2.	Informacijski sistem organizacije kao skup informacijskog podsistema	25
Slika 4.3.	Proces za upravljanje informacijskom sigurnošću prema ISO 27001:2005	29
Slika 4.4.	Projekt implementacije ISMS prema ISO 27001:2005	30
Slika 4.5.	Struktura standarda ISO 27002:2005	32
Slika 5.1.	Fizikalni model rizika	36
Slika 5.2.	Relacijski prikaz fizikalnog modela rizika	36
Slika 5.3.	Događanja nakon sigurnosnog incidenta	37
Slika 5.4.	Upravljanje rizicima (pojednostavljena shema procesa)	38
Slika 5.5.	Analiza namjernih prijetnji vezanih za ljudsko djelovanje ili nedjelovanje	40
Slika 5.6.	Primjer iskorištenja ranjivosti od strane jedne prijetnje	41
Slika 5.7.	Proces za upravljanje rizicima prema ISO 27005:2008	43
Slika 5.8.	Grafički prikaz rizika za 3 i 2 parametra	48
Slika 5.9.	Područje vrijednosti procjene rizika	49
Slika 5.10.	Matrica prihvatljivosti rizika	50
Slika 6.1.	Blok shema informacijskog sistema kao procesa	51
Slika 6.2.	Blok shema informacijskog sistema u stanju zadovoljavanja i nezadovoljavanja ulaznih zahtjeva	51
Slika 6.3.	Objekti u informacijskom sistemu	52
Slika 6.4.	Pridruživanje objektima indikatora stanja	52
Slika 6.5.	Hasse-ov dijagram sistema s tri objekta	55
Slika 6.6.	Serijska struktura objekata	55
Slika 6.7.	Paralelna struktura objekata	55
Slika 6.8.	Složena struktura objekata	56
Slika 6.9.	Graf strukture sa tri čvora	56
Slika 6.10.	Prikazi neorijentiranog grafa strukture sistema	63
Slika 6.11.	Objedinjavanje paralelnih grana u grafu strukture sistema	63
Slika 6.12.	Prikaz grafa strukture i pripadna latinska kompozicija	64
Slika 6.13.	Prikaz latinske matrice $L^{(1)}$ i pripadne reducirane latinske matrice l	64
Slika 6.14.	Modificirana latinska i reducirana latinska matrica za definicijski par (1,4)	64

Slika 6.15.	Množenje latinske i reducirane latinske matrice	65
Slika 6.16.	Množenje rezultirajuće latinske matrice $L^{(2)}$ s reduciranom matricom l	65
Slika 6.17.	Grafički prikaz putova kroz zadanu strukturu	65
Slika 7.1.	Primjeri informacijskih sistema samo sa serijskom imovinom u strukturi	68
Slika 7.2.	Grafički prikaz težine serijske strukture – sve grane imaju istu težinu	68
Slika 7.3.	Granični slučajevi serijske strukture	69
Slika 7.4.	Primjeri informacijskih sistema samo s paralelnim granama u strukturi	70
Slika 7.5.	Grafički prikaz težine paralelne strukture – sve grane imaju istu težinu	70
Slika 7.6.	Granični slučajevi paralelne strukture	71
Slika 7.7.	Graf strukture informacijskog sistema za provedenu analizu.	72
Slika 7.8.	Latinska matrica za strukturu na slici 7.7.	72
Slika 7.9.	Reducirana latinska matrica za graf na slici 7.7.	73
Slika 7.10.	Latinska matrica i reducirana latinska matrica za karakteristični par (1,5)	73
Slika 7.11.	Dijagrami proračuna rizika struktura u zavisnosti od rizika grane	75
Slika 7.12.	Analiza strukture gdje jedna grana mijenja težinu, a sve ostale imaju težinu 0,1	76
Slika 7.13.	Analiza zadane strukture za slučaj da sve grane imaju težinu 0,2 i 0,3. Mijenja se težina samo jedne grane	77
Slika 7.14.	Histogram generatora slučajnih brojeva korištenog u analizi	78
Slika 7.15.	Distribucije struktura prema težinama za slučajne težine grana	79
Slika 7.16.	Primjer orijentirane strukture informacijskog sistema	80
Slika 7.17.	Latinska matrica za strukturu na slici 7.16.	81
Slika 7.18.	Reducirana latinska matrica za primjer strukture na slici 7.16.	81
Slika 7.19.	Dijagrami proračuna težine strukture u zavisnosti od težina grana	82
Slika 7.20.	Dijagrami orijentirane strukture 1, neorijentirane strukture i jedne grane	83
Slika 7.21.	Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,1	84
Slika 7.22.	Odnos težine neorijentirane strukture 1 i težina promjenljivih grana	85
Slika 7.23.	Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,2	87
Slika 7.24.	Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,3	88
Slika 7.25.	Distribucije struktura prema težinama za slučajne težine grana	89
Slika 7.26.	Primjer orijentirane strukture 2 informacijskog sistema	90
Slika 7.27.	Latinska matrica za strukturu na slici 7.26.	90
Slika 7.28.	Reducirana latinska matrica za strukturu na slici 7.26.	91
Slika 7.29.	Dijagrami proračuna težine strukture u zavisnosti od težine grana za strukturu sa slike 7.26.	92
Slika 7.30.	Dijagrami proračuna težine strukture u zavisnosti od težine grana za strukturu 2 sa slike 7.26. i strukturu 1 sa slike 7.16.	93
Slika 7.31.	Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,1	94
Slika 7.32.	Odnos težine neorijentirane strukture 2 i težina promjenljivih grana	95

Slika 7.33.	Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale grane imaju težinu 0,2	97
Slika 7.34.	Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale grane imaju težinu 0,3	98
Slika 7.35.	Distribucija struktura prema težinama za slučajne težine grana za primjer orijentirane strukture 2	99
Slika 8.1.	Analizirane složene strukture informacijskih sistema	101
Slika 8.2.	Prikaz dijagrama težina i rizika složenih struktura sa slike 8.1.	101
Slika 8.3.	Strukture složenih informacijskih sistema sa procijenjenim rizicima u granama za svaki aspekt informacijske sigurnosti (C-I-A)	104
Slika 8.4.	Grafički prikaz rezultata proračuna rizika složenih struktura informacijskih sistema po aspektima (C-I-A)	107
Slika 8.5.	Blok shema e-mail servisa firme	108
Slika 8.6.	Blok shema procesa e-mail servisa za aspekt funkcionalnosti	109
Slika 8.7.	Blok shema procesa e-mail servisa firme s aspekta informacijske sigurnosti	110
Slika 8.8.	Pregled popisane informacijske imovine e-mail servisa	111
Slika 8.9.	Primjer upisa informacijske imovine u bazu softvera Hestia RISK	111
Slika 8.10.	Definiranje elemenata procjene prijetnji i ranjivosti u softveru Hestia RISK	112
Slika 8.11.	Definiranje kriterija prihvatljivosti u softveru Hestia RISK	113
Slika 8.12.	Definiranje značenja razina prijetnji i ranjivosti u softveru Hestia RISK	113
Slika 8.13.	Rezultati procjene rizika za e-mail servis	114
Slika 8.14.	Graf strukture e-mail servisa sa slike 8.5.	115
Slika 8.15.	Grafovi putova od ulaznog do izlaznog čvora za primjer sa slike 8.14.	116
Slika 8.16.	Graf strukture s rizicima grana na temelju procjene za aspekte C-I-A	118
Slika 8.17.	Upisana struktura e-mail servisa sa slike 8.14. u softver LATMAT	118
Slika 8.18.	Pronađeni putovi pomoću softvera LATMAT od ulaznog do izlaznog čvora za strukturu sa slike 8.14.	119
Slika 8.19.	Prikaz upisanih težina grana za e-mail strukturu u softver LATMAT za aspekte informacijske sigurnosti C-I-A respektivno	119
Slika 8.20.	Rezultati analize težina strukture e-mail servisa pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)	120
Slika 8.21.	Blok shema i pripadni graf strukture e-mail servisa za slučaj neispravnosti WiFi Access pointa	121
Slika 8.22.	Struktura sa slike 8.21. upisana u softver LATMAT	121
Slika 8.23.	Rezultati analize težina strukture e-mail servisa sa slike 8.21. pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)	122
Slika 8.24.	Blok shema i pripadni graf strukture e-mail servisa za slučaj neispravnosti WiFi Access pointa i E-mail servera	123
Slika 8.25.	Rezultati analize težina strukture e-mail servisa sa slike 8.24. pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)	123
Slika 8.26.	Grafički prikaz promjene rizika strukture e-mail servisa za aspekte informacijske sigurnosti (C-I-A)	124
Slika 9.1.	Glavni meni programa LATMAT	127
Slika 9.2.	Definiranje strukture mreže za primjer neorijentirane strukture	127

	prema slici 7.7.	
Slika 9.3.	Modificirana struktura sa slike 9.2.	128
Slika 9.4.	Promjena definiranog para	128
Slika 9.5.	Latinska matrica za strukturu sa slike 9.2.	129
Slika 9.6.	Reducirana latinska matrica sa slike 9.5.	129
Slika 9.7.	Latinska matrica za definirani par (lijevo) i reducirana latinska matrica za definirani par (desno)	129
Slika 9.8.	Proračun paralelne strukture u programu LATMAT	130
Slika 9.9.	Proračun serijske strukture u programu LATMAT	130
Slika 9.10.	Rezultat proračuna težine složene strukture u programu LATMAT	131
Slika 9.11.	Upis težina pojedinih grana u strukturi	132

PREGLED TABLICA

Tablica 2.1.	PDCA faze	12
Tablica 4.1.	PDCA faze procesa za upravljanje ISMS prema ISO 27001:2005	30
Tablica 5.1.	PDCA faze procesa za upravljanje rizicima informacijske sigurnosti	43
Tablica 5.2.	Kvalitativna skala za prijetnje	46
Tablica 5.3.	Kvalitativna skala za ranjivosti	46
Tablica 5.4.	Kvalitativna skala za posljedice	46
Tablica 5.5.	Vrijednosti rizika za primjere tablica 5.2, 5.3 i 5.4	48
Tablica 5.6.	Primjer rang skale za procijenjene rizike	49
Tablica 7.1.	Lista i broj putova za primjer sa slike 7.7.	74
Tablica 7.2.	Rezultati analize za težinu svih grana = 0,1 i jednu granu s promjenljivom težinom	75
Tablica 7.3.	Rezultati analize za težinu svih grana = 0,2 i jednu granu s promjenljivom težinom	77
Tablica 7.4.	Rezultati analize za težinu svih grana = 0,3 i jednu granu s promjenljivom težinom	77
Tablica 7.5.	Težine struktura za slučajne težine grana	79
Tablica 7.6.	Lista i broj putova za primjer sa slike 7.16.	81
Tablica 7.7.	Rezultati analize za težinu grana 0,1 i jednu granu s promjenljivom težinom	84
Tablica 7.8.	Rezultati analize za težinu grana 0,2 i jednu granu s promjenljivom težinom	86
Tablica 7.9.	Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom	86
Tablica 7.10.	Težine orijentirane strukture 1 za slučajne težine grana	89
Tablica 7.11.	Lista i broj putova za primjer sa slike 7.26.	91
Tablica 7.12.	Rezultati analize za težinu grana 0,1 i jednu granu s promjenljivom težinom	94
Tablica 7.13.	Rezultati analize za težinu grana 0,2 i jednu granu s promjenljivom težinom	96
Tablica 7.14.	Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom	96
Tablica 7.15.	Težine orijentirane strukture 2 za slučajne težine grana	99
Tablica 8.1.	Težine i rizici složenih struktura sa slike 8.1.	102
Tablica 8.2.	Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom	103
Tablica 8.3.	Primjer rizika i težina za neorijentiranu strukturu (1) sa slike 8.3	105
Tablica 8.4.	Primjer rizika i težina za orijentiranu strukturu (2) sa slike 8.3	106
Tablica 8.5.	Primjer rizika i težina za orijentiranu strukturu (3) sa slike 8.3	106
Tablica 8.6.	Ukupne težine i rizici struktura sa slike 8.1. po aspektima C-I-A informacijske sigurnosti	107
Tablica 8.7.	Prikaz latinske kompozicije za graf strukture prikazan na slici 8.14.	117
Tablica 8.8.	Rizici i težine informacijske imovine u granama grafa	117
Tablica 8.9.	Težine i rizici strukture e-mail servisa	120
Tablica 8.10.	Težine i rizici strukture e-mail servisa prema slici 8.23.	122

Tablica 8.11.	Težine i rizici strukture e-mail servisa prema slici 8.24.	124
Tablica 8.12.	Težine i rizici strukture e-mail servisa za slučajeve 8.5.4.-8.5.6.	124
Tablica 12.1.	Osnovni pojmovi i definicije	140
Tablica 12.2.	Pregled najznačajnijih prijetnji za informacijske sisteme	143
Tablica 12.3.	Pregled prijetnji kojima su izvor ljudi	145
Tablica 12.4.	Lista glavnih ranjivosti informacijskih sistema	147
Tablica 12.5.	Lista prijetnji i ranjivosti u informacijskim sistemima po sigurnosnim područjima	148
Tablica 12.6.	Težine serijske strukture sistema	152
Tablica 12.7.	Težine paralelne strukture sistema	155
Tablica 12.8.	Rezultati analize složene neorijentirane strukture s jednakim težinama u svim granama	158
Tablica 12.9	Rezultati analize složene orijentirane strukture 1 s jednakim težinama u svim granama	160
Tablica 12.10.	Rezultati analize složene orijentirane strukture 2 s jednakim težinama u svim grana	162

POPIS SKRAĆENICA

AXIAL	Analyse et Conception de Systemes d'Information Assistes par Logiciels
BSI	British Standards Institution
CASE	Computer Added Sotware Engineering
C-I-A	Confidentiality - Integrity - Availability
DAFNE	DAta and Function Networking
DSS	Decision Support Systems
DTI	Department of Trade and Industry
HIPO	Hierarchical Input and Proces Output
HOOD	Hierarchical Object Oriented Design
IDEF	Integration Definition for Function Modeling
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
JSD/JSP	Jackson System Development / Jackson System Programming method
KPI	Key Performance Indicator
LCM	Life Cycle Methodology
LRQA	Lloyd's Register Quality Assurance
MIS	Mangement Information System
NIST	National Institute of Standards and Technology
PDA	Personal Digital Assistant
PDCA	Plan Do Check Act
PIN	Personal Identification Number
SADT	System Analysis and Design Techniques
SDM	Software Development Management system
SSADM	Structured System Analysis and Design Method
TPS	Transaction processing systems
UML	Unified Modelling Language
USB	Universal Serial Bus
Wi-Fi,WiFi	Wireless Fidelity or wireless internet or mechanism for wirelessly connecting electronic devices
www	World Wide Web

Sadržaj

1. METODOLOGIJA ISTRAŽIVAČKOG RADA 1
1.1. OBRAZLOŽENJE ISTRAŽIVAČKOG RADA I PRETHODNA ISTRAŽIVANJA 1
1.2. PREDMET RADA 1
1.3. HIPOTETIČKI OKVIR 2
1.3.1. Opća hipoteza 2
1.3.2. Pojedinačne hipoteze 2
1.4. CILJEVI ISTRAŽIVAČKOG RADA 2
1.4.1. Naučni cilj 2
1.4.2. Konkretni cilj 2
1.5. TOK ISTRAŽIVAČKOG PROCESA I METODE ISTRAŽIVANJA 3
1.5.1. Tok istraživačkog procesa 3
1.5.2. Opće naučne metode 3
1.5.3. Matematičke metode 3
1.5.4. Primjena odgovarajućeg softvera 3
2. INFORMACIJSKI SISTEMI 4
2.1. UVOD 4
2.2. POJAM I DEFINICIJA INFORMACIJE 5
2.3. ZNAČAJKE INFORMACIJE 7
2.4. POJAM I DEFINICIJA INFORMACIJSKOG SISTEMA 8
2.5. UPRAVLJANJE INFORMACIJSKIM SISTEMIMA 11
2.5.1. PDCA pristup upravljanja sistemima 11
2.5.2. Procesni pristup upravljanja sistemima 13
2.5.3. Veza između PDCA kruga i procesnog pristupa 17
3. STRUKTURA INFORMACIJSKIH SISTEMA 19
3.1. KLASIČNI PRISTUP KLASIFIKACIJI INFORMACIJSKIH SISTEMA 20
3.2. SUVREMENI PRISTUP KLASIFIKACIJI INFORMACIJSKIH SISTEMA 22
4. SIGURNOST INFORMACIJSKIH SISTEMA 24
4.1. INFORMACIJSKA SIGURNOST PREMA ISO27001 27
4.1.1. Namjena i struktura standarda ISO 27001:2005 28
4.1.2. Namjena i struktura standarda ISO 27002:2005 31
4.1.3. Namjena i struktura standarda 27005:2008 33
4.2. IMPLEMENTACIJA ISMS 33
5. OSNOVI TEORIJE RIZIKA 35
5.1. FIZIKALNI MODEL RIZIKA 35
5.1.1. Prijetnje 38
5.1.2. Ranjivosti 40
5.1.3. Posljedice 42
5.2. PROCES UPRAVLJANJA RIZICIMA 42
5.3. METODOLOŠKI PRISTUP PROCJENI RIZIKA ZA ISMS 45

5.3.1. Kvantitativni metodološki pristup 45
5.3.2. Kvalitativni metodološki pristup 46
6. STRUKTURNA FUNKCIJA 51
6.1. OSNOVI TEORIJE STRUKTURE SISTEMA 51
6.2. OSNOVNI OBLICI STRUKTURNE FUNKCIJE 53
6.2.1. Serijska struktura 54
6.2.2. Paralelna struktura 54
6.3. NAČINI PRIKAZIVANJA STRUKTURNIH FUNKCIJA 54
6.4. PUTEVI I PRESJECI 57
6.5. MINIMALNI PUTEVI I MINIMALNI PRESJECI 57
6.6. MATEMATIČKE KARAKTERISTIKE PUTEVA I PRESJEKA. DUALNOST 58
6.7. TRAŽENJE SVIH MINIMALNIH PUTEVA 60
6.7.1. Latinska kompozicija 61
6.7.2. Karakteristike latinske kompozicije 62
7. RIZIK STRUKTURIRANIH INFORMACIJSKIH SISTEMA 66
7.1. ANALIZA SERIJSKE STRUKTURE 67
7.2. ANALIZA PARALELNE STRUKTURE 69
7.3. ANALIZA SLOŽENE NEORJENTIRANE STRUKTURE IS 71
7.3.1. Analiza složene strukture IS sa jednakim rizicima u svim granama 74
7.3.2. Analiza složene strukture IS sa promjenljivim rizicima jedne grane 75
7.3.3. Analiza složene strukture IS sa slučajnim rizicima u svim granama 78
7.4. ANALIZA SLOŽENE ORJENTIRANE STRUKTURE IS 80
7.4.1. Orijentirana struktura 1 80
7.4.1.1. Analiza orijentirane strukture 1 sa jednakim težinama u granama 82
7.4.1.2. Analiza orijentirane strukture 1 sa promjenljivom težinom jedne grane 83
7.4.1.3. Analiza orijentirane strukture 1 sa slučajnim težinama u svim granama 89
7.4.2. Orijentirana struktura 2 90
7.4.2.1. Analiza orijentirane strukture 2 sa jednakim težinama u granama 92
7.4.2.2. Analiza orijentirane strukture 2 sa promjenljivom težinom jedne grane 93
7.4.2.3. Analiza orijentirane strukture 2 sa slučajnim težinama u svim granama 99
8. UPRAVLJANJE RIZICIMA METODOM IZMJENE STRUKTURE 100
8.1. I. TEOREM RIZIKA SLOŽENE STRUKTURE 102
8.2. II. TEOREM RIZIKA SLOŽENE STRUKTURE 103
8.3. III. TEOREM RIZIKA SLOŽENE STRUKTURE 103
8.4. ANALIZA UTJECAJA STRUKTURE INFORMACIJSKOG SISTEMA NA INFORMACIJSKE RIZIKE U ISMS 104
8.5. PRAKTIČNI PRIMJER IMPLEMENTACIJE ANALIZA UTJECAKA STRUKTURE INFORMACIJSKOG SISTEMA NA RIZIKE U ISMS 108
8.5.1. Identifikacija i popis imovine 111

8.5.2. Procjena rizika e-mail servisa 112
8.5.3. Rezultati procjene rizika e-mail servisa 113
8.5.4. Analiza strukture e-mail servisa 115
8.5.5. Analiza strukture e-mail servisa bez funkcionalnosti WiFi segmenta 121
8.5.6. Analiza strukture e-mail servisa bez funkcionalnosti WiFi segmenta i nefunkcioniranja E-mail servera 122
8.5.7. Zaključno razmatranje primjera strukture e-mail servisa 124
9. IZGRADNJA MODELA SIMULACIJE 126
9.1. Struktura programa LATMAT 126
9.2. Definiranje struktura u programu LATMAT 127
9.3. Analiza paralelne i serijske strukture u programu LATMAT 130
9.4. Analiza složene strukture pomoću programa LATMAT 131
10. DISKUSIJA 133
11. ZAKLJUČCI 136
12. PRILOZI 140
12.1. Osnovni pojmovi i definicije 140
12.2. Pregled najznačajnijih prijetnji za informacijske sisteme 143
12.3. Pregled prijetnji kojima su izvor ljudi 145
12.4. Lista glavnih ranjivosti informacijskih sistema 147
12.5. Lista prijetnji i ranjivosti u informacijskim sistemima po sigurnosnim područjima 148
12.6. Težine serijske strukture 152
12.7. Težine paralelne strukture 155
12.8. Rezultati analize složene neorijentirane strukture s jednakim težinama u svim granama 158
12.9. Rezultati analize složene orijentirane strukture 1 s jednakim težinama u svim granama 160
12.10. Rezultati analize složene orijentirane strukture 2 s jednakim težinama u svim granama 162
13. REFERENCE I LITERATURA 164

1. METODOLOGIJA ISTRAŽIVAČKOG RADA

1.1. OBRAZLOŽENJE ISTRAŽIVAČKOG RADA I PRETHODNA ISTRAŽIVANJA

Rizici su tema stara kao što je star i sam ljudski rod. Međutim, unificiran i normiran pristup rizicima je apsolutno novost koja se tek zadnjih nekoliko godina pojavljuje u vrlo širokom spektru profesija kao vrlo usmjereno djelovanje i zajednički propisan pristup. Pri tome je jedan od najvažnijih aspekata proces upravljanja rizicima kod koga se želi osigurati niz stanja i događanja koja u sebi nose minimalnu opasnost na svim nivoima bilo koje i bilo kakve organizacije – sasvim svejedno da li je riječ o bankarskom poslovanju, izgradnji kapitalnih objekata, koordinaciji transporta ili rukovanju opasnim materijalima. Ono što je danas zajedničko za sve grane ljudskog rada i djelovanja jeste da je sve duboko prožeto gustom mrežom prikupljanja, obrade i primjene svih oblika podataka. Informacijski sistemi su danas, u punom smislu te riječi, sistem nad sistemima, temelj svih drugih aktivnosti i njihov kvalitetan rad je pretpostavka kvalitetnog rada svih drugih oblasti. Zato je sasvim razumljivo da su svi rizici, koji su karakteristični za informacijske sisteme, od izuzetnog značaja, a njihovo upravljanje apsolutna neophodnost. Usprkos tome, danas je dostupan vanredno mali broj objavljenih radova o ovoj temi, a neka područja su slabo ili nikako dotaknuta. Obzirom da se autor ovih redova bavi upravo tom temom zadnjih 15 godina (uključujući istraživački rad i sva potrebna prethodna istraživanja) i ima niz objavljenih članaka i izlaganja na Balkanu (Srbija, Hrvatska) i u Rusiji, omogućilo je da se opredijeli za detaljnu obradu upravljanja rizicima kod složenih informacijskih sistema.

1.2. PREDMET RADA

Kada se kaže – upravljanje rizicima informacijskih sistema, već je praktično vrlo dobro opisan predmet ovog rada. Dakle, riječ je o okupljanju svih novih saznanja i standarda vezanih uz rizike i njihova aktivna primjena na upravljanje rizicima kod informacijskih sistema. Poseban aspekt je dobivanje efikasnih alata, metoda i pristupa o kojima se danas vrlo malo zna, dok su neki po prvi put objelodanjeni i predstavljaju vlastiti razvoj niza hipoteza autora. Time se predmet rada može naći u razvoju novih matematičkih metoda i analiza kod sagledavanja rizika informacijskih sistema. Istovremeno, u radu se provodi niz provjera danih hipoteza i prezentiraju dobiveni rezultati.

1.3. HIPOTETIČKI OKVIR

1.3.1. Opća hipoteza

Klasično upravljanje rizicima temelji se na četiri elementa (prihvaćanje, izbjegavanje, prenošenje i smanjenje rizika). U ovom radu dodana je još jedan potpuno novi, do sada nigdje ne primijenjen ili spomenut element (barem prema istraživanju i saznanju autora):

- upravljanje rizicima složenog informacijskog sistema uz pomoć upravljanja oblikom njegove strukture.

Ova hipoteza je, prema postojećem stanju stvari, zahtijevala niz postavki i pristupa u upravljanju rizicima, koji su apsolutna novost. Glavni dio kompletnog rada u prvom redu je posvećen postavkama ove hipoteze i njene odbrane kroz testirane modele.

1.3.2. Pojedinačne hipoteze

Prilikom razrade postavki glavne ili opće hipoteze, u pojedinim fazama izračunavanja, pojedina stanja i iznosi stanja uzeti su kao konstante. Ponašanja struktura su prvo promatrana statički pa tek onda dinamički, tako da su određenom nizu vrijednosti zadavani jednaki iznosi itd. U konačnoj sintezi ponašanja rizika cijelog informacijskog sistema, te veličine su međusobno varirane i tako tražene postojeće zakonitosti i matematičke relacije.

1.4. CILJEVI ISTRAŽIVAČKOG RADA

1.4.1. NAUČNI CILJ

Ovaj rad ima naučni cilj da otvori put istraživanjima upravljanja rizicima informacijskih sistema (i ne samo njih) u sasvim novim i neistraženim domenama. Dokazi i metode u ovom radu, prema saznanju autora, prvi put su primijenjeni na složenim sistemima i znače mogućnost ulaska u potpuno nove oblasti gdje se rizici moraju imati pod punom kontrolom. Osim toga, u naučnom smislu, rad je kao cilj uzeo traženje niza postojećih relacija i zakonitosti koje su tim više dokazive što je objekt koji se obrađuje (ovdje je u pitanju informacijski sistem) složeniji i veći.

1.4.2. Konkretni cilj

Kada su u pitanju konkretni ciljevi, ovaj rad ih je imao nekoliko

a) dati moćan alat u istraživanju procesa i upravljanja procesima u složenim sistemima,
b) izgraditi algoritam rješavanja procesa i upravljanja procesima u složenim sistemima,
c) dati oblik postupanja koji bi morao rezultirati općim preporukama,
d) postići primjenu u realnim uvjetima rada s rizicima na složenim informacijskim sistema,
e) pružiti osnove za primjenu kompletne prakse na postojećim preporukama, zakonima i svim važećim standardima.

1.5. TOK ISTRAŽIVAČKOG PROCESA I METODE ISTRAŽIVANJA

1.5.1. Tok istraživačkog procesa

Istraživački proces se odvijao po slijedećim fazama

a) prepoznavanje i izdvajanje glavnih elemenata problematike,
b) pretraživanje postojeće literature (od pojedinih radova i uvida u Internetu do temeljne literature najpoznatijih svjetskih autora),
c) sistematizacija i potpuna analiza svih raspoloživih preporuka, zakona i standarda,
d) postavljanje glavne i pomoćnih hipoteza,
e) izbor odgovarajućeg logičkog i matematičkog aparata,
f) izgradnja traženih modela,
g) verifikacija hipoteze i
h) pisanje rada.

1.5.2. Opće naučne metode

Primjena općih naučnih metoda odnosila se prije svega na načine prikupljanja literature i podataka, izbor primijenjenih tehnika i tehnologija, njihovu filtraciju i sređivanje. U kasnijim fazama rada prišlo se izgradnji adekvatnog modela uz što veću primjenjivost u konkretnoj praksi.

1.5.3. Matematičke metode

U radu su široko zastupljene dvije oblasti u izgradnji i testiranju modela

a) Bool-ova algebra logičkih relacija i
b) Latinski kvadrat (posebno latinska matrica i odgovarajuće množenje latinskih matrica).

Primjena ovog matematičkog aparata za izučavanje rizika na složenim informacijskim sistemima je potpuna novost (prema saznanju autora) i zahtijevala je posebne prilagodbe i testiranja.

1.5.4. Primjena odgovarajućeg softvera

Veličina broja podataka, složenost njihove obrade te potrebno korištenje kapaciteta kompjutera (prije svega kada je u pitanje veličina memorije i trajanje obrade), nužno je zahtijevala primjenu softvera kojeg nema na tržištu. Stoga je, za primjenu u ovom radu, u potpunosti razvijen aplikativni softver za izgradnju i testiranje modela te dokazivanje postavljene hipoteze.

2. INFORMACIJSKI SISTEMI

2.1. UVOD

Veliki umreženi informacijski sistemi su danas od prvorazrednog značaja za sve aspekte života i rada. Pri tome je sasvim svejedno da li je riječ o administraciji, realizaciji proizvoda i usluga, saobraćaju ili bilo čemu drugom. Bilo kakve smetnje u takvim složenim sistemima znače smjesta ogromne materijalne gubitke, a nerijetko se radi i o ugrožavanju zdravlja i sigurnosti ljudi. Svjetska globalizacija se prije svega ogleda u stalnom razvoju i usložnjavanju niza mreža informacijskih sistema koji prerastaju u svojevrstan nervni sistem čitave planete. Zato nije ni čudo što faktori kao kvaliteta, pouzdanost, efikasnost itd. dobivaju svakodnevno na značaju. Eksponencijalni porast praktičnih i teoretskih radova na ovu temu, niz konferencija i savjetovanja te sve značajniji projekti govore o tome da normalno funkcioniranje i razvoj ljudskog društva općenito počiva na pouzdanim i kvalitetnim umreženim informacijskim sistemima. Na osnovu višegodišnjeg ispitivanja i praktičnog rada, te kroz neposredne primjere, kao i uz puno oslanjanje na postojeće standarde i literaturu razmatra se ova problematika te određuju parametri važni za korektan rad i ispunjenje zadanih ciljeva. Primaran interes posvećen je značaju ocjene rizika i svemu što je s tim povezano. Obrađuje se optimalizacija određivanja rizika i dobivanje minimalnog broja značajnih faktora koji određuju taj postupak i u okvirima analize rizika razmatraju se sve postojeće pojave osnovnih utjecaja i posljedice koje se tom prilikom javljaju. Iz teoretski neograničenog skupa svih mogućih parametara koji utiču na procjenu rizika izdvajaju se oni koji su bitni kod bilo kakvih događanja za konačnu ocjenu stanja rizičnosti promatranog objekta. Predlažu se mjere na koje se mora obavezno obratiti pažnja kod buduće ocjene rizika kod umreženih informacijskih sistema.

Cilj uspostavljanja teze je bio dokazivanje da je za konačnu ocjenu stanja rizika umreženih informacijskih sistema uvijek odgovaran relevantan ograničen broj signifikatnih faktora kao i njihovi međusobni odnosi.

Korištena teoretska podloga rada se oslanja na teoriju rizika, raspodjele funkcija, faktorsku analizu, operacijska istraživanja, teoriju velikih mreža, pouzdanost i matematičku simulaciju podržanu kompjuterom.

Analiza i testiranje ponašanja objekta, dokazivanje postavljene teze i svih popratnih pojava provodi se u potpunosti uz podršku odgovarajućih softverskih paketa i njihovom međusobnim nadopunjavanjem (upravljanje rizicima, upravljanje procesima i matematička simulacija modela).

U radu se po prvi puta pokazuje i dokazuje da je određivanje signifikatnih parametara neophodan postupak kod određivanja upravljanja rizicima i malo složenijeg objekta (sistema). Posebno se ističe neophodnost izgradnje modela i provođenje potrebnih simulacija i testiranja kod ocjene rizika umreženih informacijskih sistema.

Uz pomoć novo razvijene metode određivanja signifikatnih parametara kod određivanja upravljanja rizicima po prvi put se omogućuje pojednostavljenje, brzina i pouzdanost kod svih procesa objekata i sistema koji zahtijevaju bilo kavo bavljenje rizicima, posebno kad je u pitanju ocjena rizika kod umreženih informacijskih sistema.

Teoretski i praktični temelji na kojima se zasniva navedena teza su postojeći nacionalni i međunarodni standardi, postojeći propisi i zakonska regulativa, podaci iz literature, postojeći matematički aparati potrebni za određivanje svih potrebnih podataka i izgradnju simulacijskog modela, te rezultati višegodišnjeg teoretskog i praktičnog rada (objavljeni na nizu stručnih konferencija i savjetovanja) kao i u odgovarajućim stručnim i znanstvenim publikacijama.

U području praktične primjene i teoretskog razmatranja često se sreće niz definicija za isti pojam, što u najmanju ruku dovodi u zabunu korisnika. Razlike u definicijama istog pojma mogu biti toliko velike da se teško moći reći da objašnjavaju isti pojam. U okviru ovog rada će se koristiti terminologija koja je definirana međunarodnim standardima za područje koje je tema rada. Pojmovi su većinom preuzeti iz pojedinih međunarodnih ISO standarda. U skladu s tim međunarodnim ISO standardima su i nacionalni standardi. Time se postiže vrlo visoki stupanj razumijevanja problematike, a i kompatibilnosti s praktičnom primjenom u većini zemalja svijeta. Kod navođenja definicija pojedinih pojmova iz standarda po potrebi se daju i dodatna objašnjenja. Definicije pojmova navedene su u prilogu ovom radu.

2.2. POJAM I DEFINICJA INFORMACIJE

Kada se govori o informacijskim sistemima, ključni objekt oko kojega se izgrađuje cjelokupni sistem je informacija. Zato je nužno prije definiranja informacijskog sistema definirati pojam 'informacija'. Tu se mora odmah reći da ne postoji jedinstvena definicija pojma 'informacija'. Ona zavisi od izvora koji ju i s kojim ciljem donosi. Kao primjer može se navesti nekoliko definicija za pojam 'informacija', a koje u svakom slučaju nisu jedine i konačne:

Primjer 1 - Informacija je [91]:

- Poruka primljena i shvaćena
- Znanje stečeno kroz studij ili iskustva ili uputa
- Formalne optužbe za kazneno djelo
- Podaci: Zbirka činjenice iz kojih se može izvući zaključke; ("statistički podaci")
- (Teorija komunikacija) numerička mjera nesigurnosti ishoda, "signal koji sadržavala tisuće bita informacija"

Primjer 2 - Informacija je [92]:

> Informacija, većinom u ograničenom tehničkom smislu, uređeni niz simbola. Kao koncept, međutim, informacija ima mnogo značenja. Osim toga, koncept informacije je usko povezan s pojmovima ograničenja, komunikacija, kontrole, obrasca, instrukcije, znanja, značenja, mentalnog podražaja, uzoraka, percepcija i zastupljenosti.

Primjer 3 – Informacija je [93]:

- Informacija označava reprezenta činjenice (ili poruke) za primaoca.

Primjer 4 – Informacija je [3]

Imovina kao i svaka druga, te kao takva mora biti čuvana u organizaciji.

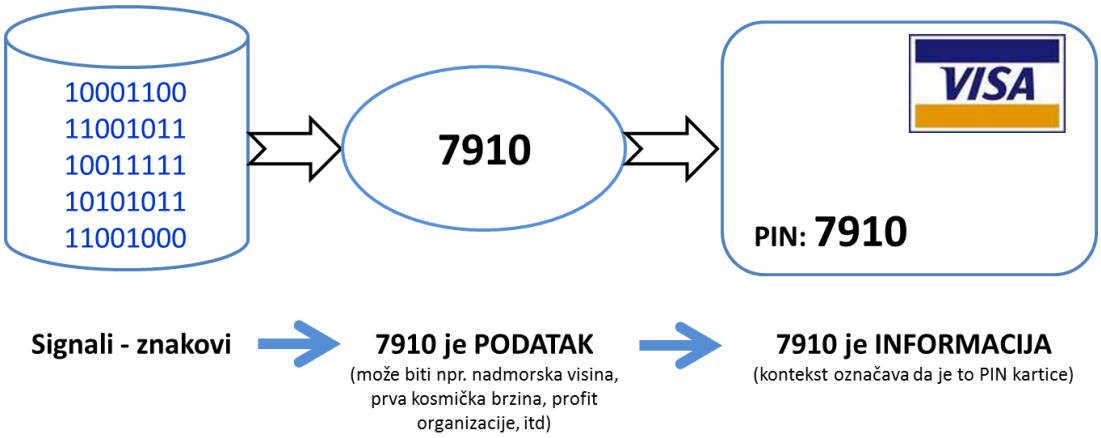
Primjer 5 – Informacija [65]

može biti definirana kao obilježje izlaza procesa, samog procesa i ulaza u proces. Ovakva definicija je neovisna od discipline gdje se želi primijeniti bez obzira na područje, od fizike do epistemologije (ili teorija znanja). Hijerarhije procesa, koje su međusobno povezane, osiguravaju komunikacijski kanal između svake od funkcija i odgovarajućih slojeva u hijerarhiji. Kroz model komunikacija (Shannon and Weaver's Model of Communication), predlaže se u skladu s tim konceptualnim okvirom, informacija kao vrijednost izlaza bilo kojeg procesa u hijerarhiji procesa. Teme ili definicije koje se uključuju u informaciju su vrijednost, funkcija, argument, proces, reverzibilnost, poruka, kanal, inverzne funkcije, reprezentacija, percepcija, vjerovanja, znanja, gubitak informacije, pogodne informacije, nepotpune informacije i dezinformacije.

Očito je iz gornjih primjera definicije pojma 'informacija' teško ili nikako ne može naći jedinstvena koja bi u potpunosti zadovoljavala sve te pristupe. Zbog toga će se u okviru ovog rada pod pojmom 'informacija' podrazumijevati slijedeća definicija:

Definicija: ***Informacija je podatak koji u nekom kontekstu ima vrijednost za korisnika.***

Naime, prema toj definiciji informacije znači da su to podaci stavljeni u neki kontekst, dok je sam podatak izvan konteksta. Drugim riječima, podatak je beskoristan sve dok ne prenosi neku informaciju. Prema toj definiciji informacija je skup znakova (podataka) koji primatelju nešto znače, odnosno otkrivaju nešto novo. Informacija je pojam s mnogo značenja, kao što se i vidi iz gornjih definicija, ovisno o kontekstu, ali je kao pravilo usko povezana s pojmovima kao što su značenje, znanje, percepcija, instrukcija, komunikacija i razni mentalni procesi. Pojednostavljeno rečeno, informacija je primljena i shvaćena poruka. Ali prije svega, ona je rezultat procesiranja, manipuliranja i organiziranja podataka na načina da isti nadograđuju znanje korisnika koji prima informaciju. Na slici 2.1 je prikazan međusobni odnos signala (niza znakova), podatka i informacije.



Slika 2.1 Ilustracija odnosa signala, podatka i informacije

2.3. ZNAČAJKE INFORMACIJE

Svaka informacija ima tri značajke koje ju identificiraju kao upotrebljivu. Te značajke informacije su: tajnost, cjelovitost i dostupnost [2,3]. Često puta se prema engleskim riječima za značajke informacije koristi skraćenica C-I-A (Confidentiality – Integrity – Availability).

Tajnost informacije (Confidentiality) se definira kao svojstvo informacije da nije dozvoljena ili objavljena za neovlaštene osobe, entitete ili procese [1].

To označava da informaciju može koristiti samo osoba koju je ovlastio u pravilu vlasnik informacije. Svim ostalim osobama nije dozvoljeno 'vidjeti' informaciju, odnosno iskoristiti ju. Ako je informacija pohranjena na kompjuteru ta se značajka najčešće rješava obaveznom upotrebom lozinke. U koliko neka osoba zna lozinku onda ona može doći u stanje da vidi i koristi informaciju. Ako je informacija zapisana na papiru, a treba se osigurati njena tajnost, u praksi se najčešće provode mjere onemogućavanja doticaja neovlaštene osobe s papirom na kojem je informacija. U koliko je informacija u glavi neke osobe, tada se tajnost te informacije čuva isključivo sviješću osobe i sankcijama koji bi se poduzele ako osoba neovlaštenoj osobi prenese tu informaciju.

Tu nije riječ samo o osobama, već i bilo kojim drugim entitetima i procesima koji automatski ili poluautomatski mogu koristiti neku informaciju. U praksi se za njih najčešće ograničava pristup ili kriptiranje podataka, tako da entitet ili proces koji ne zna enkripcijski ključ nije u stanju da koristi informaciju.

Cjelovitost informacije (Integrity) svojstvo zaštite informacije u smislu točnosti i kompletnosti same informacije [1]. Smisao je u tome da se informacija ne može promijeniti bez znanja i odobrenja vlasnika informacije. Naime, ako je sadržaj neke informacije određen skupom podataka, onda se taj skup podataka ne smije promijeniti bez odobrenja vlasnika informacije. Pojam cjelovitosti se ne odnosi samo na sadržaj informacije, nego i na sve metode i postupke kojima se te informacije obrađuju, prenose, skladište, itd.

U praksi se problem cjelovitosti informacije najčešće rješava na način da se onemogući neovlaštenim osobama pristup mjestima na kojima je moguće izmijeniti podatak (bilo na papiru, bilo u kompjuteru), ali i entitetima i procesima, npr. procesima hakiranja, ispadima sistema, itd. koji mogu dovesti do oštećenja i/ili nepotrebne izmjene informacije.

Dostupnost informaciji (Availability) je svojstvo informacije da joj se može pristupiti i koristiti na zahtjev ovlaštene osobe [1]. To znači, ovlaštena osoba može doći do potrebne informacije gdje i kada treba. Kako je postupak dolaska do informacije ovlaštene osobe unaprijed definiran, smatra se se da samo na takav način ovlaštena osoba može i mora doći do nje.

U praksi to znači da u slučaju korištenja kompjutera, korisnik mora imati pristup do informacije putem terminala, PC-a, kablovske mreže, WiFi mreže, ili na neki drugi način kako je to prethodno predviđeno, a ovlaštena osoba mora biti upoznata s time. U koliko ne radi infrastruktura koja treba osigurati dostup do informacije na kompjuteru, tada se kaže da je došlo do gubitka ove značajke informacije.

U koliko je informacija zapisana na papiru, tada se dostupnost ovlaštene osobe osigurava tako da ona ima ključ, ili netko drugi tko ima ključ od osiguranog prostora (soba, sef, itd.) bude u potrebnom trenutku prisutan da se može doći do informacije.

2.4. POJAM I DEFINICIJA INFORMACIJSKOG SISTEMA

Kao što u praksi ne postoji jedinstvena definicija za pojam 'informacija', tako i za pojam 'informacijski sistem' ne postoji jednoznačna definicija. Niz izvora pokušava iz raznih aspekata dati sveobuhvatnu definiciju informacijskog sistema, međutim u pojedinim slučajevima područja primjene neke definicije ne govore precizno o tome što je informacijski sistem. Za ilustraciju raznih definicija informacijskog sistema, evo nekoliko primjera:

Primjer 1 – Definicija informacijskog sistema [94]

> Informacijski sistem je kombinacija ljudi, hardvera, softvera, komunikacijskih uređaja, mreža i podatkovnih resursa kojima se obrađuju (može biti pohrana, pronalaženje, transformiranje) podaci i informacije za određenu namjenu. Funkcioniranje slično nekom drugom sistemu, koji treba ulaz od strane korisnika (upute i naredbe, tipkanje, skeniranje). Ulazni podaci će se obrađivati (računanje, izvještavanje) pomoću tehnologije uređaja kao što su kompjuteri, te proizvesti izlaz (ispis izvještaja, prikaz rezultata), koji će biti poslan drugom korisniku ili drugim sistemima putem mreže i povratne veze koja kontrolira rad sistema.

Primjer 2 – Definicija informacijskog sistema [95]

> Informacijski sistemi su načini na koji ljudi i organizacije korištenjem tehnologije, prikupljaju, obrađuju, pohranjuju, koristite i šire informacije.

Primjer 3 – Definicija informacijskog sistema [96]

> Informacijski sistem je integrirani set komponenti za prikupljanje, pohranu, obradu i komuniciranje informacija. Poslovne organizacije, druge organizacije i pojedinci u suvremenom društvu oslanjaju se na informacijske sisteme za upravljanje svojim operacijama, natjecanjem na tržištu, pružanjem usluga, i poboljšanjem osobnog života. Na primjer, moderna korporacija oslanja se na kompjutorizirani informacijski sistem za obradu financijskih računa i upravljanje ljudskim resursima; općinske vlasti oslanjaju na informacijske sisteme za pružanje osnovnih usluga građanima, a pojedinci koriste informacijske sisteme za studij, trgovinu, rad s bankom, ulaganje, itd.

Primjer 4 – Definicija informacijskog sistema [97]

- Bilo koji sistem za obradu podataka, ili ručni ili kompjuterizirani
- Bilo koji telekomunikacijski sistem koji ima primarnu ulogu prijenosa i/ili prikaza podataka

Primjer 5 – Definicija informacijskog sistema [98]

> Informacijski sistem je kombinacija hardvera, softvera, infrastrukture i stručnog osoblja u organizaciji kako bi se olakšalo planiranje, kontrola, koordinacija i donošenje odluka.

Primjer 6 – Definicija informacijskog sistema [53]

Telekomunikacijska i/ili kompjuterska oprema ili sistemi ili podsistemi koji se koriste u cilju dobivanja, skladištenja, manipulacije, upravljanja, kontrole, prikazivanja, prijema glasom, a obuhvaća softver, firmver i hardver.

Primjer 7 – Definicija informacijskog sistema [71]

Informacijski sistem se može definirati kao kompjuter, komunikacijski sistemi te informacijski izvori koje koriste organizacije za podršku svojih svakodnevnih operacija. To uključuje razne uređaje, uključujući i mobilne telefone i osobne digitalne pomoćnike (PDA uređaji).

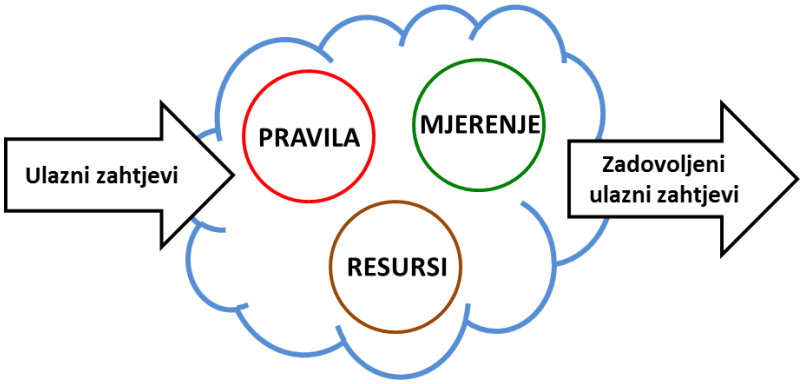
Iz gornjih primjera se vidi prilično velika nepreciznost definicija pojma 'informacijski sistem'. To samo potvrđuje pravilo da aspekt s kojeg se promatra informacijski sistem uvjetuje manje više i oblik definicije.

U svakom slučaju, informacijski sistem, kako mu i sam naziv sugerira je specijalna vrsta sistema, odnosno sistem s posebnom namjenom. U tom kontekstu se može definirati informacijski sistem na slijedeći način:

Definicija:

Informacijski sistem je uređeni dokumentirani skup resursa, pravila i mjernih metoda kojima se zadovoljavaju ulazni zahtjevi vezani za manipulaciju s informacijama da bi se dobio traženi izlaz, odnosno zadovoljenje ulaznih zahtjeva.

Pojednostavljena blok shema informacijskog sistema u skladu s gornjom definicijom prikazana je na slici 2.2.



Slika 2.2. Pojednostavljena blok shema informacijskog sistema

Objašnjenje definicije informacijskog sistema:

Sa slike 2.2 se vidi da je ulazni element informacijskog sistema jedan ili više zahtjeva za obavljanje neke funkcije samog sistema. Npr. ulazni zahtjevi mogu biti od strane nekog korisnika: želim arhivirati podatke, želim generirati listu naših poslovnih partnera, želim poslati e-mail poruku, želim pretražiti bazu podataka, želim pronaći originalni ugovor s partnerom, itd. Pored ovih 'pozitivnih' ulaznih zahtjeva, ima i tzv. 'negativnih' ulaznih

zahtjeva, kao npr. želim ilegalno pokupiti PIN brojeve kartica, želim 'srušiti' web server, želim ukrasti listu partnera, itd. Izlazu informacijskog sistema u oba slučaja je zadovoljavanje ulaznih zahtjeva. Naravno, pozitivne (korektne ili željene) ulazne zahtjeve informacijski sistem mora maksimalno zadovoljiti i dati očekivani rezultat, ali negativne (nekorektne ili neželjene) zahtjeve mora maksimalno spriječiti i onemogućiti zadovoljenje ulaznog zahtjeva.

Značenje pojma „uređeni skup“ za informacijski sistem je u tome da svi elementi koji čine taj skup ne mogu biti bilo kako uključeni, već se između svih pojedinih elemenata zna i definira njihov međusobni odnos u smislu hijerarhije, funkcija, itd.

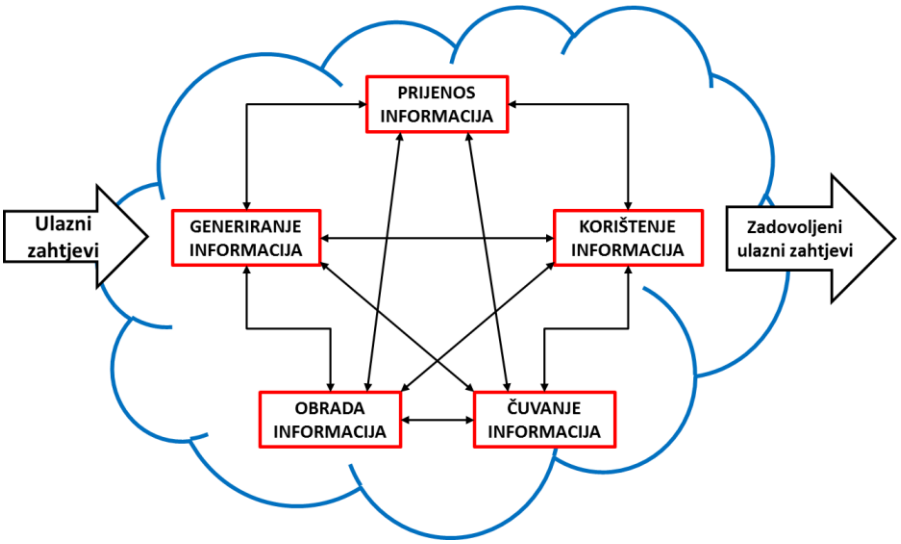
Da informacijski sistem mora biti „dokumentiran“ označava činjenicu da informacijski sistem postoji samo onda ako je u potpunosti dokumentiran, odnosno ako su za sve njegove elemente skupa dokumentacijski dokaziva i definirana funkcionalnost, sadržaj, oblik, međusobna povezanost, itd. U ovom slučaju se može reći da je entropija informacijskog sistema po svim elementima kojima se opisuje to veća što je njegova dokumentiranost manja.

Da bi u opće moglo doći do postojanja informacijskog sistema moraju postojati resursi pomoću kojih se obavlja svaki oblik funkcionalnosti informacijskog sistema. To su npr. komunikacijski sistemi, kompjuterski sistemi, osoblje u i van organizacije, energetski sistemi, mediji za pohranu i prijenos informacija, itd.

Svaki informacijski sistem mora raditi u skladu s jednim ili više pravila. Ta pravila su određena s tehnološkim ograničenjima, nacionalnom i međunarodnom legislativom, funkcionalnim pravilima organizacije u čijoj je ingerenciji informacijski sistem, a često se ne mogu zanemariti ni tradicionalna i/ili etnička, odnosno politička ograničenja vezana za funkcioniranje informacijskog sistema.

Na kraju, treba naglasiti da se kvaliteta zadovoljenja ulaznog zahtjeva mora mjeriti, ali isto tako i funkcionalnost samog informacijskog sistema i bilo kojeg njegovog segmenta. Tu se izvrsno uklapa konstatacija: „Kada ono, o čemu govorite, možete izmjeriti i brojčano izraziti, onda Vi o tome i nešto znate – ali ako ne možete izmjeriti i brojčano izraziti, onda je Vaše znanje mršavo i nezadovoljavajuće vrste!“ (Kelvin, Lord William Thomson,1824-1907).

S obzirom na funkciju informacijskog sistema on ima isključivu ulogu manipulacije s informacijama u bilo kakvom obliku. U tom kontekstu se blok shema informacijskog sistema može prikazati kao na slici 2.3.



Slika 2.3. Funkcionalna shema informacijskog sistema

Kao što je prikazano na slici 2.3. informacijski sistem može obavljati funkcionalno sve ili samo neke od funkcija vezano za manipulaciju s informacijama: generiranje, prijenos, obradu, čuvanje i korištenje informacija. U pravilu, jedan informacijski sistem se sastoji od više podsistema, a ti podsistemi onda imaju samo jednu funkcionalnu ulogu od gore navedenih. Pored toga, treba napomenuti da jedan informacijski sistem nikada nije sam, izoliran, već se nalazi u većoj ili manjoj interakciji, odnosno vezi s drugim informacijskim sistemima partnera, institucija, itd.

2.5. UPRAVLJANJE INFORMACIJSKIM SISTEMIMA

Iz područja upravljanja sistemima poznata su dva pristupa: procesni i PDCA pristup (**P**lan-**D**o –**C**heck-**A**ct). Svaki od ovih pristupa upravljanja sistemima ima svoje prednosti i nedostatke, ovisno o prirodi sistema kojim se želi upravljati.

Kada je u pitanju informacijski sistem, tada se ne može reći da li je bolji procesni ili PDCA pristup. Naime, neki podsistemi informacijskog sistema su prikladni za procesni pristup, a neki za PDCA pristup. Zbog toga će se obraditi oba pristupa.

2.5.1 PDCA pristup upravljanja sistemima

PDCA je akronim od engleskih riječi **P**lan-**D**o-**C**heck-**A**ct što bi u slobodnom prijevodu značilo Planiraj-Uradi-Provjeri-Djeluj. Često se sreće i pod nazivom Demingov krug (prema William Edwards Deming, 1900-1993). Pored ovih naziva sreće se i kao Ševartov ciklus (Shewhart cycle). Pred kraj karijere Deming je napravio modifikaciju PDCA kruga u PDSA (Plan-Do-Study-Act) kako bi bolje opisao svoje preporuke. Međutim, u praksi je ostao akronim PDCA.

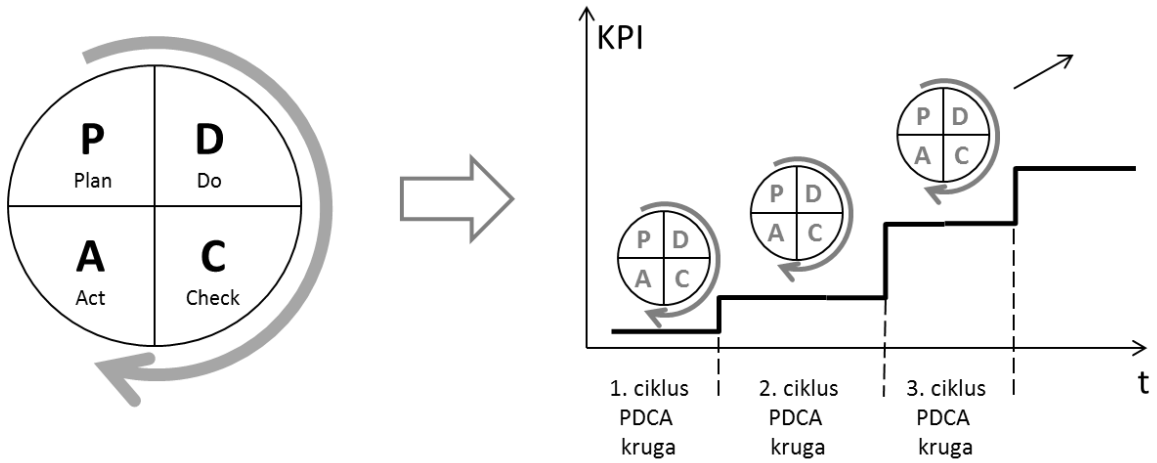
PDCA pristup upravljanja sistemima se sastoji od četiri faze prikazane u tablici 2.1.

Tablica 2.1. PDCA faze

Plan	Planiraj	U okviru ove faze potrebno je detaljno predvidjeti sve elemente i funkcije sistema, odnosno poslovnog procesa. Načine obavljanja pojedinih aktivnosti, odgovornosti, načine i metode mjerenja rada i rezultata, te očekivane rezultate. Drugim riječima do detalja projektirati sistem te njegovo funkcioniranje. Primjenjuju se obično mapiranje procesa kupac/dobavljač (odnosno svih zainteresiranih strana), dijagrami toka, Pareto analiza, oluja mozgova (Brainstorming), kao i ostali menadžerski alati.
Do	Uradi	U ovoj fazi se treba sve provesti što je planirano u okviru P faze, odnosno provesti planirane procese.
Check	Provjeri	Mjerenje svih planiranih elemenata procesa i usporedba s planiranim rezultatima iz P faze. Obično se koriste ček-liste, grafička analiza, kontrolne karte, KPI – ključni indikatori performansi (*Key Performance Indicator*)
Act	Djeluj	Analiziranje razlika mjerenih i planiranih rezultata. Određivanje gdje i zašto je došlo do odstupanja rezultata mjerenja od planiranih rezultata, te predviđanje aktivnosti kojima bi se u buduće eliminirale razlike. Uobičajeno se koristi mapiranje procesa, standardizacija procesa, kontrolirane referentne informacije, formalni treninzi za funkcioniranje procesa.

Nakon završetka A faze PDCA kruga ponovno se pokreće ciklus od P faze u kojoj se vrši redizajniranje sistema – poslovnog procesa, tako da se osigura poboljšanje funkcije u slijedećem ciklusu, odnosno spiralno se poboljšavaju performanse procesa.

Uobičajeno je da se te faze prikazuju u obliku kruga kao što je prikazano na slici 2.4.



Slika 2.4. PDCA krug i utjecaj na kvalitetu performansi sistema

Osnovni zahtjev kod upravljanja sistemom, odnosno poslovnim procesom je poboljšanje. Na slici 2.4. je prikazano da se nakon svakog ciklusa PDCA kruga poboljšavaju parametri kojima

se pokazuje neki oblik kvalitete sistema odnosno poslovnog procesa. Koliko je to poboljšanje zavisi od niza faktora, među kojima su u prvom redu spremnost uprave organizacije u investicije, osposobljenost osoblja, itd.

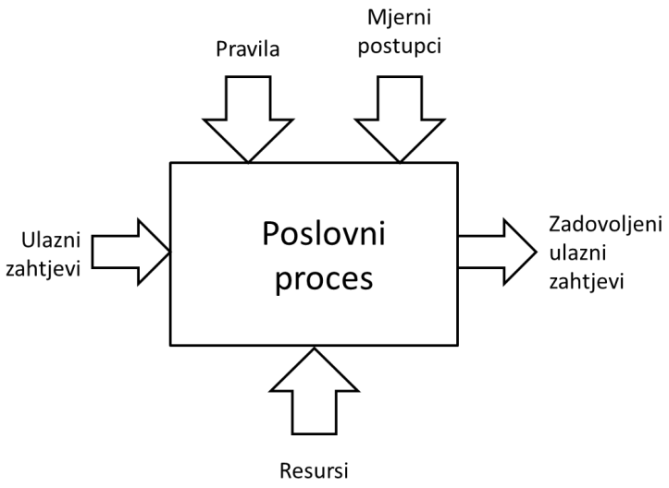
KPI (Key Performance Indicator) je zavisan od područja primjene poslovnog procesa. Tako npr. ako se govori o informacijskim sistemima to bi mogli biti efikasnost zaštite od raznih incidenata, efikasnost zadovoljavanja ulaznih zahtjeva, broj i trajanje ispada, itd.

2.5.2. Procesni pristup upravljanja sistemima

Prema ranije iznesenom, informacijski sistem se u osnovi može prikazati kao poslovni proces, odnosno bolje rečeno njegove funkcije. Naime, sastav, način uspostavljanja, održavanja i nužnost upravljanja funkcijama informacijskog sistema nedvojbeno upućuje na činjenicu da se može promatrati i kao poslovni proces. U tom slučaju upravljanje s informacijskim sistemom i njegovim funkcijama postaje relativno jednostavnije, odnosno mogu se koristiti poznati metodološki pristupi i alati iz područja teorije upravljanja procesima. Pored toga, sistemi upravljanja su obrađeni i kroz niz međunarodnih standarda. U tom smislu je najznačajnija grupa standarda za upravljanje sa sistemima ona od strane ISO (International Organization for Standardization). Takvim pristupom se postiže opće prepoznatljiv i prihvaćen način upravljanja s funkcija informacijskog sistema (ali i drugih).

Prema standardu ISO 9001 [99] preporuča se prihvaćanje procesnog pristupa, kada razvoj, primjena i poboljšavanje učinkovitosti sistema kvalitete (odnosno u ovom slučaju upravljanja informacijskom sigurnošću, nap. autora) povećavaju zadovoljstvo kupca (svih zainteresiranih strana, nap. autora) ispunjavanjem njegovih zahtjeva. Da bi organizacija koja koristi informacijski sistem radila učinkovito, mora nadzirati i upravljati brojnim uzajamno povezanim aktivnostima. Aktivnost ili niz aktivnosti gdje se upotrebljavaju resursi i kojima se upravlja kako bi se omogućila pretvorba ulaza (ulaznih zahtjeva) u izlaz (zadovoljenje ulaznih zahtjeva) mogu se smatrati procesom. Često izlaz iz jednog procesa predstavlja izravan ulaz u sljedeći proces. Primjena procesnog sustava unutar neke organizacije, zajedno s prepoznavanjem procesa i uzajamnog djelovanja tih procesa te njihovim upravljanjem kako bi se postigao željeni rezultat, može se smatrati ”procesnim pristupom”.

U tom slučaju se blok shema procesa može prikazati kao na slici 2.5.



Slika 2.5. Blok shema poslovnog procesa

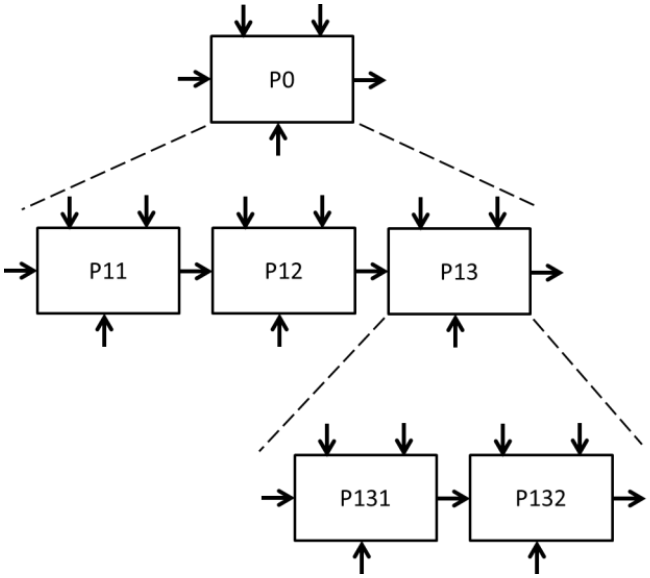
Elementi i njihovo značenje objašnjeni su ranije. Takav poslovni proces može biti npr. izrada i upravljanje sa rezervnim kopijama servera, aplikacijskih podataka, nabavka informacijske opreme, izrada aplikativnog ili sistemskog softvera, marketinške aktivnosti, osiguranje sigurnosti informacijskog sistema, itd. Kada se pogleda bilo koji od navedenih primjera može se zaključiti da za sve njih treba obaviti niz aktivnosti, često puta od strane raznih osoba, pa čak iz raznih organizacionih jedinica ili čak i organizacija, da svi oni moraju to obaviti u skladu s nekim pravilima, da se moraju znati odgovornosti za svaki segment procese, itd. Očito je da su procesi složeni od niza aktivnosti koje se obavljaju raznim resursima, a vremenski gledajući kao jedan procesni ciklus, gdje od trenutka identifikacije zahtjeva do trenutka zadovoljavanja istog može trajati od nekoliko trenutaka, do nekoliko dana, mjeseci, pa i više. Da bi se moglo upravljati bilo kojim poslovnim procesom mora se detaljno upoznati proces i identificirati sve aktivnosti, resurse, pravila, mjerne postupke, ulazne zahtjeve te oblik zadovoljenja ulaznog zahtjeva. Da bi se to moglo napraviti, provodi se tzv. postupak mapiranja poslovnog procesa.

Pod mapiranjem procesa se podrazumijevaju dvije objedinjene operacije: identifikacija ključnih procesa i uspostavljanje relacija između izdvojenih (dekomponiranih) cjelina u procesu. Konačan rezultat mapiranja je uvijek grafička interpretacija tako dekomponiranog (razloženog) procesa.

U suštini, mapiranje predstavlja crtanje «geografske karte» ili mape (engl. «map» označava geografsku kartu) bilo kojeg procesa ili grupe procesa. Mapiranje procesa počinje uvijek identifikacijom ili izdvajanjem osnovnih cjelina ili ključnih procesa (ili makroprocesa) na najvišem nivou, a onda se svaki od njih istim postupkom razrađuje na nižoj razini. Primjer mapiranja procesa po razinama prikazan je na slici 2.6.

Iz prikazanog primjera je identificiran proces P na 0-tom nivou, pa mu je oznaka P0. Daljnjom razradom tog procesa identificirano je da se on sastoji od tri podprocesa. Tako se dobila mapa na nivou 1 i sukladno tome su oznake podprocesa P11, P12 i P13. Istim postupkom se pokazalo npr. da je podproces P13 sastavljen od dva podprocesa označena sa P131 i P132. Na taj način se može ići u dubinsku analizu i mapiranje procesa do potrebnog,

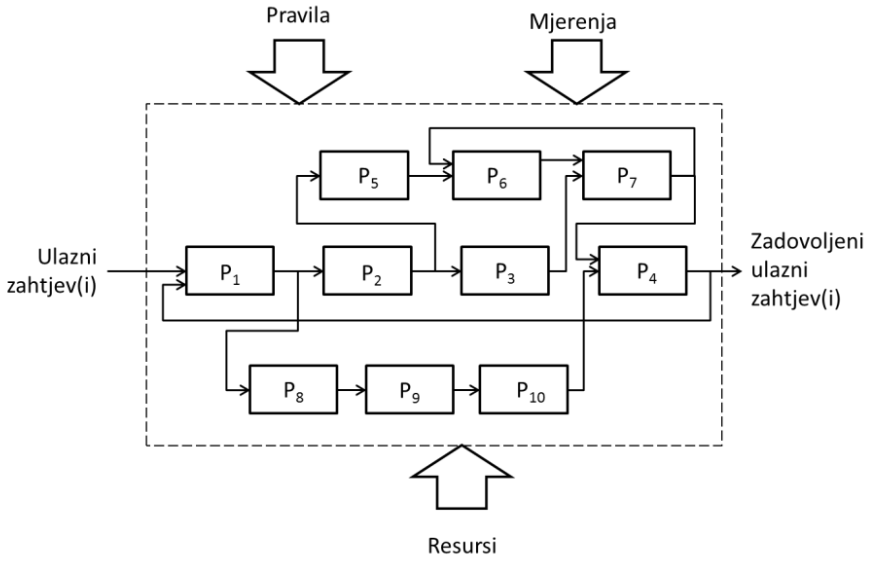
odnosno mogućeg najnižeg nivoa. Maksimalna dubina analize i mapiranja procesa je dok se ne dođe do procesne aktivnosti koja se ne može dalje razbijati.



Slika 2.6. Mapiranje poslovnih procesa po hijerarhijskim nivoima

Generalno gledajući, struktura poslovnog procesa može biti vrlo složena i u sebi sadržavati vrlo različite veze pojedinih podprocesa i procesnih aktivnosti, kao što je prikazano za ilustraciju na slici 2.7.

Na slici 2.7 nije prikazano zbog pojednostavljenja grafičkog prikaza da svaki podproces, odnosno procesna aktivnost ima resurse, pravila i mjerne postupke. To se podrazumijeva, odnosno ukupni resursi procesa su skup resursa svih podprocesa, ukupna pravila procesa su skup pravila svih podprocesa, kao i mjerni postupci procesa su skup svih mjernih postupaka podprocesa.



Slika 2.7. Blok shema primjera mapiranja složenog poslovnog procesa

Očito je sa slike 2.7. da može doći do vrlo složenih shema procesa, jer i sami procesi mogu biti vrlo složeni, pa se postavlja pitanje kako napraviti mapiranje, odnosno kojom metom mapirati neki proces. U tom smislu je razvijen niz metoda mapiranja procesa. Glavnih metoda ima oko 50, a izvedenih iz njih oko 400.

Uvid u mali uzorak glavnih metoda mapiranja (svaka od njih prvobitno razvijena isključivo za softversku branšu) koje se danas koriste u Europi može dati približan uvid u trenutno veoma šaroliko stanje na ovom području:

- **AXIAL** *akronim za*: **A**nalyse et **C**onception de **S**ystemes d'**I**nformation **A**ssistes par **L**ogiciels. Metoda je razvijena u koncernu IBM u Francuskoj i Belgiji 1974. godine,
- **DAFNE** *akronim za*: **DA**ta and **F**unction **Ne**tworking. Metoda je razvijena u Italiji 1982. godine od strane kompanije ITALSIEL i sponzorirane od Talijanskog nacionalnog savjeta za istraživanje (Italian National Research Council),
- **HOOD** *akronim za*: **H**ierarchical **O**bject **O**riented **D**esign. Metoda je razvijena u ranim 80. Godinama prošlog stoljeća po nalogu ESA (European Space Aency) od strane konzorcija tvrtki CISI INGENIERIE, CRI A/S i MATRA Espace,
- **LCM** ***akronim za:*** **L**ife **C**ycle **M**ethodology. Metoda je razvijena u SR Njemačkoj 1986. godine od strane kompanije IABG,
- **SSADM** ***akronim za:*** **S**tructured **S**ystem **A**nalysis and **D**esign **M**ethod. Metoda je razvijena u Engleskoj od strane kompanije CCTA (Central Computer and Telecommunications Agency) u ranim 80. Godinama prošlog stoljeća.

Naravno, u Europi postoji i niz metoda i alata preuzetih izvana (u prvom redu u SAD), pa tako statistika kaže da se, na primjer, u SR Njemačkoj trenutno najčešće koriste za mapiranje procesa slijedeće metode:

JSD/JSP ***akronim za:*** **J**ackson **S**ystem **D**evelopment i **J**ackson **S**ystem **P**rogramming method	31 %
HIPO *akronim za:* **H**ierarchical **I**nput and **P**roces **O**utput	26 %
SADT *akronim za:* **S**ystem **A**nalysis and **D**esign **T**echniques	20 %

Ostatak primjenjenih metoda uglavnom pripada ili **IDEF** (*akronim za:* **I**ntegration **De**finition for **F**unction Modeling), ili različitim **CASE** (*akronim za:* **C**omputer **A**dded **S**otware **E**ngineering) alatima ili objedinjenim tehnikama kao što je **UML** (*akronim za:* **U**nified **M**odelling **L**anguage). Konačno, treba obvezno i ponovo naglasiti kako se u praksi najčešće kombinira niz metoda istovremeno.

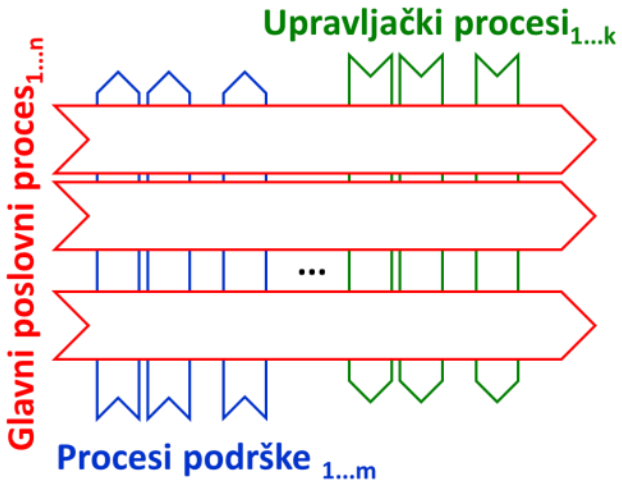
U drugim državama Europske Unije (ili pojedinim branšama, agencijama i koncernima) učestanost primjene metoda je potpuno drugačija. U Italiji je na prvom mjestu **DAFNE** (*akronim za*: **DA**ta and **F**unction **Ne**tworking), u Nizozemskoj **SDM** (*akronim za:* **S**oftware **D**evelopment **M**anagement **s**ystem), u Engleskoj **SSADM** (***akronim za:*** **S**tructured **S**ystem **A**nalysis and **D**esign **M**ethod) itd. Sve u svemu, danas još nema međunarodne opće usvojene norme u ovom području.

Kada se pogleda područje menadžmenta i sistema upravljanja koje zagovara ISO organizacija, preporuča se (nije obaveza) koristiti IDEF metodologiju koja se pokazala dovoljno jednostavna i vrlo primjenljiva za to područje. Zbog tih svojih karakteristika mogu je koristiti praktički i ljudi koji nisu školovani za projektante softverskih rješenja.

2.5.3. Veza između PDCA kruga i procesnog pristupa

Kao što je navedeno, kod upravljanja sistemima može se primijeniti PDCA pristup ili procesni pristup. Bitna razlika između ova dva pristupa je u tome što se kod PDCA pristupa ne koristi mapiranje procesa, a kod procesnog pristupa se obavezno koristi. Očito da ta dva pristupa imaju svoji prednosti i nedostatke, ovisno o situaciji u kojoj želimo primijeniti neki od njih.

U nekoj organizaciji se nalazi u pravilu tri vrste procesa: glavni procesi, procesi podrške i upravljački procesi, kao što je prikazano na slici 2.8.



Slika 2.8. Vrste poslovnih procesa u organizaciji

Glavni poslovni procesi su oni kojima se rezultat potvrđuje na tržištu, odnosno na čijem su ulazu zahtjevi kupca robe ili korisnika usluge, a na izlazu iz procesa su ili proizvod ili usluga kojom se zadovoljavaju zahtjevi ulazne strane, a organizacija to naplaćuje. To su npr. proizvodnja softvera, bilo kojih drugih proizvoda, pružanje usluge najma web servera (web hostinga), itd.

Procesi podrške su oni procesi koji postoje u organizaciji (ali i van nje u slučaju davanja izvršenja usluge vanjskim partnerima - outsourcinga) kojima se omogućava da glavni procesi obave svoju funkciju, odnosno zadovolje njihove ulazne zahtjeve. Rezultat rada tih procesa se ne naplaćuje direktno na tržištu, ali njihovi troškovi i prihodi moraju biti sadržani u dijelu efekta glavnih procesa. To su npr. procesi osiguranja električnom energijom, klima sistem, IT sektor, administracija, itd.

Upravljački procesi su oni kojima uprava organizira i provodi upravljanje s organizacijom i osigurava sve uvjete da glavni procesi i procesi podrške mogu obaviti svoje funkcije. Sve ostale značajke su iste kao i kod procesa podrške. Upravljački procesi su npr. funkcioniranje vrhovne uprave, kao i ostalih menadžera u organizaciji.

U pravilu, za glavne procese se koristi procesni pristup, za upravljačke procese u pravilu PDCA krug, a za procese podrške bilo PDCA krug bilo procesni pristup.

No i za slučaj da se koristi procesni pristup, odnosno mapiranje procesa, za takve procese se također primjenjuje PDCA krug, ali za potrebe upravljanja s tim procesom. Naime, vlasnik procesa, odnosno menadžer procesa planiranje, kontrolu izvršavanja, te analizu rezultata rada i poboljšanje obavlja na mapiranim procesima pomoću PDCA kruga. Na taj način se dolazi do zaključka, da se za sve procese koristi PDCA krug, a za neke, za koje je to pogodno vrši se i mapiranje.

3. STRUKTURA INFORMACIJSKIH SISTEMA

U kontekstu do sada iznesenog i slike 2.3. za svaki informacijski sistem se može reći da ima u sebi funkcije generiranja, prijenosa, obrade, čuvanja i korištenja informacija. Ključni objekt oko svih tih funkcija je informacija. Da bi se mogle te funkcije ostvariti mora se manipulirati s informacijama. Kako informacija nema fizički oblik da bi se s njom moglo manipulirati moraju postojati nosioci informacija pomoću kojih se obavljaju sve gore navedene funkcije.

U skladu sa standardom ISO 27001:2005 u aneksu A.7.1.1 [2] prepoznaje se šest nosioca informacije, odnosno šest vrsta imovine koje se koriste za manipulaciju s informacijama. Te vrste imovine su:

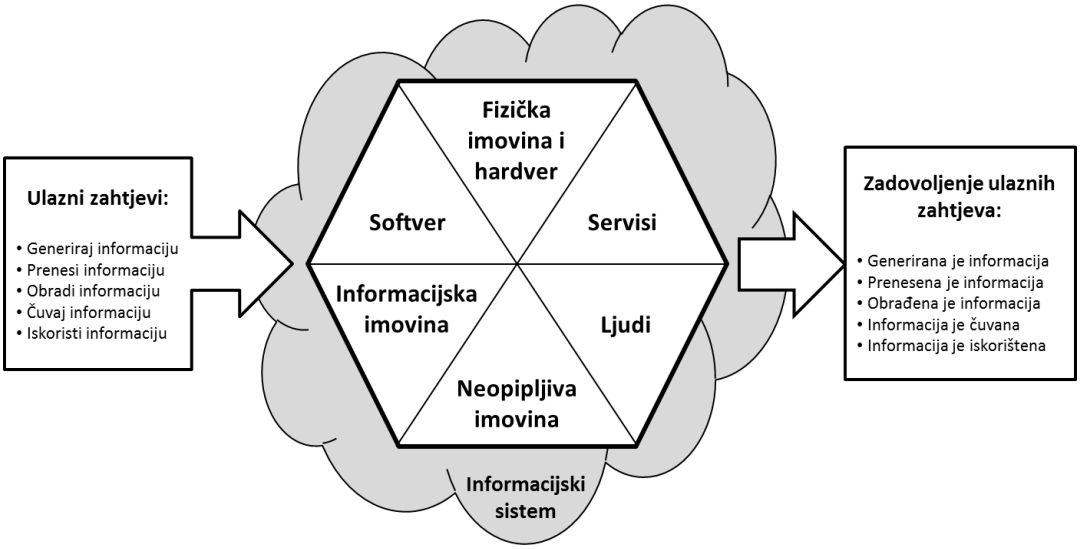
1. **Informacijska imovina** – uključuje informacije štampane ili zapisane na papir, prenošene poštom, prikazivane pomoću filmova, iznošene govornom konverzacijom, kao i informacije elektronski spremljene na serverima,web stranicama, ekstranetu, intranetu, PC kompjuterima, laptopovima, mobilnim telefonima, i PDA uređajima, na CD-romovima, flopy disketama, USB stikovima, backup trakama, ili nekim drugim magnetskim medijima, kao i informacije prenete elektronski na bilo koji način. To uključuje također i baze podataka i datoteke, ugovore i druge sporazume, sistemsku dokumentaciju, istraživačke informacije, korisničke priručnike, trening materijale, radne procedure ili procedure podrške, planove kontinuiteta poslovanja, rezultate audita, kao i arhivirane podaci.
2. **Softver** –uključuje skupove instrukcija koje govore sistemu(ima) kako da manipuliraju s informacijama, kao npr. operativni sistemi, aplikacije, razvojni alati, pomoćni programi, itd.
3. **Fizička imovina i hardver** – na kojima se manipulira sa informacijama: kompjuteri i komunikacijska oprema (npr. laptopovi, mobilni telefoni, PDA, itd.), prijenosni mediji (npr. USB stikovi, CD-ROM-ovi, magnetske trake, itd.), kao i infrastrukturna imovina, kao npr. serverske sobe, kablovi, optički kablovi, itd.
4. **Servisi** – o kojima zavise kompjuterski sistemi, kao npr. kompjuterski i komunikacijski servisi za održavanje, servisi općih funkcija, kao npr. grijanje, osvjetljenje, napajanje električnom energijom, klimatizacija, kao i npr. alarmni sistemi.
5. **Ljudi** – koji nose vrlo mnogo informacija u svojim glavama, njihove kvalifikacije, vještine i iskustvo potrebno za interakciju s organizacijskim podacima.
6. **Neopipljiva imovina** – kao što je intelektualno vlasništvo, reputacija, ugled brenda, itd.

U svjetlu ovoga se informacijski sistem može prikazati kao na slici 3.1. Interpretacija slike se daje na slijedeći način: ulazne zahtjeve svaki informacijski sistem treba da zadovolji i to angažiranjem imovine.

Zadovoljenje ulaznih zahtjeva može biti potpuno, djelomično ili u opće nema zadovoljenja ulaznih zahtjeva. Zbog jednostavnosti, ali i praktičnih razloga prihvaćanja ocjene da su ulazni zahtjevi zadovoljeni smatrat će se postojanje samo dva stanja na izlazu informacijskog

sistema: ili su potpuno zadovoljeni ulazni zahtjevi, ili nisu. Ako je djelomično ispunjeno zadovoljenje ulaznih zahtjeva, smatrat će se da zahtjevi nisu ispunjeni.

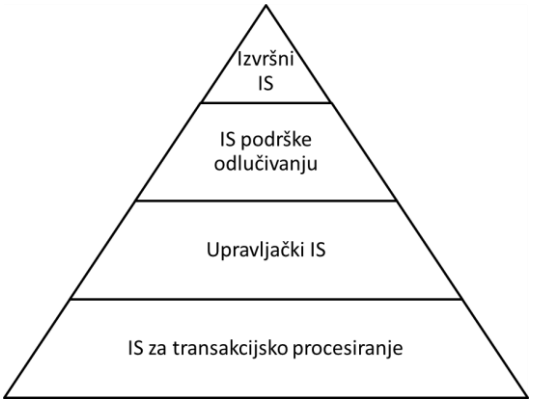
Kriterij na temelju kojega se određuje da li je informacijski sistem ispunio ulazni zahtjev ili nije, određen je ugovorom ili nekim drugim oblikom dogovora između davatelja zahtjeva (kupca – usluge i/ili proizvoda) i organizacije u čijoj je ingerenciji informacijski sistem koji treba da zadovolji taj zahtjev. U koliko su zadovoljeni svi dogovoreni elementi za obradu ulaznog zahtjeva smatra se da je zahtjev ispunjen. U protivnom nije.



Slika 3.1. Shema informacijskog sistema s obzirom na vrste imovine koje ulaze u sastav informacijskog sistema

3.1 KLASIČNI PRISTUP KLASIFIKACIJI INFORMACIJSKIH SISTEMA

Klasični način pogleda na informacijske sisteme iz 80-godina prošlog stoljeća [100] ima piramidalan oblik i koji ocrtava hijerarhijsku strukturu organizacije. Uobičajeno se ti sistemi mogu prikazati hijerarhijski kao na slici 3.2.



Slika 3.2 „Klasični“ pogled na hijerarhiju informacijskih sistema

Transakcijski sistemi obrade podataka (**TPS** - Transaction processing systems) osiguravaju automatiziranu obradu podataka za poslovanje ili transakcije, kao što su jednostavni diskretni događaji u poslovanju organizacije. Podaci o svakoj transakciji su provjereni i prihvaćeni ili odbijeni, a validirane transakcije se pohranjuju za kasniju upotrebu. Izvještaji mogu biti izrađeni odmah i daju standardnu rekapitulaciju transakcije, a transakcija može biti premještana iz procesa u proces, kako bi se obradili svi aspekti poslovanja.

Analiza i dizajn TPS znači fokusiranje organizacije na važeće postupke za obradu transakcija, bilo one procedure za ručnu ili automatsku obradu. Usredotočiti se na tekuće postupke podrazumijeva pažljivo praćenje podataka, njihov protok, obrade i izlaze. Cilj razvoja TPS je poboljšanje u obradi transakcija tako da se postigne ubrzanje, manji broj angažiranih ljudi, poboljšanje učinkovitosti i preciznosti, integracija s drugim organizacijskim informacijskim sistemima ili pružanje informacija koje prethodno nisu bile dostupne.

Upravljački informacijski sistemi (**MIS** – Mangement Information System) je sistem ili proces koji pruža učinkovite informacije potrebne za upravljanje organizacijama. Smatra se da je MIS podskup ukupnih unutarnjih kontrola i postupaka u poslovanju, koji pokrivaju primjenu ljudi, dokumenata, tehnologija, te postupci korišteni od strane menadžmenta za rješavanje svojih poslovnih problema kao što su npr. troškovi proizvodnje, usluga, itd.

Sistemi za podršku odlučivanju (**DSS** - Decision Support Systems) je informacijski sistem temeljen na IT, a koji podupire poslovanje ili aktivnosti organizacijskih odluka. DSS služi za upravljanje, poslovanje, planiranje i razine druge pomoći pri donošenju odluka, koje se mogu brzo mijenjati i nije ih lako unaprijed definirati.

DSS uključuje sisteme temeljene na znanju. Dobro dizajnirani DSS je interaktivni softver namijenjen za pomoć donositeljima odluka, prikupljanju korisnih informacije s kombinacijom sirovih podataka, dokumenata, osobnih saznanja ili poslovnih modela za identifikaciju i rješavanje problema i donošenje odluka.

Izvršni informacijski sistem (**EIS** - Executive Information System) je vrsta informacijskog sistema koji ima za cilj olakšati i podržati upravljanje i donošenje odluka za više rukovodstvo prižajući jednostavan pristup internim i/ili eksternim informacijama relevantnim za strateške ciljeve organizacije. Obično se smatra kao specijalizirani oblik sistema podrške odlučivanju (DSS),

Naglasak je da EIS omogućava grafički prikaz i jednostavnost korisničkog sučelja. EIS u pravilu nudi vrlo moćni skup izvještaja s tzv. dubinskom analizom (drill-down) mogućnostima. U posljednjih nekoliko godina, pojam EIS izgubio popularnost u korist pojma poslovne inteligencije (Business Intelligence.)

3.2 SUVREMENI PRISTUP KLASIFIKACIJI INFORMACIJSKIH SISTEMA

Kako se razvijaju nove informacijske tehnologije, tako se razvijaju i nove kategorije informacijskih sistema. Oni se više ne uklapaju na jednostavan način u izvorni model piramide informacijskih sistema. Neki primjeri takvih, suvremeno identificiranih informacijskih sistema su:

- Skladišta podataka
- Planiranje resursa
- Ekspertni sistemi
- Geografski informacijski sistemi
- Globalni informacijski sistemi
- Automatizacija ureda

Očito je da se taj pristup klasifikaciji informacijskih sistema temelji na vrstama poslova koje treba da se obave s njima i to prema djelatnostima.

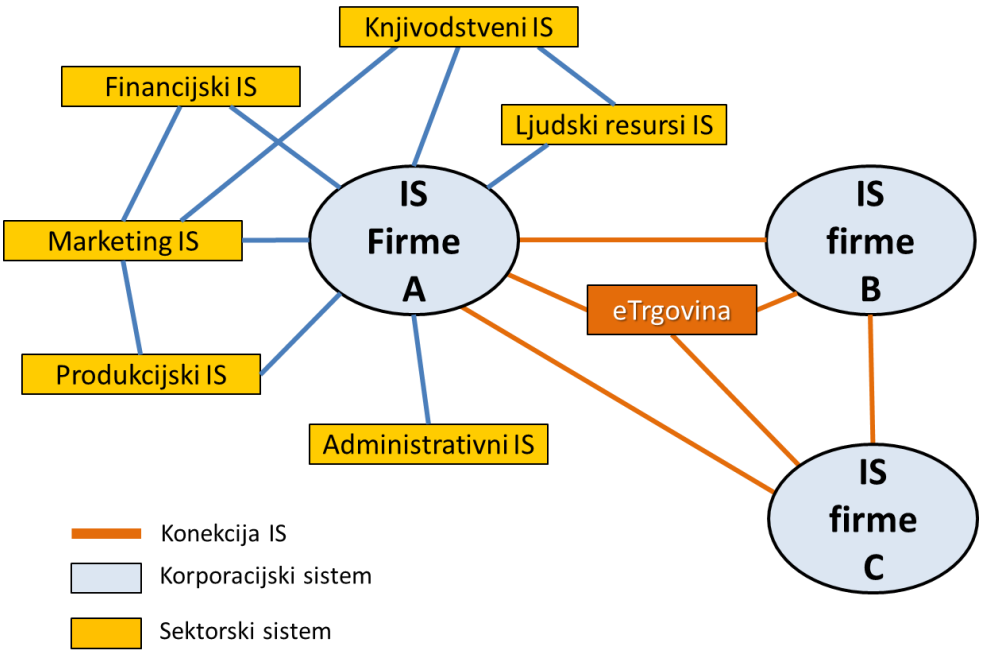
Pored toga, informacijski sistemi imaju primjenu u nizu različitih specijalističkih područja rada, kao npr.:

- Strateški informacijski sistemi
- Informacijski sistemi za upravljanje
- Informacijski sistemi za razvoj
- Informacijski sistemi sigurnosti, itd.

Tu se uočava i očekuje prema ovim klasifikacijama posebna stručnost i kvalificiranost osoblja koje treba dizajnirati, razviti, održavati i koristiti informacijske sisteme.

Široka je lepeza raznolikosti stručnosti za podršku i korištenje IS. "Radnici sa specijaliziranim tehničkim znanjima i dobrim komunikacijskim vještinama imati će najbolje izglede. Radnici s menadžerskim vještinama i razumijevanjem poslovne prakse i načela, također će imati velike mogućnosti, jer tvrtke sve više traže tu tehnologiju za ostvarenje njihovih prihoda.“ [102]

Ono što u praksi stvara dodatnu komplikaciju, jeste da unutar jedne organizacije postoji više raznih informacijskih sistema, odnosno da su oni podsistemi sveukupnog IS organizacije. Primjer je prikazan na slici 3.3.

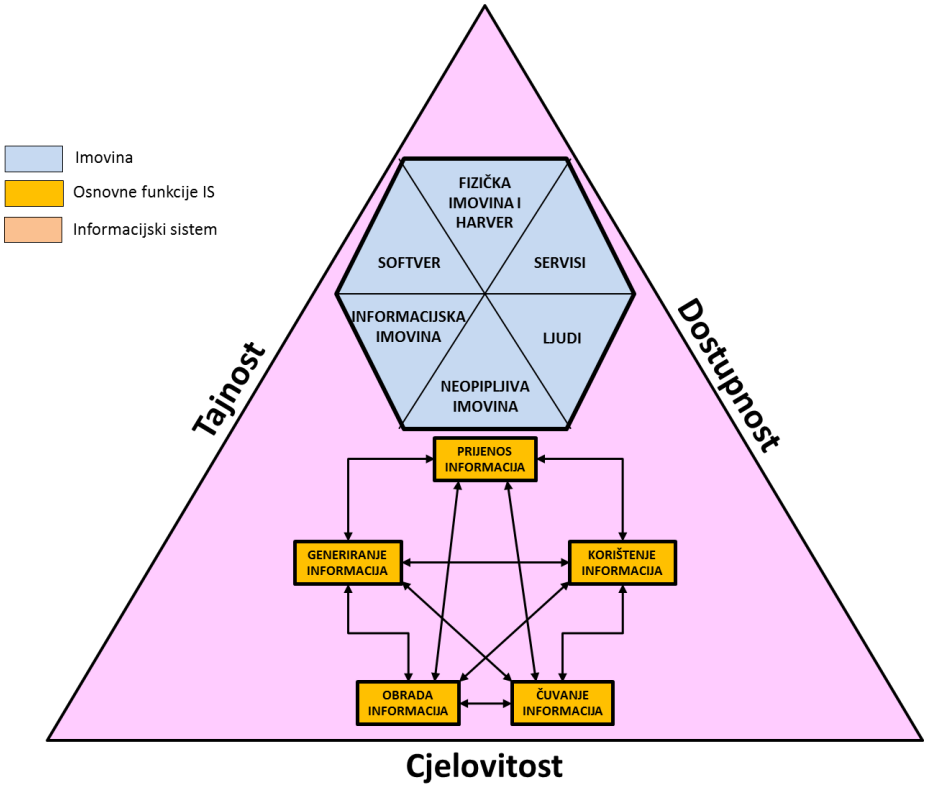


Slika 3.3. Primjer strukture složenog informacijskog sistema

Praktički svaki od ovih podsistema unutar ukupnog IS organizacije je direktno ili indirektno u interakciji s ostalim. Često puta se više IS podsistema unutar jedne organizacije koriste istim resursima – informacijskom imovinom. To samo znači da je u praksi često vrlo teško naći stroge granice između pojedinih informacijskih podsistema unutar organizacije. Naravno da se informacijski sistem neke organizacije nalazi i u sprezi s informacijskim sistemima niza drugih vanjskih organizacija, odnosno njihovih IS. Tu je situacija mnogo jednostavnija po pitanju određivanja granica između njih, jer u pravilu ne postoje zajednički resursi – informacijska imovina, osim same informacije koja se međusobno izmjenjuje.

4. SIGURNOST INFORMACIJSKIH SISTEMA

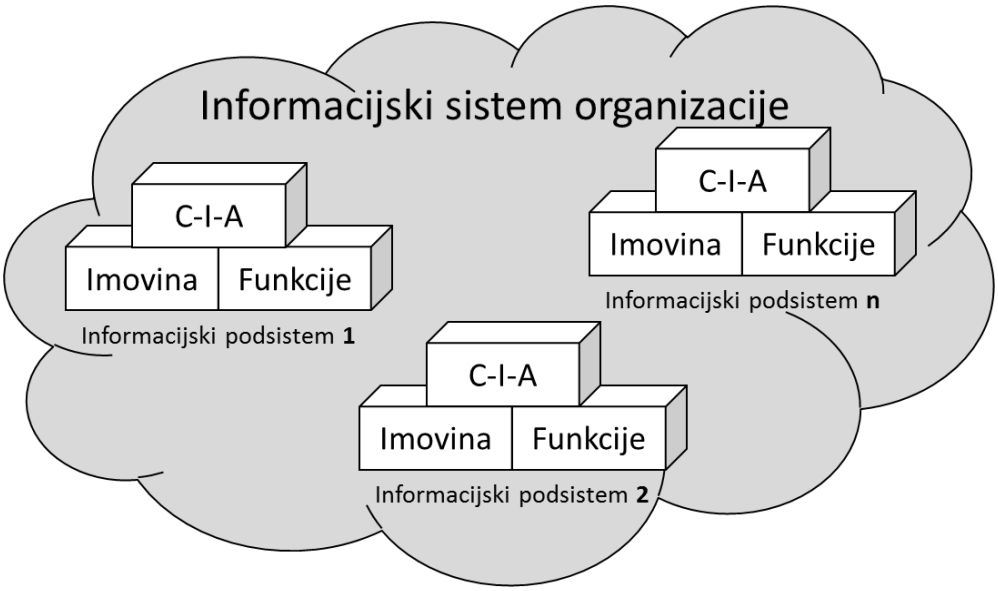
Na temelju iznesenog u poglavlju 2. i 3. može se reći da cjelokupni informacijski sistem pored funkcija koje ima prema slici 2.3. mora i osigurati u odnosu na samu informaciju njene tri značajke: tajnost, cjelovitost i dostupnost. To znači da informacijski sistem pomoću svoje imovine (fizička imovina i hardver, softver, informacije, servisi, ljudi i nematerijalna imovina) mora osigurati sve ili barem neke radne funkcije (generiranje, prijenos, obradu, čuvanje i korištenje informacija), ali obavezno konzistentnost sve tri značajke svih informacija u njemu (tajnost, cjelovitost i dostupnost). Ilustracija informacijskog sistema sa svim elementima i funkcijama prikazana je na slici 4.1.



Slika 4.1. Odnos informacijskog sistema i značajki informacija

Sve te uloge informacijskog sistema i pripadna imovina imaju isti odnos i za sve informacijske podsisteme od kojih se može sastojati cjelokupni IS organizacije.

Kao što je već prikazano, svaka organizacija se sastoji od jedne ili više organizacijskih jedinica (sektora) koje obavljaju svoje poslovne funkcije i pri tome koriste svoj informacijski sistem. Kao što su u međusobnoj interakciji organizacijski dijelovi u cilju ostvarivanja poslovnih ciljeva, tako su i njihovi informacijski sistemi u međusobnoj interakciji. Sveukupni informacijski sistem organizacije u tom slučaju predstavlja skup svih tih elemenata informacijskih sistema pojedinih organizacijskih dijelova (vidi sliku 4.2).



Slika 4.2. Informacijski sistem organizacije kao skup informacijskog podsistema

U tom slučaju na nivou organizacije, svaki informacijski sistem pojedinog organizacijskog dijela postaje informacijski podsistem informacijskog sistema organizacije.

Ako označimo da je informacijski podsistem (IPS) skup svojih elemenata imovine, svojih funkcija informacijskog podsistema, te pripadnih C-I-A, može se pokazati da je ukupni informacijski sistem definiran prema slijedećem:

$$IPS_1 = \{CIA_1, IMOVINA_1, FUNKCIJE_1\} \tag{4.1}$$

$$IPS_2 = \{CIA_2, IMOVINA_2, FUNKCIJE_2\} \tag{4.2}$$

• • •

$$IPS_n = \{CIA_n, IMOVINA_n, FUNKCIJE_n\} \tag{4.3}$$

Odnosno, ukupni informacijski sistem IS je:

$$IS = IPS_1 \bigcup IPS_2 ... \bigcup IPS_n \tag{4.4}$$

$$IS = \bigcup_{i=1}^{n} IPS_i \tag{4.5}$$

Granice između pojedinih informacijskih podsistema u pravilu su nejasne jer ista imovina se može koristi za više podsistema, kao i neke funkcije što mogu obuhvaćati više podsistema itd. Ta činjenica komplicira upravljanje sa podsistemima pa se u praksi moraju iznalaziti kompromisi da se zadovolji praktična strana upravljanja i organizacijsko-tehnološka ograničenja.

Kod jednog takvog složenog informacijskog sistema u svakom slučaju se postavlja niz pitanja vezano za njega, kako od strane vlasnika, tako i od strane korisnika, ali i od ostalih zainteresiranih strana. Svaki od ovih zainteresiranih strana ima svoje razloge, ali se u pravilu ta pitanja mogu svesti na slijedeća:

- Hoće li informacijski sistem raditi bez grešaka i prekida?
- Hoće li njegova funkcija biti u skladu s očekivanjima svih zainteresiranih strana?
- Mogu li se smanjiti troškovi njegovog održavanja?
- Može li se isti efekt funkcioniranja postići s manjim resursima?
- itd. ...

Sva ta pitanja su vezana za imovinu i funkcije informacijskog sistema. Međutim, kako je ključni element informacijskog sistema informacija, moraju se postaviti i slijedeća tri pitanja vezana za značajke informacije:

- Hoće li biti sačuvana tajnost informacije?
- Hoće li biti sačuvana cjelovitost informacije?
- Hoće li biti sačuvana dostupnost informacije?

Može se pokazati da su ova tri pitanja ključna za razmatranje nekog informacijskog sistema, posebno ako ona uključuju i ekonomsku analizu opravdanosti (Cost-Benefit Analysis).

Kada se govori o pitanjima vezanim za stalnost obavljanja funkcija informacijskog sistema problem se svodi na održavanje tehničke ispravnosti potrebnih resursa, obučenost ljudi i odgovarajuću organizaciju. Kada se analiziraju pitanja vezana za imovinu tada se problem svodi na očuvanje funkcionalnosti svake imovine koja učestvuje u informacijskom sistemu. U jednom i drugom slučaju su metode i tehnike relativno dobro poznate i kao takve se primjenjuju.

Rješavanje problema vezanih za pitanja o C-I-A informacijskog sistema još uvijek nisu u dovoljnoj mjeri poznata, a još manje primijenjena u praksi, mada se neki elementi tih rješenja koriste manje više uspješno više stotina, pa čak i tisuća godina.

Kako je problem očuvanja značajki informacija C-I-A u bilo kojem informacijskom sistemu u stvari globalan svjetski problem, niz godina se pokušava naći sistemsko rješenje, dovoljno dobro i prihvatljivo za sve zainteresirane strane. Danas je prihvaćeno u svijetu da odgovor na to pitanje u najširem smislu daje općeprihvaćeni standard ISO 27001:2005 [2], u zajednici sa serijom drugih standarda iste, ali i drugih familija. Naravno da u praksi postoje i serije drugih predloženih i manje ili šire prihvaćenih standarda (NIST u USA – National Institute of Standards and Technology – serija SP 800, BSI u Njemačkoj - Bundesamt für Sicherheit in der Informationstechnik, serija njihovih standarda 100, itd.). No svi se oni uglavnom potpuno poklapaju sa serijom standarda ISO 27001. Značajna odstupanja po tim pitanjima mogu imati specijalizirani nacionalni standardi za pojedina područja, kao npr. za vojsku, vladine službe, itd. I u tim slučajevima se može raditi paralela sa ISO 27001 i ostalim standardima iz te serije, pa se u nastavku razmatranje problema informacijske sigurnosti, odnosno očuvanja značajki informacija C-I-A može analizirati samo u kontekstu standarda ISO 27001.

4.1. INFORMACIJSKA SIGURNOST PREMA ISO 27001:2005

Formalno je standard pod punim službenim nazivom objavljen 2005 godine: ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems —Requirements. Značenje i namjena standarda je definiranje zahtjeva koje se mora ispuniti ako se želi uspostaviti sistem za upravljanje informacijskom sigurnošću (ISMS – Information Security Management System), odnosno izvršiti njegova certifikacija.

Sam standard ima svoju povijest koja započinje 1992. godine, kada je Odjel za trgovinu i industriju vlade United Kingdom (DTI – Department of Trade and Industry) publicirao dokument 'Code of Practice for Information Security Management' ('Najbolja praksa za upravljanje informacijskom sigurnošću'). Tokom 1995 godine je taj dokument izmjenjen i dopunjen, a tu novu verziju je objavio British Standards Institute (BSI) kao BS 7799. 1996 godine se počinju pojavljivati alati i podrška za standard, kao npr. COBRA. 1999. god. je objavljena prva glavna revizija BS 7799. Ona je uključivala mnoga važna proširenja. Akreditacijsku i certifikacijsku shemu objavljuje LRQA (*Lloyd's Register Quality Assurance*), a BSI postaje prvo vertifikacijsko tijelo. 2000. god. u decembru BS 7799 je ponovno objavljen, ali kao međunarodni standard pod ISO. Puni službena oznaka je bila: ISO/IEC 17799:2000. Godine 2002. objavljen je drugi dio standarda BS 7799-2. On je predstavljao specifikacije upravljanje informacijskom sigurnošću, za razliku od dobre prakse. To je bio početak procesa usklađenja sa standardima za menadžment kao što je serija ISO 9000ff. Godine 2005 je objavljen i zamijenjen ISO 7799 koji je uključivao dvije nove sekcije i uskladio se s BS 7799-2. Iste godine (2005) objavljen je ISO 27001 kao zamjena za BS 7799-2, a koji su bili potpuno jednaki. Standard ISO 27001:2005 predstavlja specifikacije za ISMS i postigao je potpuno kompatibilnost sa ISO 9001 i ISO 14001.

Za problem implementacije, održavanja i poboljšanja ISMS u organizaciji nije dovoljan samo standard ISO 27001, već se u međuvremenu pojavila serija smjernica koji su nužni, neki od njih za sve organizacije, a neki samo za specifične djelatnosti. Aktualni standardi važni za implementaciju ISMS, u trenutku pisanja ovog teksta su:

- **ISO/IEC 27000:2009** Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- **ISO/IEC 27001:2005** Information technology -- Security techniques -- Information security management systems – Requirements
- **ISO/IEC 27002:2005** Information technology -- Security techniques -- Code of practice for information security management
- **ISO/IEC 27003:2010** Information technology -- Security techniques -- Information security management system implementation guidance
- **ISO/IEC 27004:2009** Information technology -- Security techniques -- Information security management -- Measurement
- **ISO/IEC 27005:2008** Information technology -- Security techniques -- Information security risk management
- **ISO/IEC 27011:2008** Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- **ISO/IEC TR 18044:2004** Information technology. Security techniques. Information security incident management
- **BS 25999-1:2006** Business continuity management.Code of practice

- **BS 25999-2:2007** Business continuity management. Specification
- **BS 25777:2008** Information and communications technology continuity management. Code of practice
- **ISO 9001:2008** Quality management systems -- Requirements

Ta lista nije konačna i stalno se dopunjava novim standardima.

4.1.1. Namjena i struktura standarda ISO 27001:2005

Standard ISO 27001:2005 predstavlja skup zahtjeva koji se moraju ispuniti ako se želi izvršiti certifikacija sistema za upravljanje informacijskom sigurnošću.

Sama struktura standarda je uobičajena, kao i za sve druge certifikacijske ISO standarde. To znači da ima formalne dijelove: predgovor, uvod, predmet, normativne reference, nazive i definicije, zahtjeve, te anekse.

Po pitanju važnosti za primjenu u ovom standardu se naročito važni dijelovi koji se odnose na zahtjeve i aneks A.

Sam standard podržava sve principe sistema upravljanja koji su definirani u ISO seriji certifikacijskih standarda, a gdje je temeljni standard ISO 9001. Među tim principima je na prvom mjestu procesni pristup.

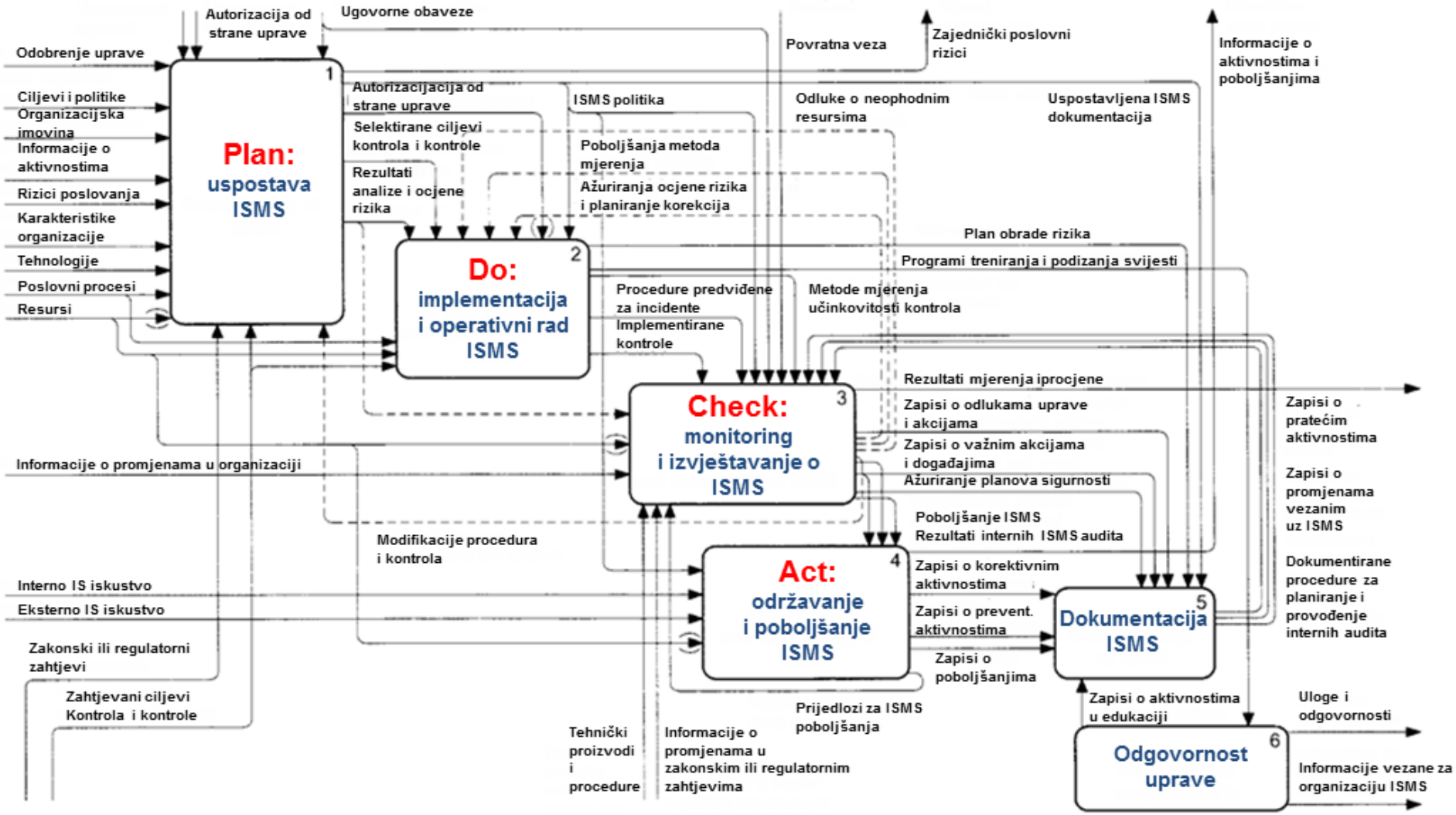
U okviru dijela vezanog za zahtjeve koji se moraju ispuniti su:

- Sistem upravljanja informacijskom sigurnošću (Poglavlje 4)
- Odgovornost uprave (Poglavlje 5)
- Interni audit (Poglavlje 6)
- Provjera ISMS-a od strane uprave (Poglavlje 7)
- Poboljšanje ISMS-a (Poglavlje 8)
- Aneks A

Svako od ovih poglavlja ima niz specifikacija – zahtjeva koji su presudni za ovakav pristup osiguranja informacijske sigurnosti.

U kontekstu standarda ISO 27001 pod pojmom informacijske sigurnosti se smatra osiguranje glavna tri aspekta informacije: tajnost, dostupnost i cjelovitost. Svi zahtjevi koji su navedeni u standardu su isključivo u funkciji ostvarenja ova tri aspekta informacijske sigurnosti.

Osnovi pristup osiguranja informacijske sigurnosti prema ISO 27001 je definiranje, implementacija i poboljšanje procesa za upravljanje informacijskom sigurnošću. Svi ključni elemente tog procesa su navedeni u standardu. Grafička interpretacija procesa je generirana prema zahtjevima standarda ISO 27001, procesnog pristupa obrađenog u poglavlju 2.5. te primjenom metodologije IDEF0.



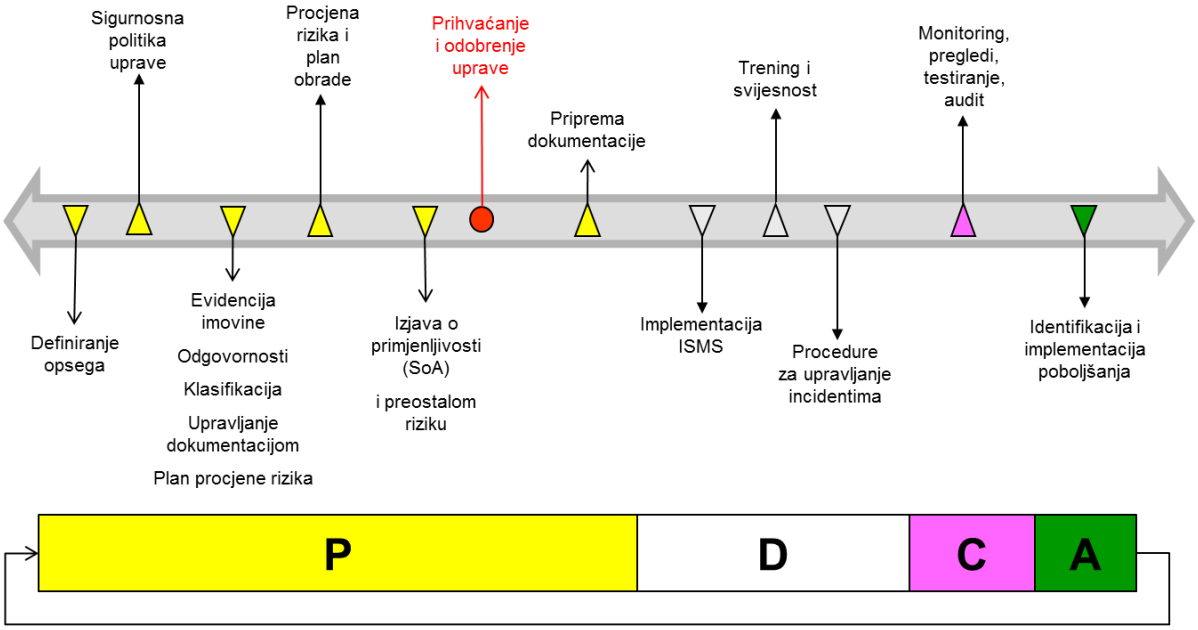
Slika 4.3. Proces za upravljanje informacijskom sigurnošću prema ISO 27001:2005

Cjelokupni proces se temelji na PDCA krugu za upravljanje, a u pojedinim fazama se prepoznaju aktivnosti prikazane u tablici 4.1.

Tablica 4.1. PDCA faze procesa za upravljanje ISMS prema ISO 27001:2005

Plan (uspostaviti ISMS)	Uspostaviti ISMS politiku, ciljeve, procese i procedure važne za upravljanje rizikom i poboljšanje informacijske sigurnosti kako bi dali rezultate u skladu s ukupnom politikom i ciljevima organizacije.
Do (implementirati i izvršavati ISMS)	Implementirati i izvršavati ISMS politiku, kontrole, procese i procedure.
Check (nadgledati i provjeravati ISMS)	Procijeniti i gdje je primjenjivo, mjeriti izvršavanje procesa u odnosu na ISMS politiku, ciljeve i praktično iskustvo te izvještavati upravu o rezultatima radi provjere.
Act (održavati i poboljšavati ISMS)	Poduzeti korektivne i preventivne akcije zasnivane na rezultatima interne ISMS prosudbe (audita) i provjere uprave ili ostalim bitnim informacijama, kako bi se postiglo stalno poboljšanje ISMS-a.

Prema standardu ISO 27001:2005 postupak implementacije ISMS se može prikazati kao na slici 4.4. gdje nakon provođenja projekta implementacije i certifikacijskog audita, projekt automatski prerasta u proces.



Slika 4.4. Projekt implementacije ISMS prema ISO 27001:2005

Kod implementacije ISMS prema ISO 27001:2005 prvi koraci su definiranje opsega, globalne politike informacijske sigurnosti, te implementacija procesa za upravljanje rizicima. Proces za upravljanje rizicima u području ISMS (vidi ISO 27005:2008) je u biti podproces cjelokupnog procesa ISMS. Da bi se provela odgovarajuća kontrola rizika, odnosno njegovo smanjenje na prihvatljivu razinu predviđen je niz kontrola (sigurnosnih mjera) koje se mogu provesti. Kategorizirani popis svih tih kontrola (sigurnosnih mjera) za smanjenje rizika, prikazan je u Aneksu A standarda ISO 27001:2005.

Važno je uočiti da se kod implementacije ISMS prema standardu ISO 27001:2005, nakon definiranja opsega i politike informacijske sigurnosti mora vršiti procjena rizika. Ta procjena rizika je temelj cjelokupne implementacije ISMS. Nakon implementacije ISMS, u cilju poboljšanja sistema opet je procjena rizika ključni korak. Iz toga se može zaključiti da je procjena rizika temeljna aktivnost za uspostavu, održavanje i poboljšanje ISMS.

Prema kategorizaciji iz Aneksa A standarda ISO 27001:2005 postoji 11 područja informacijske sigurnosti unutar kojih ima 39 kontrolnih ciljeva, te 133 kontrole, odnosno sigurnosne mjere.

Kada se u postupku obrade rizika treba odabrati kontrola za smanjenje rizika, onda se ona odabire iz Aneksa A. Ukoliko zbog eventualne specifičnosti organizacije pri implementaciji ISMS trebaju neke specijalne kontrole koje nisu predviđene u Aneksu A, standard ISO 27001:2005 dozvoljava uvođenje i vlastitih, uz uvjet da se odgovarajuće dokumentiraju.

4.1.2. Namjena i struktura standarda ISO 27002:2005

Standard ISO 27002:2005 je namijenjen da pomogne korisnicima kod implementacije kontrola – sigurnosnih protumjera. Ta se pomoć ogleda kroz predlaganje najbolje prakse i savjetovanje kako da se ta praksa primjeni, ali ne obavezuje da se drži onoga što u njemu piše. Ukoliko organizacija ima ili smatra da ima bolja rješenja od onih koja se nalaze navedena u standardu ISO 27002:2005, može ih bez ikakvog ograničenja primjenjivati.

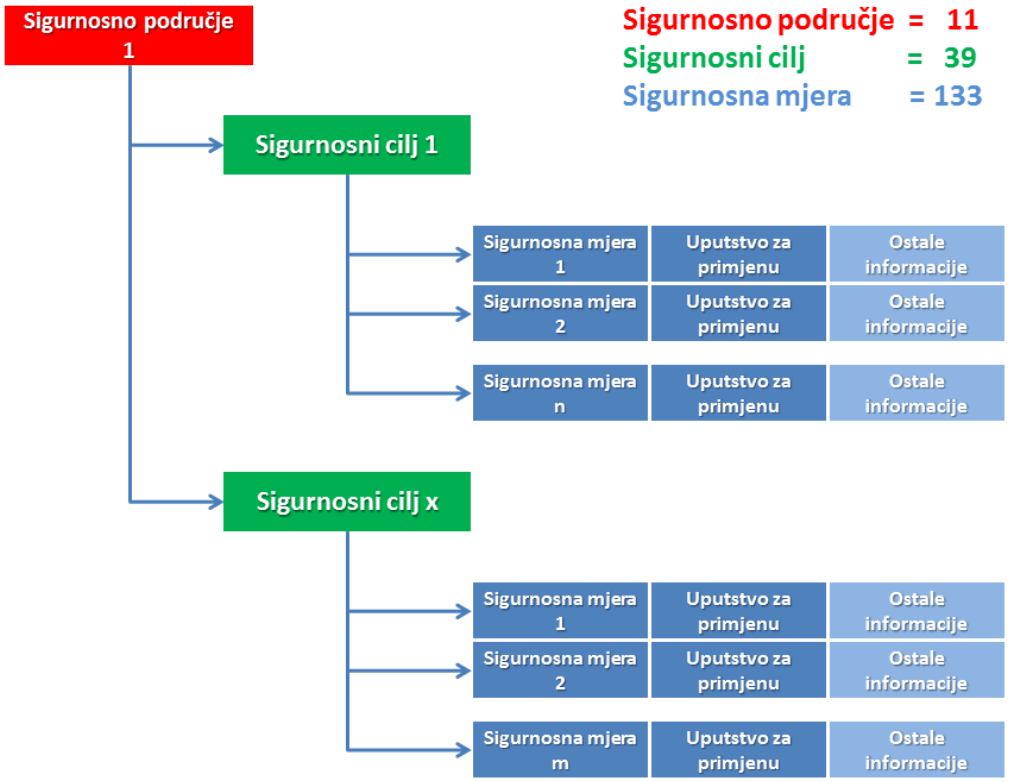
Standard ISO 27002:2005 je usko vezan za Aneks A standarda ISO 27001:2005. Naime, kao što je navedeno u točki 4.1.1., u Aneksu A se nalazi popis svih kontrola koje su prepoznate kao značajne za ISMS, a u standardu ISO 27002:2005 su sve te kontrole razrađene u smislu da se za svaku od njih predlaže kako ih realizirati u praksi.

Prema standardu ISO 27002:2005 ne može se vršiti nikakvo certificiranje, jer je on prijedlog najbolje prakse i u njemu nema nikakvih zahtjeva, već samo smjernice za implementaciju sigurnosnih mjera.

Prema Aneksu A iz ISO 27001:2005, pa prema tome i u ISO 27002:2005 definirano je 11 sigurnosnih područja. To su:

1. Politika sigurnosti (Security Policy)
2. Organizacija informacijske sigurnosti (Organization Of Information Security)
3. Upravljanje imovinom (Asset Management)
4. Sigurnost ljudskog potencijala (Human Resources Security)
5. Fizička sigurnost i sigurnost okruženja (Physical And Environmental Security)
6. Upravljanje komunikacijama i operacijama (Communications And Operations Management)
7. Kontrola pristupa (Access Control)
8. Nabava, razvoj i održavanje informacijskih sistema (Information Systems Acquisition, Development And Maintenance)
9. Upravljanje sigurnosnim incidentom (Information Security Incident Management)
10. Upravljanje kontinuitetom poslovanja (Business Continuity Management)
11. Sukladnost (Compliance)

U okviru ovih 11 sigurnosnih područja ima 39 sigurnosnih ciljeva i 133 sigurnosne mjere. Organizaciona struktura standarda prikazana je na slici 4.5.



Slika 4.5. Struktura standarda ISO 27002:2005

Kao što se može vidjeti na slici 4.5. jedno sigurnosno područje može imati jedan ili više sigurnosnih ciljeva. Svaki sigurnosni cilj ima jedna ili više sigurnosnih mjera (kontrola). Standard ISO 27002:2005 za svaku sigurnosnu mjeru navodi upute za primjenu, odnosno predlaže korisniku standarda niz elemenata o kojima bi trebalo voditi računa ako se želi implementirati ta sigurnosna mjera. U nekim slučajevima standard uz upute za implementaciju sigurnosne mjere navodi i neke dodatne informacije kojima se nastoji još bolje objasniti korisniku implementacija sigurnosne mjere.

U Aneksu A standarda ISO 27001:2005 se nalaze sva sigurnosna područja, pripadni sigurnosni ciljevi i sigurnosne mjere.

4.1.3. Namjena i struktura standarda ISO 27005:2008

Standard ISO 27005:2008 pod punim nazivom "Information technology -- Security techniques -- Information security risk management" ima status smjernice, a definira i obrađuje proces za upravljanje rizicima u području informacijske sigurnosti. Standard je u potpunosti sukladan sa ISO 31000:2009 koji opisuje proces za upravljanje rizicima, ali za sve vrste aktivnosti, poslova i sisteme upravljanja.

Standard je po svojoj strukturi ekvivalentan drugim ISO standardima iz grupe smjernica, što znači da ima slijedeće glavne dijelove: uvod, opseg, normativne reference, pojmove i definicije, strukturu međunarodnog standarda, pozadinu, pregled procesa za upravljanje rizicima informacijske sigurnosti, uspostavu konteksta, procjenu rizika informacijske sigurnosti, obrada rizika informacijske sigurnosti, prihvaćanje rizika informacijske sigurnosti, monitoring i pregled faktora rizika, monitoring upravljanja rizicima, pregledi i poboljšanje, te četiri priloga koji su informativnog karaktera.

Status 'smjernica' kojeg ima standard ISO 27005:2008 ukazuje da nije certifikacijski, već da se koristi kao prijedlog najbolje prakse kako strukturirati i definirati proces za upravljanje rizicima u području informacijske sigurnosti. Naravno da smjernice ne obavezuju nikoga da tako riješi problem upravljanja rizicima u konkretnom slučaju, ali iznalaženje vlastitog rješenja i istog procesa je daleko od normalnog, tim više što je isti, odnosno gotovo isti, proces niz godina provjeren i prihvaćen u svijetu kao optimalno rješenje, ali kroz nacionalni australsko / novozelandski standard AS/NZ 4360:2004.

Proces za upravljanje rizicima se detaljnije obrađuje u poglavlju 5.2.

4.2. IMPLEMENTACIJA ISMS

Implementacija ISMS u organizaciju se u potpunosti može provesti kroz poštivanje svih zahtjeva koje definira standard ISO 27001:2005. Međutim, zbog relativno velike složenosti problema implementacije ISMS u organizaciju objavljen je poseban standard – smjernica ISO/IEC 27003:2010 pod nazivom " Information technology -- Security techniques -- Information security management system implementation guidance". Ovaj standard ima glavnu funkciju da korisnicima, odnosno timu koji provodi implementaciju ISMS u organizaciju pruži potrebne detaljne informacije i smjernice kako implementirati sve zahtjeve iz standarda ISO 2700:2005.

Implementacija ISMS-a je važna aktivnost i općenito se treba izvršiti kao projekt u organizaciji. U okviru standarda ISO 27003:2010 prikazuju se i opisuju svi koraci implementacije ISMS s fokusom na inicijalizaciju, planiranje i definiciju projekta. Prije realizacije samog projekta implementacije potrebno je planirati provođenje slijedećih predprojektnih aktivnosti (ako već nisu provedene):

- Prezentacija ISMS i plana implementacije za upravu
- Obuka tima za implementaciju
- Prikupljanje potrebnih standarda
- Definiranje odgovornih za realizaciju projekta implementacije ISMS

Projekt implementacije ISMS realizira se kroz pet faza, i to:

a) Dobivanje odobrenja uprave za pokretanje projekta ISMS
    - Skupljanje korporacijskih poslovnih ciljeva,
    - Pregled postojećih sustavi upravljanja
    - Definiranje ciljeva, potreba sigurnosti podataka, poslovni zahtjevi za ISMS
    - Prikupljanje relevantne regulative i standarda koji se odnose na korporaciju
    - Definiranje preliminarnog opsega ISMS
    - Izrada poslovnog slučaja i plan projekta za odobrenje uprave
    - Dobivanje odobrenja uprave za predanost i pokretanje projekta za implementaciju ISMS
b) Definiranje opsega i politike ISMS-a
    - Definiranje organizacijske granice
    - Definiranje granice ICT
    - Definiranje fizičke granice
    - Finaliziranje granice za ISMS opseg
    - Definiranje politike ISMS
c) Provođenje analize organizacije
    - Definiranje zahtjeva informacijske sigurnosti kao potpora ISMS
    - Prepoznavanje imovine u definiranom opsegu ISMS
    - Izrada procjene informacijske sigurnosti
d) Provođenje procjene rizika i planiranje obrade rizika
    - Provođenje procjene rizika
    - Izbor kontrolnih ciljeva i kontrola
    - Dobivanje odobrenja uprave za implementaciju ISMS
    - Potvrda uprave za preostale rizike
    - Autorizacija uprave za implementaciju ISMS
    - Priprema dokumenta SoA
e) Projektiranje ISMS-a
    - Projektiranje organizacijske sigurnosti
    - Projektiranje ICT i fizičke sigurnosti
    - Projektiranje specifične informacijske sigurnosti u ISMS
    - Opisi za audite, praćenje i mjerenje
    - Program obuke i podizanja svijesti
    - Izrada konačnog plana projekta ISMS
    - Izvršenje konačnog plana projekta kroz realizaciju svih planiranih aktivnosti

Nakon završenih navedenih planiranih aktivnosti pristupa se konačnoj pripremi za certifikacijski audit, te provođenje internog audita.

Iz danog se vidi, ali i sa slike 4.4. da je, nakon definiranja opsega i sigurnosne politike, procjena rizika ključna faza projekta. Procjena rizika je temelj za uspostavu cijelog ISMS u organizaciju. Bez procjene rizika, odnosno bolje rečeno, bez upravljanja rizicima nemoguće je uspostaviti ISMS.

5. OSNOVI TEORIJE RIZIKA

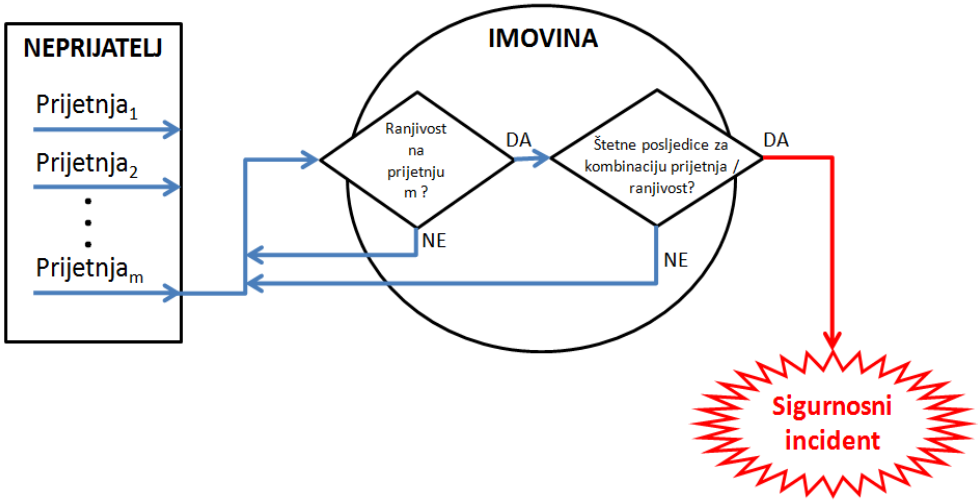
5.1 FIZIKALNI MODEL RIZIKA

Pri razmatranju principa pojave rizika na elementarnoj imovini – objektu, treba konstatirati ključnu premisu: svaka imovina ima svoju vrijednost. Ta se vrijednost može izraziti u novčanim iznosima, ali i funkcionalnošću za postizanje određenih ciljeva. U krajnjem slučaju se i funkcionalnost imovine može svesti na novčane iznose, mada je to ponekad teško, ali je moguće.

Neprijatelji sistema, odnosno pojedinci i/ili grupe koje svjesno ili nesvjesno kroz napade na imovinu imaju za cilj nanijeti štetu imovini, a time direktno sistemu, odnosno vlasniku [2] imovine. Ti napadi, koji se najčešće dešavaju iznenada u pravilu su posljedica stalnih prijetnji da će u nekom trenutku doći do napada. Šteta, kao posljedica napada može se ogledati u smanjenju vrijednosti imovine ili smanjenju funkcionalnosti imovine, odnosno onemogućavanju ili otežavanju postizanja planiranih ciljeva koje treba ostvariti imovina kroz svoju funkciju. U konačnici i taj aspekt se svodi na štetne financijske efekte.

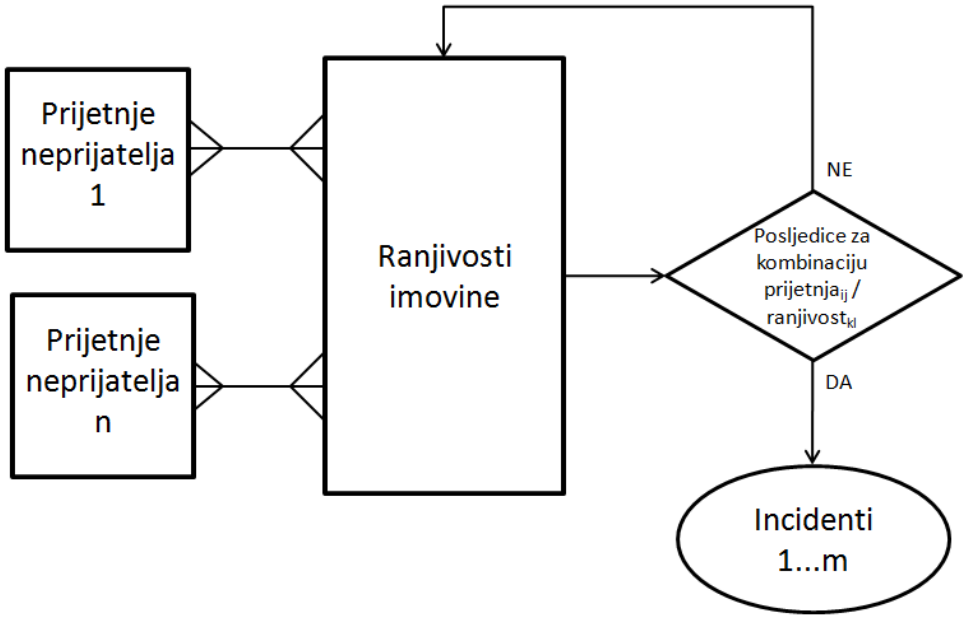
Teoretski promatrajući, napadi mogu biti pozitivnog i negativnog efekta. Pod pozitivnim efektima napada na imovinu se smatra povećanje vrijednosti imovine ili poboljšanje njene funkcionalnosti. S druge strane, negativni utjecaji napada dovode do štetnih efekata, odnosno do smanjenja vrijednosti ili funkcionalnosti imovine. Za analizu funkcioniranja imovine uvijek je bitan negativan efekt napada. Zbog toga se iz razmatranja u ovom radu isključuju pozitivni efekti napada pa se pažnja usmjerava isključivo na negativne efekte.

Pored vrijednosti imovine, kao jedne od osnovnih značajki, uvijek postoji s aspekta rizika, i tzv. ranjivost objekta na napade. Ukoliko je imovina ranjiva na jednu ili više vrsta napada, može doći do štete na njoj ukoliko je taj napad iskoristio ranjivost i izazvao posljedice. U tom slučaju govorimo o realizaciji rizika, odnosno pojavi sigurnosnog incidenta, a nastaje samo onda ako prijetnja iskoristi ranjivost sistema (imovine) i izazove štetne posljedice. Pojednostavljeno: ako nema prijetnje, i/ili nema ranjivosti i/ili nema posljedica, nema ni sigurnosnog incidenta. Ilustracija pojave rizika je prikazana na slici 5.1.



Slika 5.1. Fizikalni model rizika

Praktički gledajući, ilustracija fizičkog modela rizika prikazanog na slici 5.1 je pojednostavljena jer u pravilu postoji više neprijatelja od kojih svaki može imati niz svojih specifičnih, ali i istih ili sličnih prijetnji kao i ostali neprijatelji. S druge strane, imovina ima veći broj ranjivosti, od koji jedna ranjivost može biti zajednička za više prijetnji, odnosno jedna prijetnja može imati efekt na više ranjivosti. U kontekstu relacijskog modela može se fizikalni model rizika prikazati kao na slici 5.2:

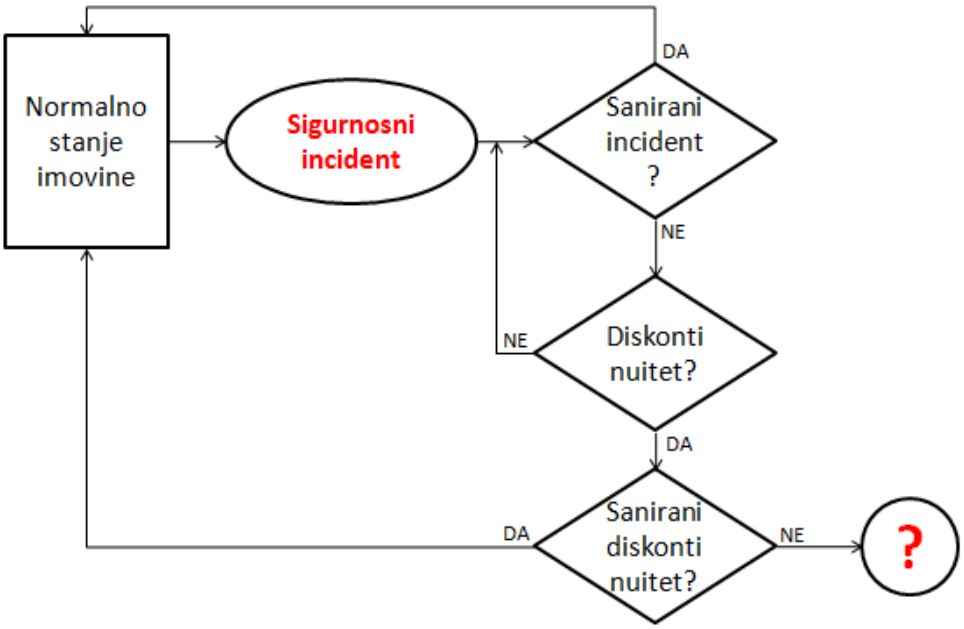


Slika 5.2. Relacijski prikaz fizikalnog modela rizika

Sa slike 5.2. se može vidjeti kompleksnost fizikalnog modela rizika koji proističe iz višedimenzionalnosti svih parametara koji učestvuju u eventualnoj realizaciji rizika. Pored ove višedimenzionalnosti modela rizika koja se ogleda kroz količinski broj realizacije incidenata, svaki od ovih elemenata (prijetnja, ranjivost i posljedica) u pravilu ima i svoju stohastičku prirodu pojavljivanja. To u konačnici daje vrlo kompliciranu sliku pojave rizika

na nekoj imovini. Zbog toga se kod analize rizika nastoji naći pojednostavljeni model koji bi bio s jedne strane dovoljno jednostavan za primjenu, a s druge strane dovoljno precizan za prihvatljivost sveukupne procjene rizika.

Ako se dogodio incident, vlasnik imovine mora osigurati sanaciju štete [2,6,7], odnosno vratiti imovinu u stanje prije pojave incidenta ili osigurati novu imovinu ako je posljedica destruktivna. Ako se ta imovina nalazi funkcionalno uključena u jedan ili više poslovnih procesa, a ne osigura se povrat stanja imovine kao što je bio prije incidenta može doći do pojave prekida poslovnog procesa. Taj događaj može dalje dovesti do novih ozbiljnih šteta, ponekad sa nesagledivim ukupnim posljedicama. Primjer događanja nakon pojave incidenta prikazan je na slici 5.3. Ako se ne može sanirati diskontinuitet poslovnog procesa tada su mogućnosti i tok događaja obično nepoznati. Moguće je čak da dođe do potpune propasti organizacije, ili isključivanja poslovnog procesa iz organizacije, eventualno uvođenje novog poslovnog procesa, promjena djelatnosti, itd.



Slika 5.3. Događanja nakon sigurnosnog incidenta

Za daljnje razmatranje fizikalnog modela rizika uvode se slijedeće pretpostavke koje imaju za cilj da područje analize modela drže u opsegu realnosti:

Rizik se kreće u granicama 0 – MaxIznos. (MaxIznos rizika zavisi od unaprijed usvojenih granica vrijednosti, od strane vrhovne uprave informacijskog sistema kroz njihove politike i procedure). Ako se izvrši normiranje rizika, tada je MaxIznos = 1.

Rizik koji je jednak 0 ne razmatra se jer on predstavlja nemoguć događaj (nema nesigurnosti)

Rizik koji je jednak MaxIznos ne razmatra se jer je on sigurni događaj (nema nesigurnosti)

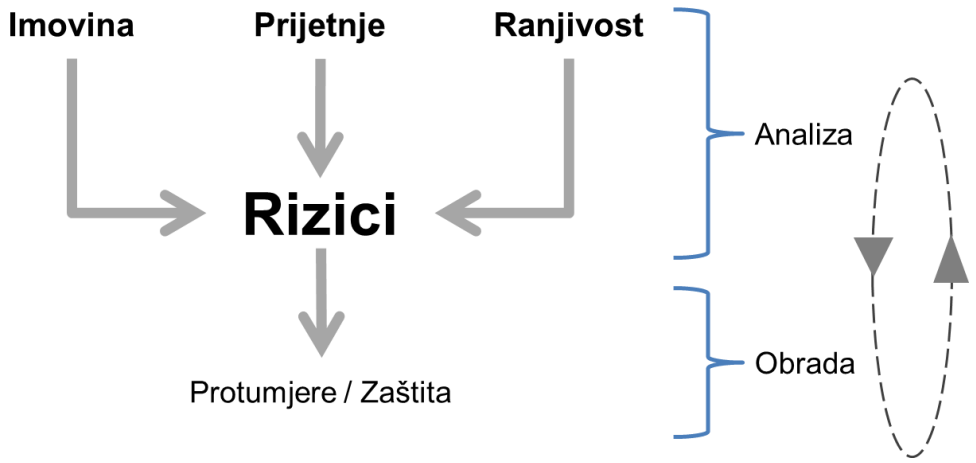
Svaki rizik nema isti značaj za vlasnika imovine (organizaciju). Mali nivoi rizika se mogu zanemariti, dok se za velike rizike (visoko vjerojatne događaje kombinacija prijetnja / ranjivost sa značajnim posljedicama) mora voditi posebna briga.

Realizacija jednog rizika može izazvati pojavu jednog ili više novih rizika.

Svaki realizirani rizik koji izaziva incidente može imati tendenciju da preraste u diskontinuitet poslovanja (pod diskontinuitetom poslovanja se smatra prekid funkcije jednog ili više glavnih poslovnih procesa).

Za sve rizike koji su od posebnog značaja, odnosno neprihvatljivi s obzirom na posljedice i vjerojatnost pojave nužno je provesti obradu rizika.

Već je rečeno da se elementi koji određuju veličinu rizika s vremenom mijenjaju, što znači da je ukupno ponašanje rizika u okviru informacijskog sistema dinamička pojava pa se nužno govori o potrebi stalnog praćenja stanja rizika i nastojanja da oni budu pod kontrolom, odnosno u prihvatljivim granicama. Taj proces kontrole stanja rizika i održavanja u prihvatljivim granicama naziva se proces upravljanja rizicima. O samom procesu za upravljanje rizicima u okviru jednog informacijskog sistema bit će kasnije riječi. Zbog jednostavnosti, na slici 5.4 je prikazana pojednostavljena verzija procesa upravljanja rizicima s ključnim elementima i dvije faze: analiza i obrada rizika.



Slika 5.4. Upravljanje rizicima (pojednostavljena shema procesa)

Kao što je slučaj sa svakim procesom i ovaj se neprestano ponavlja s težnjom unapređenja, odnosno poboljšanja, što se u slučaju upravljanja rizicima ogleda kroz smanjivanje i stabilizaciju sveukupnih rizika informacijskog sistema.

5.1.1 Prijetnje

U skladu s definicijom iz pod prijetnjama (Threat) se smatra svaki potencijalni uzrok neželjenog incidenta, koji može dovesti do posljedica (štete) na informacijskom sistemu, odnosno organizaciji.

Prema mjestu pojave u odnosu na informacijski sistem prijetnje se mogu podijeliti na unutarnje i vanjske.

Pod unutarnjim prijetnjama se smatraju sve one koje uzrokuju ljudi iz opsega informacijskog sistema, organizacija i primijenjena tehnologija, pravila i procedure rada, itd. Unutarnje prijetnje su one koje se mogu u velikoj mjeri smanjiti jer metodološki gledajući ključni razlog njihovog postojanja je u lošem menadžmentu i organizaciji informacijskog sistema.

Vanjske prijetnje se mogu podijeliti prema tipovima izvora na:

- antropogene,
- tehničko-tehnološke,
- biološko-kemijske i
- prirodne sile.

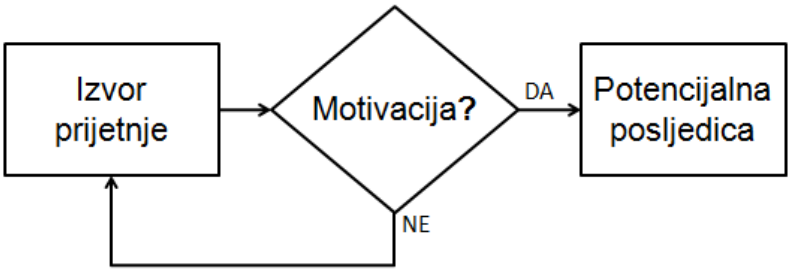
Za sve vanjske prijetnje je zajedničko da njihovi izvori nisu uključeni u informacijski sistem. Preventivno djelovanje na te prijetnje je relativno teško i malo efikasno. Kurativnim djelovanjem na neke od tih prijetnji mogu se postići određeni efekti za buduće potencijalne incidente, ali postojeći incidenti su se već dogodili.

U odnosu na sve vrste prijetnji, posebna pažnja se mora posvetiti, kada je u pitanju informacijski sistem, onima koje su posljedica aktivnosti i/ili neaktivnosti ljudi, odnosno njihovim djelovanjem i/ili nedjelovanjem. Izvori takvih prijetnji su npr. hakeri, krakeri, kompjuterski kriminal, teroristi, industrijska špijunaža, zaposlenici – članovi informacijskog sistema (zbog slabe treniranosti, nezadovoljstva, zlonamjerni, nemarni, nepošteni, odnosno zbog otkaza).

Sve prijetnje imaju u većoj ili manjoj mjeri stohastički karakter. To se ogleda u tome da nije moguće sa potpunom sigurnošću znati kada će se i kojom ozbiljnošću pojaviti neka prijetnja, te koliko će dugo trajati. Procjena vjerojatnosti pojave neke prijetnje vezana je za prirodu nastanka s obzirom na izvor. U tom smislu se razlikuju slučajne i namjerne prijetnje.

Kolika je vjerojatnost pojave slučajnih prijetnji može se procijeniti na temelju statistike i iskustva. Vjerojatnost ovih prijetnji također se može dovesti u vezu s blizinom organizacije izvorima opasnosti, kao što su glavne prometnice ili željezničke pruge, tvornice koje rade s opasnim materijalima kao što su kemijski materijali ili nafta. Geografski položaj organizacije će također utjecati na vjerojatnost ekstremnih vremenskih uvjeta. Vjerojatnost ljudske greške i neispravnost opreme su jedne od najčešćih slučajnih prijetnji.

Za razliku od njih, namjerne prijetnje u velikoj mjeri zavise od motivacije, znanja, mogućnosti i resursa koji su dostupni potencijalnim napadačima. Pri takvoj analizi jako je važno uspostaviti i prepoznati vezu između izvora prijetnji, motivacije i potencijalnih posljedica koje takve prijetnje iz tih pojedinih izvora mogu proizvesti, kao što je prikazano na slici 5.5.



Slika 5.5. Analiza namjernih prijetnji vezanih za ljudsko djelovanje ili nedjelovanje

Tako npr. ako su u pitanju hakeri ili krakeri glavni motivi su im u pravilu izazov, ego, pobuna, status, novac, itd., a posljedice su obično hakiranje, socijalni inženjering, sistem upada, provala, neovlašteni pristup sistemu, itd. Veći broj primjera za takvu analizu se može naći u [6].

Neki od tipičnih prijetnji za informacijske sisteme prikazani su u prilogu 11.3.

5.1.2 Ranjivosti

Ranjivost se definira kao slabost objekta koju može iskoristiti jedna ili više prijetnji te na taj način izazvati štetne posljedice. Sama po sebi, ranjivost ne nanosi štetu. To je samo stanje ili niz stanja koje mogu prijetnji dozvoliti uzrokovanje štete na imovini ili poslovima koje ta imovina obavlja.

Jedna imovina (objekt procjene rizika) može imati niz ranjivosti. Pri tome ne gleda se ranjivost sama za sebe, već kao slabost u odnosu na neku prijetnju. Drugim riječima, ako se ne govori o konkretnim prijetnjama, nema smisla govoriti ni o ranjivostima. Svaka ranjivost se treba povezivati s jednom ili više prijetnji, ili obrnuto, jedna prijetnja s jednom ili više ranjivosti.

Kada se govori o informacijskim sistemima, ranjivosti se na objektu imovini ogledaju u:

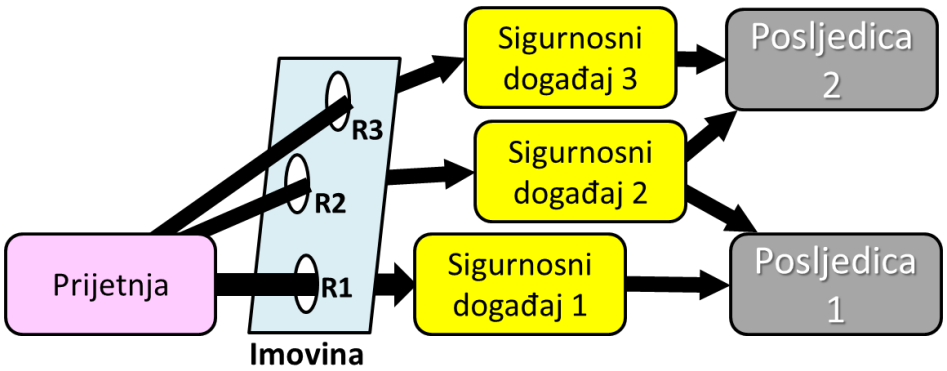
- Neadekvatnom fizičkom okruženju;
- Propustima u kadrovskim, upravnim i administrativnim postupcima i kontrolama (sigurnosnim mjerama);
- Propustima u poslovnim postupcima i uslugama koje pružaju;
- Greškama u hardveru, softveru ili komunikacijskim uređajima i opremi.
- Greškama u načinu upotrebe hardvera, softvera ili komunikacijskim uređajima i opremi.

Općenito govoreći, za ranjivost informacijskog sistema ili bilo kojeg njegovog dijela odgovornost snosi uprava organizacije kojoj pripada taj informacijski sistem. Razlog za to je u činjenici da je samo ona u stanju da pokrene, provodi i održava kontrolu niskog nivoa bilo kojeg oblika ranjivosti u organizaciji kroz svoje stručne službe i/ili pomoć vanjskih partnera.

U koliko postoji neprihvatljiva ranjivost informacijskog sistema na prijetnje to ukazuje da nisu provedene odgovarajuće kontrole (sigurnosne mjere) ili se ne provode kako je planirano.

U tom kontekstu, najefikasnija obrana od posljedica realizacije rizika je osiguranje niskog nivoa ranjivosti. Ranjivost je u biti pod kontrolom organizacije.

Na slici 5.6 prikazana je ilustracija slučaja kada je jedna prijetnja iskoristila tri ranjivosti (R1, R2 i R3) koje ima neka imovina, te time izazvala tri sigurnosna događaja, odnosno incidenta, ali za prikazanu situaciju postoje samo dvije posljedice.



Slika 5.6. Primjer iskorištenja ranjivosti od strane jedne prijetnje

Sa slike se može vidjeti da bi se eliminacijom ranjivosti onemogućila ili smanjila vjerojatnost pojave sigurnosnih događaja, odnosno posljedica.

Primjer liste dijela ranjivosti informacijskih sistema prikazana je u prilogu 11.4. Može se vidjeti da za svaku navedenu ranjivost direktnu odgovornost snosi organizacija kojoj pripada informacijski sistem.

Već je ranije pokazano da informacijski sistem ima više segmenata u kojima se mogu pojaviti razne ranjivosti koje bi onda trebalo tretirati na odgovarajući način. Neki od tih segmenata su npr: hardver, softver, mreža, osoblje, lokacija, organizacija itd. Pri analizi ranjivosti tih pojedinih segmenata informacijskog sistema nužno je uzeti u obzir i moguće prijetnje i posljedice koje se u tim slučajevima mogu pojaviti. U prilogu 11.5. je prikazan primjer kao ilustracija veze između dijela ranjivosti i dijela prijetnji koje mogu izazvati posljedice u nekom informacijskom sistemu. Priložena tablica nije konačna i u konkretnim slučajevima se nadopunjava s drugim realnim kombinacijama ranjivost – prijetnja, kao i drugim segmentima informacijskog sistema.

5.1.3 Posljedice

Posljedice su u biti šteta koja nastaje zbog realizacije rizika. To drugim riječima znači da u slučaju realizacije rizika dolazi do pojave posljedice, a organizacija mora uložiti određena resurse za sanaciju štete. Ti resursi uvijek imaju svoju interpretaciju u financijskim iznosima. Ponekad se pojavljuju teškoće izražavanja posljedice u financijskoj protuvrijednosti, ali to samo govori o nedovoljnom poznavanju problema posljedice od strane korisnika.

Moguće posljedice koje identificira organizacija mogu biti u raznim područjima, kao npr. na okoliš, profit, image, funkciju i/ili ciljeve objekta, partnere, itd. S obzirom na područje interesa i aspekta s kojeg se promatraju rizici, organizacija sama odabire koje će posljedice analizirati i u odnosu na te posljedice vršiti procjene.

Kada se govori o informacijskoj sigurnosti, tada se posljedice promatraju u odnosu na ostvarivanje sigurnosnih ciljeva informacijskih sistema, odnosno na osiguranje aspekata informacijske sigurnosti. Kako je već rečeno informacija ima tri aspekta tajnost, cjelovitost i dostupnost (C-I-A). U tom kontekstu se posljedice za informacijske sisteme definiraju kao:

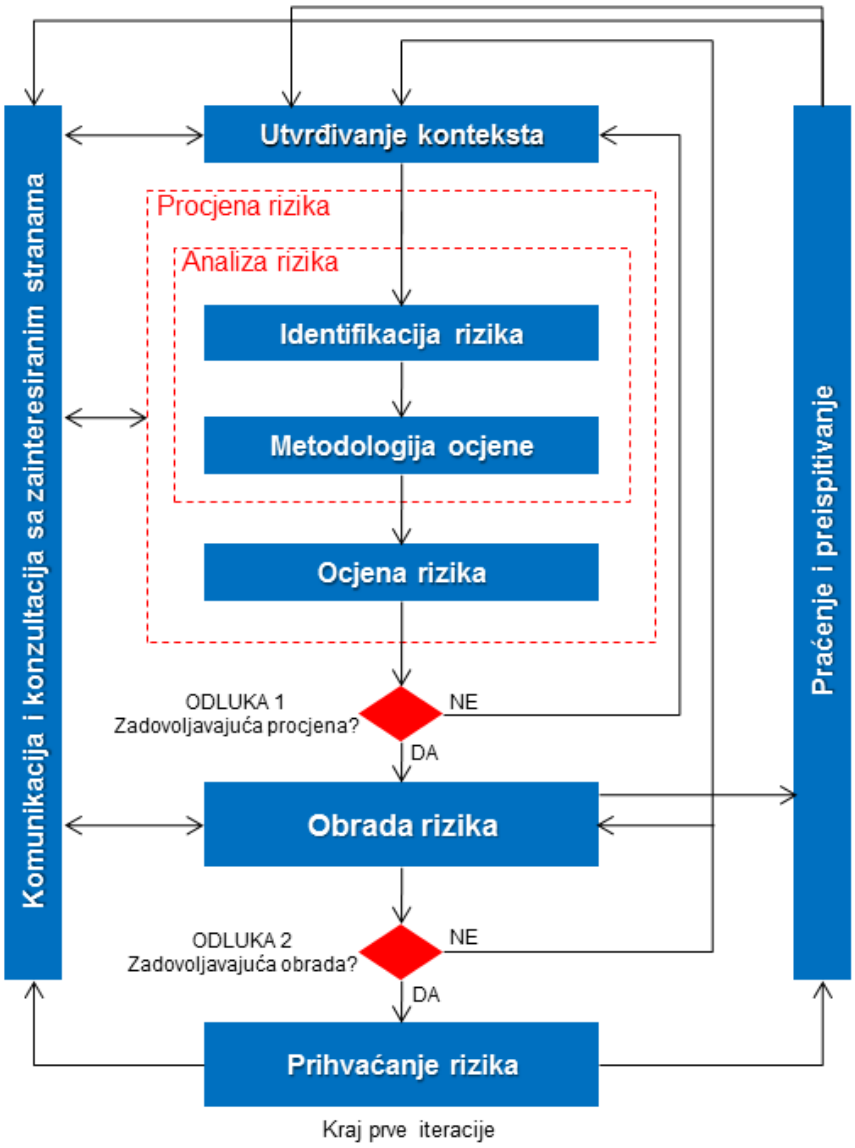
a) Gubitak tajnosti
b) Gubitak cjelovitosti, i
c) Gubitak dostupnosti.

Naravno da pored ovih posljedica koje se obavezno mora uzimati u obzir prema ISO 27001:2005, organizacije može uvesti i svoje dodatne posljedice kada analizira sigurnost informacija. Npr. kako se realizacija rizika u području informacijske sigurnosti reflektira na profit, ugled itd. No, takve dodatne posljedice na obavezne tri (gubitak tajnosti, gubitak cjelovitosti i gubitak dostupnosti) može znatno usložnjavati procjenu i obradu rizika, a uvijek postoji pitanje, koliki je značaj i korist praćenja tih dodatnih posljedica za organizaciju.

Ako se promatraju posljedice uvjetovane narušavanjem aspekata informacije (C-I-A) onda se one također vrednuju kroz financijske iznose. To vrednovanje ima smisao da govori koliko je potrebno financijskih sredstava uložiti u povrat jednog ili više aspekata informacije (C-I-A), pa da se anuliraju njihovi gubici.

5.2 PROCES UPRAVLJANJA RIZICIMA

Kao što je već rečeno, standard ISO 27005:2008 definira proces za upravljanje rizicima u području informacijske sigurnosti. Blok shema procesa za upravljanje rizicima prema ISO 27005:2008 prikazana je na slici 5.7.



Slika 5.7. Proces za upravljanje rizicima prema ISO 27005:2008

Naravno,kako se tu radi o procesu, upravljanje procesom se ostvaruje pomoću PDCA kruga. Raspodjela elemenata sa slike 5.7. po PDCA fazama je prikaza u tablici 5.1.

Tablica 5.1. PDCA faze procesa za upravljanje rizicima informacijske sigurnosti

Plan	Utvrđivanje konteksta Procjena rizika Razvijanje plana obrade rizika Prihvaćanje rizika
Do	Provedba plana obrade rizika
Check	Trajno praćenje i pregledavanje rizika
Act	Održavanje i poboljšanje procesa upravljanja rizicima za IS

Aktivnosti i značenja pojedinih blokova procesa za upravljanje rizicima sa slike 5.7. su kako slijedi:

Utvrđivanje konteksta

Predstavlja prvi korak u procesu za upravljanje informacijskim rizicima. Ulazni podaci za taj korak su sve informacije koje se odnose na informacijsku sigurnost. U okviru utvrđivanja konteksta se uključuju osnovni kriteriji potrebni za uspostavu upravljanja rizikom sigurnosti informacija, definiranje opsega i granica, te uvođenje odgovarajuće organizacije operativnih informacija za upravljanje sigurnošću informacija. Izlazni podaci iz modula su specifikacije (dokumenti) vezane za kriterije, opseg i granice, te definicija organizacije procesa upravljanja informacijskom sigurnošću.

Identifikacija rizika

Modul za identifikaciju rizika na svom ulazu treba sve izlaze iz prethodnog modula – utvrđivanje konteksta. Namjena modula za identifikaciju rizika je da se identificiraju svi rizici, kvantificiraju ili kvalitativno opišu, te izvrši određivanje prioriteta rizika u odnosu na kriterije i ciljeve. Izlaz iz modula su procjene rizika po prioritetima u odnosu na kriterije evaulacije. Ključni koraci u identifikaciji rizika su:

a) Analiza potencijalnih incidenata, odnosno, analiza što bi se sve moglo dogoditi da dođe do gubitaka, te dobivanje početnog uvida gdje i zašto se može pojaviti taj gubitak – posljedica.
b) Identifikacija informacijske imovine. Slijedeći korak je identifikacija informacijske imovine u opsegu i granicama informacijskog sistema. Pri tome se evidentiraju i vlasnici imovine, lokacija i funkcija imovine.
c) Identifikacija prijetnji. Tu se analizom ulaznih podataka (informacije o prijetnjama na temelju incidenata, vlasnika imovine, korisnika i drugih izvora, uključujući i vanjske kataloge prijetnji) stvara uvid u izvore i koje prijetnje realno postoje.
d) Identifikacija postojećih kontrola - sigurnosnih mjera. Treba se napraviti analiza već uvedenih i/ili planiranih kontrola za informacijski sistem.
e) Identifikacija ranjivosti. Treba se napraviti jedinstveni popis poznatih prijetnji te postojećih kontrola i ranjivosti koje imaju cjelokupna informacijska imovina u definiranom opsegu.
f) Identifikacija posljedica. U okviru ovog procesnog koraka treba se izvršiti prepoznavanje gubitaka povjerljivosti, cjelovitosti i dostupnosti za slučajeve realizacije rizika, odnosno realizacije kombinacija prijetnja – ranjivost za svu imovinu.

Metodologija ocjene rizika

S obzirom na realne mogućnosti treba odabrati neku od metodologija za ocjenu rizika. Te metodologije su iz skupova kvalitativnih ili kvantitativnih. O temi metodologija ocjene rizika se detaljno govori u poglavlju 5.3.

Ocjena rizika

Kroz ovaj modul se vrši validacija rizika na temelju odabrane metodologije i identificiranih kombinacija prijetnje – ranjivost – posljedica. Rezultat ovog modula je rang lista rizika po definiranim kriterijima.

Obrada rizika

Nakon izvršene ocjene rizika i rangiranja po prioritetima treba izvršiti obradu rizika. Prema standardu postoje četiri načina obrade rizika. To su:

a) **Prihvaćanje** postojećeg (ocjenjenog) rizika
b) **Transfer** rizika (npr. osiguravajuće kuće, vanjske partnere, itd.)
c) **Izbjegavanje** rizika, odnosno zabrana upotrebe informacijskog sistema ili njegovih dijelova u uvjetima u hazardnog okruženja
d) **Smanjivanje** rizika, kada se primjenom kontrola iz Aneksa A standarda ISO 27001:2005 rizici smanjuju na prihvatljivi nivo.

Prihvaćanje rizika

Nakon obrade rizika ipak ostaje neki nivo rizika i uprava organizacije mora deklarativno potpisom prihvatiti činjenicu da će raditi s tim preostalim rizikom.

Komunikacija i konzultacija sa zainteresiranim stranama

Ovaj modul se mora aktivno koristiti u svim fazama procesa za upravljanje rizicima, a osigurava da se kontinuirano izmjenjuju informacije sa svim zainteresiranim stranama o pripremi, normiranju, provedbi procjene i obrade rizika.

Praćenje i preispitivanje

Kako standard zahtjeva stalno preispitivanje metoda, organizacije, postupaka i rezultata procjene rizika, ovaj modul je također kontinuirano aktivan u svim fazama odvijanja procesa. Rezultati provođenja praćenja i preispitivanja su temelj za poboljšanje i unaprjeđenje procesa za upravljanje rizicima.

5.3 METODOLOŠKI PRISTUP PROCJENI RIZIKA ZA ISMS

Upravljanje rizicima u metodološkom smislu predstavlja vrlo ozbiljan problem koji je uvjetovan samom prirodom rizika vezanih za informacijsku sigurnost. U praksi su poznata dva metodološka pristupa:

- Kvantitativni, i
- Kvalitativni.

5.3.1 Kvantitativni metodološki pristup

Kvantitativni metodološki pristup koriste se na temelju numeričkih vrijednosti za prijetnje, ranjivosti i posljedice. Te numeričke vrijednosti su dobivene iz raznih izvora, a najčešće kada je u pitanju ISMS povijest incidenata. Problem ove metodologije nalazi se u činjenici da organizacije nemaju dovoljno veliku bazu relevantnih podataka o incidentima pa je praktički

vrlo malo upotrebljiva, posebno u početku implementacije i funkcioniranja ISMS. Povijesni podaci stari više godina mogu se dobrim dijelom smatrati relevantni, ali i tu treba biti oprezan jer se neki potencijalni incidenti u tom periodu nisu morali ni dogoditi. Ta metoda će reći da taj incident nije realan i ne treba ga razmatrati. Prednost ove metode je u egzaktnosti postupka procjene i transparentnosti rezultata. To se ogleda u činjenici da je praktički nevažno tko vrši procjenu rizika, rezultat će uvijek biti isti.

U području ISMS kvantitativni metodološki pristup je vrlo malo zastupljen upravo zbog nepostojanja relevantnih povijesnih podataka u organizaciji.

5.3.2 Kvalitativni metodološki pristup

Kvalitativni metodološki pristup se koristi opisnom skalom za nivoe prijetnji, ranjivosti i posljedice. Te opisne vrijednosti mogu biti npr. niski, srednji, visoki (ako je skala na tri nivoa). Primjeri opisnih skala za ocjene nivoa prijetnji, ranjivosti i posljedica dani su u tablicama 5.2, 5.3 i 5.4 respektivno.

Tablica 5.2. Kvalitativna skala za prijetnje

Nivo	Oznaka	Opis
1	Niska	Vrlo mala vjerojatnost pojave prijetnje na objekt procjene - imovinu
2	Srednja	Umjerena pojava prijetnje na objekt procjene - imovinu
3	Visoka	Vrlo česta pojava prijetnje na objektu procjene – imovinu

Tablica 5.3. Kvalitativna skala za ranjivosti

Nivo	Oznaka	Opis
1	Niska	Ne postoji ranjivost ili je implementirana vrlo efikasna zaštita
2	Srednja	Umjerena ranjivost, neefikasna zaštita
3	Visoka	Vrlo velika ranjivost na napad, loša ili ne postoji nikakva zaštita

Tablica 5.4. Kvalitativna skala za posljedice

Nivo	Oznaka	Opis
1	Zanemariva	< 3.000 €
2	Mala	< 8.000 €
3	Srednja	< 20.000 €
4	Velika	< 50.000 €
5	Ekstremna	>= 50.000 €

U gornjim primjerima tablica pokazana je filozofija kvalitativne metode. Skale imaju oznake i prateći tekst opisa koji je izuzetno važan, jer daje uputu procjenitelju parametra zašto da odabere nivo npr. 'Srednja' ili 'Visoka', itd. Taj opis treba definirati što preciznije da izbor nivoa parametar od strane raznih procjenitelja bude isti, ili barem približan. To ukazuje da

kvalitativna metoda ima svoju slabu stranu, a to je subjektivnost procjene, odnosno izbora nivoa parametra.

Broj nivoa u skalama je također važan. Naime, ako se definira da će skale imati više nivoa teoretski rezultat će biti precizniji u odnosu ako skale imaju manje nivoa. U gornjim primjerima tablica prijetnje i ranjivosti su definirane na tri, a skala posljedica na pet nivoa. Nedostatak definiranja većeg broja nivoa ogleda se u činjenici da je vrlo teško, praktički nemoguće napraviti opise za takve skale prema kojima bi se razlikovao nivo prijetnje npr. 8 i 9. Iz praktičnih razloga, vrlo često se za prijetnje i ranjivosti koristi skala na tri nivoa kao što je i prikazano u tablicama. Za skalu posljedica je prikazana skala na pet nivoa jer je za nju relativno jednostavno prikazati i opisati nivoe veličinama gubitaka. Tu treba obratiti pažnju samo na veličine gubitaka, jer za neku organizaciju gubitak od 8.000 € je mali, a za neku može biti značajan.

Matematički aparat kojim se vrši izračun nivoa rizika može biti različit, ali se može reći da općenito vrijedi relacija:

$$R = f(T, V, I, \ldots) \tag{5.1}$$

Gdje su: R = rizik

T = prijetnja

V = ranjivost

I = posljedica

Prema izrazu (5.1) vidi se da je rizik R funkcija više parametara. Pored navedenih, neki autori uključuju i neke druge parametre, kao npr. izloženost, elastičnost (Resiliency), itd. No, tu će se analiza ograničiti samo na tri parametra: prijetnju, ranjivost i posljedicu. Zbog praktične analize i rangiranja rizika definira se i vjerojatnost P prema izrazu:

$$P = f(T, V) \tag{5.2}$$

Funkcija koja povezuje sve te parametre najčešće je produkt pa se izrazi mogu napisati u obliku:

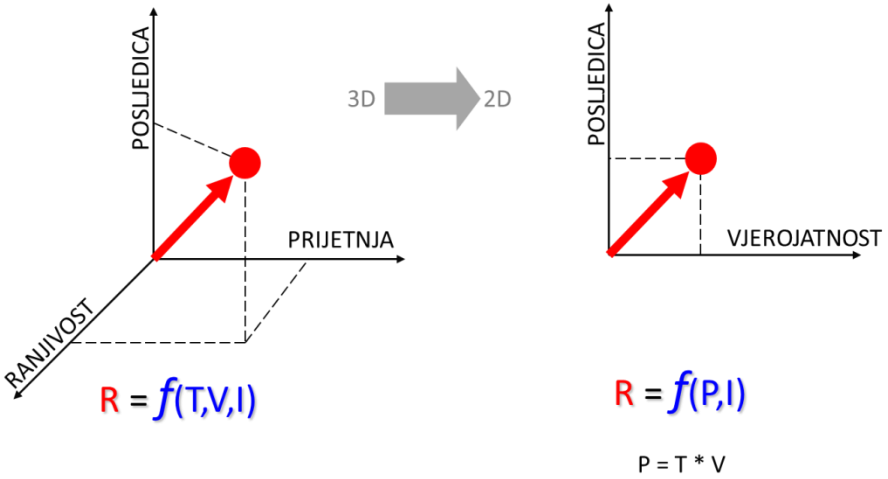
$$R = T * V * I \tag{5.3}$$

$$P = T * V \tag{5.4}$$

$$R = P * I \tag{5.5}$$

Kako se ne mogu raditi računske operacije s oznakama u tablicama 5.2., 5.3. i 5.4. u njima je uveden i podatak 'Nivo', koji predstavlja samo numeričku interpretaciju opisa.

Grafička prezentacija rizika za izraze (5.3) i (5.5) prikazana je na slici 5.8.



Slika 5.8. Grafički prikaz rizika za 3 i 2 parametra

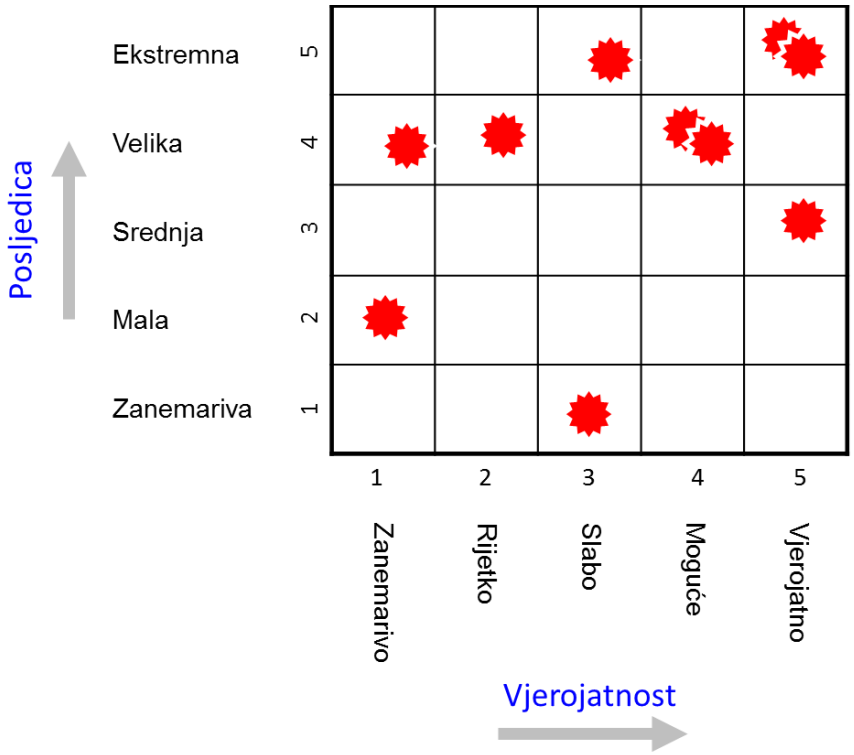
Za slučaj skala kao što je prikazan u tablicama 5.2 – 5.4 vrijednosti rizika su prikazani u tablici 5.5.

Tablica 5.5. Vrijednosti rizika za primjere tablica 5.2, 5.3 i 5.4

VJEROJATNOST	PRIJETNJA	1			2			3		
	RANJIVOST	1	2	3	1	2	3	1	2	3
POSLJEDICA	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36
	5	5	10	15	10	20	30	15	30	45

Primjenom izraza (5.5) dobiva se polje vrijednosti rezultata prikazanih na slici 5.9. Treba napomenuti da je skala vjerojatnosti normirana na vrijednosti 1-5. Naime, za tablice ocjene parametara prijetnja i ranjivost u granicama 1 – 3 može se pokazati da je područje vrijednosti za vjerojatnost prema izrazu (5.4) u granicama 1- 9. Da bi se dobila skala vjerojatnosti 1 – 5, a time i kvadratni oblik polja vrijednosti na slici 5.9. nužno je normiranje skale vjerojatnosti.

Vidi se na slici 5.9. da su se rezultati procjene rizika nalaze distribuirani po cijelom polju vrijednosti (primjer). Prema procesu za upravljanje rizicima u standardu ISO 27005:2008 nakon procjene rizika se mora provesti rangiranje rezultata i sukladno tome izvršiti obradu rizika.



Slika 5.9. Područje vrijednosti procjene rizika

Rangiranje rezultata procjene rizika se vrši prema matrici prihvatljivosti rizika, koja predstavlja ključni alat za provedbu politike sigurnosti. Da bi se definirala rang skala za rizike treba prvo utvrditi područje vrijednosti za rizike. Primjenom do sada iznesenih primjera i izrazom (5.5) može se pokazati da se rizici kreću u granicama od 1 do 25. Primjer kriterija za rangiranje rizika je prikazan u tablici 5.6. uz napomenu da je pretpostavljeno rangiranje svih rizika na tri nivoa.

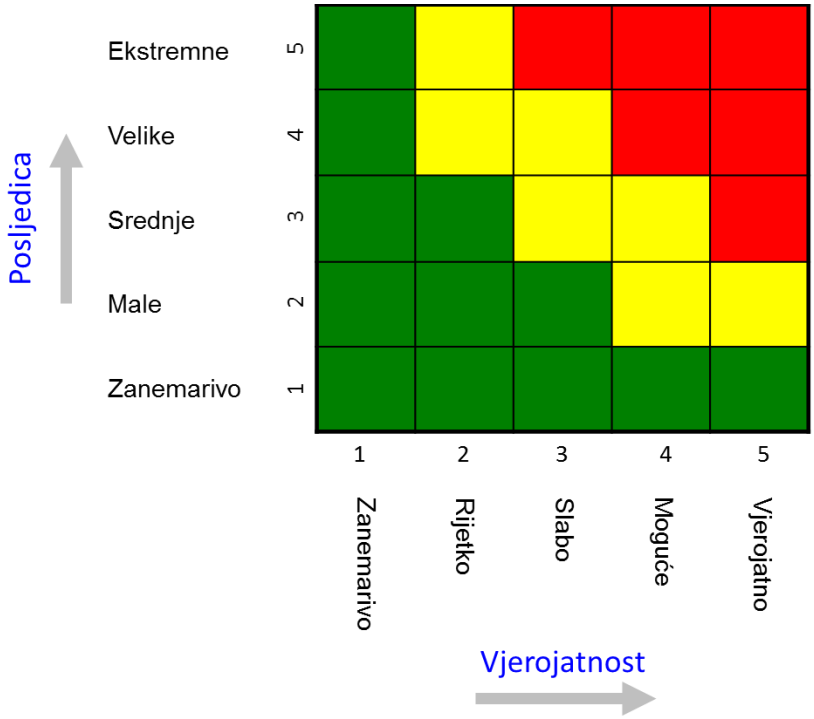
Tablica 5.6. Primjer rang skale za procijenjene rizike

Vrijednost rizika		Rang	Opis
OD	DO		
1	6	1	Prihvatljivi rizici, potrebno nadziranje
7	12	2	Zahtjeva se isplativo upravljanje i nadziranje
13	25	3	Zahtjeva se ekstenzivno upravljanje i nadziranje

Rang skala za rizike kada se prikaže u matrici prihvatljivosti rizika izgleda kao što je prikazano na slici 5.10.

Prema primjeru u tablici za rangiranje rizika 5.6. može se zaključiti da su svi rizici ranga 1 prihvatljivi i njih samo treba nadzirati. Rizike i područja ranga 2 treba smanjivati ako ima financijskog opravdanja, odnosno ako je trošak implementacije sigurnosne mjere manji od troška posljedice. Taj rizik treba također nadzirati. Konačni, za rizike iz ranga 3 zahtjeva se obavezno smanjenje, odnosno obrada i stalni nadzor.

Kriteriji na rang listi rizika rezultat su politike organizacije i njihovog stava prema problemu informacijske sigurnosti.



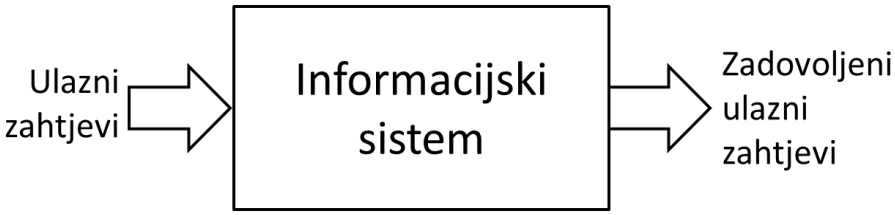
Slika 5.10. Matrica prihvatljivosti rizika

Osnovna značajka za procjenu rizika prema ISO 27001:2005, odnosno ISO 27005:2008 je u tome da se rizik procjenjuje za svaku informacijsku imovinu posebno, i to za sve kombinacije relevantnih prijetnji, ranjivosti i minimalno tri zahtijevane posljedice vezane za C-I-A. Tako npr. ako u informacijskom sistemu ima 3 imovine, za svaku od njih postoje 3 relevantne prijetnje i 3 relevantne ranjivosti za promatrane prijetnje, tada treba napraviti 81 procjenu rizika. Svaki taj procijenjeni rizik govori o stanju rizika za tu imovinu i promatrane parove prijetnja – ranjivost i u odnosu na neku posljedicu. Međutim, te procjene rizika ne govore ništa o ukupnom riziku informacijskog sistema.

6. STRUKTURNA FUNKCIJA

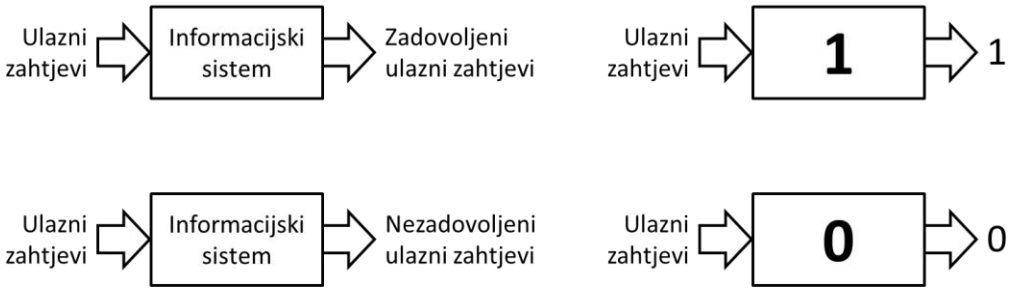
6.1. OSNOVE TEORIJE STRUKTURE SISTEMA

Ako se informacijski sistem predstavi kao proces koji ima ulogu da ulazni zahtjev pretvori u izlazno zadovoljenje tog zahtjeva, pojednostavljena blok shema je kao se vidi na slici 6.1



Slika 6.1. Blok shema informacijskog sistema kao procesa

Kao što je već rečeno funkcije informacijskog sistema mogu biti generiranje, prijenos, obrada, isporuka i arhiviranje informacija, odnosno bilo kakva kombinacija navedenih elementarnih funkcija. Informacijski sistem kao proces ima ulogu da zadovolji sve ulazne zahtjeve. Pri tome se smatra da su ulazni zahtjevi ispunjeni ako su u potpunosti realizirani, a ne samo neki ili neki od njih djelomično. U tom slučaju se govori o nefunkcioniranju informacijskog sistema. Prema tome informacijski sistem za potrebnu analizu ili zadovoljava ili ne zadovoljava ulazne zahtjeva, odnosno radi ili ne radi.

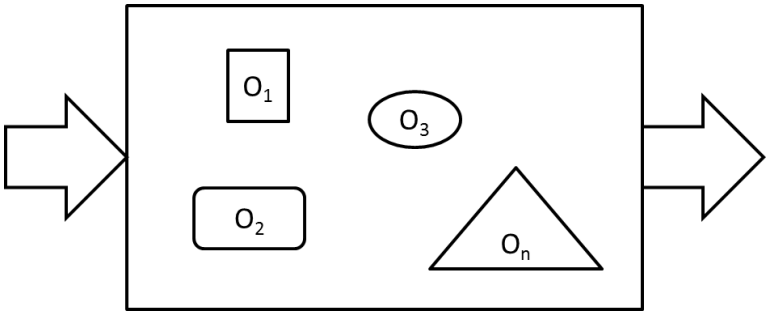


Slika 6.2. Blok shema informacijskog sistema u stanju zadovoljavanja i nezadovoljavanja ulaznih zahtjeva

U uvjetima nesigurnosti funkcioniranja informacijskog sistema, kao i okruženja stalna je opasnost neispunjavanja funkcije IS. Kolika je vjerojatnost da će se dogoditi prestanak funkcioniranja IS pokazuje se veličinom rizika. Što je rizik veći, to znači veća vjerojatnost da će doći do nefunkcioniranja IS, odnosno do nezadovoljavanja ulaznih zahtjeva. Realizacija nekog rizika u IS označava stanje kada IS više ne funkcionira barem u jednoj od svojih značajki onako kako bi trebao prema planu.

Realizacija rizika narušava u manjoj ili većoj mjeri funkcije informacijskog sistema i dovodi do pojave štete za njegovog vlasnika, odnosno korisnike.

Kako je već rečeno, svaki IS se sastoji u konačnici od niza elementarnih objekata (procesa, podprocesa, procesnih aktivnosti, uključujući i pripadna pravila, resurse i mjerenja) , svaki sa svojim specifičnostima i funkcionalnošću. Ukupna funkcionalnost IS je određena funkcionalnošću svih pojedinih objekata.

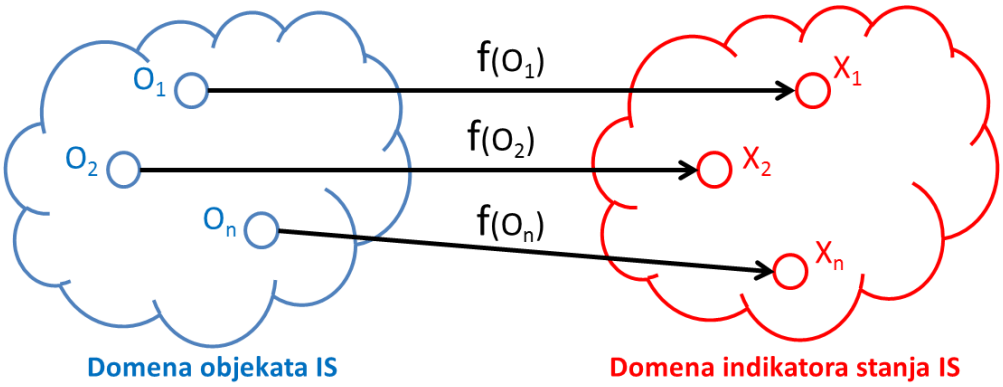


Slika 6.3. Objekti u informacijskom sistemu

Svaki elementarni objekt IS može biti u stanju nerealiziranog rizika (ispravno stanje) ili u stanju realiziranog rizika (neispravno stanje). U kontekstu toga, stanje objekta (ispravno – neispravno) može se označiti indikatorom stanja x prema slijedećoj formuli [50]

$$f(O_i) = \begin{cases} 1 & ako\ je\ O_i\ ispravno \\ 0 & ako\ je\ O_i\ neispravno \end{cases} \tag{6.1}$$

Ilustracija preslikavanja iz domene objekata IS u domenu indikatora stanja prikaza je na slici 6.4.



Slika 6.4. Pridruživanje objektima indikatora stanja

Kako je prikazano na slici 6.3. informacijski sistem se sastoji od n objekata O_i , gdje je i=1,2,...,n. U tom slučaju vrijedi relacija

$$O = (O_1, O_2, ..., O_n) \tag{6.2}$$

Prema slici 6.4. se vidi da n-torki objekata O_i odgovara n-torka objekata x_i. Kako jedna n-torka komponenata može imati 2^n različitih varijacija sa ponavljanjem, može se formirati indikator stanja skupa objekata x prema relaciji

$$X = (x_1, x_2, ..., x_n) \tag{6.3}$$

Kako prosti skup objekata još uvijek ne predstavlja sistem, nužno je za formiranje sistema pronalaženje međusobno uzročno-posljedične veze između samih objekata koji čine taj skup.

Svaki skup objekata može imati niz karakteristika koje ga opisuju. Za analizu i razmatranje ograničava se samo na jednu karakteristiku: indikator stanja. Time skup O postaje sistem **S** koji će se u buduće razmatrati u skladu s analizom pripadnog skupa **X**.

Pretpostavimo da je **y** varijabla koja predstavlja indikator stanja sistema **S**, može se tada reći da vrijedi

$$y = \begin{cases} 1 & ako\ je\ S\ ispravan \\ 0 & ako\ je\ S\ neispravan \end{cases} \tag{6.4}$$

Iz gornjih relacija se može pokazati da vrijedi

$$Y = \varphi(x) \tag{6.5}$$

Odnosno

$$y = \varphi(x_1, x_2, ..., x_n) \tag{6.6}$$

Izrazima (6.5) i (6.6) se pokazuje da je indikator stanja y funkcija. Ta se funkcija naziva „strukturna funkcija“ sistema **S**.

Za sistem S kaže se da je n-tog reda ako strukturna funkcija y označava sistem **S** od n objekata.

6.2. OSNOVNI OBLICI STRUKTURNE FUNKCIJE

Analizom mogućih praktičkih oblika struktura sistema i načina veze pojedinih objekata u sistemu prepoznaju se dva trivijalna oblika: serijska i paralelna veza objekata. U praksi se

pojavljuje i redovno kombinira veza, odnosno struktura sistema koja ima i serijske i paralelne veze pojedinih objekata.

6.2.1. Serijska struktura

Neka je

$$y = \varphi(x_1, x_2, ..., x_n) \tag{6.7}$$

$$y = x_1 \cdot x_2 \cdot .... \cdot x_n \tag{6.8}$$

$$y = \prod_{i=1}^{n} x_i \tag{6.9}$$

Ova strukturna funkcija, tzv. serijska, odgovara sistemu u kojemu svi objekti imaju ispravno stanje, odnosno za koje vrijedi trivijalno ograničenje:

$$\begin{aligned} &(\forall i, x_i = 1) \Rightarrow (y = 1) \\ &(\exists i : x_i = 0) \Rightarrow (y = 0) \end{aligned} \tag{6.10}$$

Ovakva serijska struktura podrazumijeva da su svi objekti spojeni u seriju. Prekid funkcionalnosti jednog objekta, izaziva prekid funkcionalnosti cijele strukture.

6.2.2. Paralelna struktura

Neka je

$$y = \varphi(x_1, x_2, ..., x_n) \tag{6.11}$$

$$y = 1 - (1 - x_1) \cdot (1 - x_2) \cdot ... \cdot (1 - x_n) \tag{6.12}$$

$$y = 1 - \prod_{i=1}^{n} (1 - x_i) \tag{6.13}$$

Ova strukturna funkcija odgovara stanju da je ispravna kada je barem jedan objekt ispravan, odnosno

$$\begin{aligned} &(\forall i, x_i = 0) \Rightarrow (y = 0) \\ &(\exists i : x_i = 1) \Rightarrow (y = 1) \end{aligned} \tag{6.14}$$

Ova, tzv. Paralelna struktura pretpostavlja da su svi objekti strukture spojeni paralelno.

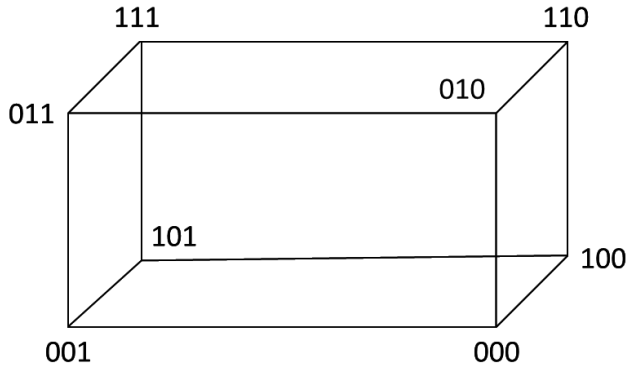
6.3. NAČINI PRIKAZIVANJA STRUKTURNIH FUNKCIJA

Prema pojmovima algebre logike, serijska funkcija odgovara koncepciji konjukcije, a paralelna koncepciji disjunkcije. Zato se strukturna funkcija može prikazati i u obliku tablice, kao i na niz drugih načina. Među tim raznim oblicima prikazivanja strukturne funkcije

najčešće se sreću: Bulo-ve tablica istine, Bulo-ve grafičke strukture, sheme (grafička prezentacija), grafovi, matrice i analitički izrazi (jednadžbe).

Bulo-ve tablice istine daju sva moguća stanja indikatora x usporedo s vrijednošću strukturne funkcije za svaku kombinaciju. Time se struktura realizira kao prekidačka funkcija putem tablice istine kao savršena disjunktivna, odnosno savršena konjuktivna forma.

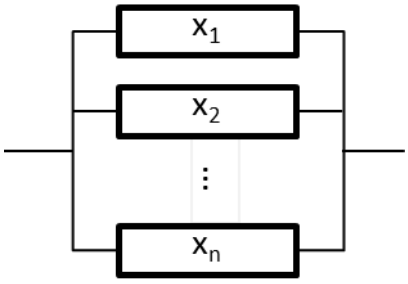
Bulo-va grafička struktura prikazuje n-torku stanja u obliku vrha pravilnog mnogokuta u višedimenzionalnom prostoru (Hasse-ov dijagram). Na svakom vrhu se nalaze dva simbola koja označavaju vrijednost strukturne funkcije sistema za dato stanje indikatora skupa elemenata, kao što je prikazano na slici 6.5.



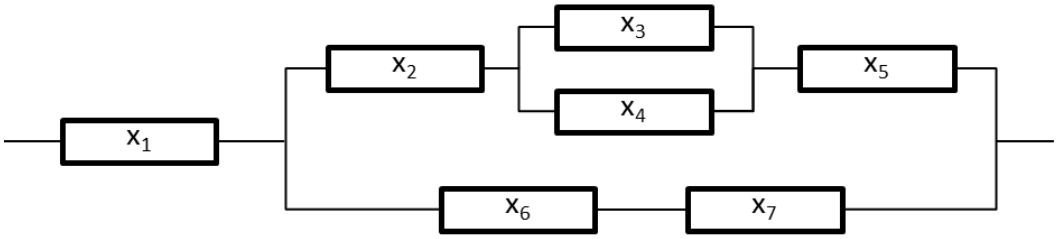
Slika 6.5. Hasse-ov dijagram sistema s tri objekta

Shema (grafička prezentacija) daje prikaz veze u nekoj strukturi s označenim objektima unutar svakog pojedinog mjesta. Na slikama (6.6), (6.7) i (6.8) prikazani su primjeri serijske, paralelne i složene strukture objekata u sistemu, respektivno.

Slika 6.6. Serijska struktura objekata

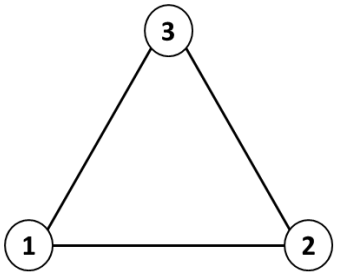


Slika 6.7. Paralelna struktura objekata



Slika 6.8. Složena struktura objekata

Grafovi su rezultat daljnjeg razvoja grafičkog shematskog prikaza strukture sistema. Pojednostavljeno, graf je figura sastavljena od točaka koje su sve ili samo neke od njih međusobno povezane linijama. Jedan od najčešćih načina matematičkog definiranja grafa kaže da je graf uređen par ***G*=(*V,g*)** gdje je ***V*** ne prazan skup, **g** binarna relacija u ***V*(*V**V*)**. Elementi skupa **V** su čvorovi (vrhovi) grafa, a elementi **g** su grane grafa. Tako npr. ako su zadani V=(1,2,3) i g={(1,2),(2,1),(1,3),(3,1),(2,3),(3,2)} graf se može prikazati kao na slici 6.9.



Slika 6.9. Graf strukture sa tri čvora

Za graf **G=(V,g)** se kaže da je neorijentiran, odnosno simetričan, ako je **g** simetrična relacija, odnosno, u suprotnom je orijentiran ili asimetričan graf.

Matrica se također koristi za prikaz strukturne funkcije (ili kraće; strukture) i to na nekoliko načina. U tom smislu uvodi se ograničenje da je veza između dva čvora uvijek jednostruka, odnosno da postoji samo jedna grana između ta dva čvora, bez obzira na orijentaciju (tzv. Dijadska matrica). Zbog toga će biti date samo dvije vrste matrica: matrica susjednosti i latinska matrica. Matrica susjednosti (Adjacency Matrix) je u stvari kvadratna matrica čiji jedan redak odgovara broju čvorova. U koliko postoji veza između čvora ***i*** i čvora ***j***, tada se na presjeku i-tog retka i j-tog stupca stavlja oznaka 1 (dijadska matrica). U suprotnom je oznaka 0. Latinska matrica je u biti proširen oblik matrice susjedstva. Razlika je u tome što se postojanje veze između čvora ***i*** i čvora ***j*** upisuje oznakom ***ij***.

Analitički izraz ili jednadžba daje strukturnu funkciju u obliku algebarske jednadžbe. Izrazi 6.9 i 6.13 su primjeri analitičkih izraza kojima se opisuje struktura.

Teoretski, svi gore prikazani primjeri opisa strukturne funkcije su ravnopravni, te njihova primjena zavisi od pogodnosti pristupa kod rješavanja nekog praktičnog problema.

6.4. PUTEVI I PRESJECI

Put između dva čvora se definira kao podskup svih objekata koji imaju ispravno stanje, pa se podrazumijeva i da je struktura ispravna. Ako su svi ostali objekti strukture neispravni, struktura je i dalje ispravna zbog postojanja puta između ulaznog i izlaznog čvora strukture.

Neka je sistem ***S*** **z**adan sa skupom objekata i definiran strukturnom funkcijom **y** prema izrazu (6.11). Pretpostavimo da je ***a***=$\{k_1,k_2,...,k_n\}$ podskup skupa ***k***, tako da vrijedi izraz

$$\begin{aligned} &a = \{k_i, i \in I\} \subset k \\ &I \leq n \end{aligned} \tag{6.15}$$

Ako je

$$\left.\begin{aligned} &x_i = 1, i \in I \\ &x_i = 0, i \notin I \end{aligned}\right\} \Rightarrow y = 1 \tag{6.16}$$

Podskup **a** se naziva **put** u sistemu **S**.

Presjek se smatra neispravno stanje bilo kojeg podskupa ***b***=$\{k_1,k_2,...,k_n\}$ u sistemu ***S***, zbog kojega je i cijeli sistem u neispravnom stanju. U koliko su svi drugi objekti sistema ***S*** ispravni, sistem je i dalje neispravan zbog neispravnosti podskupa ***b***.

Ako se u istom sistemu ***S*** definira podskup ***b*** da vrijedi

$$\begin{aligned} &b = (k_j, j \in J) \subset k \\ &J = n \end{aligned} \tag{6.17}$$

i ako je

$$\left.\begin{aligned} &x_j = 0, j \in J \\ &x_j = 1, j \notin J \end{aligned}\right\} \Rightarrow y = 0 \tag{6.18}$$

tada je podskup b **presjek** u sistemu **S**.

6.5. MINIMALNI PUTEVI I MINIMALNI PRESJECI

Ako u sistemu ***S*** postoji put ***a*** takav da ne postoji novi put ***a'*** koji je podskup skupa ***a***, onda je ***a*** minimalni put u sistemu ***S*.**

Glavna karakteristika minimalnog puta u strukturi sistema ***S*** je u tome što predstavlja skup elemenata čiji indikatori stanja imaju vrijednost 1 a prijelaz bilo kojeg od njih u vrijednost 0 prevodi strukturnu funkciju ***y*** iz 1 u 0.

Ako u sistemu ***S*** postoji presjek ***b*** takav da ne postoji novi presjek ***b'*** koji je podskup skupa ***b***, onda je ***b*** minimalni presjek u sistemu ***S***.

Glavna karakteristika minimalnog presjeka u strukturi sistema ***S*** je u tome što predstavlja skup objekata čiji indikatori stanja imaju vrijednost 0 a prijelaz bilo kojeg od njih u vrijednost 1 prevodi strukturnu funkciju ***y*** iz 0 u 1.

6.6. MATEMATIČKE KARAKTERISTIKE PUTEVA I PRESJEKA. DUALNOST

Teorem 6.1: svaka n-torka $(x_1,x_2,...,x_n)$ gdje je x_i=0 ili 1 odgovara putu ili presjeku.

Zaista, ukoliko sistem nije degeneriran i $\boldsymbol{x_i}$ za sve vrijednosti **i** = 1,2, ... ,n daje put ***a***, tada je presjek određen izrazom

$$\bar{a}\,(a \cup \bar{a} = n) \qquad (6.19)$$

pri tome je $\boldsymbol{x_i} = 0$ *za* $\boldsymbol{i} = a+1, a+2, ... , a+n$.

Drugim riječima, bilo koje stanje $x=\{x_1, x_2, ... , x_n\}$ gdje je x_i = 0 ili 1 kod koga je zadovoljeno da $\boldsymbol{k_a}(\boldsymbol{a} \subset \boldsymbol{n})$ daje strukturnu funkciju **y** = 1, označava k kao put a, $\bar{k}$ kao presjek. Ali, ako je ***y*** = 0, tada ***k*** nije put već presjek.

Na primjer, za n = 5 i k = 2, put ima slijedeći oblik $y = \varphi(1,1,0,0,0) = 1$, gdje n predstavlja broj čvorova, a k je broj objekata u putu.

Svaki put sadrži najmanje jedan minimalni put (kada je on sam taj minimalni put) a svaki presjek sadrži najmanje jedan minimalni presjek (kada je on sam taj minimalni presjek).

Svaki put sadrži najmanje jednu komponentu od svih presjeka i obrnuto. To proizlazi iz činjenice da u neregeneriranoj strukturi ***y***=1 1 za sve $\boldsymbol{x_i}$ = 1, odnosno ***y***=0 za sve $\boldsymbol{x_i}$ = 0.

Za strukturnu funkciju se kaže da je monotona ako je zadovoljena relacija

$$\varphi(x^{(1)}) \le (x^{(2)}) \qquad (6.20)$$

Na temelju Bulove algebre znači da n-torka iz $x^{(2)}$ mora dominirati nad n-torkom iz $x^{(1)}$. Na primjer $\varphi(0,0,1,1,1) > \varphi(0,0,0,1,1)$.

U vezi s putovima, to znači da je strukturna funkcija monotona onda i samo onda kad svaki skup komponenata koji sadrži put i sam predstavlja put. U takvoj strukturi indikatori stanja mogu sukcesivno poprimati samo vrijednosti 0 sve dok i sama vrijednost ***y*** konačno ne postane 0 pa i nadalje.

Teorem 6.2: Neka je A_k broj putova koji imaju *k* objekata, a B_k broj presjeka koji imaju *k* objekata. Tada je

$$A_k + B_{n-k} = \binom{n}{k} \qquad (6.21)$$

Što predstavlja broj kombinacija od ***k*** objekata uzetih iz skupa od ***n*** objekata.

Posljedica je pridruživanje svakom od podskupova (ima ih prema izrazu 6.21) s brojem objekata ***k***, n-torke s vrijednostima 1 za objekte koji pripadaju podskupu i sa vrijednosti 0 za ostale. Kroz dokaz teorema 6.1. pokazuje se da svaki podskup putova ima ***k*** objekata, a presjeci ***n-k*** objekata.

Dužina sistema S je najmanji cijeli broj λ kod kojega je $A_\lambda > 0$. Drugim riječima, to je minimalni broj objekata koji čini put. Dužina se označava sa $\lambda(S)$.

Širina sistema S je najmanji cijeli broj takav da je $B_\mu > 0$. Drugim riječima to je minimalni broj objekata koji čini presjek. Širina se označava sa $\mu(S)$.

Teorem 6.3: Dužina $\lambda(S)$ i širina $\mu(S)$ istog sistema *S* zadovoljavaju nejednadžbu

$$\lambda(S) + \mu(S) \leq n + 1 \qquad (6.22)$$

gdje je ***n*** broj objekata sistema.

Izraz (6.22) proističe iz slijedećeg razmatranja: ako je $\lambda(S)$ najmanji put tada skup $\lambda(S) - 1$ objekata ne može biti put, pa je $\mathbf{n} - \lambda(S) + 1$ obavezno presjek. U skladu s definicijom širine sistema imamo

$$\mu(S) \leq n - \lambda(S) + 1 \qquad (6.23)$$

odakle slijedi dokaz i ispravnost nejednadžbe (6.22).

Moore i Shannon su pokazali da postoji slijedeća veza između broja objekata ***n*** u sistemu ***S***, njegove dužine λ i širine μ prema

$$n \geq \lambda * \mu \qquad (6.24)$$

Degenerirani sistem. Za sistem se kaže da je degeneriran ako i samo oko je

$$\varphi(x) \equiv 1 \qquad (6.25)$$

ili

$$\varphi(x) \equiv 0 \qquad (6.26)$$

Drugim riječima, bez obzira na stanje njegovih objekata sistem je uvijek ispravan ili je uvijek u prekidu.

Dualnost. Neka je dat sistem čija je strukturna funkcija $\varphi(x)$. Sistem ***S*** se naziva dualnim sistemom ***S*** ako je strukturna funkcija

$$\bar{\varphi}(x) = 1 - \varphi(1 - x) \qquad (6.27)$$

gdje je (1-x) = (1-x_1 , 1-x_2 , ... , 1-x_n).

Karakteristike dualnosti ili odnos sistema i njegovog dualnog sistema su

1) $\overline{[\overline{\varphi}(x)]} = \varphi(x), \overline{(\overline{S})} = S$
2) Put od S je presjek od $\overline{S}$ i obratno
3) Presjek od S je put od $\overline{S}$ i obratno
4) Minimalni put od S je minimalni presjek od $\overline{S}$ i obratno
5) Minimalni presjek od S je minimalni put $\overline{S}$ i obratno

6.7. TRAŽENJE SVIH MINIMALNIH PUTEVA

Ako strukturnu funkciju predstavimo u obliku grafa s tim da čvorove označimo sa ***A***, ***B***, ... , ***Z*** ili sa 1,2, ... , n, tada su uvijek dva čvora karakteristična. Jedan od njih je početni ili ulazni dok je drugi završni ili izlazni. Karakteristični čvorovi predstavljaju definicijski par sistema ***S***. Mogući broj definicijskih parova u sistemu od ***n*** komponenti dat je sa izrazom

$$D = \binom{n}{2} \tag{6.28}$$

NAPOMENA: Ubuduće, ukoliko se drugačije ne istakne, najmanja vrijednost oznake čvora ili prvo slovo biti će početni čvor a najveća vrijednost ili završno slovo (u abecednom smislu) biti će završni čvor.

Uz odabrani definicijski par i date veze (definiranu strukturnu funkciju) traženje minimalnih putova moguće je na više načina. Obratimo pažnju na nekoliko najinteresantnijih.

- Najduža i najmukotrpnija je metoda direktnog prebiranja svakog indikatora stanja u vektoru ***x***. Ova metoda ne traži ekvivalentnu strukturu sistema ali broj pretraživanja vrlo brzo raste sa brojem čvorova tako da postaje potpuno neprimjenljiv.
- Razvoj sistema u ekvivalentnu savršenu disjunktivnu odnosno savršenu konjunktivnu formu metodama prekidačke algebre praktično odgovara po kompliciranosti metodi direktnog prebiranja tako da je i on samo od teorijskog značaja. To se posebno odnosi na sisteme čiji su grafovi nesimetrični (orijentirani).
- U teoriji i praksi postoji mnoštvo algoritama koji po suštini nisu komplicirani ali broj računanja (vrijeme) i potrebna memorija kompjutera vrlo brzo rastu i ne mogu zadovoljiti za veći broj čvorova grafa sistema. Za razmatranje će se u nastavku traženje svih minimalnih putova provesti uz pomoć tzv. “latinske matrice“ i tzv. “latinske kompozicije“ pa će ta metoda i pripadni algoritam biti posebno istaknuti.

6.7.1. Latinska kompozicija

Pretpostavimo da sistem ima strukturu od n komponenata što odgovara grafu od m čvorova $V_m(m \leq n + 1)$. U najopćenitijem slučaju svaki čvor je vezan sa svakim drugim čvorom. Očigledno je da tada, bez obzira na odabrani definicijski par, dužina sistema iznosi $\lambda(S) = 1$. Potpuno isto je i sa paralelnom strukturom gdje je također $\mu(S) = 1$. U oba ova slučaja dužina sistema je jednaka i maksimalnom putu.

S druge strane, najduži minimalni put a ujedno i jedini ima serijska struktura pa je $\lambda(S) = n$,

Rješenje općenitog sistema time se svodi na nalaženje svih mogućih minimalnih putova čije dužine idu (ako ih ima) od 1 do n.

Latinska kompozicija je sukcesivno množenje n puta latinske matrice sa tzv. "reduciranom latinskom" matricom istog reda pri čemu se dobivaju svi minimalni putovi (ako postoje) svih dužina u sistemu S od n objekata.

Latinska matrica je kvadratna čije oznake redova i stupaca odgovaraju čvorovima grafa razmatranog sistema (V_1, V_2, ... , V_m). Polja u latinskoj matrici se popunjavaju prema slijedećem pravilu:

- ako je polje (element matrice) na presjeku reda V_i i stupca V_j tada ono dobiva vrijednost 0;
- ako čvorovi reda V_i i V_j ($i = j$) nisu vezani u strukturu sistema, tada je polje na njihovom presjeku također nula;
- ako su čvorovi retka V_i i stupca V_j ($i \neq j$) vezani u strukturu sistema tada se u polje na njihovom presjeku upisuje oznaka V_i V_j.

Reducirana latinska matrica ima ista pravila za upis nula u odgovarajuća polja i jedina razlika je u tome što se na presjecima retka V_i i stupca V_j ($i \neq j$) upisuje samo oznaka stupca V_j.

Uvedimo oznaku za latinsku matricu L a za reduciranu latinsku matricu l.

Početna latinska matrica se dobiva direktno iz strukture sistema koji se rješava. Označimo još dodano početnu latinsku matricu sa $L^{(1)}$.

Proces rješavanja sistema S (traženje svih minimalnih putova) od n elemenata odvija se po slijedećem algoritmu:

a) realizira se početna latinska matrica $L^{(1)}$ i reducirana latinska matrica l prema pravilima i danoj strukturi sistema;
b) odabere se definicijski par (V_i, V_j, $i \neq j$, $l \leq i$, $j \leq n+1$) a u matricama $L^{(1)}$ i l se pridruži vrijednost nula svim elementima stupca početnog čvora V_i i svim elementima završnog čvora V_j;
c) na presjeku retka koji odgovara početnom čvoru i stupca koji odgovara završnom stupcu direktno se očita iznos minimalnog puta (0 ili V_i V_j);

d) množi se $\boldsymbol{L^{(1)}}$ sa $\boldsymbol{l}$ prema propisu za množenje matrica uz dva dodatna pravila. Neka je element matrice $\boldsymbol{L}$:$\boldsymbol{L_{i,j}}$ ($\boldsymbol{i \neq j}$) a element matrice $\boldsymbol{l}$:$\boldsymbol{l_{i,j}}$ ($\boldsymbol{i \neq j}$). Tada dodatna pravila za množenje matrica glase:

$$L_{i,j}^{(k)} \times I_{i,j} = \bigcup \left(L_{i,j}^{(k+1)} \right)$$
$$i \leq i, j \qquad (6.29)$$
$$k \leq n+1$$

$$L_{i,j}^{(k)} \times I_{i,j} = 0 \forall A_m \left(L_{i,j}^{(k+1)} \right) \qquad (6.30)$$
$$i \leq m \leq n+1$$

Izraz (6.29) govori da produkt sumanada u toku množenja matrica odgovara uniji minimalnih putova dužine $\boldsymbol{k}$+1.

Prema relaciji (6.30) svaki sumand koji nastane u toku množenja matrica poprima vrijednost 0 ukoliko se u oba faktora množenja nađe makar jedan isti čvor.

e) rezultat množenja matrica $\boldsymbol{L^{(1)}}$ x $\boldsymbol{l}$ je matrica $\boldsymbol{L^{(2)}}$ gdje su svi postojeći članovi (polja) sastavljeni od mogućih putova između tri čvora;
f) na presjeku retka koji odgovara početnom čvoru i stupca koji odgovara završnom čvoru direktno se očitava iznos minimalnih putova (0,1 ili $\bigcup$);
g) čitav postupak se ponavlja (množi se $\boldsymbol{L^{(2)}}$ x $\boldsymbol{l}$ uz navedena pravila i traže minimalni putovi) sve do dobivanja matrice $\boldsymbol{L^{(n)}}$ čime se kompletan postupak završava.

Našavši sve minimalne putove sistema sa zadanom strukturom istovremeno nalazimo i sve minimalne presjeke. To proizlazi već i iz činjenice da komplement strukturne funkcije y = 1 (put) iznosi u tom trenutku $\bar{y}$ = 0 (presjek).

Praktično, algoritam traženja minimalnih presjeka iz skupa minimalnih putova time se svodi na izdvajanje elemenata od kojih se svaki nalazi barem u jednom minimalnom putu.

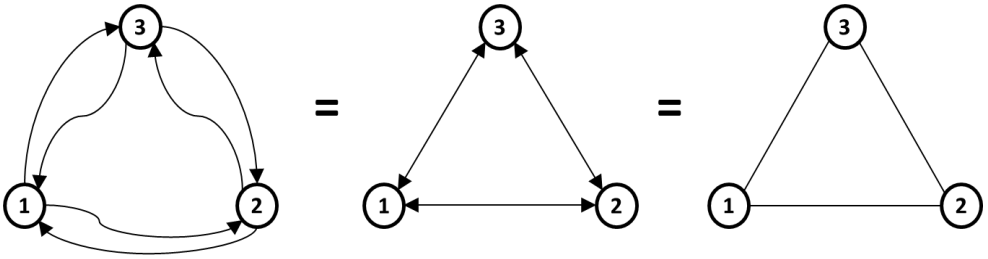
6.7.2. Karakteristike latinske kompozicije

Latinska kompozicija ima slijedeće karakteristike:

a) traženje svih minimalnih putova svodi se na sukcesivno množenje dvaju matrica istog reda;
b) broj množenja odgovara broju najdužeg minimalnog puta (ako ga ima);
c) nakon svakog množenja dobivaju se svi mogući minimalni putovi između dva odabrana čvora;
d) veza između bilo kojih vrhova $\boldsymbol{V_i}$ i $\boldsymbol{V_j}$ ($\boldsymbol{i \neq j}$) može biti proizvoljna (0, $\boldsymbol{V_i}$ $\boldsymbol{V_j}$, $\boldsymbol{V_j}$ $\boldsymbol{V_i}$ ili $\boldsymbol{V_i}$ $\boldsymbol{V_j}$ i $\boldsymbol{V_j}$ $\boldsymbol{V_i}$). Drugim riječima, orijentacija grafa strukture nema nikakvog utjecaja na rješavanje;
e) čvorovi se mogu odabirati po volji (npr. ovdje se dogovorno promatra rješenje između prvog i zadnjeg čvora ali za latinsku kompoziciju definicijski par može biti bilo koji),

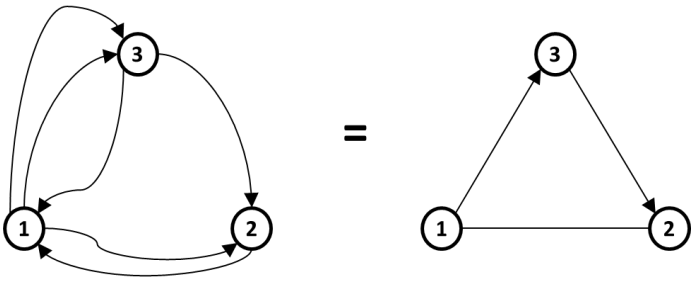
f) matrica $\boldsymbol{L}^{(1)}$ daje direktan uvid u oblik strukturne funkcije a matrica $\boldsymbol{L}^{(n)}$ (završna) i predstavlja kontrolu cijelog procesa množenja s tim da su svi elementi matrice jednaki nuli izuzev (eventualno) elemenata na presjeku retka i kolone definicijskih čvorova.
g) Od posebnog interesa za praktičan rad (općenito) je karakteristika d. Ona, u stvari, govori o orijentiranim, odnosno neorijentiranim strukturama. Na slici 6.9. dana je neorijentirana struktura uz pomoć grafičkog prikaza.

Neorijentirana struktura je sakriveni prikaz dvostruke orijentirane strukture pri čemu je moguća veza (dohvat ili spoj) od bilo kojeg čvora do bilo kojeg drugog čvora. Prikazi neorijentirane strukture je prikazana na slici 6.10.



Slika 6.10. Prikazi neorijentiranog grafa strukture sistema

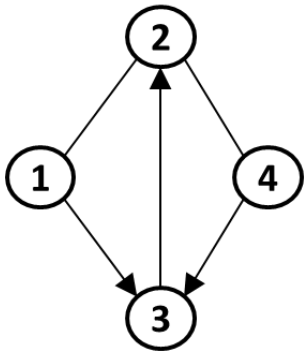
Važna je napomena da se u ovom radu u strukturi niz paralelnih grana u istom smjeru uvijek (ako se drugačije ne kaže) objedinjuje u jednu granu, kao što je prikazano na slici 6.11.



Slika 6.11. Objedinjavanje paralelnih grana u grafu strukture sistema

Da bi se pokazale karakteristike i način realizacije algoritma latinske kompozicije, uzet će se jedan jednostavan primjer. Na slici 6.12. dana je struktura nekog sistema u obliku grafa i pripadna latinska kompozicija.

Prema ranijoj napomeni, definicijski par je (1,4), odnosno čvor 1 je ulaz u strukturu, a čvor 4 je izlaz iz strukture.



$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 12 & 13 & 0 \\ 2 & 21 & 0 & 0 & 24 \\ 3 & 0 & 32 & 0 & 0 \\ 4 & 0 & 42 & 43 & 0 \end{array}$$

Slika 6.12. Prikaz grafa strukture i pripadna latinska kompozicija

Na slici 6.13. je prikazana pripadna latinska matrica i reducirana latinska matrica, koje su dobivene u skladu s pravilima opisanim u točki 6.7.1.

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 12 & 13 & 0 \\ 2 & 21 & 0 & 0 & 24 \\ 3 & 0 & 32 & 0 & 0 \\ 4 & 0 & 42 & 43 & 0 \end{array} \qquad \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 2 & 3 & 0 \\ 2 & 1 & 0 & 0 & 4 \\ 3 & 0 & 2 & 0 & 0 \\ 4 & 0 & 2 & 3 & 0 \end{array}$$

$$\mathbf{L}^{(1)} \qquad\qquad \mathbf{l}$$

Slika 6.13. Prikaz latinske matrice $\mathbf{L}^{(1)}$ *i pripadne reducirane latinske matrice* $\mathbf{l}$

U skladu s pravilom i odabranom definicijskom paru (1,4) treba u latinskoj matrici i reduciranoj latinskoj matrici postaviti sve elemente stupca 1 u retka 4 na vrijednost 0. Rezultat se vidi na slici 6.14.

$$\begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 12 & 13 & 0 \\ 2 & 0 & 0 & 0 & 24 \\ 3 & 0 & 32 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 \end{array} \qquad \begin{array}{c|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 0 & 2 & 3 & 0 \\ 2 & 0 & 0 & 0 & 4 \\ 3 & 0 & 2 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 \end{array}$$

$$\mathbf{L}^{(1)} \qquad\qquad \mathbf{l}$$

Slika 6.14. Modificirana latinska i reducirana latinska matrica za definicijski par (1,4)

Na taj način su završene točke a) i b) iz algoritma latinske kompozicije, pa se prelazi na korak c). Na presjeku retka 1 i stupca 4 provjerava se postojanje minimalnog puta dužine 1. Taj bi put direktno spajao čvorove definicijskog para. Kao što se vidi sa slike 6.14. element matrice (1,4) ima vrijednost 0, što znači da ne postoji direktna veza između ta dva čvora, odnosno da ne postoji minimalni put dužine 1. Prema točki d) algoritma treba izvršiti množenje latinske i reducirane latinske matrice. Rezultat množenja te dvije matrice je prikazan na slici 6.15.

$$\underset{L^{(1)}}{\begin{bmatrix} 0 & 12 & 13 & 0 \\ 0 & 0 & 0 & 24 \\ 0 & 32 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}} \times \underset{l}{\begin{bmatrix} 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{L^{(2)}}{\begin{bmatrix} 0 & 132 & 0 & 124 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 324 \\ 0 & 0 & 0 & 0 \end{bmatrix}}$$

Slika 6.15. Množenje latinske i reducirane latinske matrice

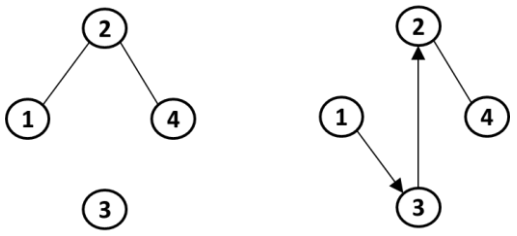
Na paru (1,4) rezultirajuće matrice $\boldsymbol{L^{(2)}}$ nalazi se podataka '124' što označava da se u strukturi nalazi jedan minimalni put dužine 2.

Sada dolazi na red točka g) algoritma, što je prikazano na slici 6.16. U tom koraku se množi matrica $\boldsymbol{L^{(2)}}$ s reduciranom latinskom matricom $\boldsymbol{l}$.

$$\underset{L^{(2)}}{\begin{bmatrix} 0 & 132 & 0 & 124 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 324 \\ 0 & 0 & 0 & 0 \end{bmatrix}} \times \underset{l}{\begin{bmatrix} 0 & 2 & 3 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}} = \underset{L^{(3)}}{\begin{bmatrix} 0 & 0 & 0 & 1324 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}$$

Slika 6.16. Množenje rezultirajuće latinske matrice $\boldsymbol{L^{(2)}}$ s reduciranom matricom $\boldsymbol{l}$

Kao što se vidi na slici 6.16. element matrice (1,4) ima vrijednost '1324'. Označava put dužine 3. To je kraj rada algoritma jer u danom primjeru ukupni broj objekata u sistemu je n=4, što znači da put može biti naviše dužine 3 (n-1). Grafički prikaz pronađenih putova za primjer prikazan je na slici 6.17.



Slika 6.17. Grafički prikaz putova kroz zadanu strukturu

7. RIZIK STRUKTURIRANIH INFORMACIJSKIH SISTEMA

Informacijski sistemi mogu se prikazati kao strukturirani, isto kao i svaki drugi složeni sistem. Kod informacijskog sistema su evidentne ulazne i izlazne točke između kojih se nalazi u pravilu veliki broj objekata koji učestvuju u obavljanju zadanih funkcija.

U poglavlju 6. su prikazani osnovi teorije struktura sistema, odnosno teoretske osnove ponašanja sistema koji se može prikazati kao struktura objekata. Za svaki sistem, pa tako i informacijski su važna dva stanja: sistem je ispravan i obavlja sve svoje funkcije kako je planirano, te stanje neispravnosti, kada sistem ne obavlja sve svoje funkcije u skladu s planom. Eventualna prelazna stanja, kada sistem djelomično radi, odnosno djelomično obavlja svoje funkcije neće se posebno tretirati jer se pod ispravnošću kao što je rečeno pretpostavlja u potpunosti obavljanje svih zadanih funkcija.

Informacijski sistem se prema ranije iznesenom sastoji od niza imovine (dobara), odnosno objekata kojima se osigurava obavljanje njegove funkcije. Da bi se osiguralo funkcioniranje sistema za obavljanje svoje funkcije nužno je osigurati funkcionalnu ispravnost svih objekata, odnosno imovine informacijskog sistema. Međutim, to je samo s točke gledišta funkcionalne ispravnosti u najužem smislu riječi. Pored takve funkcionalnosti, informacijski sistem mora osigurati i karakteristike informacije, i to: tajnost, cjelovitost i dostupnost (C-I-A). Zbog toga se pored standardnih funkcija informacijskog sistema kao što su generiranje informacije, njihova obrada, prijenos, arhiviranje, isporuka korisnicima, itd. za svaki informacijski sistem mora uključiti i dodatne tri funkcije: osiguranje tajnosti informacija, osiguranje cjelovitosti informacija i osiguranje dostupnosti informacijama. O tome je već govoreno u poglavlju 4.

Kada se kod bilo kakve analize, audita ili neke druge ocjene stanja informacijskog sistema želi dati sud o njemu i njegovoj funkcionalnosti koriste se razne metode i tehnike, kao i načini i oblici izvještavanja. No, ne postoji neka općenito prihvaćena metodologija koja daje konačnu ocjenu u obliku nekog broja pomoću kojega je moguće zaključiti na kojem nivou se nalazi informacijski sistem po pitanju neke karakteristike.

Primjenom metodologija prikazanih u ISO 27005 [6], te prikazanim procesom implementacije ISMS u ISM 27001 [2] problem osiguranja informacijske sigurnosti provodi se na temelju procjene rizika i to za svaku imovinu unutar informacijskog sistema. Ta procjena rizika se praktički ograničava na pojedinu imovinu, odnosno objekte informacijskog sistema, ne vodeći brigu od njihovom međusobnom djelovanju i cjelini sistema. Zbog toga, sama procjena rizika ne kaže u biti objektivno ništa o informacijskom sistemu, već samo o stanju rizika za pojedine objekte, odnosno imovinu.

Prelaskom na promatranje informacijskog sistema kao složenog od niza podsistema i objekata problem se može prikazati u formi složene strukture istih. U tom slučaju se nakon analize

pojedinih komponenti sistema konačna riječ daje ocjena rizika cjelokupnog informacijskog sistema. Analizom strukture i njene forme može se pokazati da ona samo po sebi može znatno uticati na sveukupni rizik informacijskog sistema, te da se izmjenom samo strukture može doći do povoljnijeg rješenja od implementacije samo sigurnosnih protumjera.

Za takvu analizu značaja strukture informacijskog sistema na ukupni rizik pretpostavlja se slijedeće:

a) Svaki objekt informacijskog sistema, odnosno imovina može biti u ispravnom i neispravnom stanju. U kontekstu ove teme se smatra da je ispravno stanje kada nije došlo do realizacije rizika. U koliko dođe do realizacije rizika, odnosno na određenoj imovini ona prelazi u neispravno stanje. Realizacija rizika se smatra da je prijetnja iskoristila ranjivost imovine i izazvala određene posljedice – štetu.

b) Svaka grana ima svoju veličinu rizika, odnosno vjerojatnost realizacije. Pri analizi se zanemaruje posljedica, već se smatra da realizacija kombinacije prijetnja-ranjivost predstavlja neispravno stanje. U kontekstu prikaza u poglavlju 5. U razmatranje će se uzimati veličina vjerojatnosti pojave rizika

c) Kako stanje objekta može biti ispravno ili neispravno, onda vjerojatnost ispravnosti objekta iznosi (1-*vjerojatnost rizika*), odnosno vrijedi relacija:

$$W = 1 - P \qquad (7.1)$$

Gdje su:

W = težina grane strukture, odnosno vjerojatnost ispravnosti imovine

P = vjerojatnost pojave rizika

U daljnjem razmatranju će se koristiti pojam težine grane strukture

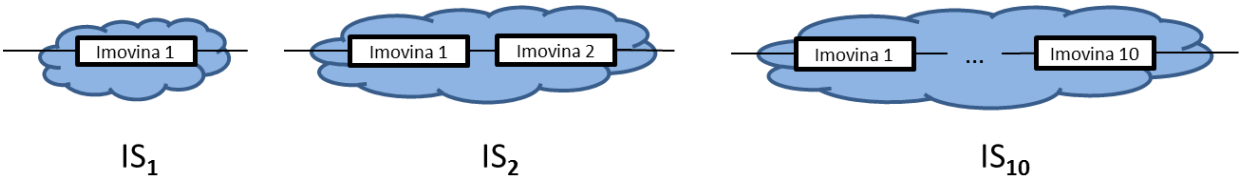
7.1. ANALIZA SERIJSKE STRUKTURE IS

Složena struktura od serijske veze objekata prikazana na slici 6.6 predstavlja situaciju u kojoj se informacijski sistem sastoji od n objekata koji su spojenu jedan iza drugoga. Funkcionalnost takvog informacijskog sistema je određena funkcionalnošću svih objekata. U slučaju gubitka funkcije jednog objekta, cijeli informacijski sistem u tom slučaju više ne funkcionira, pa prelazi u neispravno stanje.

Strukturna funkcija ovakvog informacijskog sistema je dana s relacijom (6.9).

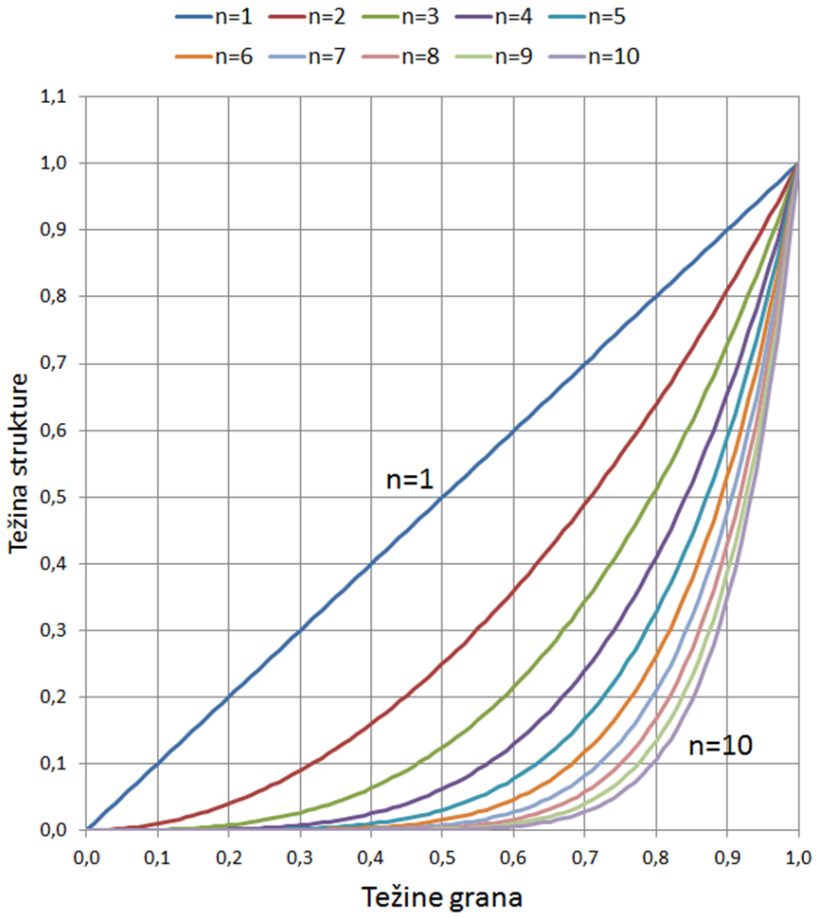
Analiza serijske veze objekata u informacijskom sistemu će se provesti uz pretpostavku da se težina grane strukture $\boldsymbol{W}$ kreće u granicama od 0 – 1, odnosno u skladu s relacijom (7.1) rizik za granu kojoj pripada ta imovina u granicama 1 – 0.

Uz to promatra se situacija kada u informacijskom sistemu postoji samo jedna serijska grana sa objektima od 1 do 10. Ilustracija takvih informacijskih sistema je prikazana na slici 7.1.



Slika 7.1. Primjeri informacijskih sistema samo sa serijskom imovinom u strukturi

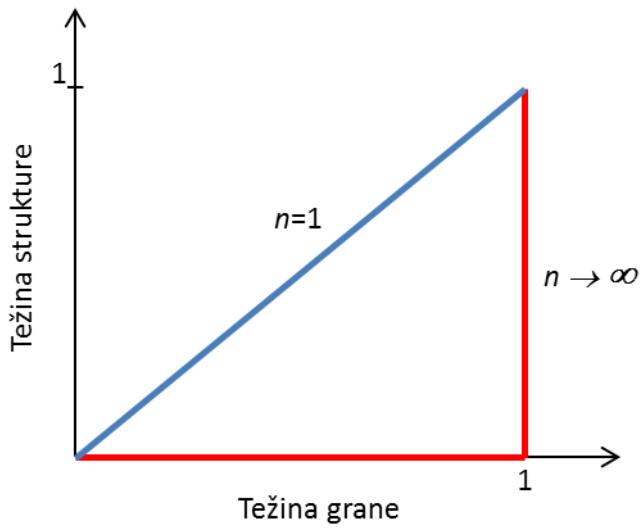
Primjenom relacije (6.9) dobivaju se rezultati prikazani na slici 7.2. Rezultati izračunavanja serijske strukture za dijagram na slici 7.2. prikazani su u prilogu 11.6.



Slika 7.2. Grafički prikaz težine serijske strukture – sve grane imaju istu težinu

Na slici se uočava da u slučaju samo jedne grane u strukturi, odnosno samo jednog objekta u informacijskom sistemu graf strukturne funkcije je pravac (n=1). U koliko se broj serijskih grana povećava dobiva se graf koji pokazuje opadanje težine čitave strukture. Granični slučajevi serijske strukture su prikazani na slici 7.3.

Sa slike se može vidjeti da za granični slučaj kada $n \rightarrow \infty$ dobiva se step funkcija koja ima vrijednost 0 za sve težine grana manje od 1. Kada je težina svih grana i strukturi jednaka 1, tada i težina strukture poprima vrijednost 1.



Slika 7.3. Granični slučajevi serijske strukture

Zaključak 7.1: u informacijskom sistemu koji ima samo serijsku granu u kojoj se nalazi određeni broj objekata, težina strukture teži prema 0 s porastom broja grana u strukturi.

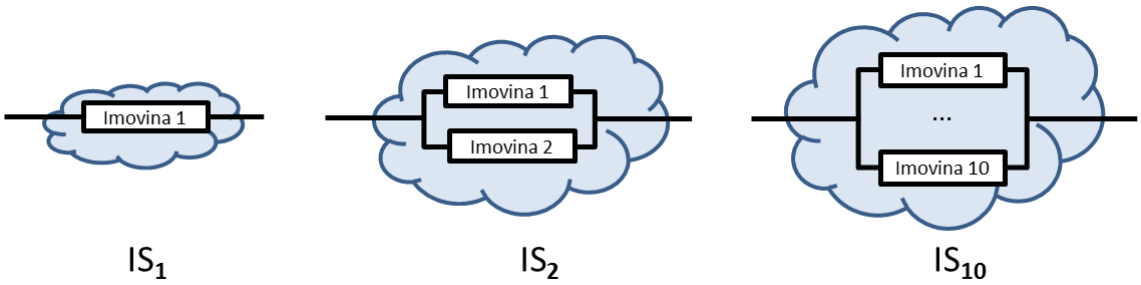
Kada se to prevede na jezik rizika i stabilnosti informacijskog sistema to znači, da bez obzira na smanjivanje rizika pojedinih imovina u serijskom informacijskom sistemu, cijeli sistem teži ka nestabilnosti, odnosno bitnom povećanju rizika cijelog sistema.

7.2. ANALIZA PARALELNE STRUKTURE IS

Informacijski sistem kao složena struktura od samo paralelnih grana, odnosno informacijski sistem kojemu su svi objekti koji ga čine u funkcionalnom smislu vezani u paralelu naziva se paralelni informacijski sistem. Osnovna shema takvog paralelne strukture sistema prikazana je na slici 6.7. Kod paralelne strukture se funkcionalnost sistema gubi ako nisu u funkciji svi objekti koji ga čine. U koliko se izgubi funkcionalnost n-1 objekata, paralelni informacijski sistem i dalje funkcionira, odnosno nalazi se u ispravnom stanju.

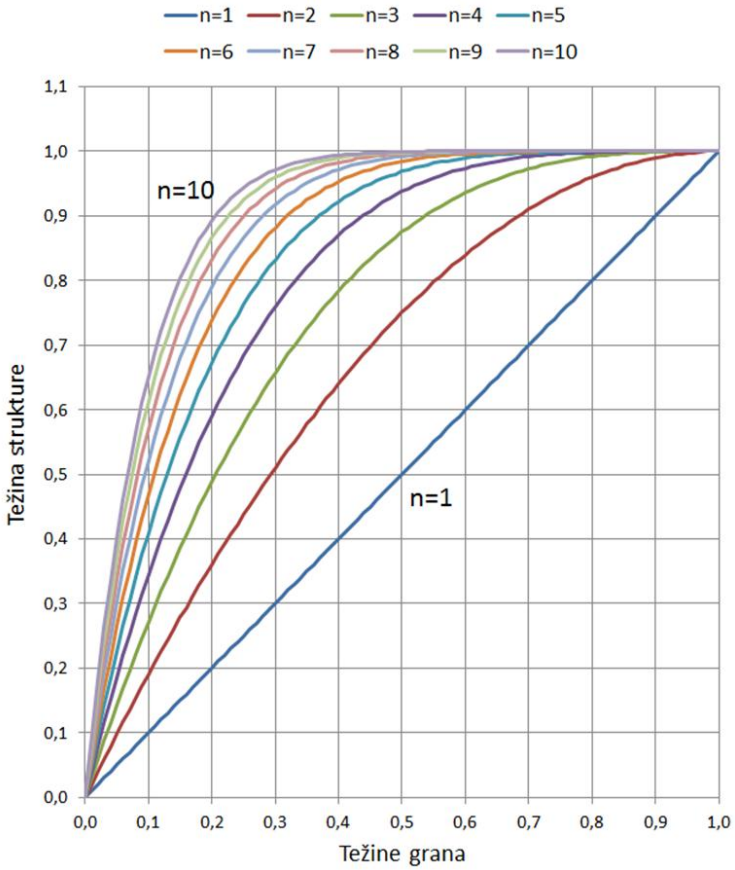
Strukturna funkcija ovakvog informacijskog sistema je dana s relacijom (6.13).

Analiza paralelne veze objekata u informacijskom sistemu će se provesti uz iste pretpostavke kao i za serijsku strukturu: težina svih grana strukture $\boldsymbol{W}$ kreće u granicama od 0 – 1, odnosno u skladu s relacijom (7.1) rizik za granu kojoj pripada ta imovina u granicama 1 – 0. Ilustracija informacijskih sistema koji su analizirani je prikazana na slici 7.4.



Slika 7.4. primjeri informacijskih sistema samo s paralelnim granama u strukturi

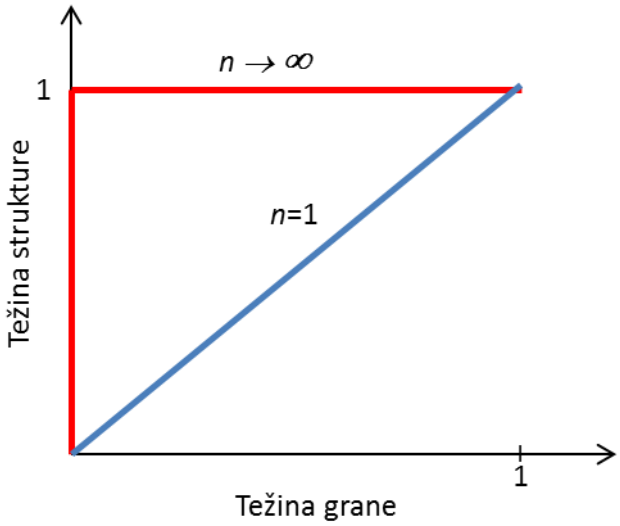
Nakon što se provede analiza u skladu s relacijom (6.13) rezultati su prikazani na slici 7.5 gdje se vidi odnos težine cijele strukture i težine pojedinih grana u zavisnosti od broja paralelnih grana u strukturi informacijskog sistema. Rezultati izračunavanja paralelne strukture prikazani na slici 7.5. nalaze se u tablici u prilogu 11.7.



Slika 7.5. Grafički prikaz težine paralelne strukture – sve grane imaju istu težinu

Može se primijetiti da za slučaj kada je n=1 pojavljuje se ista situacija kao i kod serijske strukture. Kao što se vidi, za n=1 težina strukture je jednaka težini grane, pa se u tom slučaju se ne govori ni o serijskoj ni o paralelnoj strukturi, odnosno to tada nije bitno.

Kako raste broj paralelnih grana u strukturi, tako i težina strukture sve više raste. Za granični slučaj, kada $n \rightarrow \infty$ težina strukture prelazi u step funkciju u kojoj se za težinsku vrijednost svih grana jednaku 0 dobiva i težinska vrijednost strukture jednaka 0. Ako je težinska vrijednost pojedinih grana veća od 0, tada se u paralelnoj strukturi dobiva težinska vrijednost strukture 1 ako $n \rightarrow \infty$. Na slici 7.6. su prikazani granični slučajevi paralelne strukture za slučajeve kada je n=1 i $n \rightarrow \infty$.



Slika 7.6. Granični slučajevi paralelne strukture

Zaključak 7.2: u informacijskom sistemu koji ima samo paralelne grane u kojoj se nalazi samo po jedan objekt, težina strukture teži prema 1 s porastom broja grana u strukturi.

Za problem rizika u takvim trivijalnim paralelnim informacijskim sistemima se može reći da u koliko je rizik u svakoj grani manji od 1, tada će rizik ukupnog informacijskog sistema težiti ka 0 ako broj grana teži prema ∞.

7.3. ANALIZA SLOŽENE NEORIJENTIRANE STRUKTURE IS

Složena struktura informacijskog sistema je ona koja ima kombinaciju serijske i paralelne grane. Pretpostavka je da se u jednoj grani nalazi samo jedan objekt. U koliko ih ima više tada je to serijska grana s tim brojem objekata. Za svaku strukturu informacijskog sistema bitni su slijedeći parametri:

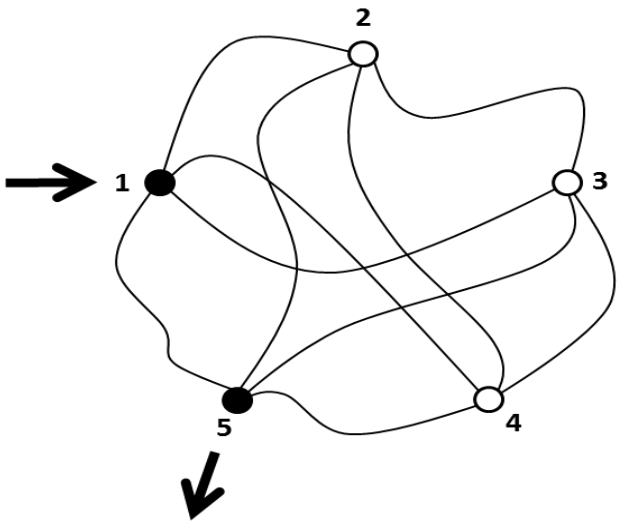
- Broj čvorova,
- Ulazni i izlazni čvor (karakteristični čvorovi),
- Veza između čvorova, odnosno grane među tim čvorovima,
- Orijentacija veza među čvorovima, te
- Težina pojedinih grana strukture.

Poznavanjem svih tih elemenata može se reći da je u potpunosti definirana struktura informacijskog sistema.

Za početnu analizu uzet će se najopćenitiji slučaj sa slijedećim parametrima:

- Broj čvorova = 5
- Ulazni čvor i izlazni čvorovi, u skladu s napomenom u 6.7, su 1 i 5 respektivni
- Veza, odnosno grane strukture postoje između svih čvorova
- Graf strukture je neorijentiran, odnosno sve grane su dvosmjerne
- Težine pojedinih grana se definiraju od vrste do vrste analize.

Tako definirana struktura informacijskog sistema se može prikazati kao na slici 7.7.



Slika 7.7. Graf strukture informacijskog sistema za provedenu analizu.

Za dani primjer latinska kompozicija ima oblik prikazan na slici 7.8.

$$\begin{bmatrix} 0 & 12 & 13 & 14 & 15 \\ 21 & 0 & 23 & 24 & 25 \\ 31 & 32 & 0 & 34 & 35 \\ 41 & 42 & 43 & 0 & 45 \\ 51 & 52 & 53 & 54 & 0 \end{bmatrix}$$

Slika 7.8. Latinska matrica za strukturu na slici 7.7.

Iz ranije iznesenog, u svaki element matrice na slici 7.8. sadrži opis veze između dva čvora. Kako je struktura sa 5 čvorova, tada je i matrica dimenzije 5x5. Tako npr. član matrice (1,2) ima vrijednost '12' što označava da postoji veza između čvora 1 i čvora 2 i to u smjeru od 1 prema 2. Prema primjeru, član matrice (2,1) ima vrijednost '21' što znači da između čvora 2 i 1 postoji veza i to u smjeru od 2 prema 1. Svi ostali članovi matrice na slici 7.8. su na isti

način određeni. Član matrice (1,5) je posebno označen samo kao naznaka da je to karakteristični par čvorova, odnosno ulazni i izlazni par. Dijagonala matrice na slici 7.8. ima vrijednost 0 jer nije dozvoljena situacija u kojoj su ulazni i izlazni čvor jedne grane isti.

Na temelju te latinske matrice i algoritma iz 6.7.1 dobiva se reducirana latinska matrica. Rezultat izrade reducirane latinske matrice prikazan je na slici 7.9.

$$\begin{bmatrix} 0 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 \\ 1 & 2 & 3 & 0 & 5 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

Slika 7.9. Reducirana latinska matrica za graf na slici 7.7.

Prema algoritmu i definiciji zadatka nužno je odrediti latinsku matricu i reduciranu latinsku matricu za slučaj poznatih ulaznih i izlaznih čvorova, odnosno karakterističan par (1,5). Te se matrice postižu tako da se u kolonu 1 i red 5 upišu iznosi 0. Rezultat latinske i reducirane latinske matrice za karakterističan par u zadanom primjeru prikazani su na slici 7.10.

$$\begin{bmatrix} 0 & 12 & 13 & 14 & 15 \\ 0 & 0 & 23 & 24 & 25 \\ 0 & 32 & 0 & 34 & 35 \\ 0 & 42 & 43 & 0 & 45 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 2 & 3 & 4 & 5 \\ 0 & 0 & 3 & 4 & 5 \\ 0 & 2 & 0 & 4 & 5 \\ 0 & 2 & 3 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Slika 7.10. Latinska matrica i reducirana latinska matrica za karakteristični par (1,5)

Analizom strukture informacijskog sistema prikazanog na slici 7.7. i prema algoritmu za pronalaženje putova može se pokazati da su postoje putovi prikazani u tablici 7.1. Iz tablice se vidi da ima ukupno 16 putova između čvora 1 i 5.

Nakon ove analize nužno je provesti i analizu težine strukture na temelju težina pojedinih grana.

Za potrebe donošenja odgovarajućih zaključaka o ponašanju ovakve složene strukture provest će se nekoliko analiza koje su prikazane u nastavku.

Tablica 7.1. Lista i broj putova za primjer sa slike 7.7.

Dužina puta	Čvorovi puta
1	15
2	125
2	135
2	145
3	1325
3	1425
3	1235
3	1435
3	1245
3	1345
4	14325
4	13425
4	14235
4	12435
4	13245
4	12345

Dužina puta	Broj puteva
1	1
2	3
3	6
4	6

7.3.1. Analiza složene strukture IS sa jednakim težinama u svim granama

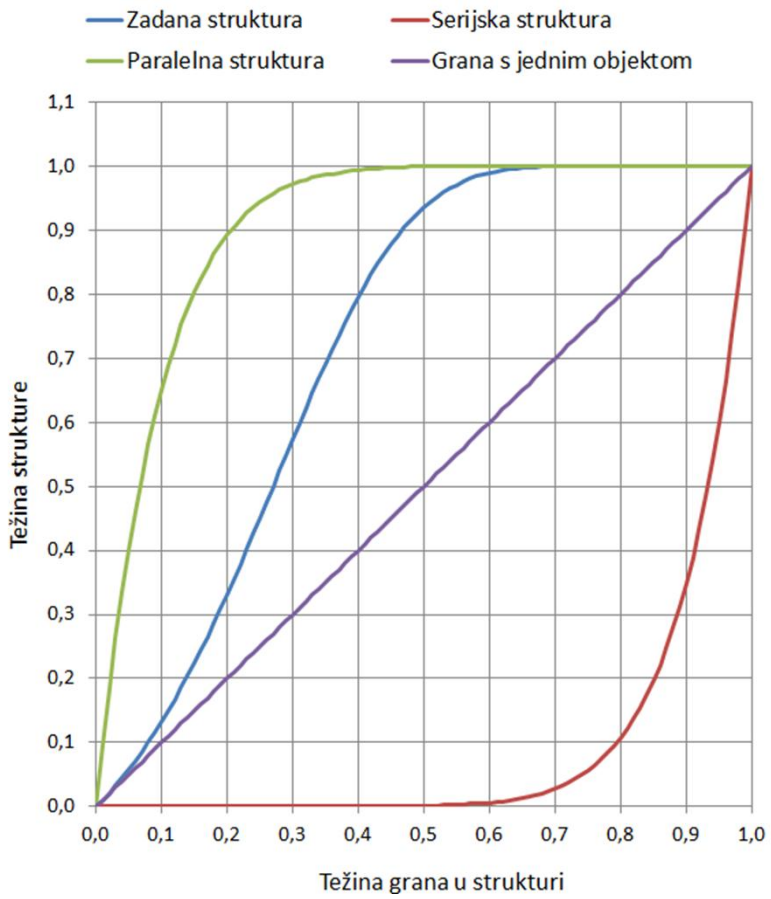
Prva analiza složene strukture sa slike 7.7. provest će se uz pretpostavku da sve grane u strukturi imaju istu težinu. Svakoj grani je pridruživana jedna težina pa izračunavana ukupna težina strukture. Za usporedbu su prikazani i rezultati serijske i paralelne strukture s istim brojem grana. Na slici 7.11. prikazani su grafički rezultati proračuna težine ukupne strukture u zavisnosti težina u svim granama.

Za razliku od trivijalnih struktura u kojima su sve grane ili serijske ili paralelne pa imaju dijagram ili konkavni ili konveksan, kod složene struktura u primjeru dijagram poprima oblik slova 'S'. Zato što u danom primjeru prevladavaju paralelne grane onda se vrijednosti ne spuštaju ispod pravca koji označava strukturu sa samo jednom granom.

Za primjer može se pogledati slučaj kada sve grane imaju težinu 0,5 tada i struktura s jednom granom ima težinu 0,5. Međutim, složena struktura iz primjera ima težinu 0,936. Za razliku od nje serijska struktura u tom slučaju ima težinu 0,001 a paralelna 0,999. Ako to prevedemo na pojam rizika može se reći slijedeće na temelju relacije (7.1):

Ako imamo zadani primjer u kojem svi objekti u granama imaju vjerojatnost rizika 0,5 tada zadana struktura ima vjerojatnost rizika 0,064. Serijska struktura bi imala vjerojatnost rizika 0,999 a paralelna struktura 0,001.

Rezultati proračuna prikazanih na slici 7.11. nalaze se u tablici u prilogu 11.8.



Slika 7.11. Dijagrami proračuna težine struktura u zavisnosti od težina grane

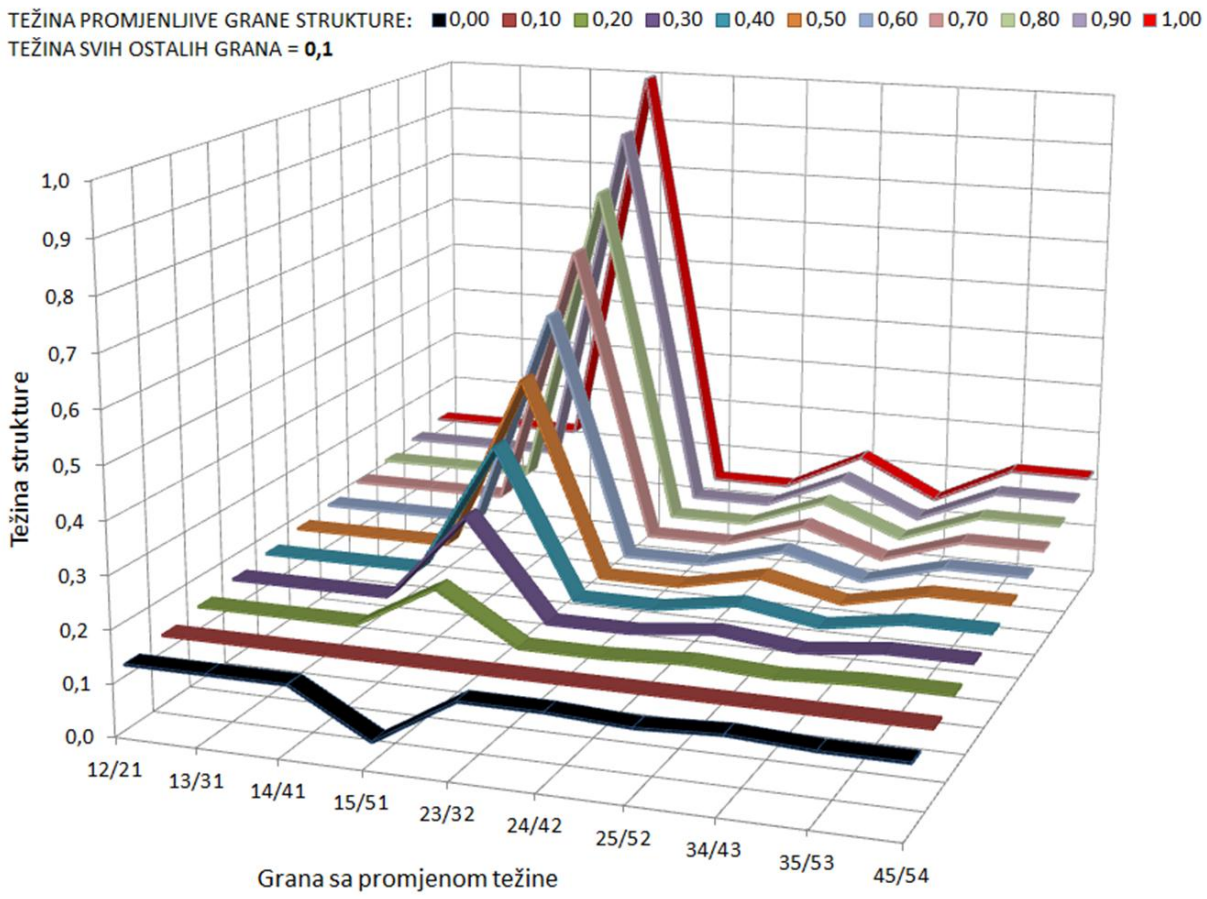
7.3.2. Analiza složene strukture IS sa promjenljivom težinom jedne grane

U ovoj analizi se pretpostavlja da je sve grane imaju istu težinu, a jednoj grani se mijenja težina u granicama 0 – 1. Rezultati analize su prikazani u tablici 7.2.

Tablica 7.2. Rezultati analize za težinu svih grana = 0,1 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,000	0,100	0,200	0,300	0,400	0,500	0,600	0,700	0,800	0,900	1,000
	TEŽINA ČITAVE MREŽE										
12/21	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227
13/31	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227
14/41	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227
15/51	0,036	0,132	0,229	0,325	0,422	0,518	0,614	0,711	0,807	0,904	1,000
23/32	0,130	0,132	0,135	0,137	0,139	0,141	0,143	0,145	0,147	0,149	0,151
24/42	0,130	0,132	0,135	0,137	0,139	0,141	0,143	0,145	0,147	0,149	0,151
25/52	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227
34/43	0,130	0,132	0,135	0,137	0,139	0,141	0,143	0,145	0,147	0,149	0,151
35/53	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227
45/54	0,122	0,132	0,143	0,154	0,164	0,175	0,185	0,196	0,206	0,217	0,227

Grafički prikaz te analize se nalazi na slici 7.12.



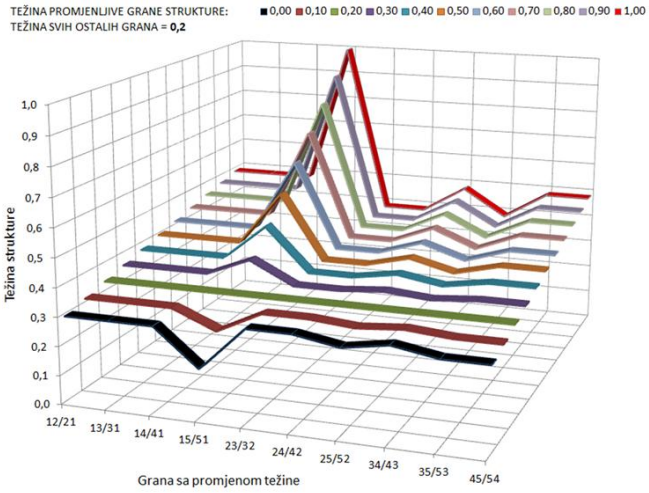
Slika 7.12. Analiza strukture gdje jedna grana mijenja težinu, a sve ostale imaju težinu 0,1

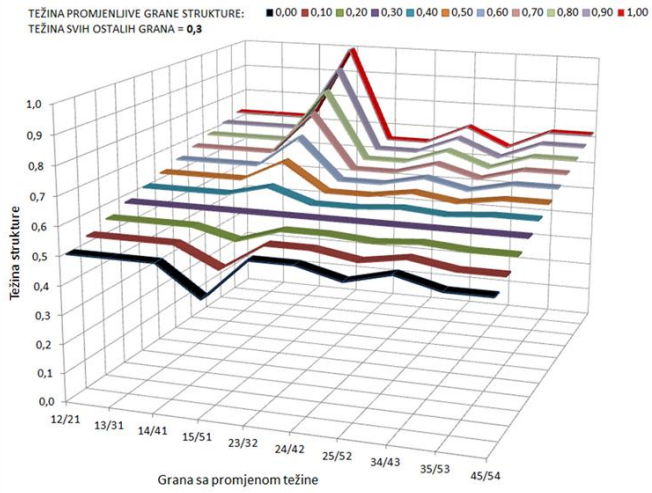
Rezultati ove analize pokazuju prirodu strukture vezanu za njen izgled. Kada je težina svih grana jednaka 0,1, a grana koja direktno veže ulazni i izlazni čvor ima težinu 0 (vjerojatnost rizika 1), odnosno kada je ta grana u prekidu cijeloj strukturi pada težina na iznos 0,036 što je znatno manje od težine bilo koje druge grane (a koja iznosi 0,1). S druge strane, ako direktna grana koja spaja ulaz i izlaz ima težinu 1, tada bez obzira na težine ostalih grana, čitava struktura ima težinu 1 (odnosno vjerojatnost rizika 0). Logički, direktna grana koja spaja ulazni i izlazni čvor u kojoj ima samo jedan objekt najviše utiče na težinu strukture.

Za ilustraciju napravljena je ista analiza, ali za slučaj da je težina svih grana 0,1 i 0,3 uz promjenu težina samo jedne grane. Dijagrami promjene težine strukture za ta slučajeve su prikazani na slici 7.13.

Sa slike se može vidjeti da se strukturi brzo raste ukupna težina, ako se malo povećava težina njenih grana. To je u skladu i s dijagramom prikazanim na slici 7.11.

Tabelarni podaci za dijagrame na slici 7.13 su prikazani u tablici 7.2 i tablici 7.3.





Slika 7.13. Analiza zadane strukture za slučaj da sve grane imaju težinu 0,2 i 0,3. Mijenja se težina samo jedne grane

Tablica 7.3. Rezultati analize za težinu svih grana = 0,2 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12/21	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485
13/31	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485
14/41	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485
15/51	0,165	0,248	0,332	0,415	0,499	0,582	0,666	0,749	0,833	0,916	1,000
23/32	0,317	0,324	0,332	0,339	0,347	0,354	0,362	0,369	0,376	0,383	0,390
24/42	0,317	0,324	0,332	0,339	0,347	0,354	0,362	0,369	0,376	0,383	0,390
25/52	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485
34/43	0,317	0,324	0,332	0,339	0,347	0,354	0,362	0,369	0,376	0,383	0,390
35/53	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485
45/54	0,291	0,311	0,332	0,352	0,372	0,392	0,411	0,430	0,449	0,467	0,485

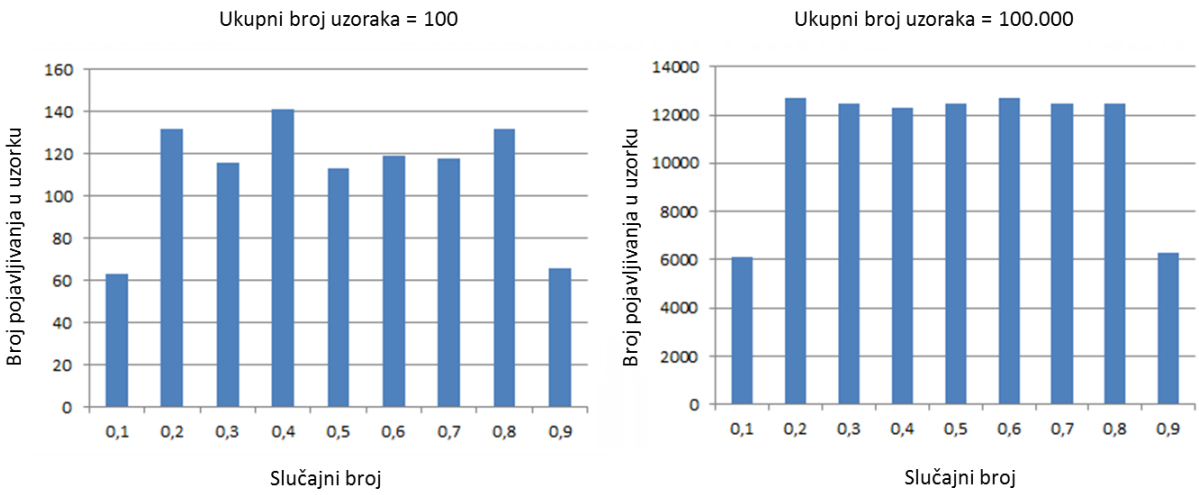
Tablica 7.4. Rezultati analize za težinu svih grana = 0,3 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12/21	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724
13/31	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724
14/41	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724
15/51	0,391	0,452	0,513	0,574	0,635	0,696	0,756	0,817	0,878	0,939	1,000
23/32	0,535	0,548	0,561	0,574	0,586	0,598	0,610	0,622	0,633	0,644	0,655
24/42	0,535	0,548	0,561	0,574	0,586	0,598	0,610	0,622	0,633	0,644	0,655
25/52	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724
34/43	0,535	0,548	0,561	0,574	0,586	0,598	0,610	0,622	0,633	0,644	0,655
35/53	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724
45/54	0,497	0,523	0,549	0,574	0,598	0,621	0,643	0,664	0,685	0,705	0,724

7.3.3. Analiza složene strukture IS sa slučajnim težinama u svim granama

U prethodnim slučajevima se u cilju analize pretpostavljali neki karakteristični podaci koji bi trebali pokazati prirodu ponašanja složene strukture informacijskog sistema. Međutim, u praksi se težine pojedinih grana, odnosno vjerojatnosti pojave rizika na pojedinim objektima koje čine ponašaju stohastički, odnosno ne postoji situacija u kojoj su težina svih grana jednake. Zato će se u ovoj točki provesti analiza zadane strukture sa slike 7.7. za slučaj da se u svim granama pojavljuju slučajne vrijednosti.

Kako se u ovoj analizi koristi generator slučajnih brojeva, izvršena je prvo kontrola ponašanja korištenih generatora. Kontrola rada generatora slučajnih brojeva je provedena tako da se pomoću histograma provjerio oblik distribucije generiranih slučajnih brojeva u granicama 0,1 do 0,9. Iz analize su isključeni brojevi 0 i 1 jer takve težine objektivno se ne pojavljuju u praksi. Na slici 7.14. su prikazane distribucije za generirani broj uzoraka slučajnih brojeva 100 i 100.000 .



Slika 7.14. Histogram generatora slučajnih brojeva korištenog u analizi

Iz slike 7.14. se može vidjeti da korišteni generator ima na već relativno malom uzorku približno uniformnu distribuciju, odnosno da nema grupiranja oko neke vrijednosti.

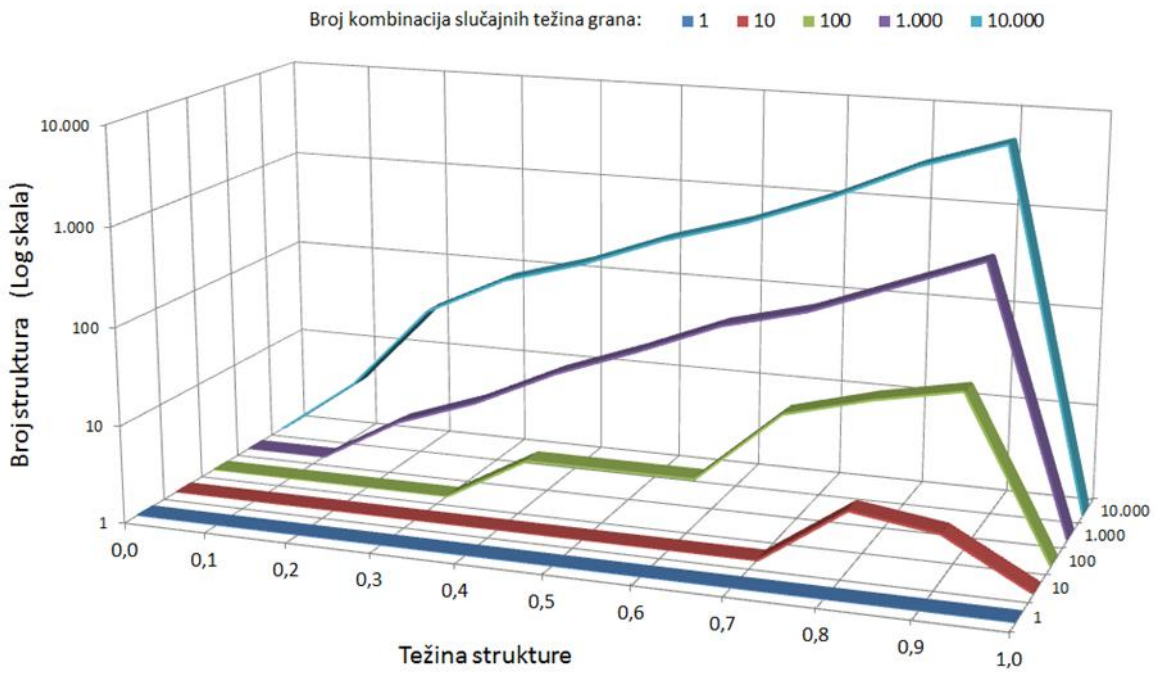
Metodologija analize slučajnih težina grana složene strukture informacijskog sistema je provedena na slijedeći način:

1) Korištena je struktura prikazana na slici 7.7.
2) Za zadanu strukturu se pomoću gore spomenutog generatora dobila težina svake grane
3) Analiza je provedena za zadanu strukturu za 1 set slučajnih težina, nakon toga za 10 setova sa slučajnim težinama, te na takav način za 100, 1.000 i 10.000 setova.
4) Nakon toga je izvršena analiza distribucije dobivenih ukupnih težina strukture.

Rezultati takve analize su prikazani u tablici 7.5. i na slici 7.15.

Tablica 7.5. Težine struktura za slučajne težine grana

BROJ ANALIZ. MREŽA	TEŽINE MREŽA										
	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
	BROJ MREŽA S UKUPNOM TEŽINOM										
1	0	0	0	0	0	0	0	1	0	0	0
10	0	0	0	0	0	1	1	1	4	3	0
100	0	0	1	1	3	3	3	17	29	43	0
1000	0	1	3	6	15	31	69	115	244	516	0
10000	1	4	31	80	142	297	534	1114	2680	5117	0



Slika 7.15. Distribucije struktura prema težinama za slučajne težine grana

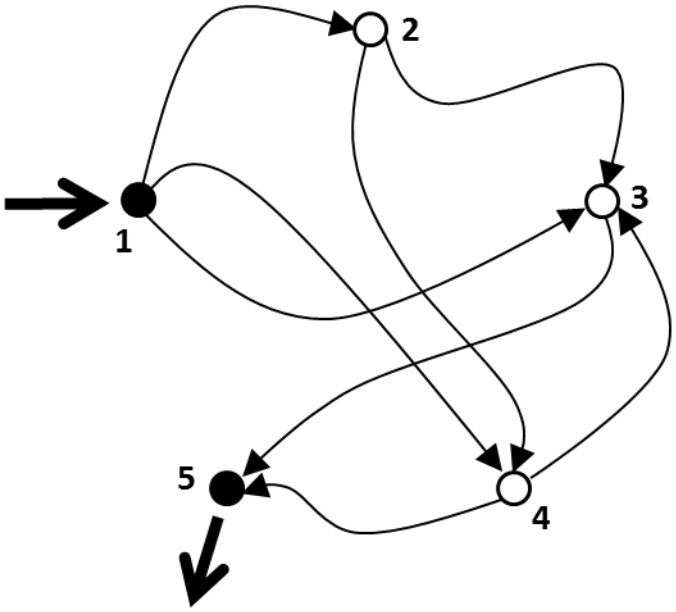
Iz dijagrama na slici 7.15., a još bolje iz tablice 7.5. se može vidjeti da uz slučajnu raspodjelu težina u pojedinim granama promatrane strukture sa slike 7.7. cjelokupna težina strukture se gomila oko većih vrijednosti sa maksimum oko 0,8 .

7.4. ANALIZA SLOŽENE ORIJENTIRANE STRUKTURE IS

7.4.1. Orijentirana struktura 1

Struktura koja je prikazana na slici 7.7. poslužila je za uvodno razmatranje i analizu stanja vezanih za odnose težina u pojedinim granama i samog oblika strukture. Kada se promatraju informacijski sistemi onda jedna takva neorijentirana struktura koja ima dvosmjerne veze između čvorova praktički ne postoji. Zato će se u ovom poglavlju provesti analiza jedne strukture koja je realno moguća, te pokazati na njoj odnose težina grana i ukupne težine strukture.

U tu svrhu zadaje se struktura prikazana na slici 7.16. Ovako zadana struktura ima pet čvorova. Ulazni je čvor 1, a izlazni čvor je 5. Ne postoji direktna veza, odnosno grana koja povezuje ulazni i izlazni čvor.



Slika 7.16. Primjer orijentirane strukture informacijskog sistema

Sve grane su orijentirane, odnosno usmjerene od jednog do drugog čvora. Smjer strelica pokazuje moguće putove kroz strukturu od ulaznog do izlaznog čvora.

Pripadna latinska matrica za strukturu sa slike 7.16. prikazana se ja slici 7.17.

$$\begin{bmatrix} 0 & 12 & 13 & 14 & 0 \\ 0 & 0 & 23 & 24 & 0 \\ 0 & 0 & 0 & 0 & 35 \\ 0 & 0 & 43 & 0 & 45 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Slika 7.17. Latinska matrica za strukturu na slici 7.16.

Za ovu latinsku matrica treba izraditi i reduciranu latinsku matricu. Ta reducirana latinska matrica je prikazana na slici 7.18.

$$\begin{bmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 3 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 3 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Slika 7.18. Reducirana latinska matrica za primjer strukture na slici 7.16.

Prema algoritmu za iznalaženje putova za strukturu potrebno je iz latinske i reducirane latinske matrice ukloniti vrijednosti koje pripadaju karakterističnom paru. U ovom primjeru je karakteristični par (1,5), a kako nema direktne veze između čvorova koji čine karakteristični par, te zbog orijentacije veza među ostalim čvorovima, već su prva kolona i peti red matrice na vrijednosti 0. Zbog toga ne treba ništa poduzimati u ovom koraku.

Pronalaženjem putova u zadanoj strukturi može se pokazati da ih ima ukupno 5 između čvorova 1 i 5. Lista putova u strukturi prikazana je u tablici 7.6.

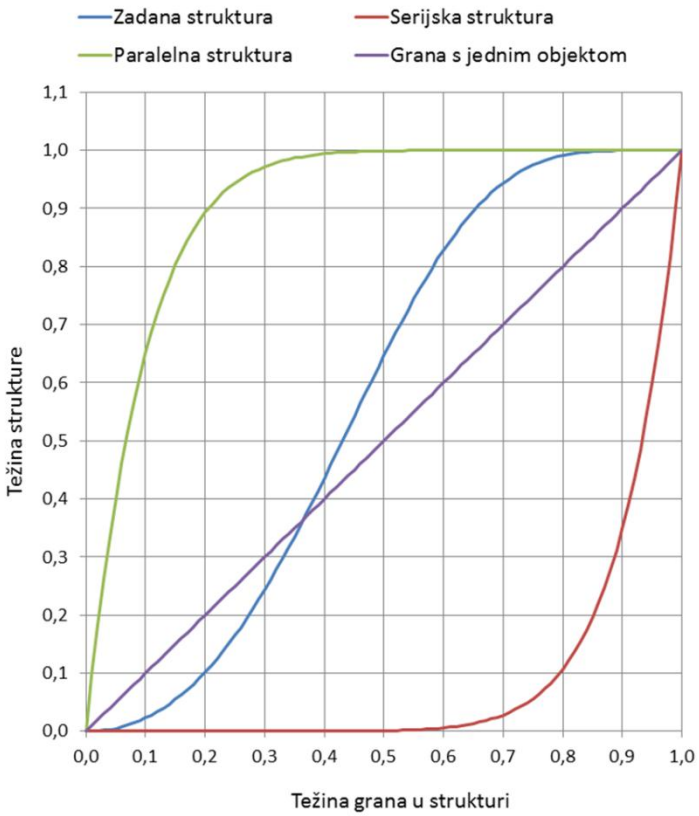
Tablica 7.6. Lista i broj putova za primjer sa slike 7.16.

Dužina puta	Čvorovi puta
1	
2	135
2	145
3	1235
3	1435
3	1245
4	12435

Dužina puta	Broj puteva
1	0
2	2
3	3
4	1

7.4.1.1. Analiza orijentirane strukture 1 sa jednakim težinama u granama

Ova analiza je provedena na ekvivalentan način kao što je za neorijentiranu strukturu to napravljeno u točki 7.3.1., s tom razlikom što u ovom slučaju korištena orijentirana struktura sa slike 7.16. Rezultati analize su prikazani u dijagramu na slici 7.19., a pripadni tabelarni rezultati na temelju kojih je napravljen dijagram su u prilogu11.9.

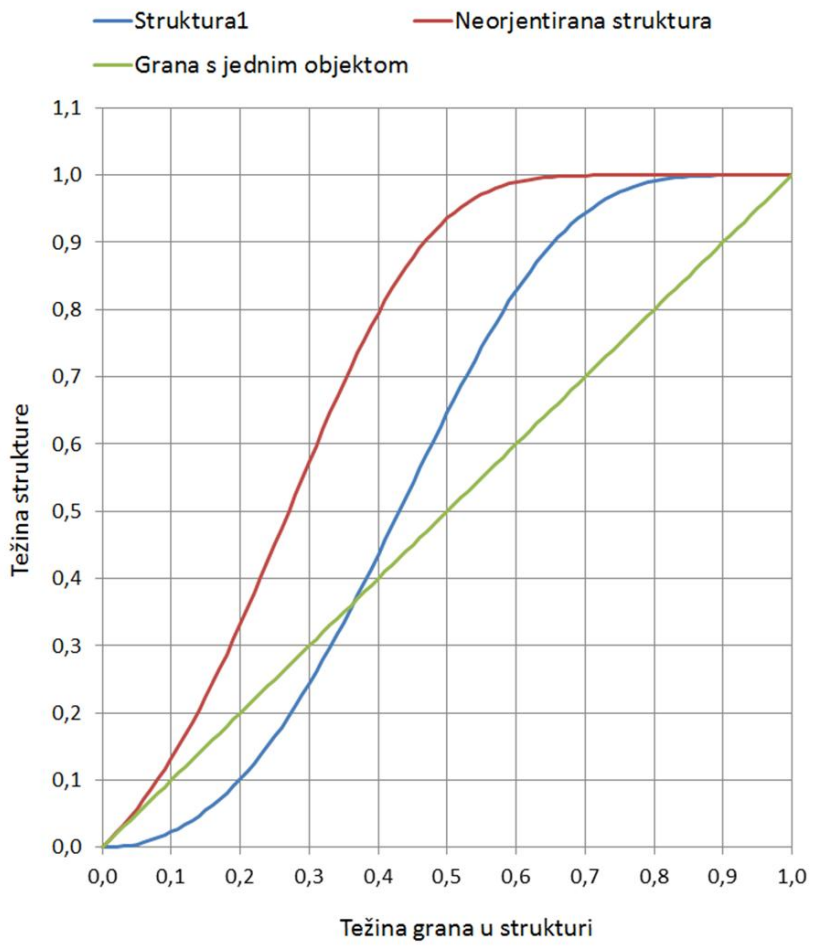


Slika 7.19. Dijagrami proračuna težine strukture u zavisnosti od težina grana

Usporedbom slike 7.11. za neorijentiranu strukturu i slike 7.19. koja se odnosi na orijentiranu strukturu 1 (sa slike 7.16.) može se uočiti bitna razlika u obliku dijagrama. Za bolju ilustraciju razlike na slici 7.20. je prikazano na istom dijagramu i graf za neorijentiranu i orijentiranu strukturu 1.

Na slici se može vidjeti da orijentirana struktura 1 sa slike 7.16. ima dijagram u obliku slova 'S' sa točkom infleksije. Neorijentirana struktura prikazana na slici 7.7. ima dijagram koji ne presijeca liniju grane koja ima samo jedan objekt. To znači da se neorijentirana struktura sa slike 7.7 ponaša kao paralelna struktura, a orijentira struktura sa slike 7.16. dijelom kao serijska, a dijelom kao paralelna struktura. Naravno da te osobine bitno zavise od same strukture.

Iz dijagrama se može zaključiti da se postizanjem težina u pojedinim granama preko težine koja određuje točku infleksije struktura svojom formom i orijentacijom grana „pojačava“ težinu. Do točke infleksije struktura „slabi“ svoju težinu u odnosu na težinu grana.



Slika 7.20. Dijagrami orijentirane strukture 1, neorijentirane strukture i jedne grane

7.4.1.2. Analiza orijentirane strukture 1 sa promjenljivom težinom jedne grane

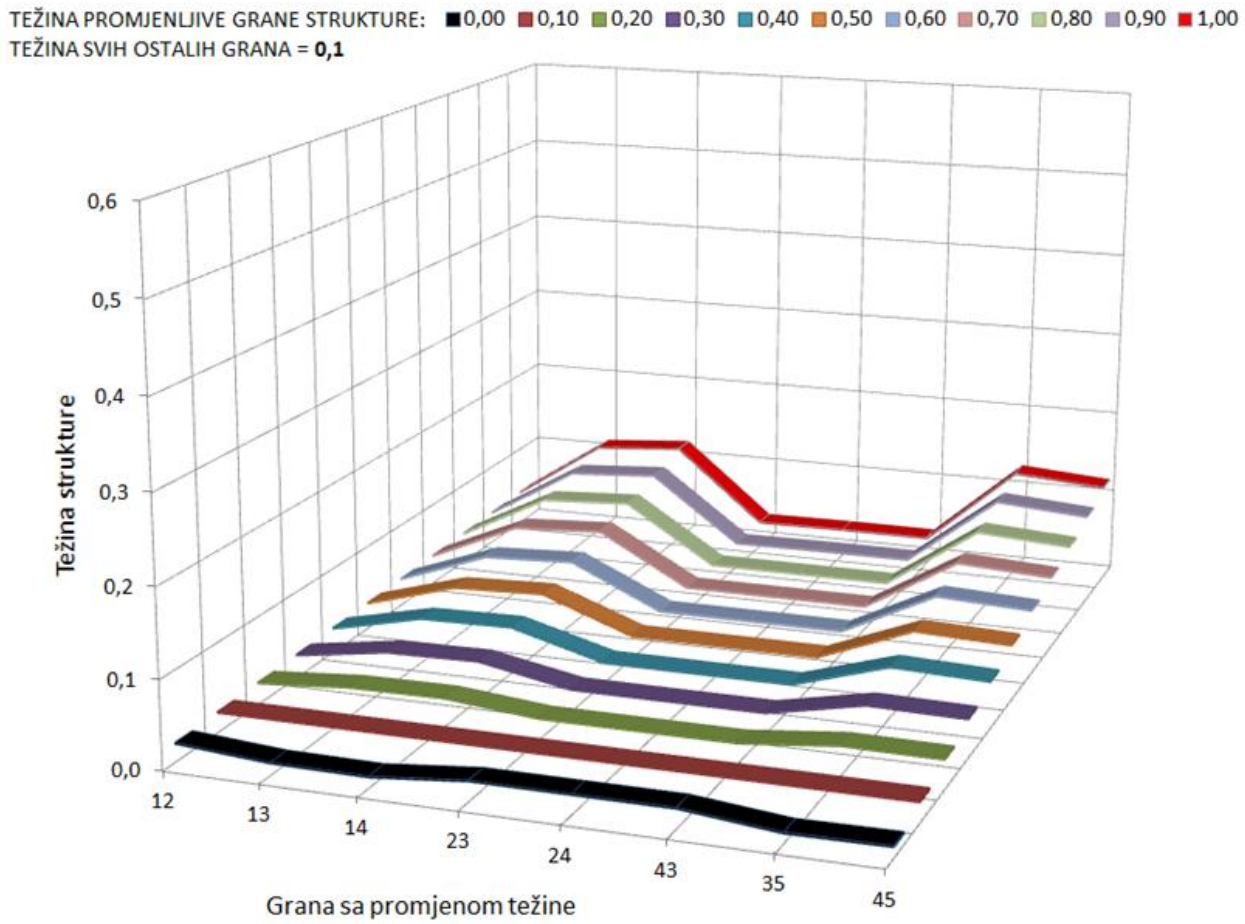
Kao i u primjeru točke 7.3.2. u ovom slučaju se za strukturu sa slike 7.16. postavljalo da sve grane imaju istu težinu, a jednoj grani se mijenjala težina. Dobiveni rezultati su prikazani u tablici 7.7.

Grafički prikaz rezultata iz tablice 7.7. prikazan je na slici 7.21. Za usporedbu s ekvivalentnom slikom 7.12. koja se odnosi neorijentiranu strukturu vidi se značajno odstupanje koje samo potvrđuje pravilo o utjecaju strukture na ukupnu težinu.

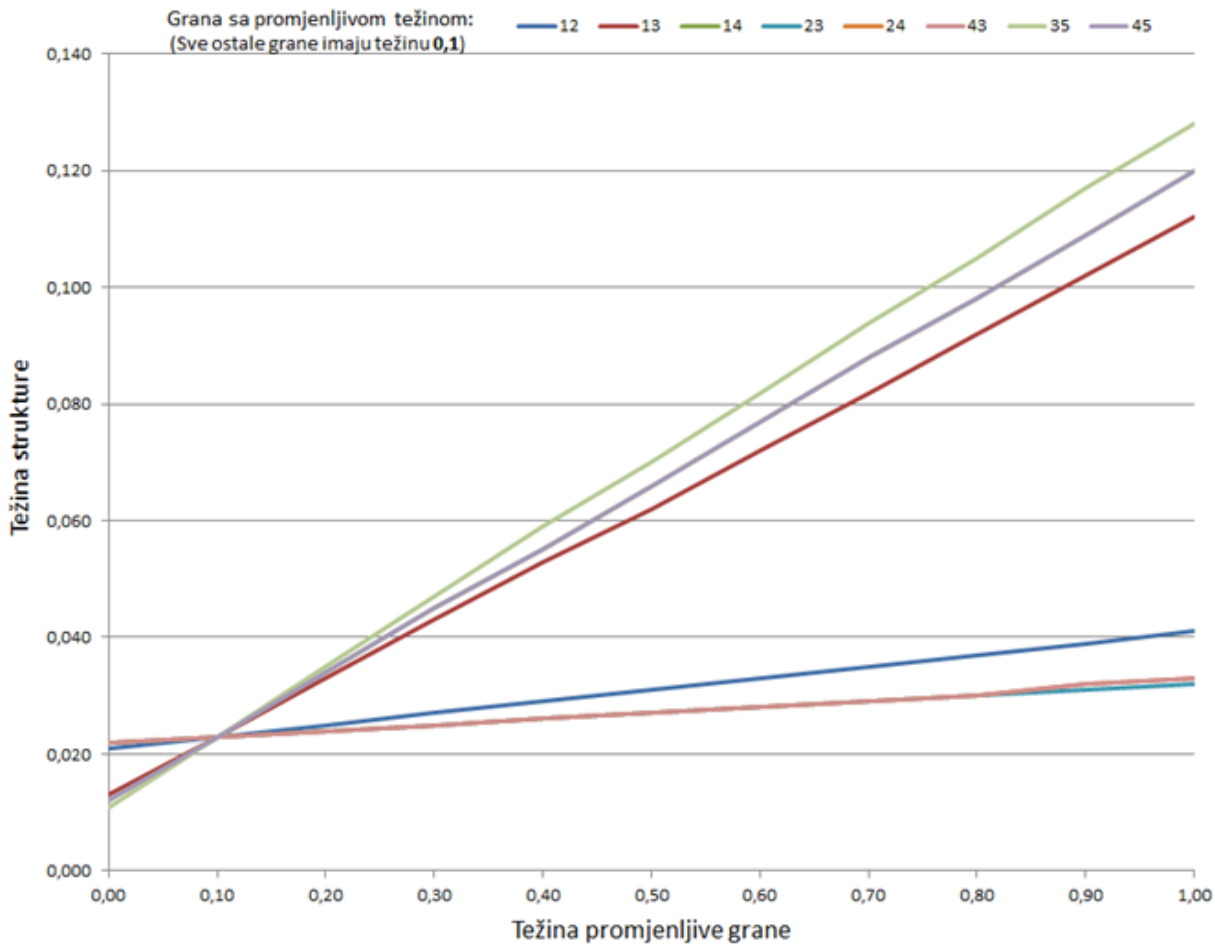
Kako je ova struktura sa slike 7.16. moguća u realnosti za informacijske sisteme u smislu orijentiranosti napravljena je i analiza ovisnosti strukture o težini promjenljive grane. Podaci korišteni za ovu analizu se također nalaze u tablici 7.7. Dijagram ovisnosti ukupne težine strukture o težini jedne promjenljive grane prikazan je na slici 7.22.

Tablica 7.7. Rezultati analize za težinu grana 0,1 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00
	TEŽINA ČITAVE MREŽE										
12	0,021	0,023	0,025	0,027	0,029	0,031	0,033	0,035	0,037	0,039	0,041
13	0,013	0,023	0,033	0,043	0,053	0,062	0,072	0,082	0,092	0,102	0,112
14	0,012	0,023	0,034	0,045	0,055	0,066	0,077	0,088	0,098	0,109	0,120
23	0,022	0,023	0,024	0,025	0,026	0,027	0,028	0,029	0,030	0,031	0,032
24	0,022	0,023	0,024	0,025	0,026	0,027	0,028	0,029	0,030	0,032	0,033
43	0,022	0,023	0,024	0,025	0,026	0,027	0,028	0,029	0,030	0,032	0,033
35	0,011	0,023	0,035	0,047	0,059	0,070	0,082	0,094	0,105	0,117	0,128
45	0,012	0,023	0,034	0,045	0,055	0,066	0,077	0,088	0,098	0,109	0,120



Slika 7.21. Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,1



Slika 7.22. Odnos težine neorijentirane strukture 1 i težina promjenljivih grana

Na slici 7.22. se može vidjeti da svaka grana nema isti utjecaj na težinu strukture. U danom primjeru orijentirane strukture na slici 7.16., prema dijagramu na slici 7.22. najveći utjecaj na težinu strukture ima grana 35, odnosno veza između čvorova (3,5).

Zbog značaja promjena težina pojedinih grana na ukupnu težinu strukture provedena je također analiza za slučajeve da su fiksne težine 0,2 i 0,3 dok se i dalje jednoj grani mijenjala težina.

U tablici 7.8. prikazani su numerički rezultati analize za slučaj da sve grane (osim promjenljive) imaju težinu 0,2 a u tablici 7.9. imaju težinu 0,3.

Tablica 7.8. Rezultati analize za težinu grana 0,2 i jednu granu s promjenljivom težinom

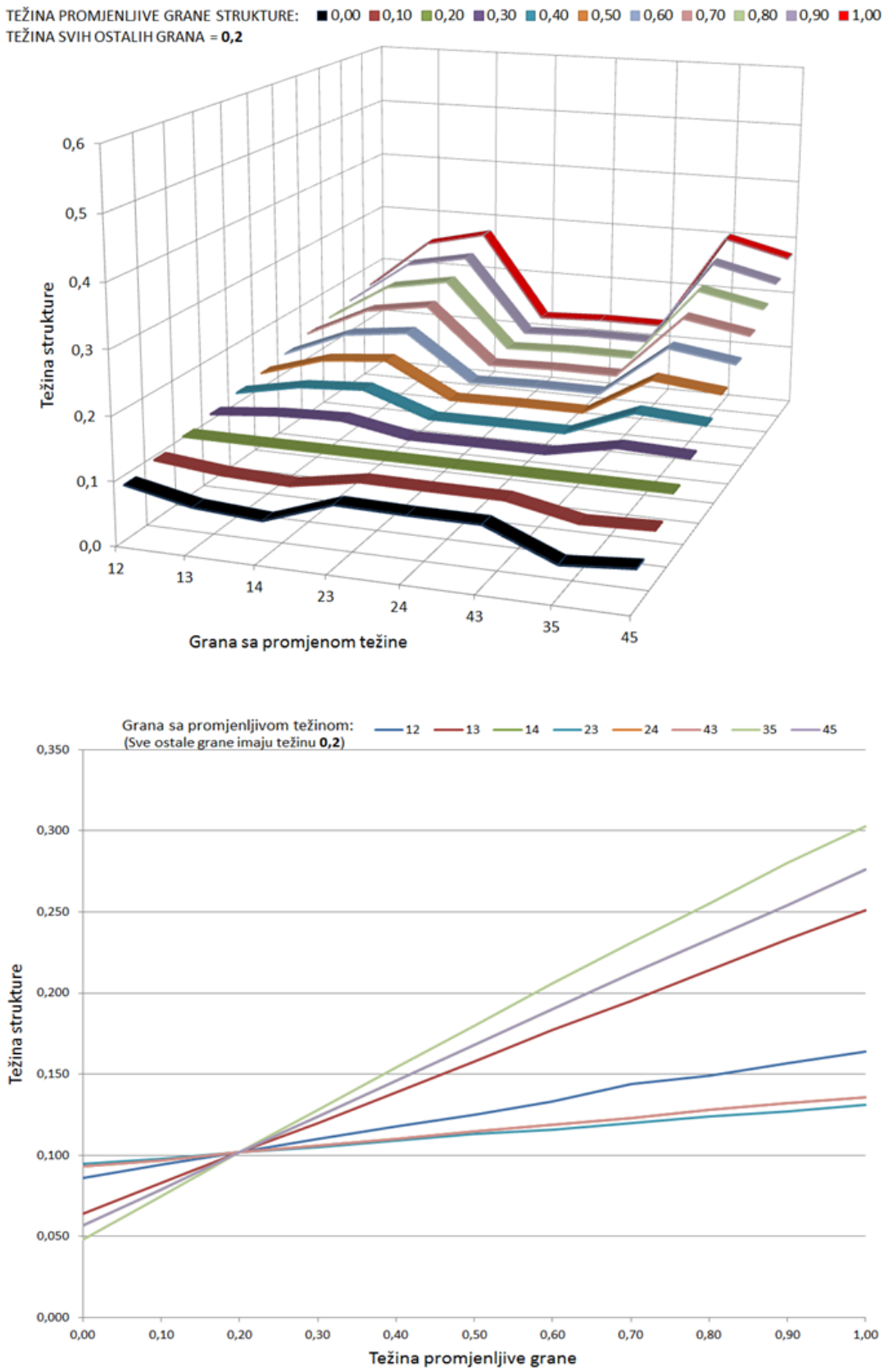
GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12	0,086	0,094	0,102	0,110	0,118	0,125	0,133	0,144	0,149	0,157	0,164
13	0,064	0,083	0,102	0,120	0,139	0,158	0,177	0,195	0,214	0,233	0,251
14	0,057	0,079	0,102	0,124	0,146	0,168	0,190	0,212	0,233	0,254	0,276
23	0,095	0,098	0,102	0,105	0,109	0,113	0,116	0,120	0,124	0,127	0,131
24	0,093	0,097	0,102	0,106	0,110	0,115	0,119	0,123	0,128	0,132	0,136
43	0,093	0,097	0,102	0,106	0,110	0,115	0,119	0,123	0,128	0,132	0,136
35	0,048	0,075	0,102	0,128	0,154	0,180	0,206	0,231	0,255	0,280	0,303
45	0,057	0,079	0,102	0,124	0,146	0,168	0,190	0,212	0,233	0,254	0,276

Tablica 7.9. Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom

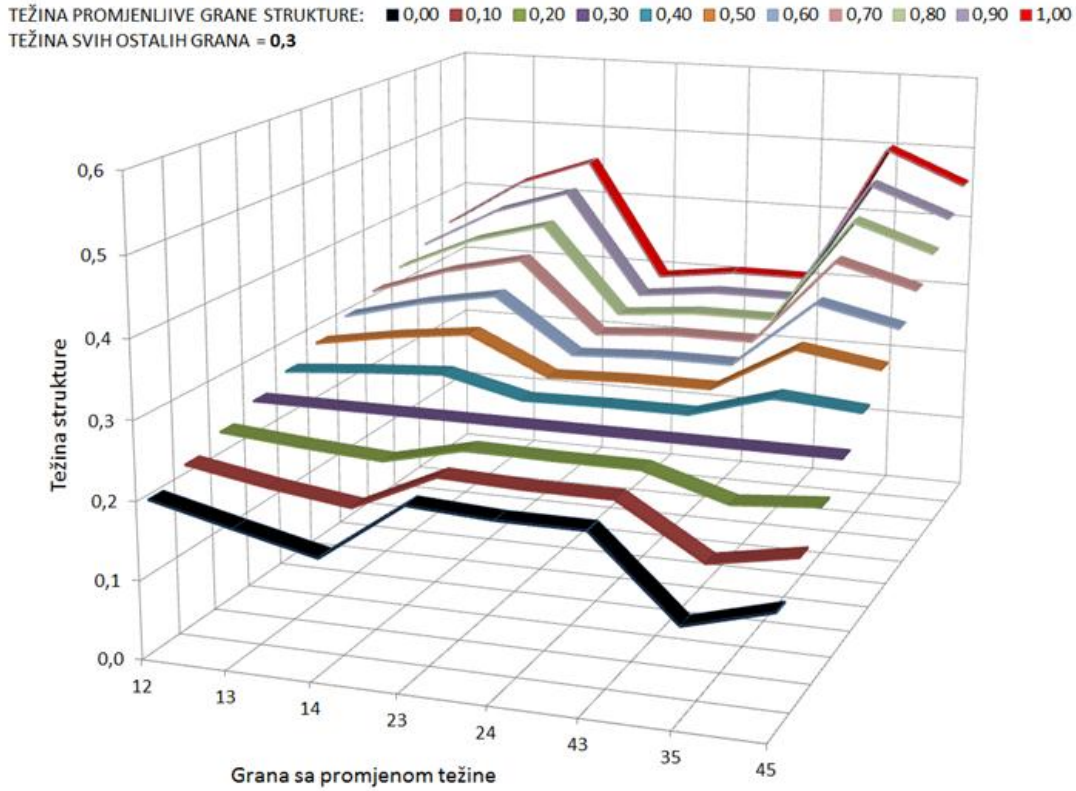
GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12	0,194	0,211	0,227	0,243	0,259	0,275	0,291	0,306	0,321	0,336	0,351
13	0,169	0,193	0,218	0,243	0,268	0,293	0,318	0,343	0,368	0,393	0,418
14	0,145	0,179	0,211	0,243	0,275	0,306	0,337	0,367	0,397	0,427	0,456
23	0,222	0,229	0,236	0,243	0,250	0,257	0,264	0,271	0,278	0,285	0,292
24	0,216	0,225	0,234	0,243	0,252	0,261	0,270	0,279	0,288	0,297	0,306
43	0,216	0,225	0,234	0,243	0,252	0,261	0,270	0,279	0,288	0,297	0,306
35	0,115	0,159	0,202	0,243	0,284	0,323	0,361	0,397	0,433	0,467	0,501
45	0,145	0,179	0,211	0,243	0,275	0,306	0,337	0,367	0,397	0,427	0,456

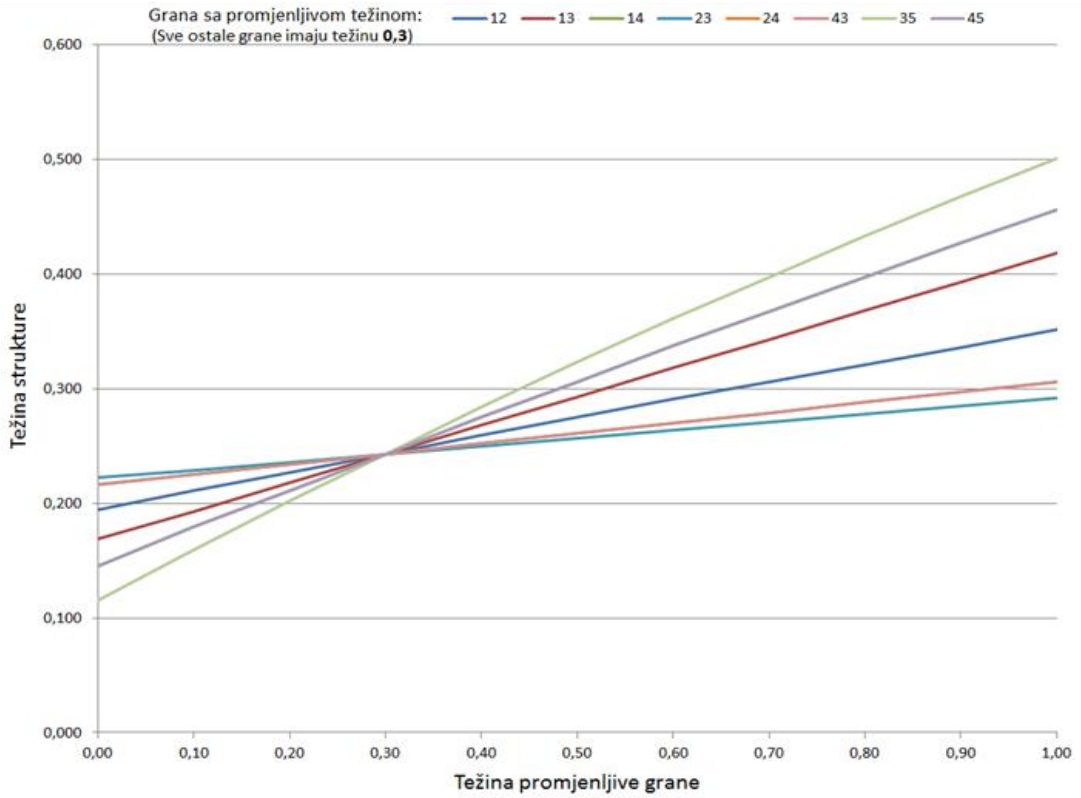
Ekvivalentni dijagrami za rezultate iz tablica 7.8. i 7.9. su prikazani na slikama 7.23. i 7.24. respektivno.

Na svakoj slici se nalazi prvo prikaz ovisnosti ukupne težine orijentirane strukture u odnosu na granu s promjenljivom težinom, a onda odnos ukupne težine strukture prema težini promjenljive grane.



Slika 7.23. Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,2





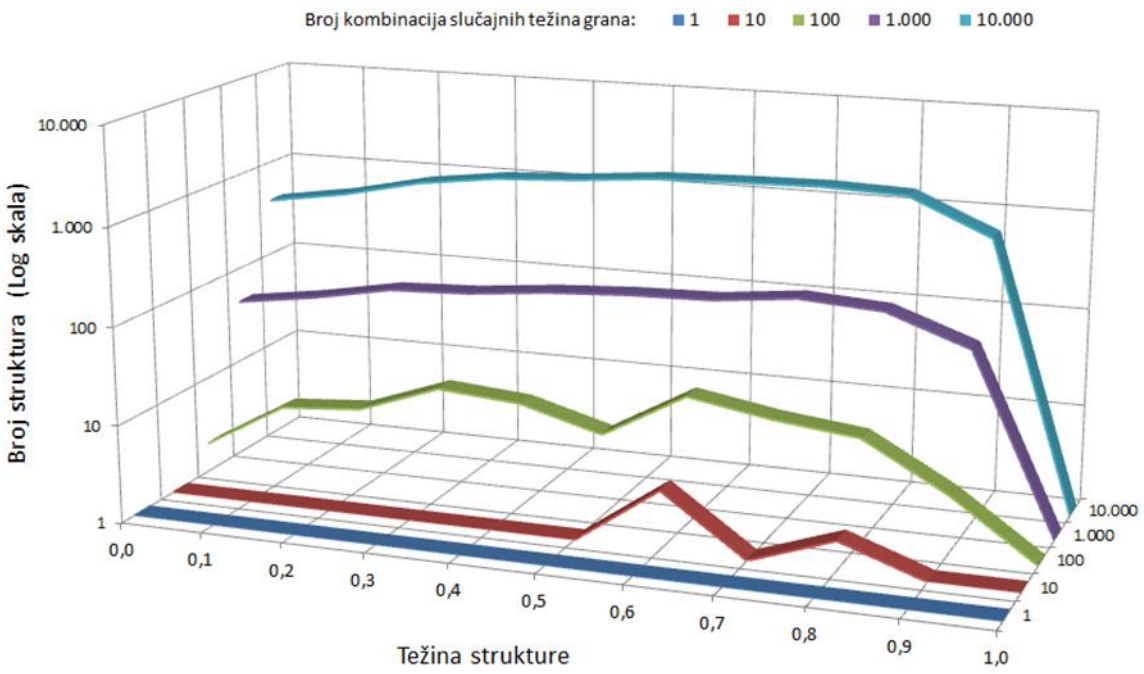
Slika 7.24. Analiza neorijentirane strukture 1 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,3

7.4.1.3. Analiza orijentirane strukture 1 sa slučajnim težinama u svim granama

Analiza je provedena na isti način kao i što je napravljeno u slučaju neorijentirane strukture obrađeno u točki 7.3.3. rezultati su prikazani tablici 7.10, a graf na slici 7.25.

Tablica 7.10. Težine orijentirane strukture 1 za slučajne težine grana

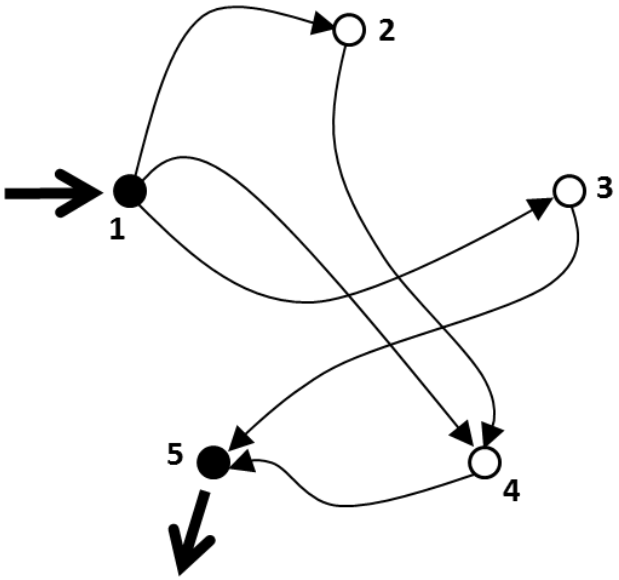
BROJ ANALIZ. MREŽA	TEŽINE MREŽA										
	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
	BROJ MREŽA S UKUPNOM TEŽINOM										
1	0	0	0	0	0	0	1	0	0	0	0
10	0	0	1	0	0	1	4	1	2	1	0
100	2	6	7	14	12	7	21	15	12	4	0
1.000	44	58	83	90	109	122	128	158	139	69	0
10.000	383	517	787	1.011	1.126	1.334	1.411	1.464	1.378	589	0



Slika 7.25. Distribucije struktura prema težinama za slučajne težine grana

7.4.2 Orijentirana struktura 2

Složena struktura koja se analizira u ovom odjeljku prikazana je na slici 7.26. Na slici se može vidjeti da je struktura nastala na temelju prethodnih isključivanjem nekih grana. U ovom slučaju funkcija strukture je kao i u prethodnim omogućavanje funkcionalne veze između ulaznog (1) i izlaznog čvora (5). Broj čvorova je ostao nepromijenjen (5). Na slici se može vidjeti da su sve grane u strukturi orijentirane, odnosno da na njima funkcionalni smjer ide samo u pravcu od jednog do drugog čvora, ali ne i obrnuto.



Slika 7.26. Primjer orijentirane strukture 2 informacijskog sistema

Pripadna latinska matrica za strukturu na slici 7.26. je prikazana na slici 7.27, a pripadna reducirana latinska matrica na slici 7.28.

$$\begin{bmatrix} 0 & 12 & 13 & 14 & 0 \\ 0 & 0 & 0 & 24 & 0 \\ 0 & 0 & 0 & 0 & 35 \\ 0 & 0 & 0 & 0 & 45 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Slika 7.27. Latinska matrica za strukturu na slici 7.26.

$$\begin{bmatrix} 0 & 2 & 3 & 4 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Slika 7.28. Reducirana latinska matrica za strukturu na slici 7.26.

Primjenom opisanog algoritma pronalaze se putovi u zadanoj strukturi, a rezultat je prikazan u tablici 7.11.

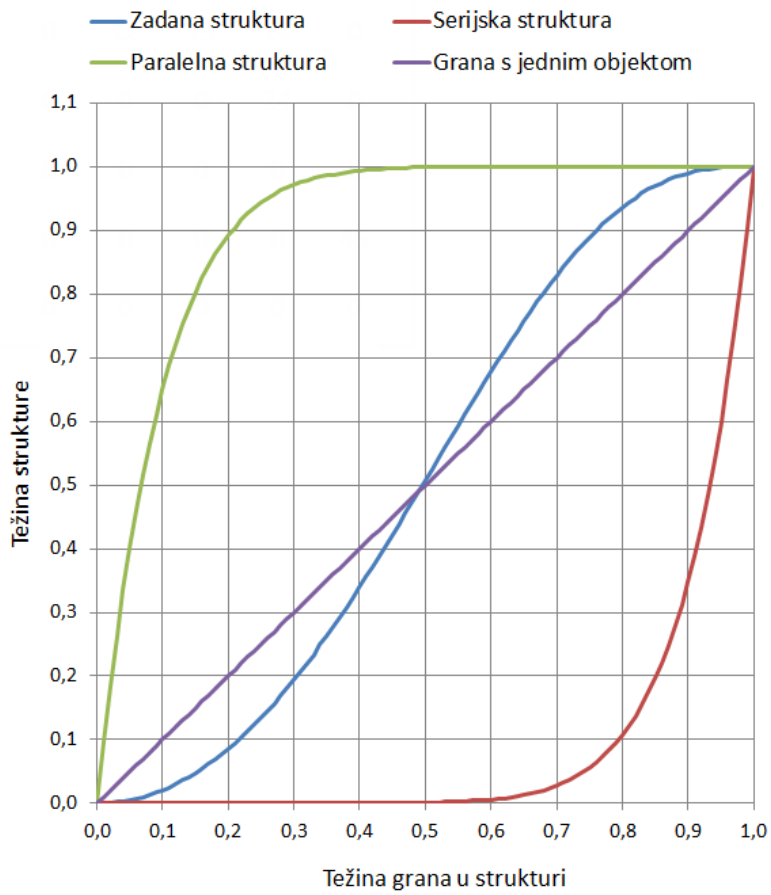
Tablica 7.11. Lista i broj putova za primjer sa slike 7.26.

Dužina puta	Čvorovi puta
1	
2	135
2	145
3	1245

Dužina puta	Broj putova
1	0
2	2
3	1
4	0

7.4.2.1 Analiza orijentirane strukture 2 sa jednakim težinama u granama

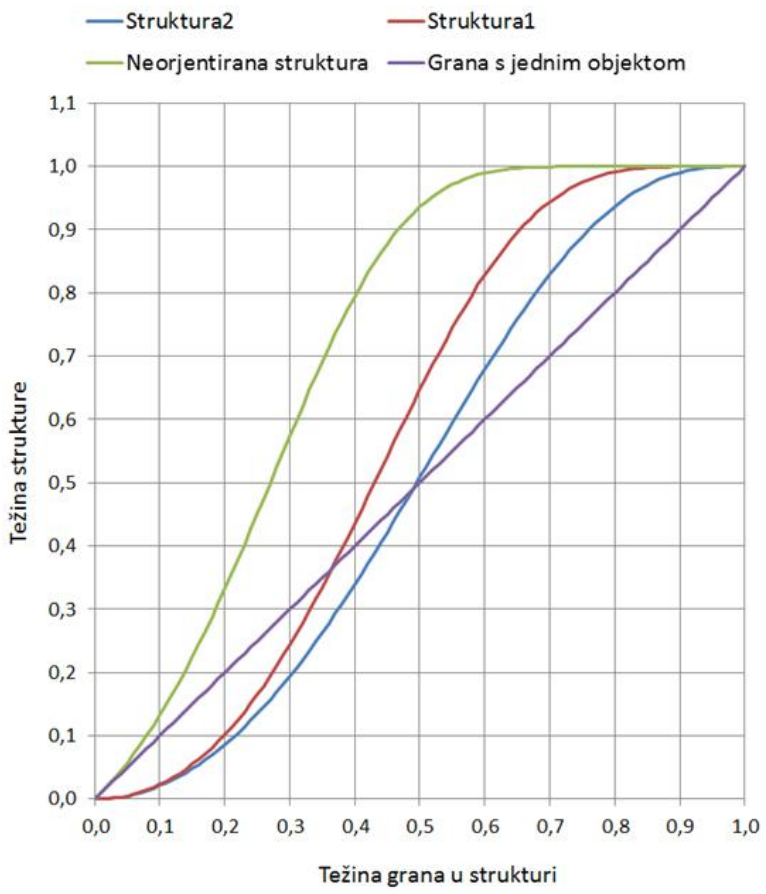
Za orijentiranu strukturu sa slike 7.26. provedena je matematička analiza primjenom algoritma kao i za neorijentiranu strukturu (slika 7.7) i orijentiranu strukturu 1 (slika 7.16.). Rezultati ove analize u grafičkom obliku prikazani su na slici 7.29., a tabelarni rezultati na temelju kojih je napravljen spomenuti graf u prilogu 11.10.



Slika 7.29. Dijagrami proračuna težine strukture u zavisnosti od težine grana za strukturu sa slike 7.26.

Kao i u slučaju dijagrama za orijentiranu strukturu 1 i u ovom slučaju se uočava razlika u odnosu na neorijentiranu strukturu. Zbog bolje usporedbe, na slici 7.30. su prikazani dijagrami za neorijentiranu strukturu (sa slike 7.7), te dijagrami za orijentiranu strukturu 1 (sa slike 7.16.) i orijentiranu strukturu 2 (sa slike 7.26.).

Na slici se može uočiti trend kretanja dijagrama u desno, odnosno neorijentirana struktura 2 pokazuje osobinu kretanja po karakteristikama ka serijskoj strukturi u odnosu na orijentiranu strukturu 1.



Slika 7.30. Dijagrami proračuna težine strukture u zavisnosti od težine grana za strukturu 2 sa slike 7.26. i strukturu 1 sa slike 7.16.

Iz dijagrama na slici 7.30. evidentno je da uz iste težine pojedinih grana struktura utiče na ukupnu težinu strukture, odnosno na veličinu rizika.

7.4.2.2 Analiza orijentirane strukture 2 sa promjenljivom težinom jedne grane

Kod ove analize pretpostavlja se da u sve grane strukture imaju jednaku težinu, a jednoj grani se mijenja težina. Rezultati takve analize za orijentiranu strukturu 2 prikazani su u tablici 7.12.

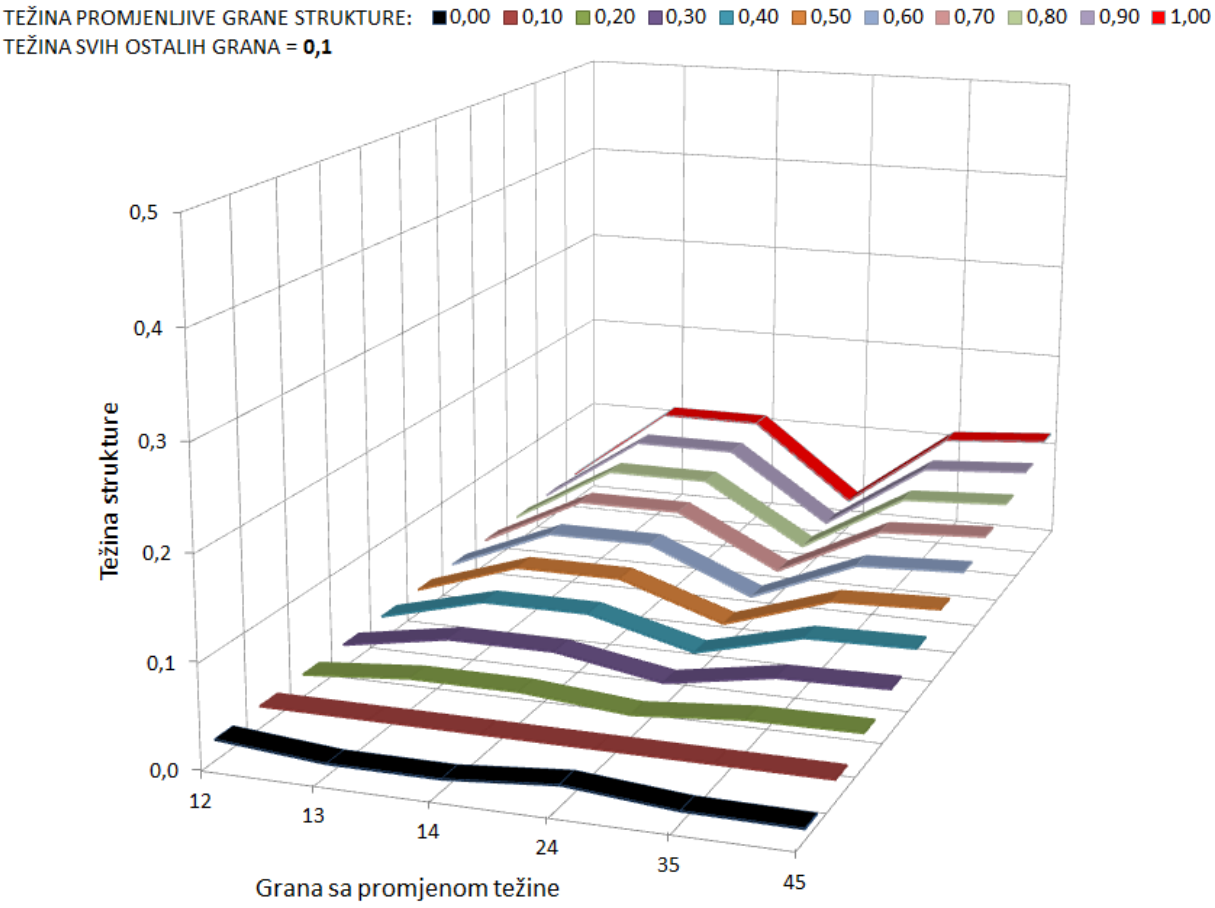
U analizi sa rezultatima prikazanim u tablici 7.12. sve grane strukture imaju težinu 0,1 a jednoj se grani mijenjala težina.

Podaci ove analize su prikazani u grafičkom obliku na slici 7.31.

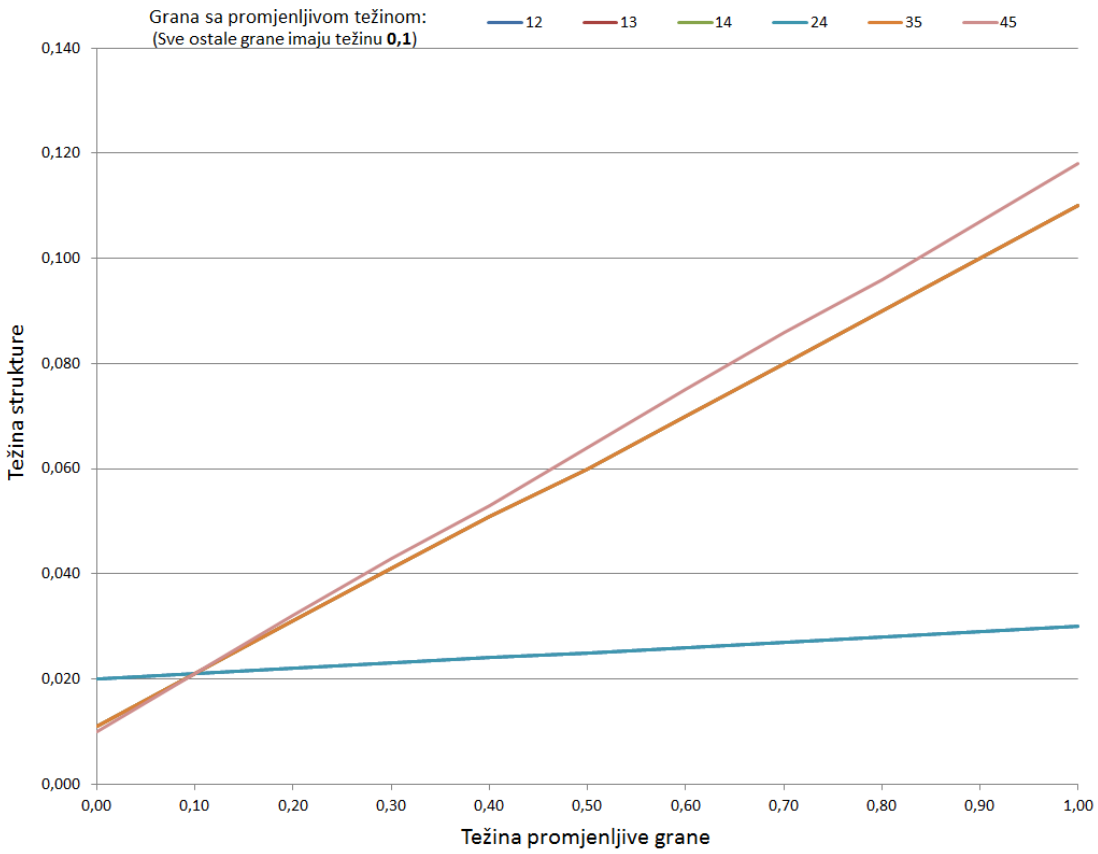
Za isti primjer orijentirane strukture 2 na slici 7.32. prikazan je dijagram ovisnosti ukupne težine strukture o težini jedne promjenljive grane.

Tablica 7.12. Rezultati analize za težinu grana 0,1 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12	0,020	0,021	0,022	0,023	0,024	0,025	0,026	0,027	0,028	0,029	0,030
13	0,011	0,021	0,031	0,041	0,051	0,060	0,070	0,080	0,090	0,100	0,110
14	0,011	0,021	0,031	0,041	0,051	0,060	0,070	0,080	0,090	0,100	0,110
24	0,020	0,021	0,022	0,023	0,024	0,025	0,026	0,027	0,028	0,029	0,030
35	0,011	0,021	0,031	0,041	0,051	0,060	0,070	0,080	0,090	0,100	0,110
45	0,010	0,021	0,032	0,043	0,053	0,064	0,075	0,086	0,096	0,107	0,118



Slika 7.31. Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale imaju težinu=0,1



Slika 7.32. Odnos težine neorijentirane strukture 2 i težina promjenljivih grana

I u ovom slučaju je evidentno da svaka grana nema jednaki utjecaj na ukupnu težinu strukture. Može se vidjeti da glavni utjecaj na ukupnu težinu strukture stvara grana (3,5), između čvorova 3 i 5.

Da bi se provela analiza i u drugim stanjima težina neorijentirane strukture proveden je proračun za slučajeve da su fiksne težine svih grana 0,2 i 0,3 osim za promjenljivu granu.

U tablici 7.13. prikazani su rezultati proračuna da sve grane, osim promjenljive, imaju težinu 0,2, a u tablici 7.14. imaju težinu 0,3.

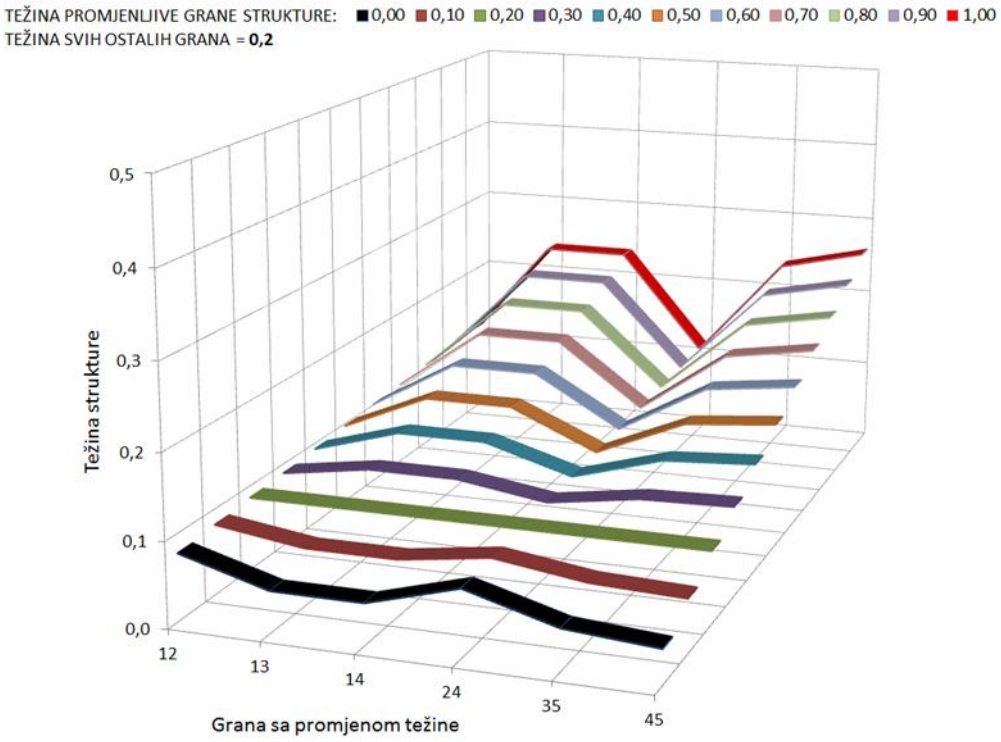
Tablica 7.13. Rezultati analize za težinu grana 0,2 i jednu granu s promjenljivom težinom

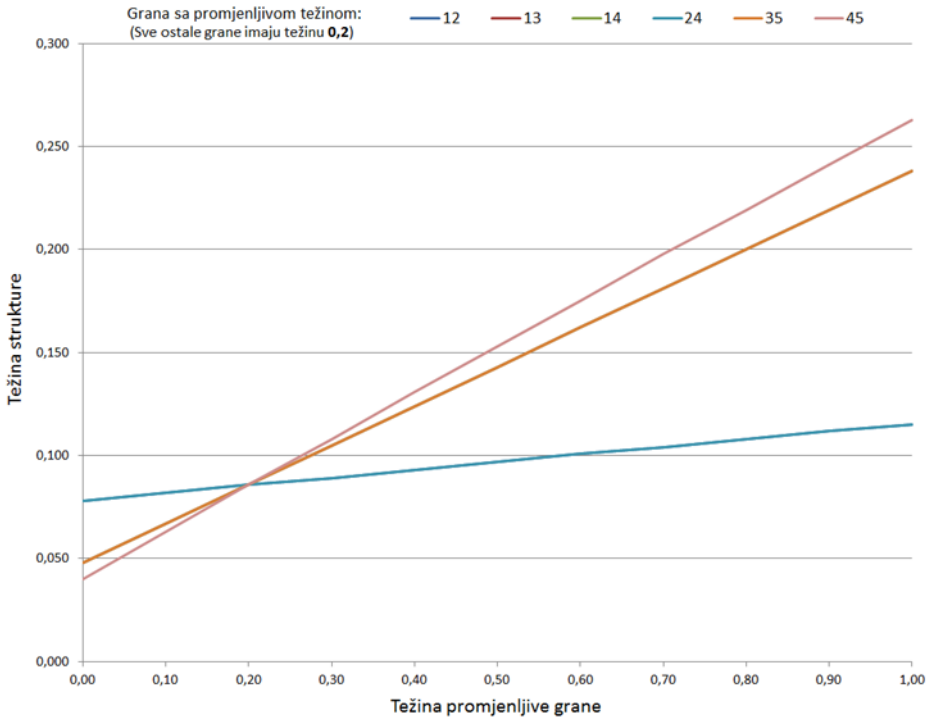
GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12	0,078	0,082	0,086	0,089	0,093	0,097	0,101	0,104	0,108	0,112	0,115
13	0,048	0,067	0,086	0,105	0,124	0,143	0,162	0,181	0,200	0,219	0,238
14	0,048	0,067	0,086	0,105	0,124	0,143	0,162	0,181	0,200	0,219	0,238
24	0,078	0,082	0,086	0,089	0,093	0,097	0,101	0,104	0,108	0,112	0,115
35	0,048	0,067	0,086	0,105	0,124	0,143	0,162	0,181	0,200	0,219	0,238
45	0,040	0,063	0,086	0,108	0,131	0,153	0,175	0,198	0,219	0,241	0,263

Tablica 7.14. Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom

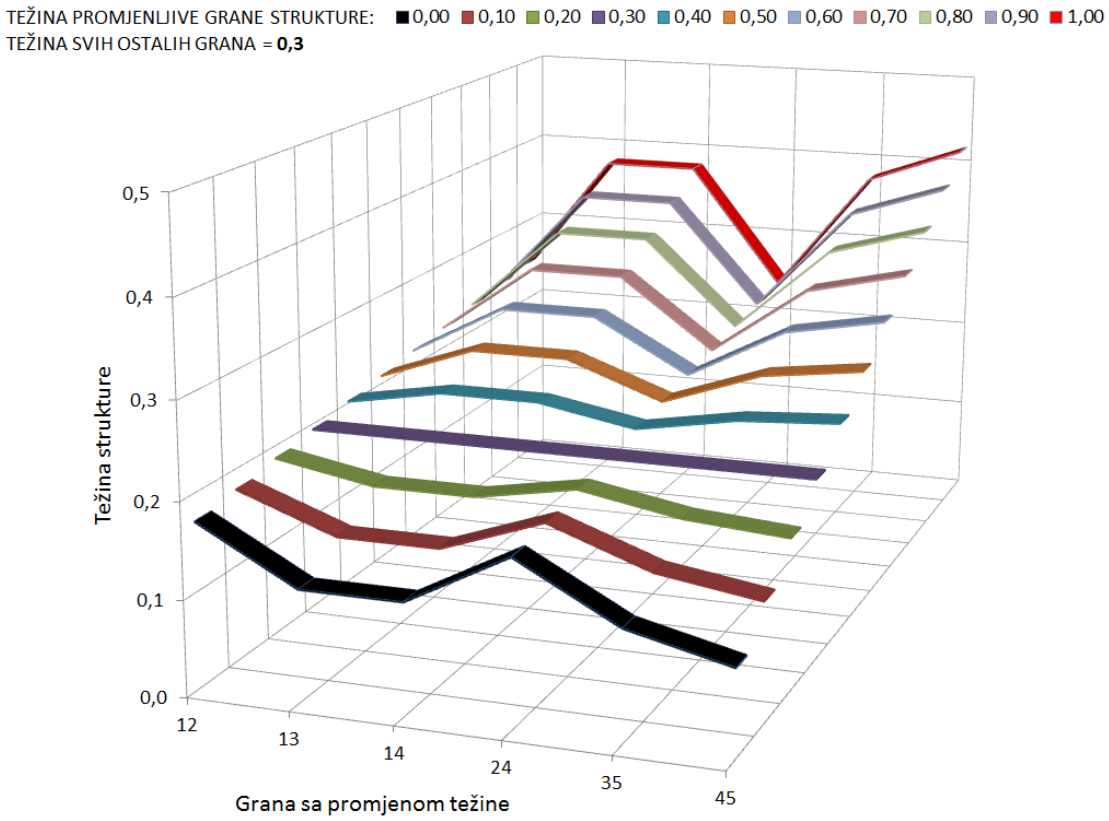
GRANA S IZMJENOM TEŽINE	TEŽINA IZMJENLJIVE GRANE MREŽE										
	0,00	**0,10**	**0,20**	**0,30**	**0,40**	**0,50**	**0,60**	**0,70**	**0,80**	**0,90**	**1,00**
	TEŽINA ČITAVE MREŽE										
12	0,172	0,179	0,187	0,194	0,202	0,209	0,217	0,224	0,232	0,239	0,246
13	0,115	0,141	0,168	0,194	0,221	0,247	0,274	0,301	0,327	0,354	0,380
14	0,115	0,141	0,168	0,194	0,221	0,247	0,274	0,301	0,327	0,354	0,380
24	0,172	0,179	0,187	0,194	0,202	0,209	0,217	0,224	0,232	0,239	0,246
35	0,115	0,141	0,168	0,194	0,221	0,247	0,274	0,301	0,327	0,354	0,380
45	0,090	0,125	0,160	0,194	0,228	0,261	0,294	0,326	0,358	0,390	0,420

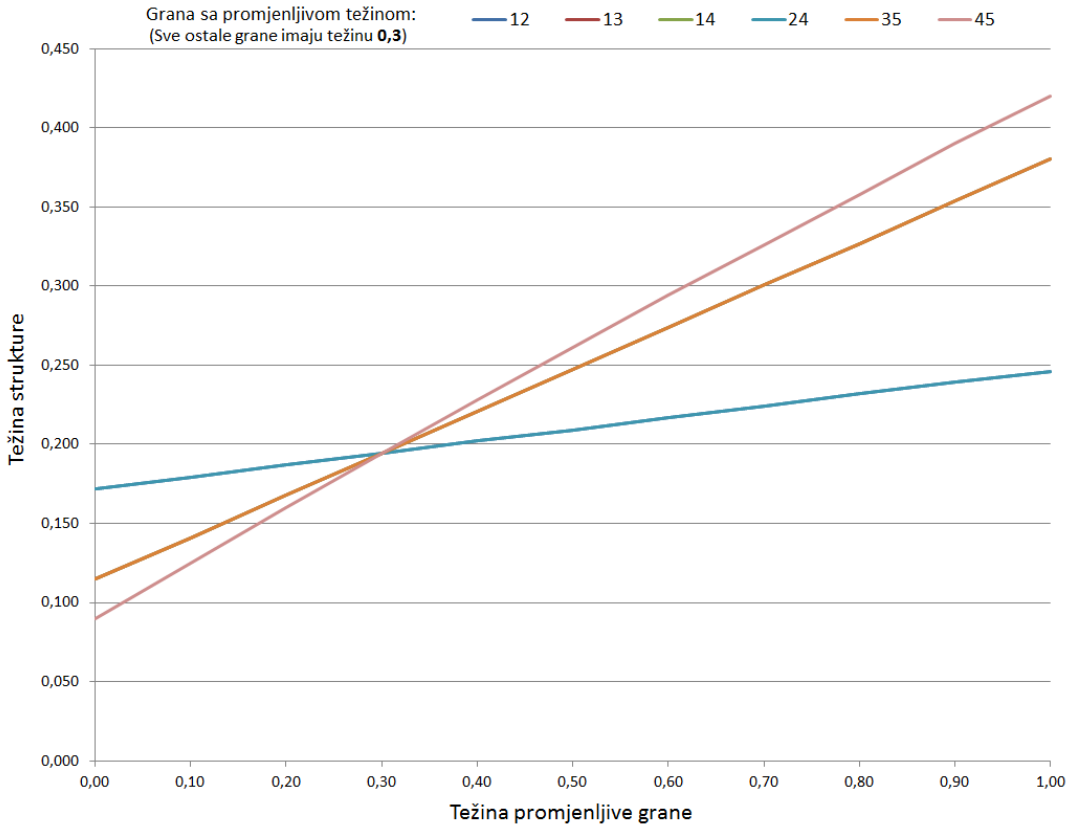
Dijagrami za rezultate analize u tablicama 7.13. i 7.14. su prikazani na slikama 7.33. i 7.34. respektivno.





Slika 7.33. Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale grane imaju težinu 0,2





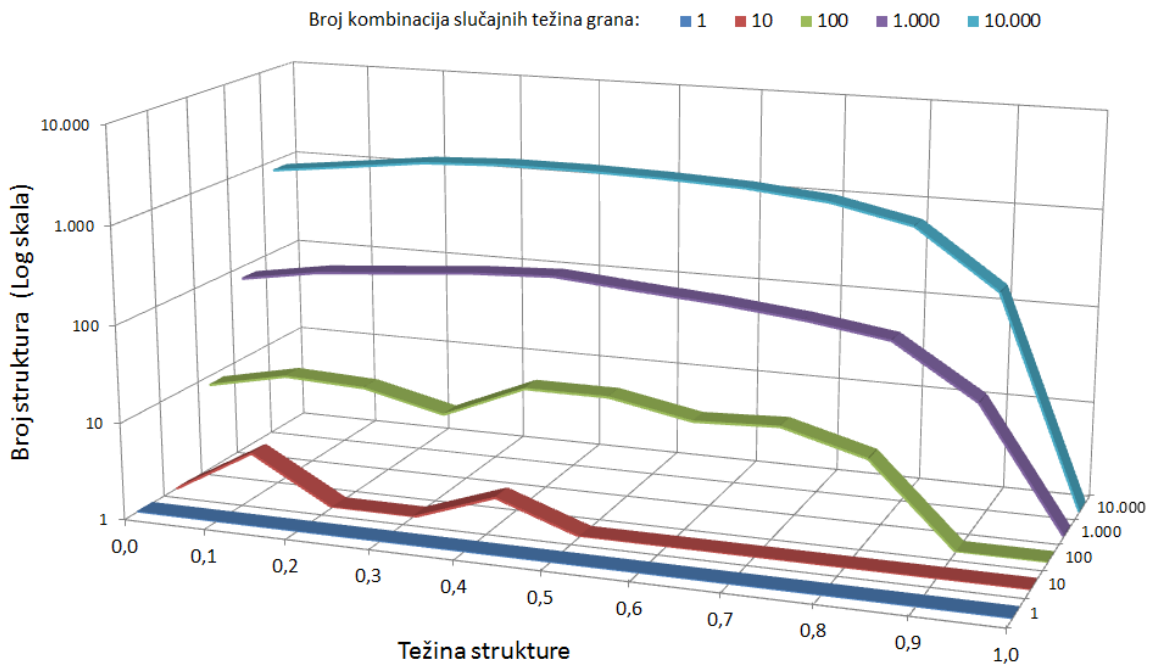
Slika 7.34. Analiza neorijentirane strukture 2 gdje jedna grana mijenja težinu, a sve ostale grane imaju težinu 0,3

7.4.2.3 Analiza orijentirane strukture 2 sa slučajnim težinama u svim granama

Analiza orijentirane strukture 2 sa slučajnim težinama u svim granama, metodološki je provedena isto kao i za slučaj neorijentirane strukture i orijentirane strukture 1. Rezultati analize prikazani su u tablici 7.15., a dijagram na slici 7.35.

Tablica 7.15. Težine orijentirane strukture 2 za slučajne težine grana

BROJ ANALIZ. MREŽA	TEŽINE MREŽA										
	0,0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
	BROJ MREŽA S UKUPNOM TEŽINOM										
1	1	0	0	0	0	0	0	0	0	0	0
10	1	3	1	1	2	1	0	1	0	0	0
100	8	12	11	7	16	16	11	12	7	0	0
1.000	74	101	118	139	152	129	111	90	67	19	0
10.000	787	985	1.245	1.356	1356	1.295	1.187	983	646	160	0



Slika 7.35. Distribucija struktura prema težinama za slučajne težine grana za primjer orijentirane strukture 2

8. Upravljanje rizicima metodom izmjene strukture

Analizom zahtjeva standarda ISO 27001:2005 za implementacijom ISMS pokazano je da se procjena rizika i upravljanje rizicima svrstava u kategoriju njenih temeljnih zahtjeva koji se moraju ispuniti. Tek nakon procjene rizika i obrade rizika, odnosno definiranja sigurnosnih mjera može se pristupiti implementaciji elemenata zaštite informacijskog sistema, a kasnije i poboljšanju.

Ono što zahtjeva standard ISO 27001:2005 je izvršiti rangiranje rizika nakon provedene procjene rizika. Nakon toga se na temelju sigurnosne politike i drugih zahtjeva određuju kriteriji koliko i koje rizike će se smanjivati. Pri tome se ne zna koliki je ukupni rizik informacijskog sistema sa aspekta informacijske sigurnosti. Činjenica je da svako smanjenje rizika za sobom povlači i neke troškove koji mogu biti značajnog iznosa, čak i toliko veliki da su neprihvatljivi za organizaciju. U tom slučaju organizacija nastavlja koristiti informacijski sistem sa tim neprihvatljivim rizikom uz pismenu izjavu o saznanju za takve velike rizike.

Standard ISO 27001:2005 u okviru borbe za smanjenje rizika informacijskog sistema ne vodi računa o riziku ukupnog sistema niti o tome da li ima smisla smanjivati rizik nekoj informacijskoj imovini, jer se objektivno ne smanjuje ukupni rizik sistema.

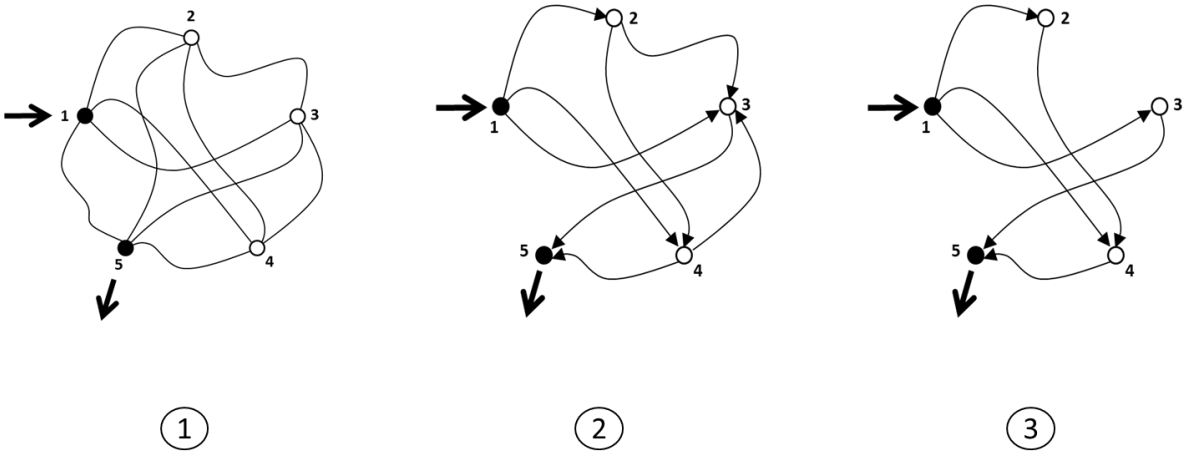
Osnovna filozofija odnosa prema riziku informacijskog sistema, kako zagovara standard ISO 27001:2005 je: *smanjivanje svih neprihvatljivih rizika informacijske imovine, čime informacijski sistem postaje sigurniji*.

Ono što je manjkavo u toj filozofiji ISO 27005:2005, u svjetlu racionalizacije i optimizacije borbe protiv rizika informacijskog sistema, je neselektivnost izbora imovine kojoj se smanjuje rizik zasnovan na dokazivim efektima povećanja sigurnosti sistema.

Slijedeći problem kod standarda ISO 27001:2005 je zahtjev da se kroz vrijeme periodički mora dokazati napredak u povećanju sigurnosti informacija, odnosno poboljšanje ISMS. Prema ISO 27001:2005 nema konkretnog parametra, kao npr. neke veličine koja iskazuje koliki je rizik (sigurnost) konkretnog informacijskog sistema. Zbog toga nezavisni auditori, koji imaju ulogu ocjenitelja poboljšanja vezanih za informacijsku sigurnost, vjeruju da se na temelju poduzetih preventivnih i korektivnih radnji povećala sigurnost, odnosno smanjio rizik informacijskog sistema. Objektivno za to nemaju materijalni dokaz.

Na temelju svega iznesenog u poglavlju 6 i 7 pokazano je da se te nedorečenosti vezane za upravljanje informacijskom sigurnošću, a s time i vezanim rizicima prema ISO 27001:2005, mogu značajno racionalizirati i optimizirati primjenom nove metode upravljanja rizicima izmjenom strukture sistema. U tom smislu se definiraju tri teorema upravljanja rizicima metodom izmjene strukture. Ova tri teorema će biti iznesena u nastavku ovog poglavlja.

Za analizu i dokaze teorema koristit će se strukture obrađene u poglavlju 7. Te strukture su prikazane na slici 8.1.



Slika 8.1. Analizirane složene strukture informacijskih sistema

Prema izrazu (5.5) rizik se definira kao vjerojatnost∗posljedica. Uz uvažavanje pretpostavke da je posljedica normirana i jednaka 1, te na temelju izraza (7.1) može se napisati:

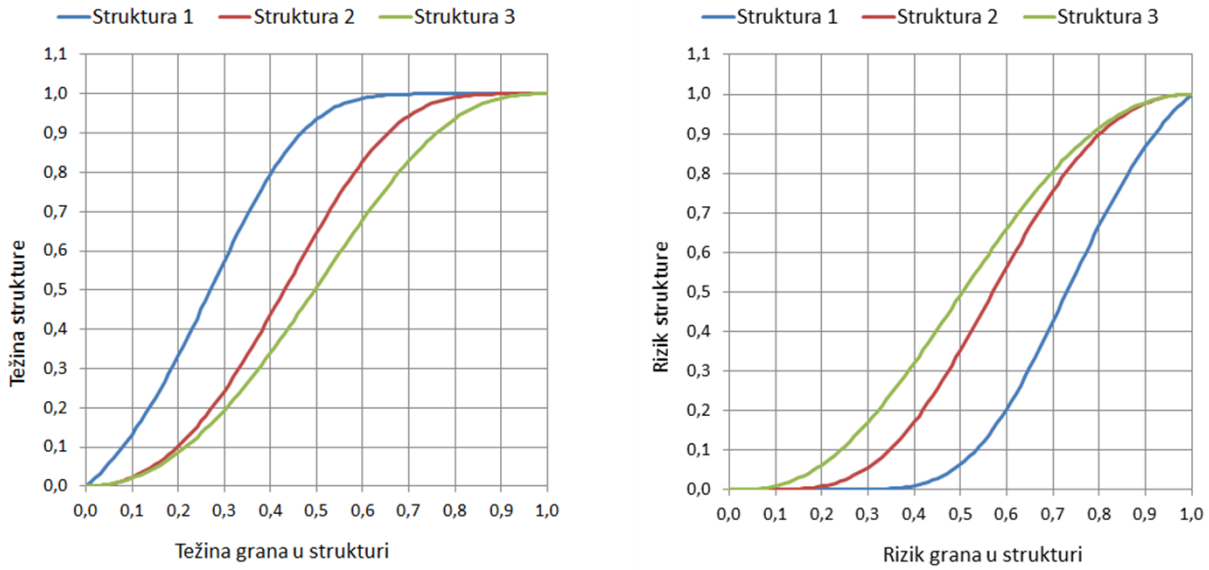
$$P = 1 - W \tag{8.1}$$

Gdje su: P = vjerojatnost pojave rizika (odnosno, rizik za posljedicu 1)

W = težina

Izraz (8.1) vrijedi kao za rizike grane, tako i za rizik strukture.

Značenje relacije (8.1) za odnos težine i rizika, odnosno vjerojatnosti pojave rizika ilustriran je na slici 8.2. Pri tome je važno naglasiti da sve grane u strukturi imaju istu težinu, odnosno rizik.



Slika 8.2. Prikaz dijagrama težina i rizika složenih struktura sa slike 8.1.

Numerički podaci koji su na dijagramima slike 8.2. prikazani su u tablici 8.1.

Tablica 8.1. Težine i rizici složenih struktura sa slike 8.1.

Težina grana	**Težina** struktura		
	Struktura 1	Struktura 2	Struktura 3
0,000	0,000	0,000	0,000
0,100	0,132	0,023	0,021
0,200	0,332	0,102	0,086
0,300	0,574	0,243	0,194
0,400	0,795	0,436	0,340
0,500	0,936	0,647	0,508
0,600	0,989	0,828	0,679
0,700	0,999	0,944	0,829
0,800	1,000	0,991	0,937
0,900	1,000	1,000	0,990
1,000	1,000	1,000	1,000

Rizik grana	**Rizik** struktura		
	Struktura 1	Struktura 2	Struktura 3
0,000	0,000	0,000	0,000
0,100	0,000	0,000	0,010
0,200	0,000	0,009	0,063
0,300	0,001	0,056	0,171
0,400	0,011	0,172	0,321
0,500	0,064	0,353	0,492
0,600	0,205	0,564	0,660
0,700	0,426	0,757	0,806
0,800	0,668	0,898	0,914
0,900	0,868	0,977	0,979
1,000	1,000	1,000	1,000

8.1 I. TEOREM RIZIKA SLOŽENE STRUKTURE

Za bilo kakvu složenu strukturu može se odrediti ukupan rizik sistema.

I teorem govori da se na temelju analize može odrediti numerička vrijednost koja predstavlja ukupni rizik složene strukture informacijskog sistema, bez obzira na oblike i veličinu strukture.

Kao dokaz dovoljno se pozvati na tri strukture koje su obrađivane u poglavlju 7, a prikazane sna zajedničkoj slici 8.1. i dijagram sa slike 8.2.

Na osnovi analiza pojedinih struktura provedenih u poglavlju 7, usporedni dijagrami pojedinih struktura sa slike 8.1. prikazani su na slici 8.2.

Sa slike 8.2., odnosno tablici 8.1. može se vidjeti da se za slučaj iznosa rizika 0,5 u svim granama struktura dobiva rizik strukture 1 iznosa 0.064, za strukturu 2 iznosa 0,353 i za strukturu 3 iznosa 0,492.

8.2 II. TEOREM RIZIKA SLOŽENE STRUKTURE

Promjenom strukture mijenja se ukupni rizik strukture.

Ovaj teorem se dokazuje ilustracijom sa slike 8.2. i/ili tablice 8.1.

Očito je da se promjenom strukture mijenja i težina ukupne strukture.

8.3 III. TEOREM RIZIKA SLOŽENE STRUKTURE

Promjenom rizika bilo koje grane koja čini dio barem jednog puta u složenoj strukturi, mijenja se i rizik ukupne strukture.

U III teoremu rizika složene strukture se govori o utjecaju rizika (težine) pojedine grane na ukupnu težinu.

U svrhu dokaza koriste se podaci iz tablice 7.9., a odnose se na strukturu 2 sa slike 8.1.

Tablica 8.2. Rezultati analize za težinu grana 0,3 i jednu granu s promjenljivom težinom

GRANA S IZMJENOM **TEŽINE**	**TEŽINA** IZMJENLJIVE GRANE MREŽE										
	0,00	0,10	0,20	0,30	0,40	0,50	0,60	0,70	0,80	0,90	1,00
	TEŽINA ČITAVE MREŽE										
12	0,194	0,211	0,227	0,243	0,259	0,275	0,291	0,306	0,321	0,336	0,351

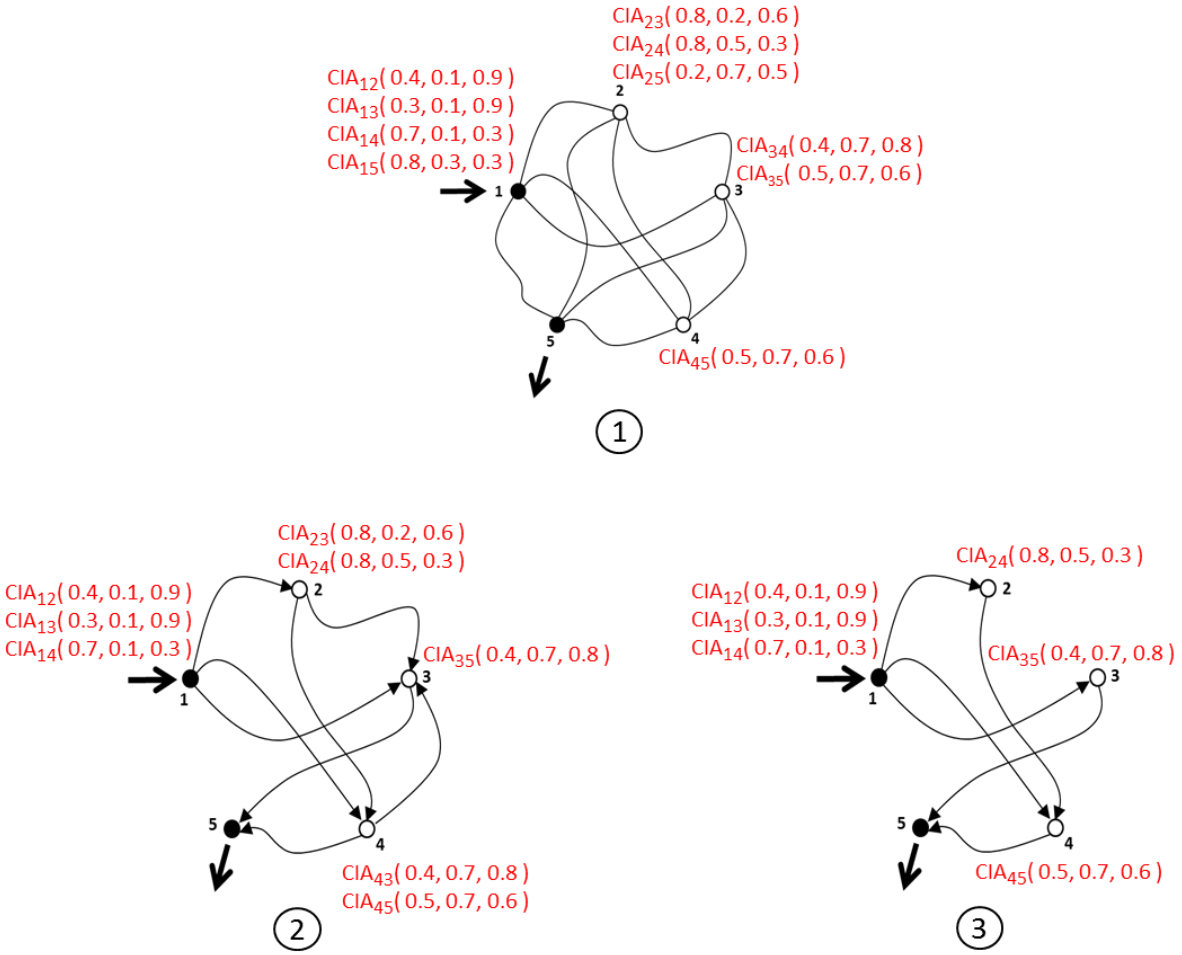
GRANA S IZMJENOM **RIZIKA**	**RIZIK** IZMJENLJIVE GRANE MREŽE										
	1,00	0,90	0,80	0,70	0,60	0,50	0,40	0,30	0,20	0,10	0,00
	RIZIK ČITAVE MREŽE										
12	0,806	0,789	0,773	0,757	0,741	0,735	0,709	0,694	0,679	0,664	0,649

8.4 ANALIZA UTJECAJA STRUKTURE INFORMACIJSKOG SISTEMA NA INFORMACIJSKE RIZIKE U ISMS

U skladu s točkom 4.2 kod implementacije ISMS prema standardu ISO 27001 jedan od ključnih koraka je procjena rizika. Pri tome se za svaki element informacijskog sistema (informacijsku imovinu) određuju rizici, posebno za svaki od tri aspekta informacijske sigurnosti:

- Rizik narušavanja dostupnosti
- Rizik narušavanja tajnosti, i
- Rizik narušavanja cjelovitosti.

Primjenom metodologije kvalitativne procjene rizika opisane u točki 5.3.2. za slučaj strukture prikazane na slici 8.1. za neorijentiranu strukturu treba procijeniti rizike (odnosno težine) za svaku granu i to za sva tri aspekta informacijske sigurnosti C-I-A. Pretpostavljeni rezultati takve procjene rizika za svaku granu strukture su prikazani na slici 8.3., odnosno u tablici 8.3.



Slika 8.3. Strukture složenih informacijskih sistema sa procijenjenim rizicima u granama za svaki aspekt informacijske sigurnosti (C-I-A)

Pri tome treba naglasiti da se u tablici 8.3. nalaze procijenjeni rizici za svaku granu (crveni brojevi) kao i ekvivalentne težine (crni brojevi) što korespondira s izrazom (7.1). Pored toga u zadnjem redu tablice 8.3. navedeni su ukupni rizici i ukupna težina cijele strukture za svaki aspekt informacijske sigurnosti proračunato na temelju ranije prikazanog algoritma i programa LATMAT (vidi poglavlje 9). Ovi rezultati su napravljeni uz pretpostavku međusobne nezavisnosti veličine rizika (težine) pojedinih aspekata informacijske sigurnosti u jednoj grani i/ili između bilo kojih grana. Ta pretpostavka znači da promjena rizika bilo kojeg aspekta informacijske sigurnosti u bilo kojoj grani ne izaziva nikakvu promjenu rizika bilo kojeg aspekta u bilo kojoj grani.

*Tablica 8.3. Primjer rizika i težina za **neorijentiranu** strukturu (1) sa slike 8.3*

Grana	**RIZICI** narušavanja aspekata			**TEŽINE** narušavanja aspekata		
	C	**I**	**A**	**C**	**I**	**A**
12	0.4	0.1	0.9	0.6	0.9	0.1
13	0.3	0.1	0.9	0.7	0.9	0.1
14	0.7	0.1	0.3	0.3	0.9	0.7
15	0.8	0.3	0.3	0.2	0.7	0.7
23	0.8	0.2	0.6	0.2	0.8	0.4
24	0.8	0.5	0.3	0.2	0.5	0.7
25	0.2	0.7	0.5	0.8	0.3	0.5
34	0.4	0.7	0.8	0.6	0.3	0.2
35	0.5	0.7	0.6	0.5	0.3	0.4
45	0.5	0.7	0.6	0.5	0.3	0.4
Ukupno za strukturu	**0.10**	**0,03**	**0,11**	**0.90**	**0.97**	**0,89**

Na temelju neorijentirane strukture na slici 8.3.(1) i tablice 8.3. napravljene su i orijentirane strukture prikazane na slici 8.3.(2) i 8.3.(3). Ekvivalentni podaci takvih struktura su prikazani su u tablicama 8.4. i 8.5. I u ovom slučaju je napravljen proračun ukupne težine, odnosno rizika svake strukture, za svaki aspekt informacijske sigurnosti.

*Tablica 8.4. Primjer rizika i težina za **orijentiranu** strukturu (2) sa slike 8.3.*

Grana	RIZICI narušavanja aspekata			TEŽINE narušavanja aspekata		
	C	I	A	C	I	A
12	0.4	0.1	0.9	0.6	0.9	0.1
13	0.3	0.1	0.9	0.7	0.9	0.1
14	0.7	0.1	0.3	0.3	0.9	0.7
23	0.8	0.2	0.6	0.2	0.8	0.4
24	0.8	0.5	0.3	0.2	0.5	0.7
35	0.5	0.7	0.6	0.5	0.3	0.4
43	0.4	0.7	0.8	0.6	0.3	0.2
45	0.5	0.7	0.6	0.5	0.3	0.4
Ukupno za strukturu	**0.43**	**0.32**	**0.62**	**0.57**	**0.68**	**0.38**

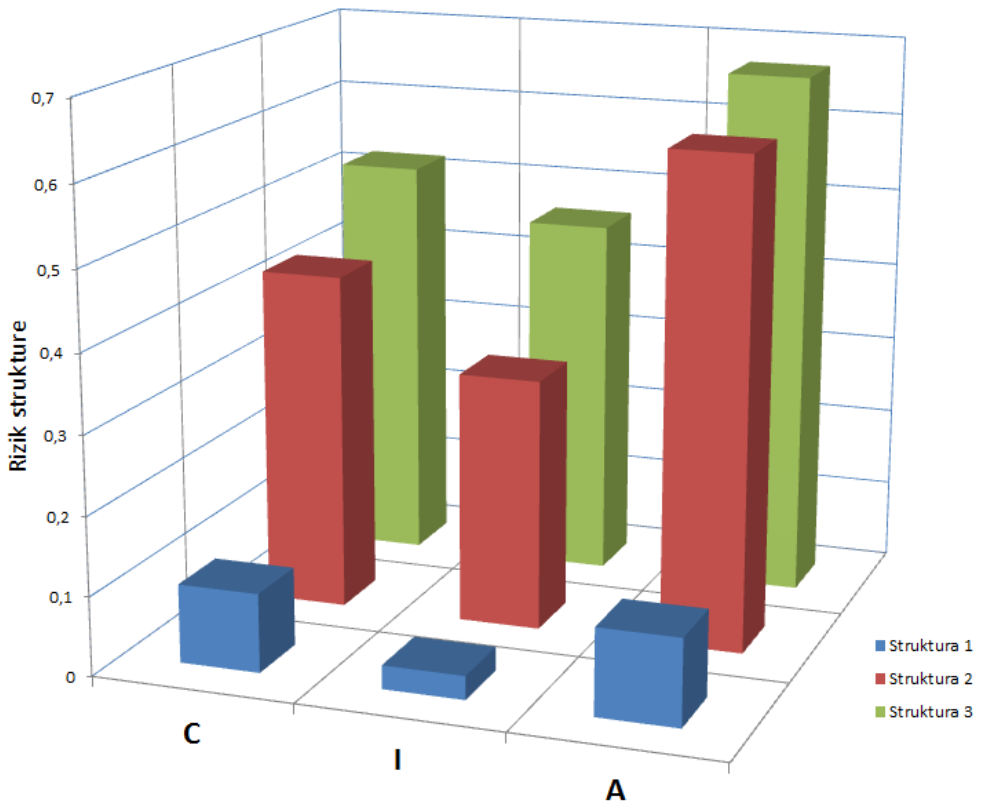
*Tablica 8.5. Primjer rizika i težina za **orijentiranu** strukturu (3) sa slike 8.3.*

Grana	RIZICI narušavanja aspekata			TEŽINE narušavanja aspekata		
	C	I	A	C	I	A
12	0.4	0.1	0.9	0.6	0.9	0.1
13	0.3	0.1	0.9	0.7	0.9	0.1
14	0.7	0.1	0.3	0.3	0.9	0.7
24	0.8	0.5	0.3	0.2	0.5	0.7
35	0.5	0.7	0.6	0.5	0.3	0.4
45	0.5	0.7	0.6	0.5	0.3	0.4
Ukupno za strukturu	**0.52**	**0.46**	**0.67**	**0.48**	**0.54**	**0.33**

Na temelju ovih podataka prikazanih u tablicama 8.3 – 8.5 mogu se prikazati zbirni rezultati promjene rizika ove tri strukture informacijskog sistema za svaki aspekt informacijske sigurnosti kao što se vidi u tablici 8.6. Podaci proračuna ukupnog rizika složene strukture informacijskog sistema iz tablice 8.6. prikazani su grafički na slici 8.4. Na slici se može vidjeti da se rizici za svaki aspekt informacijske sigurnosti mijenjaju u zavisnosti od strukture, što je i pokazano ranije u ovom poglavlju kroz razmatranje utjecaja strukture na težinu.

Tablica 8.6. Ukupne težine i rizici struktura sa slike 8.1. po aspektima C-I-A informacijske sigurnosti

Grana	RIZICI narušavanja aspekata			TEŽINE narušavanja aspekata		
	C	I	A	C	I	A
Ukupno za Strukturu (1)	0.10	0,03	0,11	0.90	0.97	0,89
Ukupno za Strukturu (2)	0.43	0.32	0.62	0.57	0.68	0.38
Ukupno za Strukturu (3)	0.52	0.46	0.67	0.48	0.54	0.33

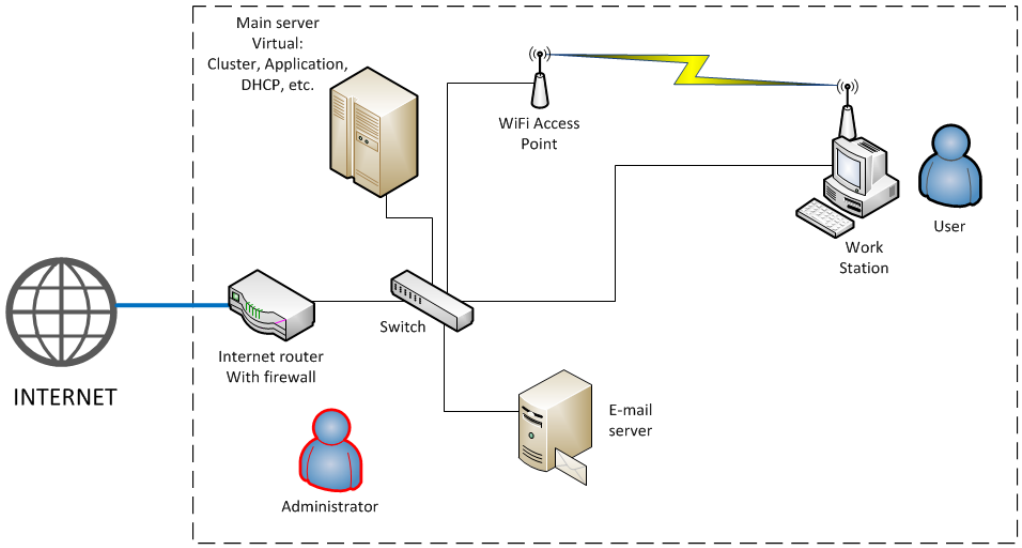


Slika 8.4. Grafički prikaz rezultata proračuna rizika složenih struktura informacijskih sistema po aspektima (C-I-A)

8.5 PRAKTIČNI PRIMJER IMPLEMENTACIJE ANALIZA UTJECAJA STRUKTURE INFORMACIJSKOG SISTEMA NA RIZIKE U ISMS

Za praktični primjer implementacije analize utjecaja strukture informacijskog sistema na rizike u ISMS koristit će se jedan segment cjelokupnog ISMS-a koji se odnosi na servis e-maila u firmi. Kroz primjer će se pokazati postupak implementacije analize od identifikacije informacijske imovine i funkcionalne blok sheme, preko procjene rizika i određivanja pripadnih težina, definiranje grafa strukture grana i analiza utjecaja strukture na rizike, odnosno težine pojedinih grana strukture, kao i na kompletan sistem.

Blok shema informacijskog podsistema je prikazana na slici 8.5.



Slika 8.5. Blok shema e-mail servisa firme

Polazna pretpostavka: prema zahtjevima sigurnosne politike i politike upotrebe e-mail servisa koje je firma definirala u okviru svog ISMS-a, e-mail servis firme treba osigurati visoku pouzdanost rada, odnosno svesti rizik funkcije na minimalnu moguću mjeru. Zbog specifične djelatnosti firme koja cjelokupnu svoju aktivnost temelji na stalnom i pouzdanom funkcioniranju e-mail servisa treba osigurati stalnost funkcioniranja, ali i informacijsku sigurnost u skladu sa zahtjevima standarda ISO 27001. Pod funkcionalnošću e-mail servisa se smatra mogućnost prijema i slanja e-mail poruka uz potpuno poštivanje pretpostavljene tajnosti informacija i sadržaja e-mail poruka.

Funkcionalni opis strukture uspostavljenog E-mail servisa firme prikazanog na slici 8.5 je kako slijedi:

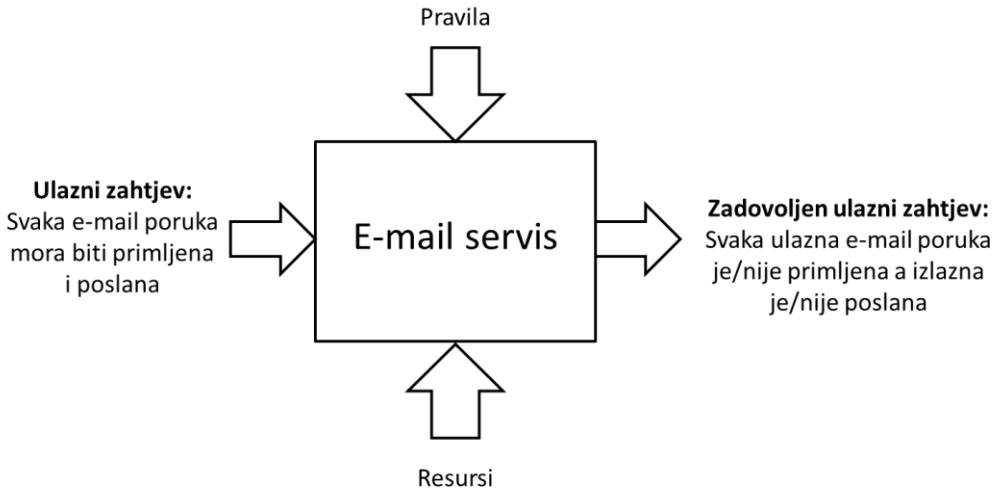
a) Ulazno/izlazna linija iz/u internet okruženje dolazi na Internet router u kojemu je ugrađen firewall.
b) Izlaz Internet routera je spojen na switch čija je funkcija povezivanje svih elemenata IT opreme e-mail servisa u funkcionalnu cjelinu.
c) E-mail server je zasebni server na kojem se nalazi instaliran softver za sveobuhvatnu manipulaciju ulazno/izlaznih e-mail poruka. Na e-mail serveru je softver za e-mail servis

instaliran u virtualno okruženje i na njemu se ne obavljaju nikakvi drugi IT poslovi za potrebe firme. Razlog virtualizacije e-mail servera je zbog mogućnost brze fizičke zamjene servera sa nekim novim u koliko dođe do njegovog oštećenja i prestanka rada, ali i mogućnosti njegove replikacije na cluster serveru.

d) Main server je centralni kompjuter na kojem se obrađuju sve aktivnosti firme vezane za IT obradu podataka (marketing, knjigovodstvo, iznajmljivanje kompjuterskih resursa partnerima, razvoj aplikativnog softvera, itd.). Zbog sigurnosti i nezavisnosti rada na Main serveru su instalirane potrebne virtualne mašine za pojedine poslove. Jedna od virtualnih mašina je namijenjena da radi u clusteru sa samostalnim E-mail serverom.
e) Dva servera (Main i e-mail server) su međusobno vezana preko switcha. Veza ima zadatak da se automatski sve promjene na e-mail serveru automatski zapisuje i na virtualni e-mail server koji se nalazi na Main serveru. Time se osigurava da u slučaju prestanka rada glavnog e-mail servera njegova virtualna slika može odmah preuzeti funkciju e-mail servisa firme.
f) Preko WiFi access pointa se može komunicirati sa Main serverom, kao i e-mail serverom samo u slučaju da se izgubi komunikacija preko kablovske strukture u firmi, bilo dijela mreže, bilo da cijela mreža ne funkcionira.
g) User se pored nekih poslova vezanih za funkcioniranje firme obavezno koristi s implementiranim e-mail servisom.
h) Administrator je osoba koja je zadužena za administraciju i tehničku podršku IT opreme.
i) Serveri se napajaju preko UPS uređaja.

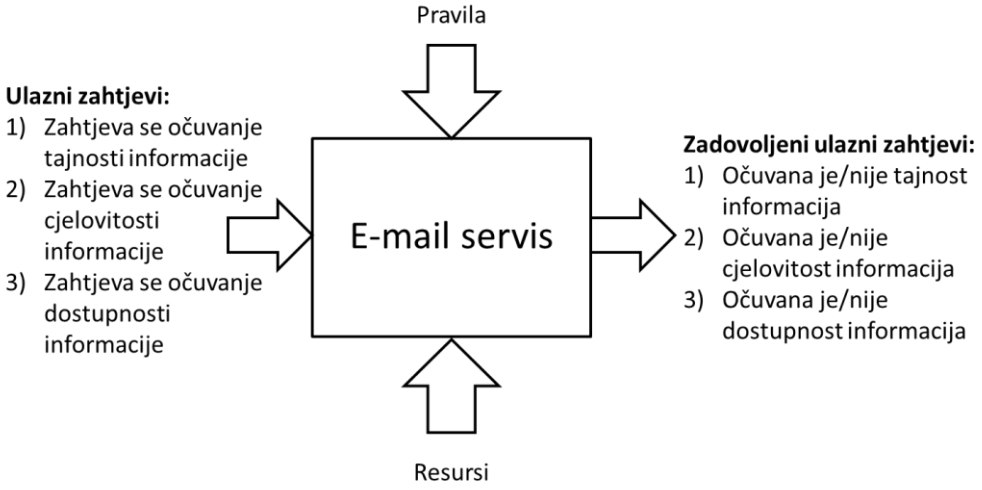
Pretpostavlja se da u firmi ima više Work stationa i Usera, ali svi oni imaju u funkcionalnom i sigurnosnom smislu potpuno iste karakteristike i konfiguracije. Zbog toga je na shemi prikazana samo jedna Work station i jedan User.

Ovakva struktura e-mail servisa se može u funkcionalnom smislu promatrati kao poslovni proces u cilju upravljanja (vidi 2.5). Pri tome treba se razlikovati s kojeg aspekta se želi prikazati funkcionalnost e-mail servisa. Ako se gleda s aspekta obične funkcionalnosti tada se proces može prikazati kao na slici 8.6.



Slika 8.6. Blok shema procesa e-mail servisa za aspekt funkcionalnosti

Međutim, s aspekta informacijske sigurnosti blok shema procesa e-mail servisa se mijenja. Naime, u kontekstu standarda ISO 27001 ulazni zahtjevi za sistem upravljanja informacijskom sigurnošću su: očuvanje tajnosti, očuvanje cjelovitosti i očuvanje dostupnosti informacija. U tom slučaju proces e-mail servisa firme se može prikazati kao na slici 8.7.



Slika 8.7. Blok shema procesa e-mail servisa firme s aspekta informacijske sigurnosti

Može se pokazati da proces e-mail servisa (kao i bilo koji drugi proces) s aspekta ISMS-a u biti implicitno sadržava i funkcionalni zahtjev kroz zahtjev očuvanja cjelovitosti i dostupnosti informacija. Prema tome, u koliko se zadovolje svi ulazni zahtjevi ISMS-a za e-mail servis, sigurno je ispunjen i zahtjev funkcionalnosti.

Veza između slike 8.5, te slika 8.6 i 8.7 je kako slijedi:

a) resursi su elementi prikazani na slici 8.5,
b) pravila su interni dokumenti (politike, procedure, radne upute), nacionalna legislativa, strukovna pravila, te eventualne ugovorne obaveze partnera firme. Naravno, od navedenih pravila uzimaju se u obzir samo ona koja su relevantna za proces e-mail servisa.

Za gore prikazan slučaj e-mail servisa i opisana stanja za potrebe analize utjecaja strukture na rizike koristit će se slijedeći koraci:

a) identifikacija i popis informacijske imovine
b) procjena rizika (sa identifikacijom prijetnji, ranjivosti i posljedica)
c) definiranje grafa složene strukture na temelju blok sheme e-mail servisa
d) definiranje matrice strukture
e) analiza utjecaja strukture na težine grana, odnosno rizike.

Za potrebe procjene rizika koristi će se vlastiti razvijeni softver Hestia RISK, a za potrebe analize utjecaja strukture na ukupne rizike e-mail servisa, također vlastiti razvijeni softver LATMAT.

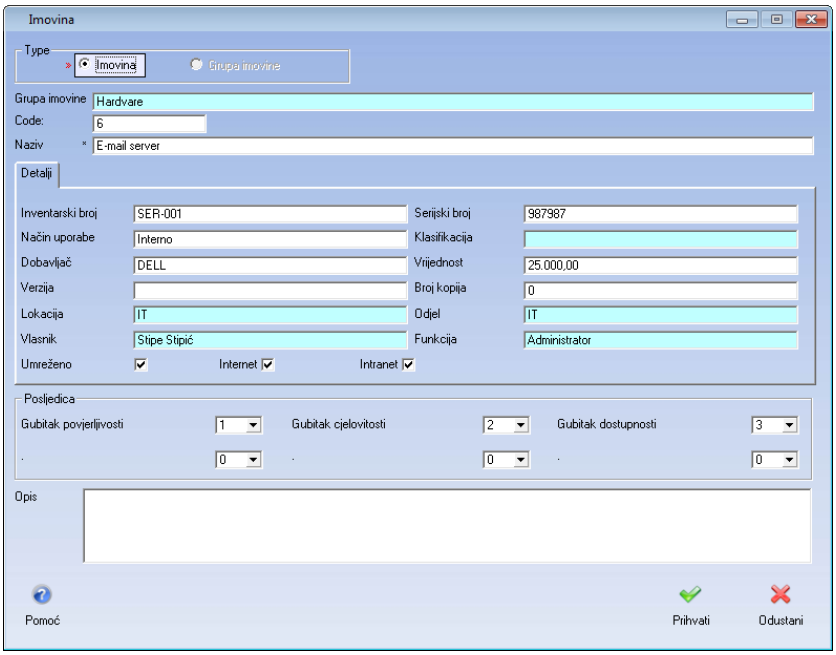
8.5.1 Identifikacija i popis imovine

Identifikacija i popis informacijske imovine koja se nalazi u okviru e-mail servisa organizacije (Slika 8.5) napravljen je u skladu sa smjernicama standarda ISO/IEC 27005:2011. Podaci o informacijskoj imovinu su upisani u softver Hestia RISK. Primjer popisa informacijske imovine u softver Hestia ISMS za slučaj e-mail servisa prikazan je na slici 8.8.

Br	Naziv imovine	Ser.broj	Inv.broj	Model	Dobavljač	Vlasnik
Hardver						
1	Internet router	YW-O123	NET-021		CISCO	Admin
2	Switch	3213AXW	NET-011		CISCO	Admin
3	Main Server	17243-123	SER-002		IBM	Admin
4	E-mail Server	987987	SER-001		DELL	Admin
5	WiFi Access Point	RTF977JK	NET-098		DELL	Admin
6	Work Station	IK00-Q-12	WS-025		IBM	Admin
Ljudi						
1	Admin	-	-	-	-	Org.menadžer
2	End User	-	-	-	-	Org.menadžer

Slika 8.8. Pregled popisane informacijske imovine e-mail servisa

U zadnjoj koloni se nalazi podatak o vlasniku informacijske imovine. Pojam vlasnika tu treba uzeti uvjetno. Naime, vlasnik je osoba odgovorna za pravilnu upotrebu informacijske imovine i pripadnih rizika na njoj. Vlasništvo u ovom kontekstu nema nikakve veze sa imovinskim vlasništvom. Posebno se to odnosi na informacijsku imovinu 'LJUDI' u kom slučaju se pojam vlasništva posebno naglašava postojanjem samo funkcionalne odgovornosti „vlasnika“. Za ilustraciju, na slici 8.9. je prikazan način upisa informacijske imovine u bazu softvera Hestia RISK.

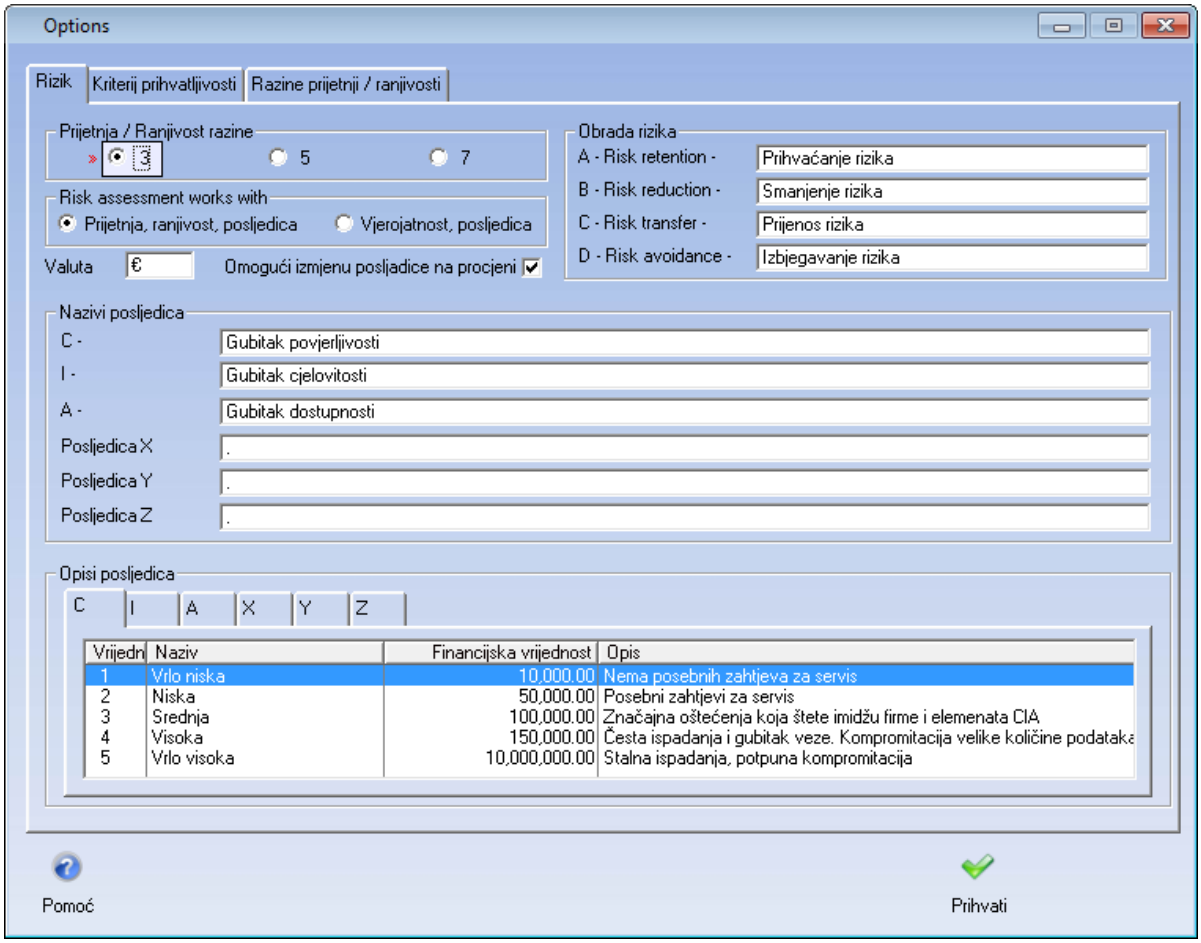


Slika 8.9. Primjer upisa informacijske imovine u bazu softvera Hestia RISK

Na slici 8.9. je dan primjer za E-mail servera, a sličan je postupak i za ostalu imovine koja se nalazi u okviru e-mail servisa organizacije.

8.5.2 Procjena rizika e-mail servisa

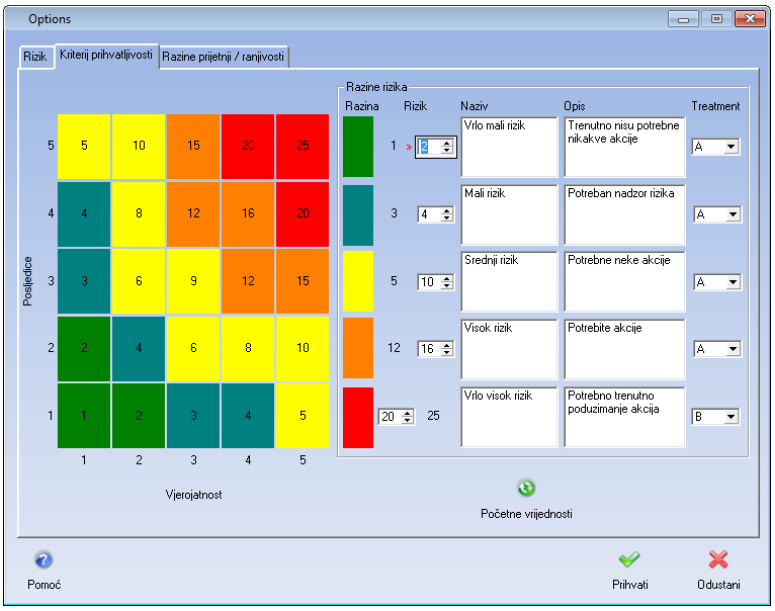
Da bi se moglo pristupiti procjeni rizika, nužno je prema ISO/IEC 27001:2005 i ISO/IEC 27005:2011 definirati elemente okvira za procjenu rizika. Načini definiranja tih elemenata (elementi kvalitativne metodologije, skale i kriteriji za procjenu, itd.) prikazani su na slikama 8.10. do 8.12.



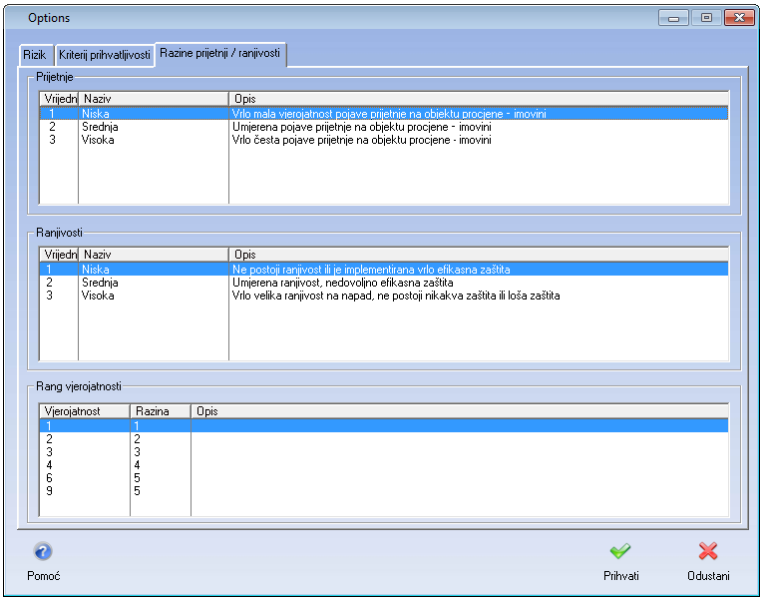
Slika 8.10. Definiranje elemenata procjene prijetnji i ranjivosti u softveru Hestia RISK

Slike prikazuju praktički cjelokupni okvir procjene rizika za ISMS neke organizacije, a time i za e-mail servis te organizacije. Može se vidjeti da je odabrana skala prijetnji i ranjivosti na 3 nivoa, te skale vjerojatnosti i posljedica na 5 nivoa.

Matematički aparat koji se koristi u softveru Hestia RISK za procjenu rizika opisan je izrazima (5.3, 5.4 i 5.5).



Slika 8.11. Definiranje kriterija prihvatljivosti u softveru Hestia RISK



Slika 8.12. Definiranje značenja razina prijetnji i ranjivosti u softveru Hestia RISK

Podaci na slikama 8.10. do 8.12. za ISMS firme moraju biti definirani kroz odgovarajuće dokumente koje odobrava ovlašteno lice, i tada je metodološki pristup procjene rizika jedinstveno definiran i obavezan za cijeli ISMS.

8.5.3 Rezultati procjene rizika e-mail servisa

Na temelju identificiranih podataka o informacijskoj imovini e-mail servisa, te metodologije i kriterija procjene rizika može se pristupiti procjeni rizika. Ovdje se neće prikazivati cijeli postupak procjene rizika pomoću softvera Hestia RISK, već samo konačni rezultat procjene rizika. Na slici 8.13 prikazani su rezultati procjene rizika. Korišteni su elementi za procjenu prikazani na slikama 8.10-8.12. Obojani podaci u koloni RRI (Relativni rizik) upućuje na rang rizika u skladu sa matricom prihvatljivosti prikazanoj na slici 8.11.

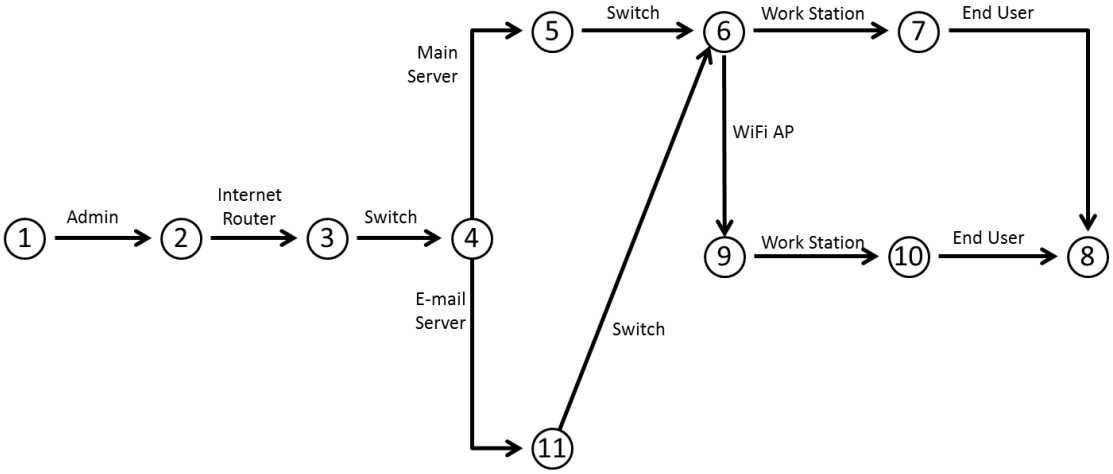
1	**Imovina**	**ADMIN**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Krađa medija ili dokumenata / Rad bez nadzora osoblja	2	2	3	12	**0,3**
	Cjelovitost (I)	Nedostupnost zaposlenika / Odsutnost zaposlenika	1	2	2	4	**0,1**
	Dostupnost (A)	Greška pri korištenju / Pogrešno korištenje HW i SW	2	3	3	18	**0,4**
2	**Imovina**	**INTERNET ROUTER**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Kvar softvera / Nedostatak efektivnih kontrola za promjenu	2	2	2	8	**0,2**
	Cjelovitost (I)	Neovlašt.korištenje podataka / Omogućeni nepotrebni servisi	2	3	1	6	**0,1**
	Dostupnost (A)	Kvar telekomunikacijske opreme / Loši spojevi kablova	3	2	4	24	**0,5**
3	**Imovina**	**SWITCH**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Gubitak napajanja / Osjetljivost na varijacije napona	2	2	1	4	**0,1**
	Cjelovitost (I)	Gubitak napajanja / Osjetljivost na varijacije napona	2	2	1	4	**0,1**
	Dostupnost (A)	Gubitak napajanja / Osjetljivost na varijacije napona	2	2	3	12	**0,3**
4	**Imovina**	**MAIN SERVER**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Povreda prava / Nedostatak formalnih procedura za prijavu i odjavu korisnika	3	2	4	24	**0,5**
	Cjelovitost (I)	Korupcija podataka / Nedostatak formalnih procedura za nadzor podataka ISMS-a	3	2	4	24	**0,5**
	Dostupnost (A)	Uništenje opreme ili medija / Nedostatak shema za periodičke izmjene	3	3	3	27	**0,6**
5	**Imovina**	**E-MAIL SERVER**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Prisluškivanje / Nezaštićene komunikacijske linije	3	2	3	18	**0,4**
	Cjelovitost (I)	Ilegalno procesiranje podataka / Nedostatak nadzornih mehanizama	3	3	3	27	**0,6**
	Dostupnost (A)	Uništenje opreme ili medija / Neadekvatno korištenje kontrola za pristup zgradama i sobama	3	3	3	27	**0,6**
6	**Imovina**	**WI-FI ACCESS POINT**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Greška pri korištenju / Pogrešno podešavanja parametara	3	2	3	18	**0,4**
	Cjelovitost (I)	Gubitak napajanja / Nestabilna mreža napajanja	1	2	3	6	**0,1**
	Dostupnost (A)	Krađa opreme / Nedostatak fizičke zaštite zgrada, vrata i prozora	3	2	3	18	**0,4**
7	**Imovina**	**WORK STATION**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Povreda prava / Ne odjavljivanje na odlasku sa radne stanice	3	3	3	27	**0,6**
	Cjelovitost (I)	Greška u korištenju / Nedostatak učinkovite kontrole za promjenu konfiguracije	2	2	2	8	**0,2**
	Dostupnost (A)	Neovlašteno korištenje opreme / Nedostatak politika za ispravno korištenje telekomunikacijskih medija i poruka	2	2	4	16	**0,4**
8	**Imovina**	**END USER**					
	Aspekt	**Prijetnja / ranjivost**	**PR**	**RA**	**PO**	**RI**	**RRI**
	Tajnost (C)	Greška pri korištenju / Nedovoljna oduka za zaštitu	3	2	4	24	**0,5**
	Cjelovitost (I)	Neovlašteno korištenje opreme / Nedostatak politika za ispravno korištenje telekomunikacijskih medija i poruka	1	2	2	4	**0,1**
	Dostupnost (A)	Ilegalno procesiranje podataka / Nedostatak nadzornih mehanizama	1	3	3	9	**0,2**
Legenda:		**PR**=prijetnja **RA**=ranjivost **PO**=posljedica **RI**=rizik **RRI**=relativni rizik					

Slika 8.13. Rezultati procjene rizika za e-mail servis

U procesu procjene rizika za e-mail servis analizirane su sve relevantne kombinacije prijetnja / ranjivost koje mogu izazvati posljedice. Od njih su na slici 8.13 prikazani samo oni slučajevi koji izazivaju najveći rizik u trenutku analize i procjene. Kombinacije prijetnja / ranjivost koji su analizirani za procjenu rizika preuzeti su iz priloga 12.5.

8.5.4 Analiza strukture e-mail servisa

Na temelju blok sheme e-mail servisa firme prikazanog na slici 8.5. i opisa metodologije definiranja grafa strukture (vidi 6.) može se nacrtati shema strukture e-mail servisa. Graf strukture e-mail servisa je prikazan na slici 8.14.

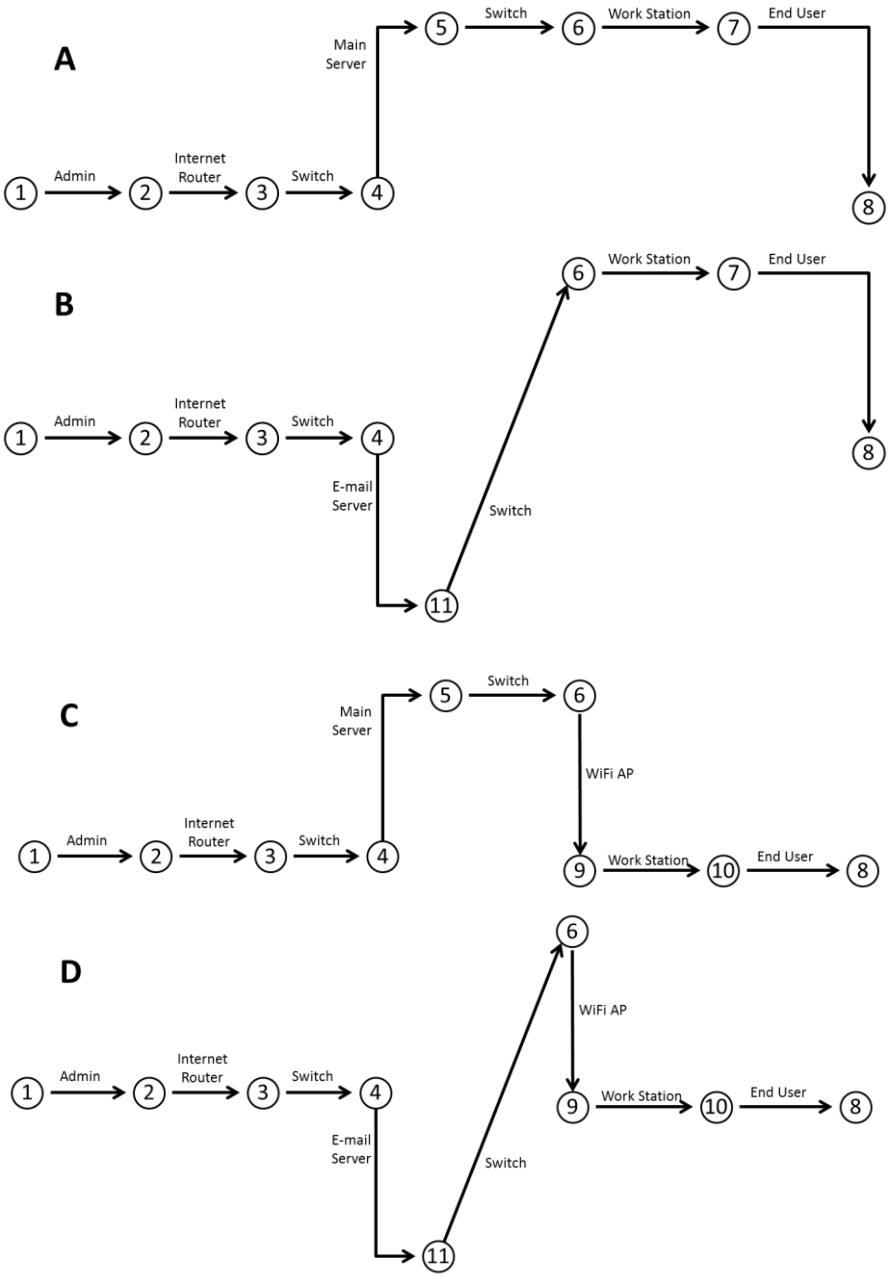


Slika 8.14. Graf strukture e-mail servisa sa slike 8.5.

Prema usvojenim pravilima u poglavlju 6. grane grafa predstavljaju informacijsku imovinu identificiranu prema slici 8.5. Na ulazu u strukturu kao serijski element rizika (težine) za informacijsku sigurnost su stavljeni Administrator, Internet router i Switch. Smjer strelica na granama grafa ukazuje na mogući smjer kretanja informacije (e-maila). Slika ilustrira način prijema e-maila s interneta, odnosno e-mail servera. Što se tiče slanja e-mail poruka od strane korisnika problem je potpuno jednak u sigurnosnom smislu. Naime, ako su postignuti određeni nivoi sigurnosti za aspekte C-I-A izražene kroz pripadne rizike za dolazne e-mail poruke, tada je potpuno ista situacija i za odlazne e-mail poruke.

Napomena: ista fizička informacijska imovina se može nalaziti više puta u jednom grafu strukture. Time se postiže prikaz mogućeg funkcionalnog puta informacije. Glavna značajka tako replicirane imovine u više grana je da takva grana uvijek imaju istu težinu (rizike) koji su definirani za pripadnu informacijsku imovinu. Primjer takvog prikaza su Switch u tri grane, Work station u dvije grane, kao i User u dvije grane.

Može se uočiti na slici 8.14. da postoje četiri grane kojima se osigurava funkcioniranje E-mail servisa. Prikaz pojedinih putova kroz graf su prikazani na slici 8.15. Grafovi A i B odnose se na dva puta u kojima ima 7 grana, a grafovi C i D imaju putove od 8 grana.



Slika 8.15. Grafovi putova od ulaznog do izlaznog čvora za primjer sa slike 8.14.

Na temelju grafa prikazanog na slici 8.14. treba napraviti latinsku kompoziciju. Rezultat identifikacije strukture i konverzije u latinsku strukturu prikazan je u tablici 8.7. Zbog broja čvorova koji prelazi 9, svi su označeni dvoznamenkastim brojem, tako da je npr. veza između čvora 2 i čvora 3 prikaza kodom '0203'.

U tablici 8.8 su prikazani rizici i ekvivalentne težine pojedinih grana latinske strukture. Pri tome je korišten odnos rizika i težine prema izrazu (7.1). Veličine rizika su dobivene putem procjene usvojenom metodologijom u firmi, a provedenom pomoću softvera Hestia RISK.

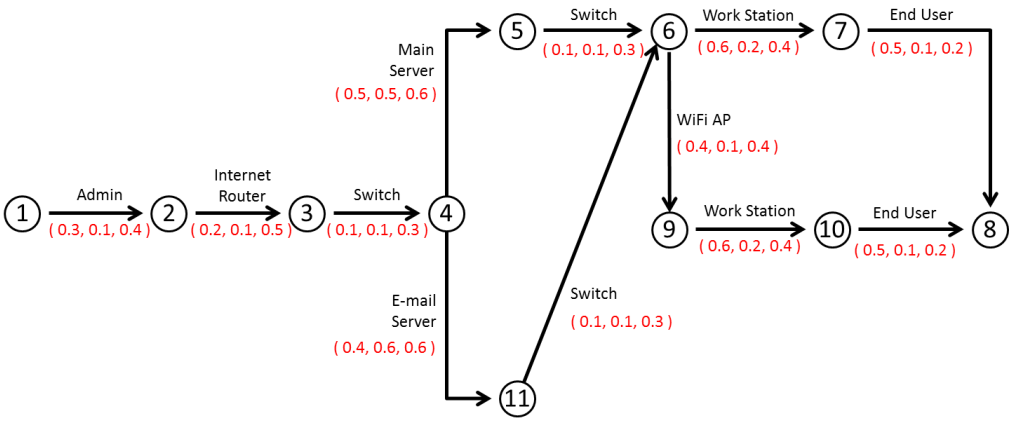
Tablica 8.7. Prikaz latinske kompozicije za graf strukture prikazan na slici 8.14.

	01	02	03	04	05	06	07	08	09	10	11
01	0	**0102**	0	0	0	0	0	0	0	0	0
02	0	0	**0203**	0	0	0	0	0	0	0	0
03	0	0	0	**0304**	0	0	0	0	0	0	0
04	0	0	0	0	**0405**	0	0	0	0	0	**0411**
05	0	0	0	0	0	**0506**	0	0	0	0	0
06	0	0	0	0	0	0	**0607**	0	**0609**	0	0
07	0	0	0	0	0	0	0	**0708**	0	0	0
08	0	0	0	0	0	0	0	0	0	0	0
09	0	0	0	0	0	0	0	0	0	**0910**	0
10	0	0	0	0	0	0	0	**1008**	0	0	0
11	0	0	0	0	0	**1106**	0	0	0	0	0

Tablica 8.8. Rizici i težine informacijske imovine u granama grafa

Grana	Informacijska imovina	Rizik (C, I, A)	Težina (C, I, A)
0102	Admin	(0.3, 0.1, 0.4)	(0.7, 0.9, 0.6)
0203	Internet Router	(0.2, 0.1, 0.5)	(0.8, 0.9, 0.5)
0304, 0506, 1106	Switch	(0.1, 0.1, 0.3)	(0.9, 0.9, 0.7)
0405	Main Server	(0.5, 0.5, 0.6)	(0.5, 0.5, 0.4)
0411	E-mail Server	(0.4, 0.6, 0.6)	(0.6, 0.4, 0.4)
0609	WiFi Access Point	(0.4, 0.1,0.4)	(0.6, 0.9, 0.6)
0607, 0910	Work Station	(0.6, 0.2, 0.4)	(0.4, 0.8, 0.6)
0708, 1008	End User	(0.5, 0.1, 0.2)	(0.5, 0.9, 0.8)

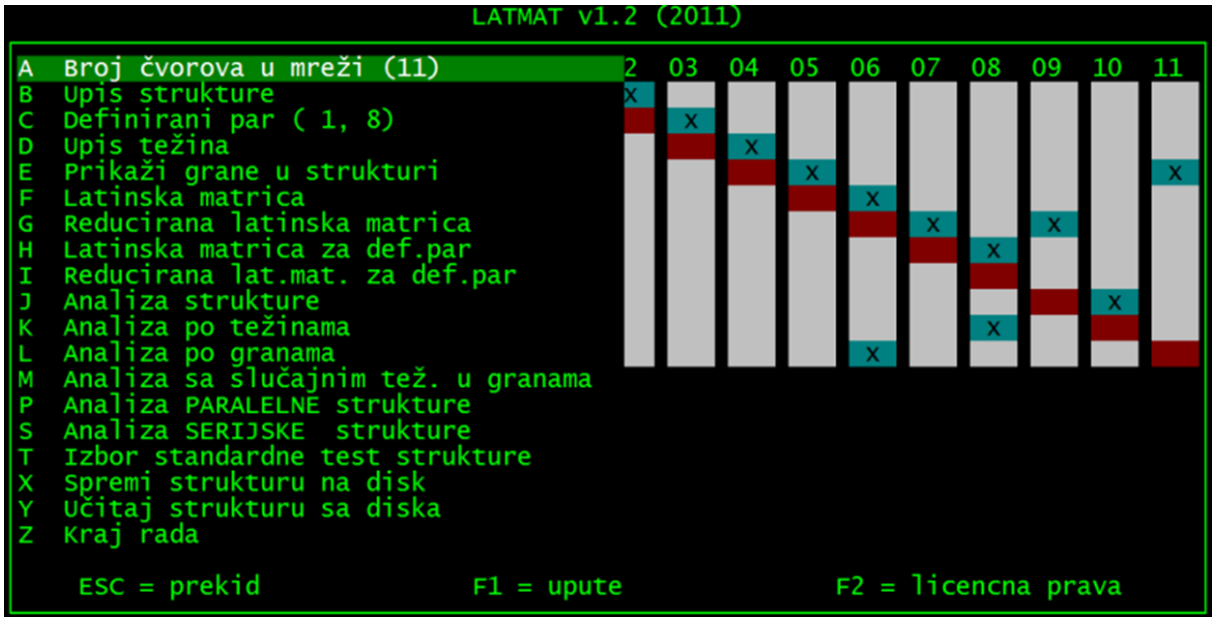
Na temelju gore iznesenog može se nacrtati graf strukture e-mail servisa s pripadnim veličinama rizika u pojedinim granama. Rizici u zagradama se odnose na aspekte C-I-A respektivno. Tako dobiveni graf sa upisanim rizicima pojedinih grana prikazan je na slici 8.16.



Slika 8.16. Graf strukture s rizicima grana na temelju procjene za aspekte C-I-A

Ovako dobiveni podaci grafa i procjene rizika se trebaju upisati u softver LATMAT koji se koristio za daljnju analizu ukupnog rizika (težine) strukture e-mail servisa firme.

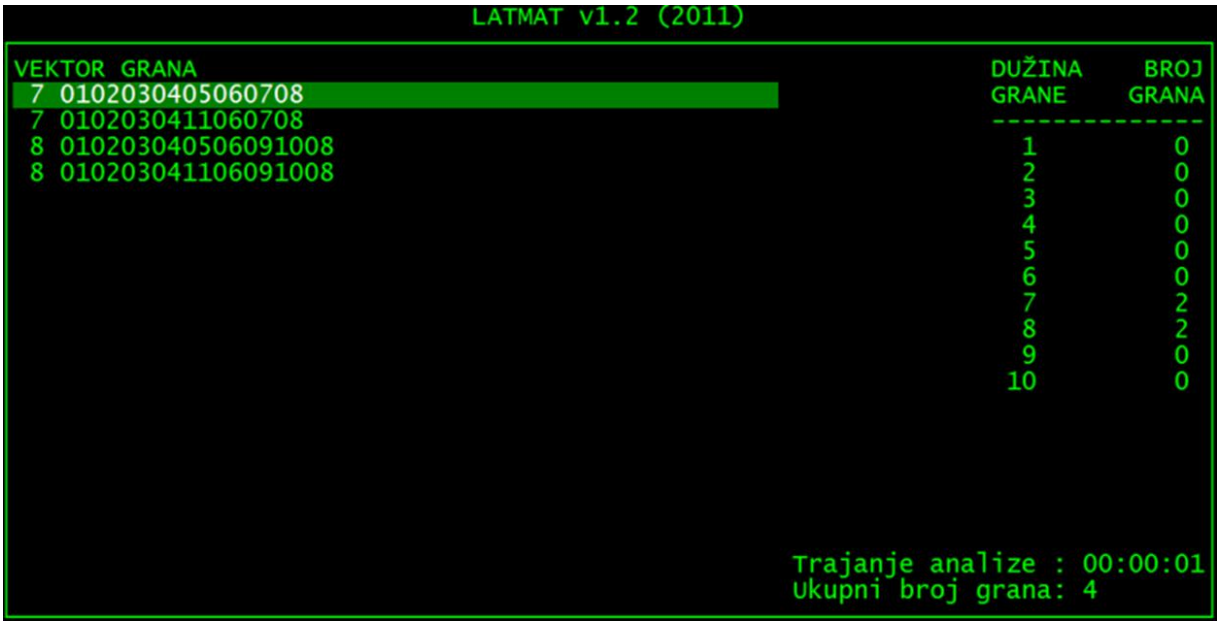
Primjeri upisanih podataka u softver LATMAT za strukturu e-mail servisa sa slike 8.14, prikazan je na slici 8.17.



Slika 8.17. Upisana struktura e-mail servisa sa slike 8.14. u softver LATMAT

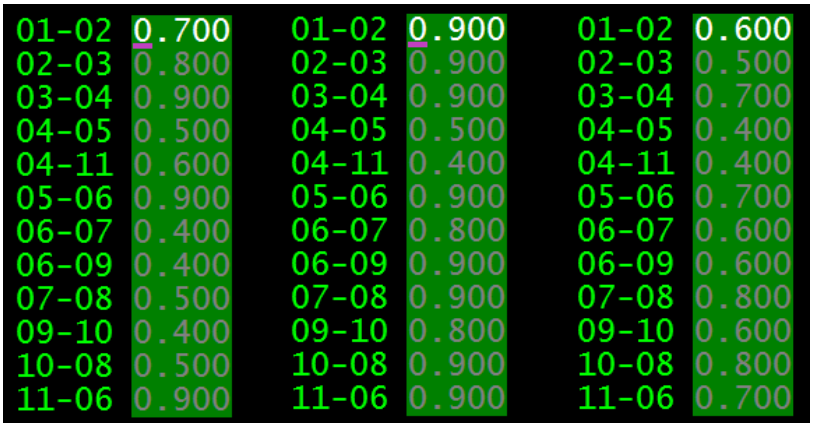
Putovi koji povezuju ulazni i izlazni čvor kako ih je pronašao softver LATMAT na temelju analize latinske kompozicije prikazan je na slici 8.18.

Može se vidjeti da je softver pronašao ukupno četiri puta, i to dva dužine 7 i dva dužine 8 segmenata – grana. Vektori putova povezuju čvorove 01-02-03-04-05-06-07-08, itd.



Slika 8.18. Pronađeni putovi pomoću softvera LATMAT od ulaznog do izlaznog čvora za strukturu sa slike 8.14.

U softver LATMAT nužno je upisati i težine svake grane grafa složene strukture e-mail servisa. U tu svrhu koristit će se podaci prikazani u tabeli 8.8. U sam softver LATMAT će biti upisane težine grana (ne rizici) iz navedene tablice i to za svaki aspekt informacijske sigurnosti (tajnost, cjelovitost i dostupnost). Upisane težine grana strukture za svaki aspekt informacijske sigurnosti prikazane su na slici 8.19.



Slika 8.19. Prikaz upisanih težina grana za e-mail strukturu u softver LATMAT za aspekte informacijske sigurnosti C-I-A respektivno

Na slici se vide tri kolone. Svaka kolona predstavlja težine grana za jedan aspekt informacijske sigurnosti. S lijeva na desno: tajnost (C), cjelovitost (I) i dostupnost (A) respektivno.

Na temelju tako upisanih podataka za zadanu strukturu e-mail servisa, pomoću softvera LATMAT se može napraviti analiza težine strukture za svaki aspekt informacijske sigurnosti posebno.

Rezultat analize strukture pomoću softvera LATMAT prikazani su na slici 8.20.

(C)

Ukupan broj grana u strukturi 4 UKUPNA TEŽINA STRUKTURE 0.1329983

Grane u strukturi	Težine u granama								Tež.SERIJ. grane
7 010203040	0.700	0.800	0.900	0.500	0.900	0.400	0.500		0.0453600
7 010203041	0.700	0.800	0.900	0.600	0.900	0.400	0.500		0.0544320
8 010203040	0.700	0.800	0.900	0.500	0.900	0.400	0.400	0.500	0.0181440
8 010203041	0.700	0.800	0.900	0.600	0.900	0.400	0.400	0.500	0.0217728

(I)

Ukupan broj grana u strukturi 4 UKUPNA TEŽINA STRUKTURE 0.5951628

Grane u strukturi	Težine u granama								Tež.SERIJ. grane
7 010203040	0.900	0.900	0.900	0.500	0.900	0.800	0.900		0.2361960
7 010203041	0.900	0.900	0.900	0.400	0.900	0.800	0.900		0.1889568
8 010203040	0.900	0.900	0.900	0.500	0.900	0.900	0.800	0.900	0.2125764
8 010203041	0.900	0.900	0.900	0.400	0.900	0.900	0.800	0.900	0.1700611

(A)

Ukupan broj grana u strukturi 4 UKUPNA TEŽINA STRUKTURE 0.0873645

Grane u strukturi	Težine u granama								Tež.SERIJ. grane
7 010203040	0.600	0.500	0.700	0.400	0.700	0.600	0.800		0.0282240
7 010203041	0.600	0.500	0.700	0.400	0.700	0.600	0.800		0.0282240
8 010203040	0.600	0.500	0.700	0.400	0.700	0.600	0.600	0.800	0.0169344
8 010203041	0.600	0.500	0.700	0.400	0.700	0.600	0.600	0.800	0.0169344

Slika 8.20. Rezultati analize težina strukture e-mail servisa pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)

Na slici 8.20. su prikazani rezultati za svali aspekt informacijske sigurnosti. Može se vidjeti da je težina cijele strukture za aspekt tajnosti (C) iznosi 0.1329983, odnosno u skladu s izrazom (7.1) rizik cijele strukture u tom slučaju je 0.8670017. Na isti način se može dobiti rezultat i za ostala dva aspekta informacijske sigurnosti.

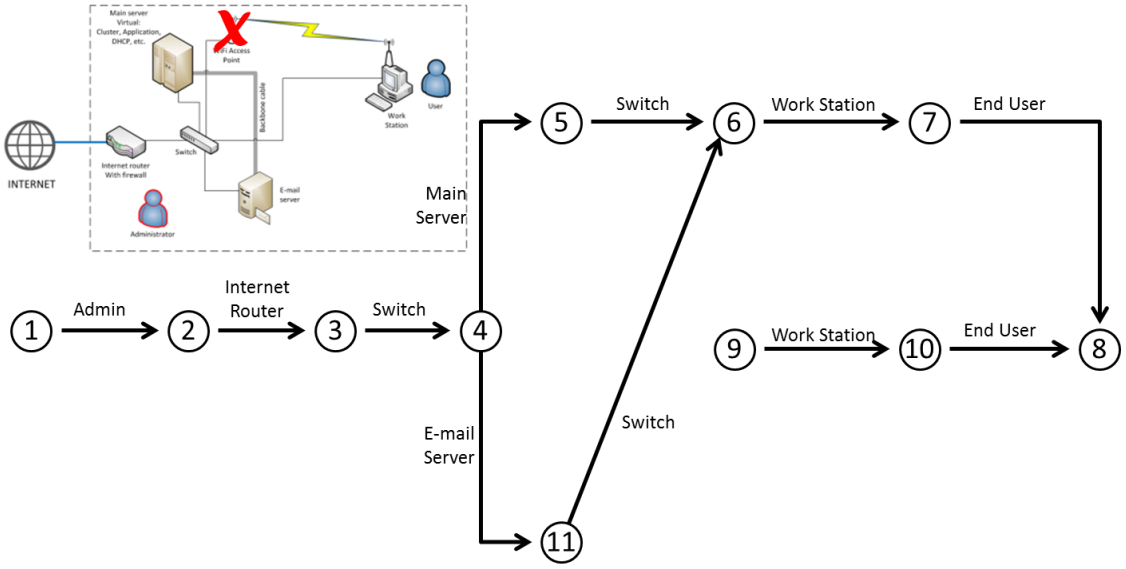
Rezultati analize težine cijele strukture e-mail servisa prikazanog na slici 8.5. može se vidjeti u tablici 8.9.

Tablica 8.9. Težine i rizici strukture e-mail servisa

Aspekt informacijske sigurnosti	Težina strukture	Rizik strukture
C - Tajnost	0.1329983	0.8670017
I - Cjelovitost	0.5951628	0.4048372
A - Dostupnost	0.0873645	0.9126355

8.5.5 Analiza strukture e-mail servisa bez funkcionalnosti WiFi segmenta

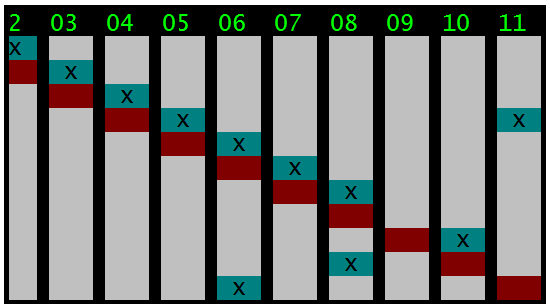
Ako pretpostavimo da je WiFi segment strukture e-mail servisa van funkcije, odnosno da se ne može komunicirati preko WiFi mreže treba napraviti analizu rizika u tom slučaju. Kako su svi elementi isti sa slike 8.5. kao i procijenjeni rizici pojedinih elementa strukture osim što WiFi Access Point ne funkcionira, graf strukture sa slike 8.14. se treba modificirati i imat će oblik prikazan na slici 8.21.



Slika 8.21. Blok shema i pripadni graf strukture e-mail servisa za slučaj neispravnosti WiFi Access pointa

Promjena u odnosu na sliku 8.14. je isključenje grane 06-09 (WiFi AP). Logično, kao posljedica nove nastale situacije mogu se isključiti i grane 09-10 i 10-08 jer objektivno one više nisu dijelovi nekog spojnog puta od ulaznog do izlaznog čvora strukture. Međutim, ako i ostanu u strukturi, a softver LATMAT ih neće koristiti u analizi. Time se može ilustrirati funkcionalnost algoritma i softvera LATMAT u smislu da se evidentiraju sve grane sa svojim pripadnim težinama, a u rezultatu analize se mogu pojaviti samo oni putovi koji stvarno postoje u danom trenutku i situaciji funkcionalnosti strukture.

U skladu s načinom rada sa softverom LATMAT prikazanim u poglavlju 8.5.4. latinska kompozicija za strukturu sa slike 8.21. imat će oblik prikazan kao na slici 8.22.



Slika 8.22. Struktura sa slike 8.21. upisana u softver LATMAT

Sa slike se može vidjeti da je ispuštena smo grana 06-09 u odnosu na cijelu funkcionalnu strukturu. Ako se dalje primjeni potpuno isti postupak analize strukture kao i prethodnom slučaju opisanom u poglavlju 8.5.4. dobit će se dva spojna puta od ulaznog do izlaznog čvora: 01-02-03-04-05-06-07-08 i 01-02-03-04-11-06-07-08. Svaki taj put ima po sedam segmenata (grana). Rezultati analize težine (rizika) tako nove nastale strukture prikazani su na slici 8.23.

(C)

Ukupan broj grana u strukturi 2 UKUPNA TEŽINA STRUKTURE 0.0973230

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.700	0.800	0.900	0.500	0.900	0.400	0.500	0.0453600
7 010203041	0.700	0.800	0.900	0.600	0.900	0.400	0.500	0.0544320

(I)

Ukupan broj grana u strukturi 2 UKUPNA TEŽINA STRUKTURE 0.3805220

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.900	0.900	0.900	0.500	0.900	0.800	0.900	0.2361960
7 010203041	0.900	0.900	0.900	0.400	0.900	0.800	0.900	0.1889568

(A)

Ukupan broj grana u strukturi 2 UKUPNA TEŽINA STRUKTURE 0.0556514

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.600	0.500	0.700	0.400	0.700	0.600	0.800	0.0282240
7 010203041	0.600	0.500	0.700	0.400	0.700	0.600	0.800	0.0282240

Slika 8.23. Rezultati analize težina strukture e-mail servisa sa slike 8.21. pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)

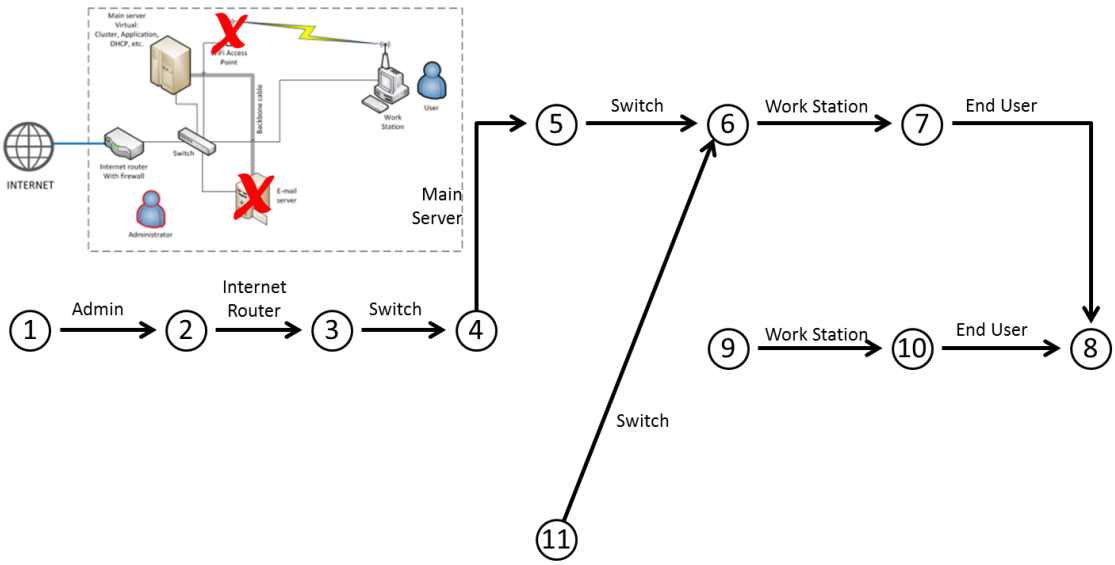
Rezultati analize težine cijele strukture e-mail servisa prikazanog na slici 8.21. može se vidjeti u tablici 8.10.

Tablica 8.10. Težine i rizici strukture e-mail servisa prema slici 8.23.

Aspekt informacijske sigurnosti	Težina strukture	Rizik strukture
C - Tajnost	0.0973230	0.9026770
I - Cjelovitost	0.3805220	0.6194780
A - Dostupnost	0.0556514	0.9443486

8.5.6 Analiza strukture e-mail servisa bez funkcionalnosti WiFi segmenta i nefunkcioniranja E-mail servera

Za ilustraciju utjecaja strukture na ukupan rizik, može se pretpostaviti da ne funkcionira glavni e-mail server, odnosno da ne postoji grana 04-11 (vidi sliku 8.21.). Stanje strukture u tom slučaju (ne funkcionalan WiFi Acces point i E-mail server) prikazano je na slici 8.11.



Slika 8.24. Blok shema i pripadni graf strukture e-mail servisa za slučaj neispravnosti WiFi Access pointa i E-mail servera

Ponavljanjem postupaka prikazanim u poglavljima 8.5.4. i 8.5.5. za provođenje analize strukture i težina pomoću programa LATMAT, kao prvo se utvrđuje da postoji samo jedan put koji povezuje ulazni i izlazni čvor strukture. Taj put je određen granama: 01-02-03-04-05-06-07-08. Težine strukture za svaki aspekt informacijske sigurnosti prikazan je na slici 8.25.

(C)

Ukupan broj grana u strukturi	1	UKUPNA TEŽINA STRUKTURE	0.0453600

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.700	0.800	0.900	0.500	0.900	0.400	0.500	0.0453600

(I)

Ukupan broj grana u strukturi	1	UKUPNA TEŽINA STRUKTURE	0.2361960

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.900	0.900	0.900	0.500	0.900	0.800	0.900	0.2361960

(A)

Ukupan broj grana u strukturi	1	UKUPNA TEŽINA STRUKTURE	0.0282240

Grane u strukturi	Težine u granama							Tež.SERIJ. grane
7 010203040	0.600	0.500	0.700	0.400	0.700	0.600	0.800	0.0282240

Slika 8.25. Rezultati analize težina strukture e-mail servisa sa slike 8.24. pomoću softvera LATMAT za svaki aspekt informacijske sigurnosti (C-I-A)

Rezultati analize težine cijele strukture e-mail servisa prikazanog na slici 8.24. može se vidjeti u tablici 8.11.

Tablica 8.11. Težine i rizici strukture e-mail servisa prema slici 8.24.

Aspekt informacijske sigurnosti	Težina strukture	Rizik strukture
C - Tajnost	0.0453600	0.9546400
I - Cjelovitost	0.2361960	0.7638040
A - Dostupnost	0.0282240	0.9717760

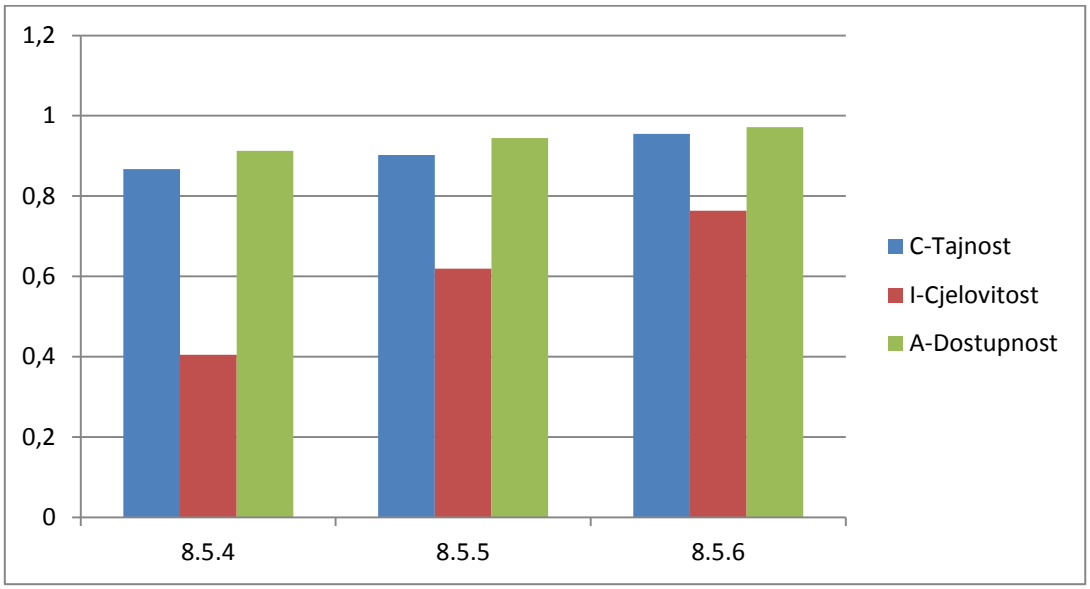
8.5.7 Zaključno razmatranje primjera strukture e-mail servisa

Na temelju provedene analize težina strukture kroz poglavlja 8.5.4 do 8.5.6 može se prikazati ukupnu rezultat u usporednoj tablici 8.12.

Tablica 8.12. Težine i rizici strukture e-mail servisa za slučajeve 8.5.4.-8.5.6.

Aspekt informacijske sigurnosti	Težine strukture			Rizici strukture		
	8.5.4	8.5.5	8.5.6	8.5.4	8.5.5	8.5.6
C - Tajnost	0.1329983	0.0973230	0.0453600	0.8670017	0.9026770	0.9546400
I - Cjelovitost	0.5951628	0.3805220	0.2361960	0.4048372	0.6194780	0.7638040
A - Dostupnost	0.0873645	0.0556514	0.0282240	0.9126355	0.9443486	0.9717760

Na slici 8.26. je grafički prikazana promjena rizika složene strukture e-mail servisa za slučajeve ne funkcioniranja pojedinih segmenata mreže i to za sva tri aspekta informacijske sigurnosti.



Slika 8.26. Grafički prikaz promjene rizika strukture e-mail servisa za aspekte informacijske sigurnosti (C-I-A)

Iz prikazanih rezultata analize se zorno pokazuje kako izmjena strukture utiče na rizike bilo kojeg aspekta informacijske sigurnosti. Prikazani primjer samo potvrđuje s praktične strane iznesene zaključke vezane za utjecaj strukture na ukupne rizike.

Prema danom primjeru (koji je, radi preglednosti, krajnje jednostavan) utvrđeno je slijedeće:

a) Postojeća struktura od **n** fiksno ustanovljenih elemenata ima uvijek točno određeni iznos rizika na temelju mogućnosti određivanja pripadnih rizika za svaki aspekt informacijske sigurnosti C-I-A,
b) Prema navedenim metodama u ovom radu i kroz obrađeni primjer dokazano je da se ovaj rizik može jednoznačno izračunati (ukupno, i za svaku aspekt informacijske sigurnosti C-I-A),
c) Temeljna pretpostavka je da dana struktura obavlja zadanu funkciju (funkcije) u okviru promjene povezivanja uvijek istih elemenata,
d) Kod bilo kakve promjene veze elemenata strukture, rizici pojedinih elemenata ostaju potpuno isti,
e) Kroz dani primjer i provjeru od strane razvijenih alata, jednoznačno je utvrđeno da se ukupni rizik rada cijelog sistema i njegovih osnovnih komponenata (C-I-A) mijenja u zavisnosti od unutrašnjeg povezivanja njegovih elemenata.

Ovaj primjer je pokazao i dokazao slijedeće važne zaključke:

1. Ukupan iznos rizika po volji velike strukture moguće je (uz poznavanje rizika njenih komponenata i načina njihovog povezivanja) jednoznačno izračunati,
2. Rizik informacijske sigurnosti cijele strukture moguće je jednoznačno izračunati na temelju rizika komponenti za svaki aspekt (C-I-A),
3. Moguće je mijenjanje oblika strukture (uz zadržavanje svih komponenata) a da se izvršavaju zadane funkcija (funkcije) sistema,
4. Svaka promjena strukture uz iste elemente i njihove fiksne pripadne rizike daje uvijek drugačiji ukupni rizik sistema koji je moguće izračunati,
5. Moguće je, a što je i dokazano da se sa ukupnim rizikom sistema može upravljati uz promjene njegove strukture i zadržavanje zadanih funkcija.

9. IZGRADNJA MODELA SIMULACIJE

Za potrebe simulacije i analize ponašanja složenih struktura informacijskih sistema razvijen je originalni program kojim su dobiveni svi rezultati prikazani u poglavlju 7.

Pri tome je korišten matematički model za analizu složenih struktura opisan u poglavlju 6.

Kod razvoja aplikacije za analizu posebna pažnja je posvećena optimizaciji obrade velikih matrica u cilju skraćivanja vremena matematičke obrade. Kod toga su se koristile mogućnosti i prednosti odabranog alata na temelju kojega je razvijena i realizirana aplikacija.

Programski jezik je odabran xHarbour koji ima izuzetno velike mogućnosti manipulacije s višedimenzionalnim matricama, a prevođenjem se dobiva aplikacijski kod u C jeziku. Time se osiguralo izuzetno velika brzina izvođenja aplikacije, u slučajevima većeg broja čvorova zadane strukture.

Za grafičku interpretaciju dobivenih rezultata korišten je MS Excel® 2010.

Aplikacija je kompajlirana i linkana u 32-bitnom kodu zbog mogućnosti izvođenja na većini kompjutera.

Aplikacija je nazvana LATMAT.

9.1. Struktura programa LATMAT

Aplikacija LATMAT je razvijana modularno, tako da se cijela aplikacija sastoji od niza modula sa odgovarajućim funkcijama i procedurama. Glavni moduli aplikacije LATMAT su:

- Inicijalizacijski modul
- Glavni izbornik
- Modul za obradu matrica
- Modul izvještavanja

U okviru inicijalnog modula se inicijaliziraju sve globalne varijable i matrice potrebne za pravilno funkcioniranje programa.

Glavni izbornik se koristi za pristup svim funkcijama programa od strane korisnika.

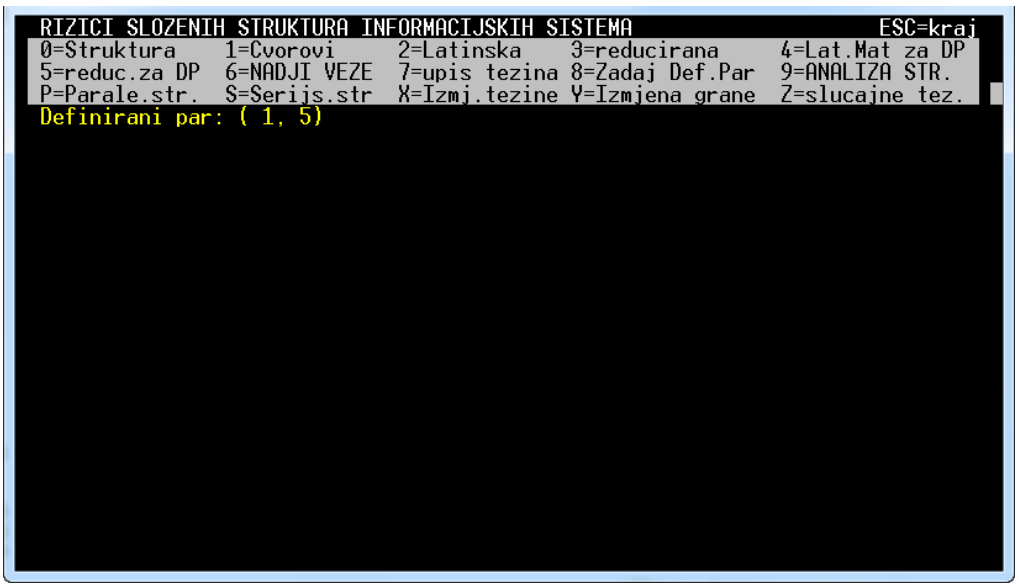
Modul za obradu matrica je razvijen za obavljanje svih manipulacija matricama i izvođenje računskih operacija s njima u skladu s algoritmom i matematičkim modelom opisanim u poglavlju 6.

U okviru modula za izvještavanje dobivaju se pregledi na ekranu, ali i mogućnost eksporta podataka pogodnom za učitavanje u druge razne programske alate koji su uobičajeni za

grafičku ili neku drugu obradu. Naime, program LATMAT nije u osnovi namijenjen za konačni prikaz rezultata matematičke analize, već za dobivanje rezultata, a onda prijenosom u neki program se ti rezultati mogu prikazati u željenom obliku. U okviru ovog rada za grafičku prezentaciju rezultata matematičke analize iz programa LATMAT korišten je program, kao što je već navedeno, MS Excel® 2010.

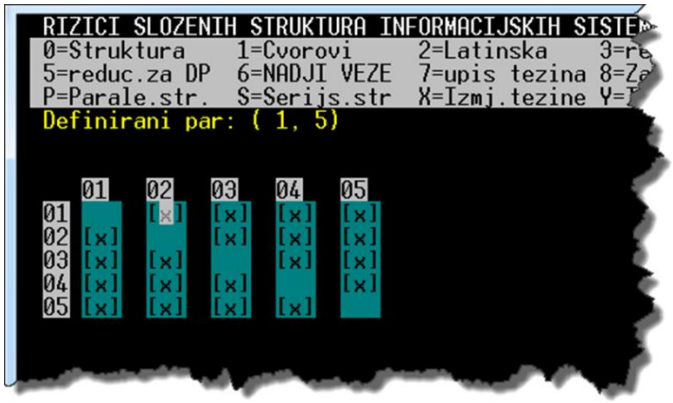
9.2. Definiranje struktura u programu LATMAT

Pokretanjem programa LATMAT dobiva se ekran s glavnim menijem preko kojega se može doći do svih predviđenih funkcija. Na slici 9.1. prikazan je izgled glavnog menia programa LATMAT.



Slika 9.1. Glavni meni programa LATMAT

Pritiskom na tipku 0 dobiva se mogućnost upisa strukture. Primjer je prikazan na slici 9.2.

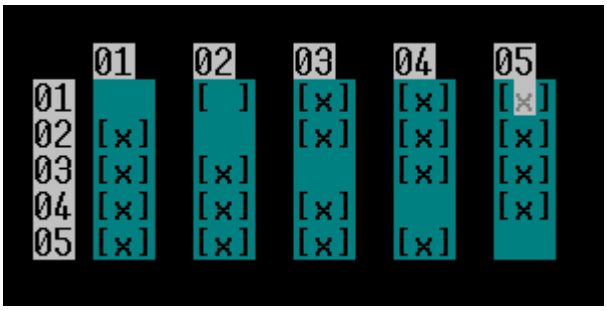


Slika 9.2. Definiranje strukture mreže za primjer neorijentirane strukture prema slici 7.7.

Nakon što se dobije ekran prikazan na slici 9.2. može se definirati matrica strukture. Ako se postavi X u polje (01,02) program LATMAT to tumači da postoji veza između čvora 01 i 02 i to sa usmjerenjem od 01 do 02. Ako se postavi X u polje (02,01) tada to isto znači da postoji veza između čvora 01 i 02, ali sa usmjerenjem od 02 prema 01. Za slučaj kao što je prikazano na slici 9.2. program tumači da je veza između čvora 01 i 02 dvosmjerna, odnosno da je neorijentirana. Ista logika vrijedi i za ostale čvorove i veze.

Čvorovi (01,01), (02,02), …, (05,05) nemaju stanje X, pa program tumači da ne postoji veza između njih. U praksi za to znači da se ne dozvoljava grana koja počinje u jednom čvoru i završava i istom čvoru. Zbog toga program kontrolira da dijagonala matrice bude prazna.

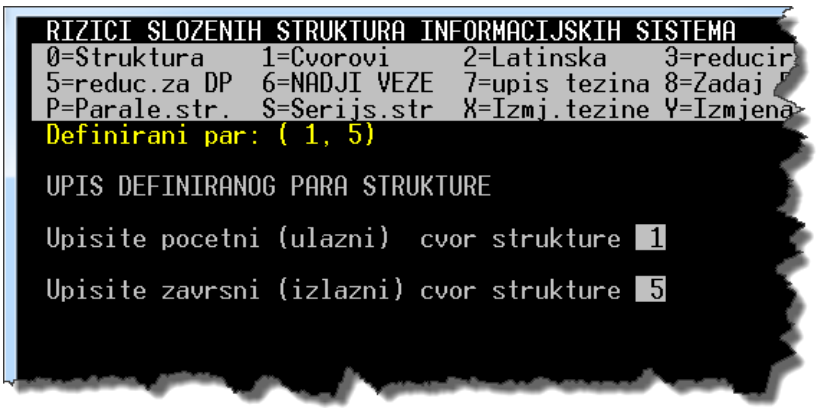
Ako se postavi stanje strukture kao na slici 9.3. to označava da ne postoji veze od čvora 01 do čvora 02, ali postoji veza od čvora 02 do 01. To program tumači kao orijentiranu granu sa usmjerenjem od čvora 02 do čvora 01.



Slika 9.3. Modificirana struktura sa slike 9.2.

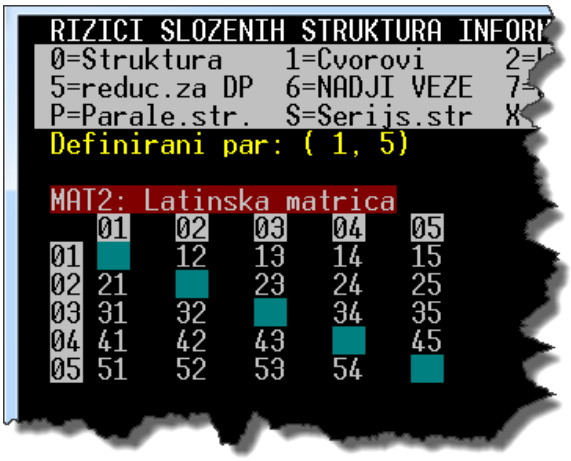
U glavnom meniu, pritiskom na tipku 1 dobiva se pregled zadane strukture, bez mogućnosti promjene stanja bilo kojeg čvora, odnosno veze između čvorova.

Da bi se moglo raditi analiza nužno je zadati definirani par čvorova, odnosno ulazni i izlazni čvor strukture. To se može dobiti pritiskom na tipku 8 u glavnom meniu. Tada se dobiva mogućnost redefiniranja definiranog para, kao što je prikazano na slici 9.4.



Slika 9.4. Promjena definiranog para

Na temelju gore zadanih podataka program sam određuje latinsku matricu. Prikaz latinske matrice koju je pronašao program LATMAT vidi se na slici 9.5.

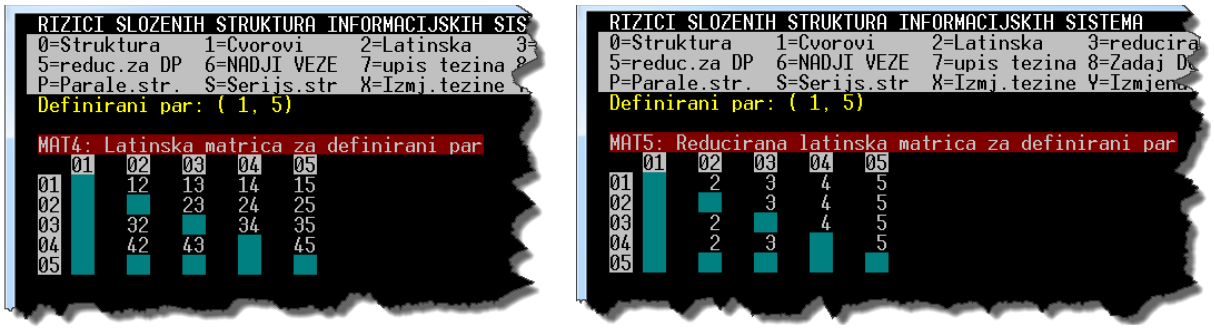


Slika 9.5. Latinska matrica za strukturu sa slike 9.2.

Za zadanu strukturu i definirani par (01,05) program sam nalazi reduciranu latinsku matricu prikazanu na slici 9.6.

Slika 9.6. Reducirana latinska matrica sa slike 9.5.

Na isti način program sam određuje latinsku matricu na temelju algoritma latinsku matricu za definirani par i ekvivalentnu reduciranu matricu za definirani par, kao što je prikazano na slici 9.7.



Slika 9.7. Latinska matrica za definirani par (lijevo) i reducirana latinska matrica za definirani par (desno)

9.3. Analiza paralelne i serijske strukture u programu LATMAT

Nezavisno od zadane strukture program LATMAT provodi proračun težine paralelne i serijske strukture. Pri tome se pretpostavlja da sve grane paralelne i serijske strukture imaju jednake težine, te da su sve grane ili paralelno ili serijski spojene. Rezultat proračuna težina paralelne strukture prikazan je na slici 9.8., a serijske na slici 9.9.

PARALELNA STRUKTURA: TABLICA STATISTICKIH TEZINSKIH FAKTORA STRUKTURE

0	0.000	0.100	0.200	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
1	0.000	0.100	0.200	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
2	0.000	0.190	0.360	0.510	0.640	0.750	0.840	0.910	0.960	0.990	1.000
3	0.000	0.271	0.488	0.657	0.784	0.875	0.936	0.973	0.992	0.999	1.000
4	0.000	0.344	0.590	0.760	0.870	0.938	0.974	0.992	0.998	1.000	1.000
5	0.000	0.410	0.672	0.832	0.922	0.969	0.990	0.998	1.000	1.000	1.000
6	0.000	0.469	0.738	0.882	0.953	0.984	0.996	0.999	1.000	1.000	1.000
7	0.000	0.522	0.790	0.918	0.972	0.992	0.998	1.000	1.000	1.000	1.000
8	0.000	0.570	0.832	0.942	0.983	0.996	0.999	1.000	1.000	1.000	1.000
9	0.000	0.613	0.866	0.960	0.990	0.998	1.000	1.000	1.000	1.000	1.000
10	0.000	0.651	0.893	0.972	0.994	0.999	1.000	1.000	1.000	1.000	1.000
11	0.000	0.686	0.914	0.980	0.996	1.000	1.000	1.000	1.000	1.000	1.000
12	0.000	0.718	0.931	0.986	0.998	1.000	1.000	1.000	1.000	1.000	1.000
13	0.000	0.746	0.945	0.990	0.999	1.000	1.000	1.000	1.000	1.000	1.000
14	0.000	0.771	0.956	0.993	0.999	1.000	1.000	1.000	1.000	1.000	1.000
15	0.000	0.794	0.965	0.995	1.000	1.000	1.000	1.000	1.000	1.000	1.000

Slika 9.8. Proračun paralelne strukture u programu LATMAT

SERIJSKA STRUKTURA: TABLICA STATISTICKIH TEZINSKIH FAKTORA STRUKTURE

0	0.000	0.100	0.200	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
1	0.000	0.100	0.200	0.300	0.400	0.500	0.600	0.700	0.800	0.900	1.000
2	0.000	0.010	0.040	0.090	0.160	0.250	0.360	0.490	0.640	0.810	1.000
3	0.000	0.001	0.008	0.027	0.064	0.125	0.216	0.343	0.512	0.729	1.000
4	0.000	0.000	0.002	0.008	0.026	0.063	0.130	0.240	0.410	0.656	1.000
5	0.000	0.000	0.000	0.002	0.010	0.031	0.078	0.168	0.328	0.590	1.000
6	0.000	0.000	0.000	0.001	0.004	0.016	0.047	0.118	0.262	0.531	1.000
7	0.000	0.000	0.000	0.000	0.002	0.008	0.028	0.082	0.210	0.478	1.000
8	0.000	0.000	0.000	0.000	0.001	0.004	0.017	0.058	0.168	0.430	1.000
9	0.000	0.000	0.000	0.000	0.000	0.002	0.010	0.040	0.134	0.387	1.000
10	0.000	0.000	0.000	0.000	0.000	0.001	0.006	0.028	0.107	0.349	1.000
11	0.000	0.000	0.000	0.000	0.000	0.000	0.004	0.020	0.086	0.314	1.000
12	0.000	0.000	0.000	0.000	0.000	0.000	0.002	0.014	0.069	0.282	1.000
13	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.010	0.055	0.254	1.000
14	0.000	0.000	0.000	0.000	0.000	0.000	0.001	0.007	0.044	0.229	1.000
15	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.005	0.035	0.206	1.000

Slika 9.9. Proračun serijske strukture u programu LATMAT

Ako se želi napraviti eksport podataka za grafičku analizu program vrši proračun promjene težine pojedinih grana sa znatno manjim korakom promjene težina, tako da se dobivaju glatke funkcije. Na slikama 9.8. i 9.9 prirast težina grana je 0,1.

9.4. Analiza složene strukture pomoću programa LATMAT

Ako se zada složena struktura kao što je na slici 9.2. program LATMAT može provesti proračun težine strukture po svim aspektima. Rezultat se toga proračuna se prikazuje na ekranu (a može se i eksportirati). Na slici 9.10. se nalazi prikaz rezultata proračuna složene strukture zadane na slici 9.2. Ovaj pregled se dobiva pritiskom na tipku '9' u glavnom meniu.

ANALIZA RIZIKA SLOZENE STRUKTURE INFORMACIJSKOG SISTEMA

Veze strukt.	Tez.u segmentima veze	Tez.SER.grane	Tez.strukture
1 15	0.150	0.1500000	0.3291454
2 125	0.120 0.250	0.0300000	
2 135	0.130 0.350	0.0455000	
2 145	0.140 0.450	0.0630000	
3 1325	0.130 0.230 0.250	0.0074750	
3 1425	0.140 0.240 0.250	0.0084000	
3 1235	0.120 0.230 0.350	0.0096600	
3 1435	0.140 0.340 0.350	0.0166600	
3 1245	0.120 0.240 0.450	0.0129600	
3 1345	0.130 0.340 0.450	0.0198900	
4 14325	0.140 0.340 0.230 0.250	0.0027370	
4 13425	0.130 0.340 0.240 0.250	0.0026520	
4 14235	0.140 0.240 0.230 0.350	0.0027048	
4 12435	0.120 0.240 0.340 0.350	0.0034272	
4 13245	0.130 0.230 0.240 0.450	0.0032292	
4 12345	0.120 0.230 0.340 0.450	0.0042228	

Slika 9.10. Rezultat proračuna težine složene strukture u programu LATMAT

U prvoj koloni 'Veze strukt.' se nalaze podaci koji govore koliko grana je uključeno u vezu između definiranog para.

Druga kolona pokazuje koje su grane uključene u vezu između ulaznog i izlaznog čvora. Npr. u 11 redu se nalazi u prvoj koloni 4, što znači postoje četiri grane koje su uključene u put veze između ulaznog i izlaznog čvora. U drugoj koloni se nalazi podatak '14325'. To znači da su u put uključene grane: (1,4), (4,3), (3,2) i (2,5).

U trećoj koloni 'Tez.u segmentima veze' nalaze se podaci o zadanim težinama u pojedinim granama koje čine put definiranog para.

Četvrta kolona 'Tez.SER.grane' sadržava podatke koji su proračunata težina serijske grane, odnosno puta za definirani par.

U petoj koloni 'Tez.strukture' se nalazi ukupna težina cijele složene strukture.

Upis težina za pojedinu granu se može napraviti pritiskom na tipku '7' u glavnom meniu. Tada se dobiva ekran prikazan na slici 9.11.

Slika 9.11. Upis težina pojedinih grana u strukturi

Grane za koje se mogu upisati težine su samo one koje učestvuju u nekom od putova od ulaznog do izlaznog čvora, odnosno definiranog para. Naravno, program automatski podrazumijeva da je težina grane (1,2) jednaka težini grane (2,1).

10. DISKUSIJA

Osnovni problem koji se javio prilikom nastanka ovog rada, kada su u pitanju rizici (specijalno rizici informacijskih sistema) bio je potpuno odsustvo bilo kakvih dostupnih nagovještaja i zapisa o postojećoj tematici (konferencije, biblioteke, internet). Radi se o tome da se do sada, u praksi, govori samo o četiri tzv. klasična i „jedina“ načina smanjenja iznosa rizika u bilo kojem području nauke, tehnike i tehnologije:

- prihvaćanje,
- prijenos na trećeg,
- smanjenje i
- izbjegavanje.

Osim toga, u svim radovima, standardima i preporukama uvijek se radilo isključivo o strogo izdvojenim i definiranim elementarnim podsistemima, preciznije, elementarnim jedinicama koje se nisu mogle dalje razložiti. Informacijski sistemi po tome nisu bili nikakva iznimka.

Međutim, moje višegodišnje bavljenje informatikom (od početka radne karijere) i problemima rizika (preko 15 godina) jasno su upućivala na još jedan neizbježan element rizika bilo kojeg iole složenijeg objekta:

- njegovu strukturu.

Na samom početku radilo se o čistim osjećajima i empiriji – bez ikakvih dokaza i odgovarajuće podrške. Međutim, tokom vremena je sve više indicija upućivalo da se radi o problematici koju itekako vrijedi istražiti.

Upoznajući se sa složenim strukturama i njihovim ponašanjima, u jednom trenutku sam došao do radova koji se odnose na prekidačke složene mreže i pouzdanost sistema višega reda. U ovim radovima je konačno moja pretpostavka potvrđena:

- niz parametara cjelokupnog složenog objekta ili sistema oštro zavisi od njegove strukture i stanja elemenata koji tu strukturu izgrađuju.

Posljedica ovakvih saznanja je rezultirala višegodišnjim istraživanjima struktura raznih oblika, tipova i vrsta složenih sistema. U literaturi, analizi prekidačkih mreža, teoriji pouzdanosti itd. nedvosmisleno se tvrdilo uz dani matematički aparat, izgrađene modele i simulacije kako se svjesno može upravljati određenim značajkama cijele strukture ciljanim izmjenama na određene podstrukture.

Sada je ove činjenice trebalo primijeniti i adaptirati na dokaz mogućnosti potpuno novog načina smanjenja rizika a time i kompletnog upravljanja rizicima složenih struktura, prvenstveno kada su u pitanju bili složeni informacijski sistemi.

Međutim, to se pokazalo kao vrlo krupan zalogaj koji nije bilo lako savladati odjednom i u kratkom vremenu. Zato je bilo neophodno dobro proanalizirati i proučiti, u sasvim specifičnom području rizika, pored ostalog i slijedeća tri područja:

- informacije i informacijske sisteme,
- analizu i sintezu složenih sistema,
- teoriju rizika i sve pripadne aspekte vezane uz rizike.

Svemu tome obavezno treba dodati i solidno poznavanje svi temeljnih zakona, standarda, preporuke i najbolje prakse koja strogo propisuju ponašanje i tretman u navedenim područjima.

Standardi, posebno međunarodni, ne dozvoljavaju bilo kakvo kretanje izvan propisanih granica, definicija i odrednica, što je sve skupa dodatno usložnjavalo istraživanja. Pri tome treba znati da nije riječ o dva ili tri standarda po oblasti, već su uvijek u pitanju cijele serije, tzv. familije standarda i niz smjernica koje ih prate. Neispunjavanje strogih direktiva u standardima značilo bi istovremeno i potpuno obezvređenje cijelog istraživanja, što je bilo nedopustivo.

Kada se doda i neosporna potreba kombinacija navedena tri osnovna područja, sve skupa je došlo do takvog nivoa da je preraslo u višegodišnji zaseban projekt. U tom vremenskom periodu bilo je potrebno obaviti slijedeće radnje:

- planiranje,
- prikupljanje dokumentacije,
- proučavanje, analiza i sinteza problema,
- izgradnja hipoteza,
- izgradnja modela,
- njihovo fragmentarno iznošenje u javnost (naučni skupovi, konferencije, članci),
- realizacija i testiranje hipoteza,
- realizacija i testiranje modela,
- potvrda modela u obliku programskih rješenja,
- dobivanje kvalitativnih rezultata,
- dobivanje kvantitativnih rezultata,
- formiranje konačnih zaključaka (vezanih uz potvrdu hipoteza).

Kao i svako kretanje u nepoznatom području, projekt je bio često opterećen naizgled nerješivim problemima, višemjesečnim zastojima, sumnjama i ponavljanjem niza koraka projekta. Možda je najveći problem bio što, uz nedostatak potrebne literature, nije bilo pravog odziva jer je većina stručnjaka vezana za vrlo specialističko područje a ne za presjek nekoliko naučnih i stručnih oblasti.

Navedimo sasvim konkretne primjere:

- već sama definicija informacijskog sistema prema raznoj dostupnoj literaturi stvara zbrku. Razlog za to je u činjenici da ne postoji jedinstvena definicija informacijskog sistema. U svakom području primjene razni autori su donosili svoje definicije koje se vrlo često toliko razlikuju jedna od druge da je u nekim slučajevima teško prepoznati činjenicu da se radi o istom sistemu. Zbog tog razloga je trebalo napraviti novu

definiciju informacijskog sistema koja bi odražavala specifičnost područja primjene: upravljanje sistemima i sigurnošću.

- Slijedeći problem koji se pojavio na početku bio je vezan za definiciju informacije. Također i u ovom slučaju, postoji obilje definicija u raznim izvorima, ali ni jedna nije bila prikladna za područje informacijske sigurnosti. Zato se trebala napraviti nova definicija pojma informacije, koja bi bila odgovarajuća za primjenu u području informacijske sigurnosti.

- Analiza složene strukture (već i za skroman broj elemenata) moguća je isključivo uz pomoć kompjutera. Istovremeno, programski paketi (dostupni na tržištu) nikako nisu zadovoljavale zadane postavke: algoritmi na kojima su radili vrlo brzo su iscrpljivali memorijske kapacitete a vrijem obrade je raslo tako da su bilo kakvi ozbiljniji zahvati bili praktično neupotrebljivi.

- Tek kada se došlo do primjene posebne tehnike vezane uz specijalna područja matematike (poznate pod nazivom obrada latinskih kvadrata ili latinskih matrica - latinska kompozicija) projekt se znatno ubrzao i krenuo dalje. Ali zato je bilo neophodno razviti vlastiti softver, odnosno programski paket koji je u razumnom vremenu davao tražene rezultate.

Ne manje poteškoće je stvarao i ugrađeni konzervativni pristup (i u nekim stavovima autora ovih redova) o mogućnosti analize rizika samo na elementima složene strukture i nemogućnosti dobivanja rizike kompletnog sistema. Tu je trebalo prevladati zvanična i ustaljena mišljenja i stavove i zakoračiti u nepoznato. Tek kroz simulacija na modelu, izgradnji niza primjera i analizi ogromne količine podataka, počeli su se jasno pojavljivati rezultati koji su jasno ukazivali na točnost postavljenih hipoteza i potvrdu izgrađenih modela.

Jednom potvrđene hipoteze i modeli još su bili daleko od cilja kompletnog projekta. Sve skupa je moralo proći kroz oštre zakonske i druge normativne filtre i pri tome nigdje izaći van granica koje propisuju postojeći standardi. Istovremeno, ma kao to zvučalo, jednako velike a možda još veće poteškoće stvaralo je potpuno odsustvo zakona, standarda, preporuke i najbolje prakse – prije svega upravo na rubnim područjima tri navedene oblasti.

Na samom kraju, bio je neophodan vrlo ozbiljan i težak niz aktivnosti, razmišljanja i rješavanja dilema o načinu prezentacije dobivenih rezultata i njihovu uvjerljivu i razumljivu formu. Nakon svih mogućih diskusija sa kolegama i stručnjacima, izlaganja na profesionalnim skupovima i objavljivanja radova, iskristalizirala se ideja o njivom jedinstvenom obliku:

- to je rad koji upravo čitate.

11. ZAKLJUČCI

1. Rizici su opće priznata kategorija koja nije samo svojstvena ljudima već svim razvijenijim životinjskim vrstama, bez izuzetka. Sasvim svejedno radi li se o poduzimanju bilo kakve akcije, govori li se o trenutnoj ulozi lovca ili lovljenog ili je u pitanju dugoročna strategija – od točne procjene rizika je često zavisio i sam opstanak jedinke ili grupe. Razvojem ljudskog društva sve povezano s rizicima je dobilo složeniji i sveobuhvatniji značaj. Vođenje ratova, veliki građevinski i drugi poduhvati, upravljanje državom i financijama, da se dalje ne nabraja uvijek su bili čvrsto povezani sa rizicima. Pravilno ocjenjivanje rizika nije bilo ništa manje važno ni kada su bile u pitanju struke (medicina, građevina, poljoprivreda itd.) pa ni egzistencija svakog pojedinca. Međutim, sve do prije nekoliko godina (u vrijeme pisanja ovih redova) rizici su ostali u okvirima odlučivanja pojedinca ili su striktno primjenjivani u pojedinim strukama sa vlastitim direktivama i filozofijom (bankarstvo, medicina, osiguranja, vojne akcije itd.). Jedinstvenog pristupa nije bilo kao ni jedinstvene filozofije i odrednica.

2. Moderna teorija obrade i upravljanja rizicima doživjela je svoje prvo općesvjetsko značenje i priznanje pojavom međunarodnog standarda ISO 31000:2008. Istovremeno, u području informacijskih sistema, ova problematika je obrađena u seriji ISO 27000ff, preciznije kroz standard ISO 27005:2008. Oba ova dokumenta su direktni nasljednici nacionalnog australsko-novozelandskog standarda AS/NZ 3460:2004 i stoga imaju praktično istu osnovnu strukturu, rječnik i definicije. Svim ovim standardima je osnovni cilj prepoznavanje i smanjenje rizika što u konačnici omogućava svjesno upravljanje rizicima.

3. Pojava navedenih standarda je svakako ogroman doprinos unifikaciji njihove obrade, povećala mogući zajednički pristup i razumijevanje i opću primjenu u svim područjima znanosti, tehnike i tehnologije, bez obzira o kakvim strukama i djelatnostima je riječ. Pri tome je u standardima istaknut značaj jedinstvene definicije rizika, njegovog prepoznavanja, kategoriziranja i ocjenjivanja.

4. Samo prepoznavanje i ocjena rizika je prva faza za glavnu namjenu rada s rizicima: radi se o mogućem smanjivanju na nivo koji odgovara proklamiranoj politici upravljanja rizicima organizacije bez obzira da li je riječ o proizvodnji ili davanju usluga, industriji, poljoprivredi, javnim financijama, administraciji ili školstvu. Sve ove aktivnosti daju saznanja koja su praktično uvijek od neprocjenjive vrijednosti za donošenje odluka bilo koje uprave na bilo kojem hijerarhijskom nivou.

5. Postoje četiri osnovna načina obrade rizika:

    a. Prihvaćanje postojećeg rizika
    b. Smanjenje na prihvatljivi nivo
    c. Izbjegavanje hazardne situacije
    d. Prenošenjem na treće.

    Van ovih načina standardi ne poznaju ni jednu drugu primjenljivu metodu ili tehniku.

6. U standardima se uvijek obrada rizika odnosi na strogo izdvojene cjeline unutar bilo kojeg složenog sistema ili strukture. Nigdje se ne govori o veoma važnom aspektu: ukupnoj ocjenjenoj, procijenjenoj ili izračunatoj vrijednosti cijelog sistema ili složene strukture.

7. Ma koliko standardi bili korisni, navedeni nedostaci se veoma neugodno odražavaju u praksi, posebno kad je riječ o IT i informacijskim sistemima. Stoga je cilj ovog rada bio traženje odgovora na dane probleme;

    a. da li je moguće izračunati ukupan rizik ne samo informacijskog sistema već bilo kojeg sistema ili složene strukture, i

    b. u kakvoj vezi stoje i prema kojim zakonima se ponašaju rizici sistema u zavisnosti od vrijednosti rizika pojedinih elemenata.

8. Višegodišnje bavljenje ovom specijalnom problematikom bilo je prvenstveno posvećeno istraživanjima u slijedeće tri oblasti

    a. informacijskim sistemima,

    b. složenim sistemima i strukturama i

    c. rizicima.

    Najveći dio posla je, međutim, bio usmjeren upravo na rubna područja ovih oblasti i na moguća preklapanja koja bi omogućila eventualno nalaženje rješenja.

9. Rezultati cijelog navedenog višegodišnjeg projekta doveli su do stvaranja odgovarajućih hipoteza koje su se morale dokazati i modela koji su zahtijevali višestruku provjeru. Pri tome su se sva istraživanja strogo držala oficijelnih definicija i direktiva danih kroz usvojene međunarodne standarde i rješenja najbolje prakse.

10. Prva odgovarajuća dokaziva rješenja pojavila su se tek kod primjene tehnika i metoda za analize složenih struktura (Bool-ova algebra, teorija grafova, matrična analiza). Konačno je odlučeno da se složene strukture analiziraju uz pomoć takozvane latinske kompozicije koja je nudila najbolji prilaz.

11. Sisteme i složene strukture je u iole ozbiljnijoj razradi i istraživanju nemoguće sagledati bez primjene kompjutera na sasvim konkretnom modelu. Budući da na postojećem

svjetskom tržištu nije bilo moguće doći do specijalnog komercijalnog oblika izračunavanja latinske kompozicije, razvijen je vlastiti program LATMAT. Uz pomoć LATMAT-a bilo je moguće razmatrati ponašanje složene strukture u zavisnosti od veza i odabranih parametara svakog pojedinog elementa.

12. Niz testiranja svih mogućih oblika veza elemenata i njihovih veza unutar strukture kao i općeg oblika težine svakog pojedinog elementa (pa tako i sa proizvoljno odabranim iznosima rizika) dao je vrlo jasne i nedvojbene rezultate koji se mogu izraziti u slijedećim tvrdnjama:

    a. Ukupni iznos težine (bilo koje vrijednosti, pa tako i rizika) cijelog sistema ili složene strukture moguće je izračunati (dobiti sasvim konkretan kvantitativni iznos) bez obzira o kojoj oblasti se radi (pa tako i informacijskim sistemima),

    b. Promjena strukture (veze između elemenata) mijenja ukupnu konačnu težinu cijelog sistema ili složene strukture,

    c. Promjena težine bilo kojeg elementa (ili grupe njih) uvijek se odražava na ukupno opterećenje cijelog sistema ili složene strukture.

13. Analiza ponašanja informacijskih sistema (posebno kada se radi o rizicima) u potpunosti se uklapa u zahtjeve i postavke modela kao što i model zadovoljava sve zahtjeve i postavke koje su karakteristične za informacijske modele.

14. Konačni rezultati su pokazali da se, u području obrade, ocjene i smanjenja rizika kod informacijskih sistema (i ne samo kod njih) mogu dati i dokazati slijedeće tvrdnje i teoremi:

    a. Ukupan rizik sistema i složene strukture moguće je izračunati,

    b. Promjenom strukture moguće je smanjiti ukupan rizik cijelog sistema,

    c. Promjenom pojedinačnih rizika moguće je smanjiti ukupan rizik cijelog sistema (i to vrlo usmjereno, racionalno i upravljivo).

15. Dobiveni rezultati i teoremi pokazuju da je obradu rizika a time i upravljanje njima moguće ne samo na četiri klasična načina već i kroz novi, peti: izmjenama u strukturi sistema.

16. Teoretski rezultati dobiveni i navedeni u ovom radu otvaraju dva nova, u navedenom smislu još nedovoljno obrađena područja:

    a. daljem teoretskom i znanstvenom istraživanju i

    b. dokazima u praksi (prije svega kada je riječ o informacijskim sistemima).

17. Iako je na početku rečeno kako su rizici stari kao i ljudski rod, njihova temeljita naučna i svjesna obrada tek treba da donese plodove kako u području informacijskih sistema

tako i ostalim oblastima kroz opće povećanje sigurnosti i pouzdanosti. Ovaj rad bi trebao biti doprinos u tom smislu.

12. PRILOZI

12.1. OSNOVNI POJMOVI I DEFINICJE

U tablici su prikazane definicije pojmova preuzete iz standarda ISO/IEC 27000:2009 [1]

ID	Engl. Pojam	Pojam	Opis
2.1	access control	**kontrola pristupa**	označava osiguranje pristupa **imovini** (2.3) ovlaštenima i ograničeno na temelju poslovnih i sigurnosnih zahtjeva
2.2	accountability	**odgovornost**	odgovornost entiteta za svoje postupke i odluke
2.3	asset	**imovina**	sve što ima vrijednost za organizaciju. NAPOMENA Postoje mnoge vrste imovine, uključujući: a) **informacije** (2.18); b) softver, kao što su kompjuterski programi; c) fizički uređaji, kao što su kompjuteri; d) usluge; e) ljudi, njihove kvalifikacije, vještine i iskustvo, i f) nematerijalna imovina, kao što su ugled i imidž.
2.4	attack	**napad**	pokušaj da se uništenja, izlaganja, izmijene, onemogućavanja, krađe, dobivanja neovlaštenog pristupa ili neovlašteno korištenje **imovine** (2.3)
2.5	authentication	**ovjera**	odredba o osiguranju kojom se tvrdi da je karakteristika entiteta ispravna
2.6	authenticity	**autentičnost**	tvrdnja subjekta da je svojstvo entiteta onakvo kako se tvrdi
2.7	availability	**dostupnost**	svojstvo da se može pristupiti i koristiti na zahtjev ovlaštene osobe
2.8	business continuity	**kontinuitet poslovanja**	**proces** (2.31) i/ili **postupak** (2.30) koji osiguravaju nastavak poslovanja
2.9	confidentiality	**tajnost**	svojstvo informacije da nije dozvoljena ili objavljena za neovlaštene osobe, entitete, ili **procese** (2.31)
2.10	control	**kontrola**	sredstva za upravljanje **rizikom** (2.34), uključujući **politike** (2,28), **postupke** (2.30), **smjernice** (2.16), praksu ili organizacijske strukture, koje mogu biti administrativne, tehničke, menadžment, ili pravne naravi NAPOMENA: Kontrola se također koristi kao sinonim za zaštitu i protumjere.
2.11	control objective	**cilj kontrole**	izjava kojom se opisuje kakav se rezultat želi postići provedbom **kontrole** (2.10)
2.12	corrective action	**korektivna aktivnost**	akcija kojom se uklanjaju uzroci otkrivenih nesukladnosti ili drugih neželjenih situacija
2.13	effectiveness	**efektivnost**	stepen realizacije planiranih aktivnosti i postignutih planiranih rezultata

ID	Engl. Pojam	Pojam	Opis
2.14	efficiency	**efikasnost**	odnos između postignutih rezultata i korištenih resursa
2.15	event	**događaj**	pojava posebnog skupa okolnosti
2.16	guideline	**preporuka**	preporuka o tome što se očekuje da će biti učinjeno kako bi se postigla cilj
2.17	impact	**posljedica**	ostvareni utjecaj na promjenu razine poslovnih ciljeva
2.18	information asset	**informacijska imovina**	znanja ili podaci koji imaju vrijednost za organizaciju
2.19	information security	**informacijska sigurnost**	očuvanje **povjerljivosti** (2.9), **cjelovitosti** (2.25) i **raspoloživosti** (2,7) informacija NAPOMENA Osim toga, druga svojstva, kao što su **autentičnost** (2.6), **odgovornost** (2.2), **neporecivost** (2.27), te **pouzdanost** (2.33) također mogu biti uključeni.
2.20	information security event	**događaj informacijske sigurnosti**	identificirana pojava sistema, usluga ili stanja mreže koja ukazuje na moguća kršenja **informacijske sigurnosti** (2.19), **politika** (2.28), greške u **kontroli** (2.10), odnosno nepoznate situacije koje mogu biti relevantne za sigurnost
2.21	information security incident	**incident informacijske sigurnosti**	jedan ili niz neželjenih ili neočekivanih **događaja informacijske sigurnosti** (2.20) koji imaju značajnu vjerojatnost ugrožavanja poslovanja i prijete **informacijskoj sigurnosti** (2.19)
2.22	information security incident management	**upravljanje incidentima informacijske sigurnosti**	**proces** (2.31) za otkrivanje, izvještavanje, procjenu, odgovaranje na incidente i učenje iz **incidenata informacijske sigurnosti** (2.21)
2.23	information security management system ISMS	**sistem upravljanja informacijskom sigurnošću (isms)**	dio cjelokupnog **sistema upravljanja** (2.26), temeljen na pristupu poslovnom riziku, implementaciji, radu, nadzoru, pregledu, održavanju i poboljšanju **informacijske sigurnosti** (2.19)
2.24	information security risk	**rizik informacijske sigurnosti**	potencijal da će **prijetnje** (2.45) iskorištavati **ranjivost** (2.46) **imovine** (2.3) ili grupu imovine i time nanijeti štetu organizaciji
2.25	integrity	**cjelovitost**	svojstvo zaštite imovine u smislu točnosti i kompletnosti **imovine** (2.3)
2.26	management system	**sistem upravljanja**	okvir **politike** (2.28), **postupci** (2.30), **smjernice** (2.16) i povezani resursi za postizanje ciljeva organizacije
2.27	non-repudiation	**neporecivost**	sposobnost dokazivanja nastanka tvrdnje **događaja** (2.15) ili djelovanja izvornog subjekata, kako bi se rješavali sporovi o nastanku ili ne-nastanku **događaja** (2.15) ili djelovanja i uključivanja osoba u **događaj** (2.15)
2.28	policy	**politika**	ukupna namjera i smjer formalno izražena od

ID	Engl. Pojam	Pojam	Opis
			strane uprave
2.29	preventive action	**preventivna aktivnost**	akcija kako bi se uklonio uzrok potencijalne nesukladnosti ili drugih neželjenih potencijalnih situacija
2.30	procedure	**procedura**	specificiran način provođenja aktivnosti ili **procesa** (2.31)
2.31	process	**proces**	skup međusobno povezanih aktivnosti koji pretvara ulaze u izlaze
2.32	record	**zapis**	dokument s navodima postignutih rezultata ili dokaz o provedenim aktivnostima
2.33	reliability	**pouzdanost**	svojstvo imovine da se ponaša u skladu namjene i rezultata
2.34	risk	**rizik**	Kombinacija vjerojatnosti **događaja** (2.15) i njegove posljedice
2.35	risk acceptance	**prihvaćanje rizika**	odluka za prihvaćanje **rizika** (2.34)
2.36	risk analysis	**analiza rizika**	sustavna uporaba informacija za identifikaciju izvora i procjenu **rizika** (2.34) NAPOMENA: Analiza rizika daje osnovu za procjenu **rizika** (2,41), **obradu rizika** (2.43) i **prihvaćanje rizika** (2.35).
2.37	risk assessment	**procjena rizika**	ukupni **proces** (2.31**) analize rizika** (2.36) i **ocjene rizika** (2.41)
2.38	risk communication	**komunikacija**	razmjena ili dijeljenje informacija o **riziku** (2.34) između donositelja odluka i drugih zainteresiranih strana
2.39	risk criteria	**kriterij rizika**	opis posla kojim se procjenjuje važnost **rizika** (2.34)
2.40	risk estimation	**validacija rizika**	aktivnost dodjeljivanja vrijednosti vjerojatnosti i posljedicama **rizika** (2.34)
2.41	risk evaluation	**ocjena rizika**	**proces** (2.31) usporedbe procijenjenih **rizika** (2.34) s određenim **kriterijima rizika** (2.39) u cilju utvrđivanja značaja **rizika** (2.34)
2.42	risk management	**upravljanje rizicima**	koordinirane aktivnosti za upravljanje i kontrolu organizacije u svezi s **rizikom** (2.34) NAPOMENA: upravljanje rizikom općenito uključuje procjenu **rizika** (2.37), **obradu rizika** (2.43), **prihvaćanje rizika** (2.35), **komunikaciju rizika** (2.38), praćenje i pregled rizika
2.43	risk treatment	**obrada rizika**	**proces** (2.31) selekcije i implementacije protumjera za modifikaciju **rizika** (2.34)
2.44	statement of applicability (SoA)	**izjava o primjenljivosti (SoA)**	dokumentirana izjava **ciljeva kontrole** (2.11) i **kontrola** (2.10) koji su relevantni i odnosi se na **ISMS** (2.23) organizacije
2.45	threat	**prijetnja**	potencijalni uzrok neželjenog incidenta, koji može dovesti do štete na sustavu ili organizaciji
2.46	vulnerability	**ranjivost**	slabost **imovine** (2.3) ili **kontrole** (2.10) koju može iskoristiti **prijetnja** (2.45)

12.2. PREGLED NAJZNAČAJNIJIH PRIJETNJI ZA INFORMACIJSKE SISTEME

Skupine prijetnji nisu u redoslijedu po važnosti.

Tip	**Prijetnja**	**Porijeklo**		
		Slučajne prijetnje izazvane od strane ljudi	**Namjerne prijetnje** izazvane od strane ljudi	**Prijetnje okruženja** i nisu posljedica ljudskih aktivnosti
Fizičko oštećenje	Požar	•	•	•
	Oštećenje vodom	•	•	•
	Zagađenje	•	•	•
	Značajni akcident	•	•	•
	Uništenje opreme ili medija	•	•	•
	Prašina	•	•	•
	Korozija	•	•	•
	Zamrzavanje	•	•	•
Prirodni događaji	Klimatski fenomeni			•
	Seizmički fenomeni			•
	Vulkanski fenomeni			•
	Meteorološki fenomeni			•
	Poplava			•
Gubitak bitnih servisa	Greške klima-uređaja	•	•	
	Greška ventilacije	•	•	
	Nema snabdijevanja vodom	•	•	•
	Gubitak napona napajanja	•	•	•
	Nefunkcioniranje kanalizacije	•	•	•
	Greška telekomunikacijske opreme	•	•	
Poremećaj zbog zračenja	Elektromagnetsko zračenje	•	•	•
	Termičko zračenje	•	•	•
	Elektromagnetski impuls	•	•	•
Kompromitacija informacija	Presretanje kompromitirajućih signala na sučelju		•	
	Udaljeno špijuniranje		•	
	Prisluškivanje		•	
	Krađa medija ili dokumenata		•	
	Krađa opreme		•	
	Dohvat recikliranih ili odbačenih medija		•	
	Odavanje	•	•	
	Podaci iz nepovjerljivih izvora	•	•	
	Neovlašteno diranje hardvera		•	
	Neovlašteno diranje softvera	•	•	
	Otkrivanje pozicije		•	

Tehničke greške	Greške u opremi	•		
	Kvar opreme	•		
	Zasićenost informacijskog sustava	•	•	
	Kvar softvera	•		
	Prodor u sustav održavanja informacijskog sustava	•	•	
Neautorizirane aktivnosti	Neautorizirana upotreba opreme		•	
	Lažno kopiranje softvera		•	
	Korištenje lažnog ili kopiranog softvera	•	•	
	Oštećenje podataka		•	
	Ilegalna obrada podataka		•	
Kompromitacija funkcija	Pogrešna upotreba	•		
	Povreda prava	•	•	
	Krivotvorenje prava		•	
	Odbijanje akcija		•	
	Povreda dostupnosti osoblja	•	•	•

12.3. PREGLED PRIJETNJI KOJIMA SU IZVOR LJUDI

Posebna pažnja treba biti posvećena ljudskim izvorima prijetnji. One su specificiranje u sljedećoj tablici [6]:

Izvor prijetnje	Motivacija	Moguće posljedice
Haker, kraker	Izazov Ego Pobuna Status Novac	• Hakiranje • Socijalni inženjering • Sistem upada, provala • Neovlašten pristup sustavu
Kompjuterski kriminal	Uništenje informacija Nelegalno otkrivanje podataka Novčana dobit Neovlaštena promjena podataka	• Kompjuterski zločin (npr. cyber uhođenje) • Prevare (npr. ponavljanje, oponašanje, presretanje) • Mito • Podvala • Provala u sustav
Teroristi	Ucjena Uništenje Eksploatacija Osveta Politička dobit Medijska pokrivenost	• Bomba/Terorizam • Rat informacijama • Sistemski napadi (npr. DDOS napadi) • Penetracija sistema • Petljanje u sistem
Industrijska špijunaža (Tvrtke, strane vlade, ostali državni interesi)	Konkurentske prednosti Ekonomska špijunaža	• Prednosti odbrane • Političke prednosti • Gospodarska eksploatacija • Krađa informacija • Nametanje na osobnu privatnost • Socijalni inženjering • Sistem penetracije • Neovlašten pristup sistemu (pristup klasificiranim, privatnim, i/ili informacijama vezanima za tehnologiju)
Zaposlenici (loše obučeni, nezadovoljni, zlonamjerni, nepošteni, otpušteni)	Znatiželja Ego Inteligencija Novčana dobit Osveta Slučajne pogreške (npr. greška kod unosa, programerske pogreške)	• Napad na zaposlenika • Ucjena • Pregled privatnih podataka • Zlouporaba kompjutera • Prevara i krađa • Informacijski mito • Unos lažnih, pogrešnih podataka • Presretanje malicioznog koda (npr. virus, logičke bombe, trojanski konj) • Prodaja privatnih informacija

Izvor prijetnje	Motivacija	Moguće posljedice
		• Sistemski bug-ovi • Upad u sistem • Sabotaža sistema • Neovlašten pristup u sistem

12.4. LISTA GLAVNIH RANJIVOSTI INFORMACIJSKIH SISTEMA

- Odsustvo nadzora
- Nedovoljna svest o sigurnosti
- Loše dokumentiran software
- Nedostatak mehanizma za nadzor
- Neprikladna procedura zapošljavanja
- Nedovoljna kontrola fizičkog pristupa lokacijama
- Nedostatak fizičke zaštite
- Lokacije u području podložnom poplavama
- Nezaštićen prostor za pohranu – arhiviranje
- Nedovoljno održavanje medija za arhiviranje
- Nedostatak shema za periodičnu zamjenu opreme
- Odbacivanje ili ponovno korištenje medija za arhiviranje bez prikladnog brisanja
- Osjetljivost opreme na prašinu / vlagu
- Osjetljivost opreme na promjene temperature
- Osjetljivost opreme na promjene napona napajanja
- Nestabilan izvor napajanja nezaštićene komunikacione linije
- Nedostatak kriterija za autentikaciju i identifikaciju
- Prenošenje lozinki u čistom obliku
- Nedostatak dokaza o slanju i prijemu poruke
- Nezaštićen osjetljiv promet
- Neprikladno upravljanje mrežom
- Nedostatak pažnje pri odbacivanju materijala
- Složeno korisničko sučelje
- Nedostatak dokumentacije
- Nedostatak efikasne kontrole promjena
- Loše upravljanje lozinkama
- Pogrešno dodjeljivanje prava pristupa
- Nejasne specifikacije za razvojne inženjere

12.5. Lista prijetnji i ranjivosti u informacijskim sistemima po sigurnosnim područjima

Primjer dijela kombinacija ranjivosti i prijetnji koje mogu izazvati posljedice u informacijskom sistemu [6].

Sigurnosno područje: HARDVER	
Primjer ranjivosti	**Primjer prijetnji**
Nedovoljno održavanje / neispravna instalacija arhivskih medija	Narušavanje održavanja informacijskog sustava
Nedostatak shema za periodičke izmjene	Uništenje opreme ili medija
Osjetljivost na vlagu, prašinu, nečistoću	Prašina, korozija, zamrzavanje
Osjetljivost na elektromagnetsko zračenje	Elektromagnetsko zračenje
Nedostatak učinkovite kontrole za promjenu konfiguracije	Greška u korištenju
Osjetljivost na varijacije napona	Gubitak napajanja
Osjetljivost na temperaturne varijacije	Meteorološki fenomen
Nezaštićena pohrana	Krađa medija ili dokumenata
Nedostatak zaštite kod bacanja u smeće	Krađa medija ili dokumenata
Nekontrolirano kopiranje	Krađa medija ili dokumenata

Sigurnosno područje: SOFTVER	
Primjer ranjivosti	**Primjer prijetnji**
Nedovoljno testiranje softvera	Povreda prava
Poznate greške u softveru	Povreda prava
Ne odjavljivanje na odlasku sa radne stanice	Povreda prava
Uništavanje ili ponovno korištenje bez ispravnog brisanja	Povreda prava
Nedostatak zapisa sa audita	Povreda prava
Pogrešna dodjela prava pristupa	Povreda prava
Široko distribuirani softver	Oštećenje podataka
Primjena programa na krive podatke u pitanju vremena	Oštećenje podataka
Komplicirano korisničko sučelje	Greška pri korištenju
Nedostatak dokumentacije	Greška pri korištenju
Pogrešno podešavanja parametara	Greška pri korištenju
Pogrešni datumi	Greška pri korištenju

Sigurnosno područje: MREŽA	
Primjer ranjivosti	**Primjer prijetnji**
Nedostatak mehanizama za identifikaciju i autentifikaciju korisnika	Krivotvorenje prava
Nezaštićena tablica lozinki	Krivotvorenje prava
Loš sustav upravljanja lozinkama	Krivotvorenje prava
Omogućeni nepotrebni servisi	Neovlašteno korištenje podataka
Nezreo ili novi softver	Kvar softvera

Sigurnosno područje: MREŽA	
Primjer ranjivosti	**Primjer prijetnji**
Nejasne ili nepotpune specifikacije razvojnog tima	Kvar softvera
Nedostatak efektivnih kontrola za promjenu	Kvar softvera
Nekontrolirano preuzimanje i korištenje softvera	Petljanje sa softverom
Nedostatak arhivskih kopija	Petljanje sa softverom
Nedostatak fizičke zaštite zgrada, vrata i prozora	Krađa medija ili dokumenata
Nemogućnost prikaza menadžerskih izvještaja	Neovlašteno korištenje opreme
Nedostatak dokaza o slanju ili primanju poruke	Odbijanje akcija
Nezaštićene komunikacijske linije	Prisluškivanje
Nezaštićen osjetljiv promet	Prisluškivanje
Loše spojevi kablova	Kvar telekomunikacijske opreme
Greška na jednoj točci	Kvar telekomunikacijske opreme
Nedostatak identifikacije i autentifikacije pošiljaoca ili primatelja	Krivotvorenje prava
Nesigurna mrežna arhitektura	Udaljeno špijuniranje
Prijenos nemaskiranih lozinki	Udaljeno špijuniranje
Neadekvatno upravljanje mrežom (otpornost usmjeravanja)	Zasićenost informacijskog sustava
Nezaštićene konekcije javnih mreža	Neovlašteno korištenje opreme

Sigurnosno područje: OSOBLJE	
Primjer ranjivosti	**Primjer prijetnji**
Odsutnost zaposlenika	Nedostupnost zaposlenika
Neadekvatne procedure zapošljavanja	Uništenje opreme ili medija
Nedovoljna oduka za zaštitu	Greška pri korištenju
Pogrešno korištenje softvera i hardvera	Greška pri korištenju
Nedostatak svjesnosti o sigurnosti	Greška pri korištenju
Nedostatak nadzornih mehanizama	Ilegalno procesiranje podataka
Rad bez nadzora vanjskog osoblja	Krađa medija ili dokumenata
Nedostatak politika za ispravno korištenje telekomunikacijskih medija i poruka	Neovlašteno korištenje opreme

Sigurnosno područje: LOKACIJA	
Primjer ranjivosti	**Primjer prijetnji**
Neadekvatno korištenje kontrola za pristup zgradama i sobama	Uništenje opreme ili medija
Lokacije u području podložno poplavi	Poplava
Nestabilna mreža napajanja	Gubitak napajanja
Nedostatak fizičke zaštite zgrada, vrata i prozora	Krađa opreme

Sigurnosno područje: ORGANIZACIJA	
Primjer ranjivosti	**Primjer prijetnji**
Nedostatak formalnih procedura za prijavu i odjavu korisnika	Povreda prava
Nedostatak formalnih procesa za reviziju prava pristupa	Povreda prava
Nedostatak ili nedovoljne odredbe (u svezi sigurnosti) u ugovorima s klijentima i / ili trećim osobama	Povreda prava
Nedostatak procedura za nadzor postrojenja za procesiranje informacija	Povreda prava
Nedostatak redovnih audita (nadzor)	Povreda prava
Nedostatak procedura za identifikaciju i procjenu rizika	Povreda prava
Nedostatak izvještaja o kvarovima u administratorskim i korisničkim zapisima	Povreda prava
Neadekvatna usluga održavanja	Kršenje održavanja informacijskog sustava
Nedostatak ili loš ugovor o održavanju	Kršenje održavanja informacijskog sustava
Nedostatak kontrole procedure za promjenu	Kršenje održavanja informacijskog sustava
Nedostatak formalne procedure za kontrolu ISMS dokumentacije	Korupcija podataka
Nedostatak formalnih procedura za nadzor podataka ISMS-a	Korupcija podataka
Nedostatak formalnih procesa za autorizaciju javno dostupnih podataka	Podaci od nepouzdanih izvora
Nedostatak odgovarajuće raspodjele odgovornosti informacijske sigurnosti	Odbijanje akcija
Nedostatak planova za kontinuitet poslovanja	Kvar opreme
Nedostatak politike za korištenje e-maila	Greška pri korištenju
Nedostatak procedura za uvođenje softvera u radnu okolinu	Greška pri korištenju
Nedostatak zapisa u administratorskim i korisničkim zapisima	Greška pri korištenju
Nedostatak procedura za upravljanje klasificiranim informacijama	Greška pri korištenju
Nedostatak odgovornosti za informacijski sustav u opisima posla	Greška pri korištenju
Nedostatak ili nedovoljno odredbi (o informacijskoj sigurnosti) u ugovorima sa zaposlenicima	Neovlašteno procesiranje podataka
Nedostatak definiranih disciplinskih postupka u slučaju incidenata informacijske sigurnosti	Krađa opreme
Nedostatak formalne politike za upotrebu mobilnih kompjutera	Krađa opreme
Nedostatak kontrola za dislociranu imovinu	Krađa opreme
Nedostatak ili nedovoljno dobra politika „čistog stola“	Krađa opreme ili medija
Nedostatak autorizacije postrojenja za obradu informacija	Krađa opreme ili medija

Sigurnosno područje: ORGANIZACIJA	
Primjer ranjivosti	**Primjer prijetnji**
Nedostatak uspostavljenih mehanizama za nadzor narušavanja sigurnosti	Krađa opreme ili medija
Nedostatak redovnih revizija uprave	Neovlašteno korištenje opreme
Nedostatak procedura za prijavu sigurnosnih slabosti	Neovlašteno korištenje opreme
Nedostatak procedure u skladu s odredbama prava intelektualnog vlasništva	Korištenje lažnog ili kopiranog softvera

12.6. Težine serijske strukture

Težina grana u strukturi	UKUPNA TEŽINA SERIJSKE STRUKTURE									
	Broj grana serijske strukture									
	1	2	3	4	5	6	7	8	9	10
0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,010	0,010	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,020	0,020	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,030	0,030	0,001	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,040	0,040	0,002	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,050	0,050	0,003	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,060	0,060	0,004	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,070	0,070	0,005	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,080	0,080	0,006	0,001	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,090	0,090	0,008	0,001	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,100	0,100	0,010	0,001	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,110	0,110	0,012	0,001	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,120	0,120	0,014	0,002	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,130	0,130	0,017	0,002	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,140	0,140	0,020	0,003	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,150	0,150	0,023	0,003	0,001	0,000	0,000	0,000	0,000	0,000	0,000
0,160	0,160	0,026	0,004	0,001	0,000	0,000	0,000	0,000	0,000	0,000
0,170	0,170	0,029	0,005	0,001	0,000	0,000	0,000	0,000	0,000	0,000
0,180	0,180	0,032	0,006	0,001	0,000	0,000	0,000	0,000	0,000	0,000
0,190	0,190	0,036	0,007	0,001	0,000	0,000	0,000	0,000	0,000	0,000
0,200	0,200	0,040	0,008	0,002	0,000	0,000	0,000	0,000	0,000	0,000
0,210	0,210	0,044	0,009	0,002	0,000	0,000	0,000	0,000	0,000	0,000
0,220	0,220	0,048	0,011	0,002	0,001	0,000	0,000	0,000	0,000	0,000
0,230	0,230	0,053	0,012	0,003	0,001	0,000	0,000	0,000	0,000	0,000
0,240	0,240	0,058	0,014	0,003	0,001	0,000	0,000	0,000	0,000	0,000
0,250	0,250	0,063	0,016	0,004	0,001	0,000	0,000	0,000	0,000	0,000
0,260	0,260	0,068	0,018	0,005	0,001	0,000	0,000	0,000	0,000	0,000
0,270	0,270	0,073	0,020	0,005	0,001	0,000	0,000	0,000	0,000	0,000
0,280	0,280	0,078	0,022	0,006	0,002	0,000	0,000	0,000	0,000	0,000
0,290	0,290	0,084	0,024	0,007	0,002	0,001	0,000	0,000	0,000	0,000
0,300	0,300	0,090	0,027	0,008	0,002	0,001	0,000	0,000	0,000	0,000
0,310	0,310	0,096	0,030	0,009	0,003	0,001	0,000	0,000	0,000	0,000
0,320	0,320	0,102	0,033	0,010	0,003	0,001	0,000	0,000	0,000	0,000
0,330	0,330	0,109	0,036	0,012	0,004	0,001	0,000	0,000	0,000	0,000
0,340	0,340	0,116	0,039	0,013	0,005	0,002	0,001	0,000	0,000	0,000
0,350	0,350	0,123	0,043	0,015	0,005	0,002	0,001	0,000	0,000	0,000
0,360	0,360	0,130	0,047	0,017	0,006	0,002	0,001	0,000	0,000	0,000
0,370	0,370	0,137	0,051	0,019	0,007	0,003	0,001	0,000	0,000	0,000
0,380	0,380	0,144	0,055	0,021	0,008	0,003	0,001	0,000	0,000	0,000
0,390	0,390	0,152	0,059	0,023	0,009	0,004	0,001	0,001	0,000	0,000

Težina grana u strukturi	UKUPNA TEŽINA SERIJSKE STRUKTURE									
	Broj grana serijske strukture									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,400	0,400	0,160	0,064	0,026	0,010	0,004	0,002	0,001	0,000	0,000
0,410	0,410	0,168	0,069	0,028	0,012	0,005	0,002	0,001	0,000	0,000
0,420	0,420	0,176	0,074	0,031	0,013	0,005	0,002	0,001	0,000	0,000
0,430	0,430	0,185	0,080	0,034	0,015	0,006	0,003	0,001	0,001	0,000
0,440	0,440	0,194	0,085	0,037	0,016	0,007	0,003	0,001	0,001	0,000
0,450	0,450	0,203	0,091	0,041	0,018	0,008	0,004	0,002	0,001	0,000
0,460	0,460	0,212	0,097	0,045	0,021	0,009	0,004	0,002	0,001	0,000
0,470	0,470	0,221	0,104	0,049	0,023	0,011	0,005	0,002	0,001	0,001
0,480	0,480	0,230	0,111	0,053	0,025	0,012	0,006	0,003	0,001	0,001
0,490	0,490	0,240	0,118	0,058	0,028	0,014	0,007	0,003	0,002	0,001
0,500	0,500	0,250	0,125	0,063	0,031	0,016	0,008	0,004	0,002	0,001
0,510	0,510	0,260	0,133	0,068	0,035	0,018	0,009	0,005	0,002	0,001
0,520	0,520	0,270	0,141	0,073	0,038	0,020	0,010	0,005	0,003	0,001
0,530	0,530	0,281	0,149	0,079	0,042	0,022	0,012	0,006	0,003	0,002
0,540	0,540	0,292	0,157	0,085	0,046	0,025	0,013	0,007	0,004	0,002
0,550	0,550	0,303	0,166	0,092	0,050	0,028	0,015	0,008	0,005	0,003
0,560	0,560	0,314	0,176	0,098	0,055	0,031	0,017	0,010	0,005	0,003
0,570	0,570	0,325	0,185	0,106	0,060	0,034	0,020	0,011	0,006	0,004
0,580	0,580	0,336	0,195	0,113	0,066	0,038	0,022	0,013	0,007	0,004
0,590	0,590	0,348	0,205	0,121	0,071	0,042	0,025	0,015	0,009	0,005
0,600	0,600	0,360	0,216	0,130	0,078	0,047	0,028	0,017	0,010	0,006
0,610	0,610	0,372	0,227	0,138	0,084	0,052	0,031	0,019	0,012	0,007
0,620	0,620	0,384	0,238	0,148	0,092	0,057	0,035	0,022	0,014	0,008
0,630	0,630	0,397	0,250	0,158	0,099	0,063	0,039	0,025	0,016	0,010
0,640	0,640	0,410	0,262	0,168	0,107	0,069	0,044	0,028	0,018	0,012
0,650	0,650	0,423	0,275	0,179	0,116	0,075	0,049	0,032	0,021	0,013
0,660	0,660	0,436	0,287	0,190	0,125	0,083	0,055	0,036	0,024	0,016
0,670	0,670	0,449	0,301	0,202	0,135	0,090	0,061	0,041	0,027	0,018
0,680	0,680	0,462	0,314	0,214	0,145	0,099	0,067	0,046	0,031	0,021
0,690	0,690	0,476	0,329	0,227	0,156	0,108	0,074	0,051	0,035	0,024
0,700	0,700	0,490	0,343	0,240	0,168	0,118	0,082	0,058	0,040	0,028
0,710	0,710	0,504	0,358	0,254	0,180	0,128	0,091	0,065	0,046	0,033
0,720	0,720	0,518	0,373	0,269	0,193	0,139	0,100	0,072	0,052	0,037
0,730	0,730	0,533	0,389	0,284	0,207	0,151	0,110	0,081	0,059	0,043
0,740	0,740	0,548	0,405	0,300	0,222	0,164	0,122	0,090	0,067	0,049
0,750	0,750	0,563	0,422	0,316	0,237	0,178	0,133	0,100	0,075	0,056
0,760	0,760	0,578	0,439	0,334	0,254	0,193	0,146	0,111	0,085	0,064
0,770	0,770	0,593	0,457	0,352	0,271	0,208	0,160	0,124	0,095	0,073
0,780	0,780	0,608	0,475	0,370	0,289	0,225	0,176	0,137	0,107	0,083
0,790	0,790	0,624	0,493	0,390	0,308	0,243	0,192	0,152	0,120	0,095
0,800	0,800	0,640	0,512	0,410	0,328	0,262	0,210	0,168	0,134	0,107
0,810	0,810	0,656	0,531	0,430	0,349	0,282	0,229	0,185	0,150	0,122

Težina grana u strukturi	UKUPNA TEŽINA SERIJSKE STRUKTURE									
	Broj grana serijske strukture									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,820	0,820	0,672	0,551	0,452	0,371	0,304	0,249	0,204	0,168	0,137
0,830	0,830	0,689	0,572	0,475	0,394	0,327	0,271	0,225	0,187	0,155
0,840	0,840	0,706	0,593	0,498	0,418	0,351	0,295	0,248	0,208	0,175
0,850	0,850	0,723	0,614	0,522	0,444	0,377	0,321	0,272	0,232	0,197
0,860	0,860	0,740	0,636	0,547	0,470	0,405	0,348	0,299	0,257	0,221
0,870	0,870	0,757	0,659	0,573	0,498	0,434	0,377	0,328	0,286	0,248
0,880	0,880	0,774	0,681	0,600	0,528	0,464	0,409	0,360	0,316	0,279
0,890	0,890	0,792	0,705	0,627	0,558	0,497	0,442	0,394	0,350	0,312
0,900	0,900	0,810	0,729	0,656	0,590	0,531	0,478	0,430	0,387	0,349
0,910	0,910	0,828	0,754	0,686	0,624	0,568	0,517	0,470	0,428	0,389
0,920	0,920	0,846	0,779	0,716	0,659	0,606	0,558	0,513	0,472	0,434
0,930	0,930	0,865	0,804	0,748	0,696	0,647	0,602	0,560	0,520	0,484
0,940	0,940	0,884	0,831	0,781	0,734	0,690	0,648	0,610	0,573	0,539
0,950	0,950	0,903	0,857	0,815	0,774	0,735	0,698	0,663	0,630	0,599
0,960	0,960	0,922	0,885	0,849	0,815	0,783	0,751	0,721	0,693	0,665
0,970	0,970	0,941	0,913	0,885	0,859	0,833	0,808	0,784	0,760	0,737
0,980	0,980	0,960	0,941	0,922	0,904	0,886	0,868	0,851	0,834	0,817
0,990	0,990	0,980	0,970	0,961	0,951	0,941	0,932	0,923	0,914	0,904
1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

12.7. Težine paralene strukture

Težina grana u strukturi	UKUPNA TEŽINA PARALELNE STRUKTURE									
	Broj grana paralelne strukture									
	1	2	3	4	5	6	7	8	9	10
0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
0,010	0,010	0,020	0,030	0,039	0,049	0,059	0,068	0,077	0,086	0,096
0,020	0,020	0,040	0,059	0,078	0,096	0,114	0,132	0,149	0,166	0,183
0,030	0,030	0,059	0,087	0,115	0,141	0,167	0,192	0,216	0,240	0,263
0,040	0,040	0,078	0,115	0,151	0,185	0,217	0,249	0,279	0,307	0,335
0,050	0,050	0,098	0,143	0,185	0,226	0,265	0,302	0,337	0,370	0,401
0,060	0,060	0,116	0,169	0,219	0,266	0,310	0,352	0,390	0,427	0,461
0,070	0,070	0,135	0,196	0,252	0,304	0,353	0,398	0,440	0,480	0,516
0,080	0,080	0,154	0,221	0,284	0,341	0,394	0,442	0,487	0,528	0,566
0,090	0,090	0,172	0,246	0,314	0,376	0,432	0,483	0,530	0,572	0,611
0,100	0,100	0,190	0,271	0,344	0,410	0,469	0,522	0,570	0,613	0,651
0,110	0,110	0,208	0,295	0,373	0,442	0,503	0,558	0,606	0,650	0,688
0,120	0,120	0,226	0,319	0,400	0,472	0,536	0,591	0,640	0,684	0,721
0,130	0,130	0,243	0,341	0,427	0,502	0,566	0,623	0,672	0,714	0,752
0,140	0,140	0,260	0,364	0,453	0,530	0,595	0,652	0,701	0,743	0,779
0,150	0,150	0,278	0,386	0,478	0,556	0,623	0,679	0,728	0,768	0,803
0,160	0,160	0,294	0,407	0,502	0,582	0,649	0,705	0,752	0,792	0,825
0,170	0,170	0,311	0,428	0,525	0,606	0,673	0,729	0,775	0,813	0,845
0,180	0,180	0,328	0,449	0,548	0,629	0,696	0,751	0,796	0,832	0,863
0,190	0,190	0,344	0,469	0,570	0,651	0,718	0,771	0,815	0,850	0,878
0,200	0,200	0,360	0,488	0,590	0,672	0,738	0,790	0,832	0,866	0,893
0,210	0,210	0,376	0,507	0,610	0,692	0,757	0,808	0,848	0,880	0,905
0,220	0,220	0,392	0,525	0,630	0,711	0,775	0,824	0,863	0,893	0,917
0,230	0,230	0,407	0,543	0,648	0,729	0,792	0,840	0,876	0,905	0,927
0,240	0,240	0,422	0,561	0,666	0,746	0,807	0,854	0,889	0,915	0,936
0,250	0,250	0,438	0,578	0,684	0,763	0,822	0,867	0,900	0,925	0,944
0,260	0,260	0,452	0,595	0,700	0,778	0,836	0,878	0,910	0,933	0,951
0,270	0,270	0,467	0,611	0,716	0,793	0,849	0,890	0,919	0,941	0,957
0,280	0,280	0,482	0,627	0,731	0,807	0,861	0,900	0,928	0,948	0,963
0,290	0,290	0,496	0,642	0,746	0,820	0,872	0,909	0,935	0,954	0,967
0,300	0,300	0,510	0,657	0,760	0,832	0,882	0,918	0,942	0,960	0,972
0,310	0,310	0,524	0,671	0,773	0,844	0,892	0,926	0,949	0,965	0,976
0,320	0,320	0,538	0,686	0,786	0,855	0,901	0,933	0,954	0,969	0,979
0,330	0,330	0,551	0,699	0,798	0,865	0,910	0,939	0,959	0,973	0,982
0,340	0,340	0,564	0,713	0,810	0,875	0,917	0,945	0,964	0,976	0,984
0,350	0,350	0,578	0,725	0,821	0,884	0,925	0,951	0,968	0,979	0,987
0,360	0,360	0,590	0,738	0,832	0,893	0,931	0,956	0,972	0,982	0,988
0,370	0,370	0,603	0,750	0,842	0,901	0,937	0,961	0,975	0,984	0,990
0,380	0,380	0,616	0,762	0,852	0,908	0,943	0,965	0,978	0,986	0,992
0,390	0,390	0,628	0,773	0,862	0,916	0,948	0,969	0,981	0,988	0,993

Težina grana u strukturi	UKUPNA TEŽINA PARALELNE STRUKTURE									
	Broj grana paralelne strukture									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,400	0,400	0,640	0,784	0,870	0,922	0,953	0,972	0,983	0,990	0,994
0,410	0,410	0,652	0,795	0,879	0,929	0,958	0,975	0,985	0,991	0,995
0,420	0,420	0,664	0,805	0,887	0,934	0,962	0,978	0,987	0,993	0,996
0,430	0,430	0,675	0,815	0,894	0,940	0,966	0,980	0,989	0,994	0,996
0,440	0,440	0,686	0,824	0,902	0,945	0,969	0,983	0,990	0,995	0,997
0,450	0,450	0,698	0,834	0,908	0,950	0,972	0,985	0,992	0,995	0,997
0,460	0,460	0,708	0,843	0,915	0,954	0,975	0,987	0,993	0,996	0,998
0,470	0,470	0,719	0,851	0,921	0,958	0,978	0,988	0,994	0,997	0,998
0,480	0,480	0,730	0,859	0,927	0,962	0,980	0,990	0,995	0,997	0,999
0,490	0,490	0,740	0,867	0,932	0,965	0,982	0,991	0,995	0,998	0,999
0,500	0,500	0,750	0,875	0,938	0,969	0,984	0,992	0,996	0,998	0,999
0,510	0,510	0,760	0,882	0,942	0,972	0,986	0,993	0,997	0,998	0,999
0,520	0,520	0,770	0,889	0,947	0,975	0,988	0,994	0,997	0,999	0,999
0,530	0,530	0,779	0,896	0,951	0,977	0,989	0,995	0,998	0,999	0,999
0,540	0,540	0,788	0,903	0,955	0,979	0,991	0,996	0,998	0,999	1,000
0,550	0,550	0,798	0,909	0,959	0,982	0,992	0,996	0,998	0,999	1,000
0,560	0,560	0,806	0,915	0,963	0,984	0,993	0,997	0,999	0,999	1,000
0,570	0,570	0,815	0,920	0,966	0,985	0,994	0,997	0,999	0,999	1,000
0,580	0,580	0,824	0,926	0,969	0,987	0,995	0,998	0,999	1,000	1,000
0,590	0,590	0,832	0,931	0,972	0,988	0,995	0,998	0,999	1,000	1,000
0,600	0,600	0,840	0,936	0,974	0,990	0,996	0,998	0,999	1,000	1,000
0,610	0,610	0,848	0,941	0,977	0,991	0,996	0,999	0,999	1,000	1,000
0,620	0,620	0,856	0,945	0,979	0,992	0,997	0,999	1,000	1,000	1,000
0,630	0,630	0,863	0,949	0,981	0,993	0,997	0,999	1,000	1,000	1,000
0,640	0,640	0,870	0,953	0,983	0,994	0,998	0,999	1,000	1,000	1,000
0,650	0,650	0,878	0,957	0,985	0,995	0,998	0,999	1,000	1,000	1,000
0,660	0,660	0,884	0,961	0,987	0,995	0,998	0,999	1,000	1,000	1,000
0,670	0,670	0,891	0,964	0,988	0,996	0,999	1,000	1,000	1,000	1,000
0,680	0,680	0,898	0,967	0,990	0,997	0,999	1,000	1,000	1,000	1,000
0,690	0,690	0,904	0,970	0,991	0,997	0,999	1,000	1,000	1,000	1,000
0,700	0,700	0,910	0,973	0,992	0,998	0,999	1,000	1,000	1,000	1,000
0,710	0,710	0,916	0,976	0,993	0,998	0,999	1,000	1,000	1,000	1,000
0,720	0,720	0,922	0,978	0,994	0,998	1,000	1,000	1,000	1,000	1,000
0,730	0,730	0,927	0,980	0,995	0,999	1,000	1,000	1,000	1,000	1,000
0,740	0,740	0,932	0,982	0,995	0,999	1,000	1,000	1,000	1,000	1,000
0,750	0,750	0,938	0,984	0,996	0,999	1,000	1,000	1,000	1,000	1,000
0,760	0,760	0,942	0,986	0,997	0,999	1,000	1,000	1,000	1,000	1,000
0,770	0,770	0,947	0,988	0,997	0,999	1,000	1,000	1,000	1,000	1,000
0,780	0,780	0,952	0,989	0,998	0,999	1,000	1,000	1,000	1,000	1,000
0,790	0,790	0,956	0,991	0,998	1,000	1,000	1,000	1,000	1,000	1,000
0,800	0,800	0,960	0,992	0,998	1,000	1,000	1,000	1,000	1,000	1,000
0,810	0,810	0,964	0,993	0,999	1,000	1,000	1,000	1,000	1,000	1,000

Težina grana u strukturi	UKUPNA TEŽINA PARALELNE STRUKTURE									
	Broj grana paralelne strukture									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0,820	0,820	0,968	0,994	0,999	1,000	1,000	1,000	1,000	1,000	1,000
0,830	0,830	0,971	0,995	0,999	1,000	1,000	1,000	1,000	1,000	1,000
0,840	0,840	0,974	0,996	0,999	1,000	1,000	1,000	1,000	1,000	1,000
0,850	0,850	0,978	0,997	0,999	1,000	1,000	1,000	1,000	1,000	1,000
0,860	0,860	0,980	0,997	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,870	0,870	0,983	0,998	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,880	0,880	0,986	0,998	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,890	0,890	0,988	0,999	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,900	0,900	0,990	0,999	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,910	0,910	0,992	0,999	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,920	0,920	0,994	0,999	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,930	0,930	0,995	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,940	0,940	0,996	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,950	0,950	0,998	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,960	0,960	0,998	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,970	0,970	0,999	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,980	0,980	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
0,990	0,990	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

12.8. Rezultati analize složene neorijentirane strukture s jednakim težinama u svim grana

Shema zadane strukture je prikazana na slici 7.7.

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,000	0,000	0,000	0,000	0,000
0,010	0,010	0,000	0,096	0,010
0,020	0,021	0,000	0,183	0,020
0,030	0,033	0,000	0,263	0,030
0,040	0,045	0,000	0,335	0,040
0,050	0,058	0,000	0,401	0,050
0,060	0,071	0,000	0,461	0,060
0,070	0,086	0,000	0,516	0,070
0,080	0,101	0,000	0,566	0,080
0,090	0,116	0,000	0,611	0,090
0,100	0,132	0,000	0,651	0,100
0,110	0,149	0,000	0,688	0,110
0,120	0,167	0,000	0,721	0,120
0,130	0,186	0,000	0,752	0,130
0,140	0,205	0,000	0,779	0,140
0,150	0,224	0,000	0,803	0,150
0,160	0,245	0,000	0,825	0,160
0,170	0,266	0,000	0,845	0,170
0,180	0,287	0,000	0,863	0,180
0,190	0,309	0,000	0,878	0,190
0,200	0,332	0,000	0,893	0,200
0,210	0,355	0,000	0,905	0,210
0,220	0,378	0,000	0,917	0,220
0,230	0,402	0,000	0,927	0,230
0,240	0,426	0,000	0,936	0,240
0,250	0,451	0,000	0,944	0,250
0,260	0,475	0,000	0,951	0,260
0,270	0,500	0,000	0,957	0,270
0,280	0,525	0,000	0,963	0,280
0,290	0,549	0,000	0,967	0,290
0,300	0,574	0,000	0,972	0,300
0,310	0,598	0,000	0,976	0,310
0,320	0,622	0,000	0,979	0,320
0,330	0,646	0,000	0,982	0,330
0,340	0,669	0,000	0,984	0,340
0,350	0,692	0,000	0,987	0,350
0,360	0,714	0,000	0,988	0,360

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,370	0,735	0,000	0,990	0,370
0,380	0,756	0,000	0,992	0,380
0,390	0,776	0,000	0,993	0,390
0,400	0,795	0,000	0,994	0,400
0,410	0,814	0,000	0,995	0,410
0,420	0,831	0,000	0,996	0,420
0,430	0,848	0,000	0,996	0,430
0,440	0,863	0,000	0,997	0,440
0,450	0,878	0,000	0,997	0,450
0,460	0,891	0,000	0,998	0,460
0,470	0,904	0,001	0,998	0,470
0,480	0,915	0,001	0,999	0,480
0,490	0,926	0,001	0,999	0,490
0,500	0,936	0,001	0,999	0,500
0,510	0,944	0,001	0,999	0,510
0,520	0,952	0,001	0,999	0,520
0,530	0,959	0,002	0,999	0,530
0,540	0,966	0,002	1,000	0,540
0,550	0,971	0,003	1,000	0,550
0,560	0,976	0,003	1,000	0,560
0,570	0,980	0,004	1,000	0,570
0,580	0,984	0,004	1,000	0,580
0,590	0,987	0,005	1,000	0,590
0,600	0,989	0,006	1,000	0,600
0,610	0,992	0,007	1,000	0,610
0,620	0,993	0,008	1,000	0,620
0,630	0,995	0,010	1,000	0,630
0,640	0,996	0,012	1,000	0,640
0,650	0,997	0,013	1,000	0,650
0,660	0,998	0,016	1,000	0,660
0,670	0,998	0,018	1,000	0,670
0,680	0,999	0,021	1,000	0,680
0,690	0,999	0,024	1,000	0,690
0,700	0,999	0,028	1,000	0,700
0,710	1,000	0,033	1,000	0,710
0,720	1,000	0,037	1,000	0,720
0,730	1,000	0,043	1,000	0,730

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,740	1,000	0,049	1,000	0,740
0,750	1,000	0,056	1,000	0,750
0,760	1,000	0,064	1,000	0,760
0,770	1,000	0,073	1,000	0,770
0,780	1,000	0,083	1,000	0,780
0,790	1,000	0,095	1,000	0,790
0,800	1,000	0,107	1,000	0,800
0,810	1,000	0,122	1,000	0,810
0,820	1,000	0,137	1,000	0,820
0,830	1,000	0,155	1,000	0,830
0,840	1,000	0,175	1,000	0,840
0,850	1,000	0,197	1,000	0,850
0,860	1,000	0,221	1,000	0,860
0,870	1,000	0,248	1,000	0,870

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,880	1,000	0,279	1,000	0,880
0,890	1,000	0,312	1,000	0,890
0,900	1,000	0,349	1,000	0,900
0,910	1,000	0,389	1,000	0,910
0,920	1,000	0,434	1,000	0,920
0,930	1,000	0,484	1,000	0,930
0,940	1,000	0,539	1,000	0,940
0,950	1,000	0,599	1,000	0,950
0,960	1,000	0,665	1,000	0,960
0,970	1,000	0,737	1,000	0,970
0,980	1,000	0,817	1,000	0,980
0,990	1,000	0,904	1,000	0,990
1,000	1,000	1,000	1,000	1,000

12.9. Rezultati analize složene orijentirane strukture 1 s jednakim težinama u svim grana

Shema zadane strukture je prikazana na slici 7.16.

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,000	0,000	0,000	0,000	0,000
0,010	0,000	0,000	0,096	0,010
0,020	0,001	0,000	0,183	0,020
0,030	0,002	0,000	0,263	0,030
0,040	0,003	0,000	0,335	0,040
0,050	0,005	0,000	0,401	0,050
0,060	0,008	0,000	0,461	0,060
0,070	0,011	0,000	0,516	0,070
0,080	0,014	0,000	0,566	0,080
0,090	0,018	0,000	0,611	0,090
0,100	0,023	0,000	0,651	0,100
0,110	0,028	0,000	0,688	0,110
0,120	0,034	0,000	0,721	0,120
0,130	0,040	0,000	0,752	0,130
0,140	0,047	0,000	0,779	0,140
0,150	0,055	0,000	0,803	0,150
0,160	0,063	0,000	0,825	0,160
0,170	0,072	0,000	0,845	0,170
0,180	0,081	0,000	0,863	0,180
0,190	0,091	0,000	0,878	0,190
0,200	0,102	0,000	0,893	0,200
0,210	0,113	0,000	0,905	0,210
0,220	0,125	0,000	0,917	0,220
0,230	0,138	0,000	0,927	0,230
0,240	0,151	0,000	0,936	0,240
0,250	0,165	0,000	0,944	0,250
0,260	0,179	0,000	0,951	0,260
0,270	0,195	0,000	0,957	0,270
0,280	0,210	0,000	0,963	0,280
0,290	0,227	0,000	0,967	0,290
0,300	0,243	0,000	0,972	0,300
0,310	0,261	0,000	0,976	0,310
0,320	0,279	0,000	0,979	0,320
0,330	0,297	0,000	0,982	0,330
0,340	0,316	0,000	0,984	0,340
0,350	0,335	0,000	0,987	0,350
0,360	0,355	0,000	0,988	0,360

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,370	0,375	0,000	0,990	0,370
0,380	0,395	0,000	0,992	0,380
0,390	0,415	0,000	0,993	0,390
0,400	0,436	0,000	0,994	0,400
0,410	0,457	0,000	0,995	0,410
0,420	0,478	0,000	0,996	0,420
0,430	0,500	0,000	0,996	0,430
0,440	0,521	0,000	0,997	0,440
0,450	0,542	0,000	0,997	0,450
0,460	0,563	0,000	0,998	0,460
0,470	0,584	0,001	0,998	0,470
0,480	0,605	0,001	0,999	0,480
0,490	0,626	0,001	0,999	0,490
0,500	0,647	0,001	0,999	0,500
0,510	0,667	0,001	0,999	0,510
0,520	0,687	0,001	0,999	0,520
0,530	0,706	0,002	0,999	0,530
0,540	0,725	0,002	1,000	0,540
0,550	0,744	0,003	1,000	0,550
0,560	0,762	0,003	1,000	0,560
0,570	0,779	0,004	1,000	0,570
0,580	0,796	0,004	1,000	0,580
0,590	0,813	0,005	1,000	0,590
0,600	0,828	0,006	1,000	0,600
0,610	0,843	0,007	1,000	0,610
0,620	0,857	0,008	1,000	0,620
0,630	0,871	0,010	1,000	0,630
0,640	0,883	0,012	1,000	0,640
0,650	0,895	0,013	1,000	0,650
0,660	0,907	0,016	1,000	0,660
0,670	0,917	0,018	1,000	0,670
0,680	0,927	0,021	1,000	0,680
0,690	0,936	0,024	1,000	0,690
0,700	0,944	0,028	1,000	0,700
0,710	0,951	0,033	1,000	0,710
0,720	0,958	0,037	1,000	0,720
0,730	0,964	0,043	1,000	0,730

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,740	0,970	0,049	1,000	0,740
0,750	0,975	0,056	1,000	0,750
0,760	0,979	0,064	1,000	0,760
0,770	0,983	0,073	1,000	0,770
0,780	0,986	0,083	1,000	0,780
0,790	0,989	0,095	1,000	0,790
0,800	0,991	0,107	1,000	0,800
0,810	0,993	0,122	1,000	0,810
0,820	0,995	0,137	1,000	0,820
0,830	0,996	0,155	1,000	0,830
0,840	0,997	0,175	1,000	0,840
0,850	0,998	0,197	1,000	0,850
0,860	0,999	0,221	1,000	0,860
0,870	0,999	0,248	1,000	0,870

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,880	0,999	0,279	1,000	0,880
0,890	1,000	0,312	1,000	0,890
0,900	1,000	0,349	1,000	0,900
0,910	1,000	0,389	1,000	0,910
0,920	1,000	0,434	1,000	0,920
0,930	1,000	0,484	1,000	0,930
0,940	1,000	0,539	1,000	0,940
0,950	1,000	0,599	1,000	0,950
0,960	1,000	0,665	1,000	0,960
0,970	1,000	0,737	1,000	0,970
0,980	1,000	0,817	1,000	0,980
0,990	1,000	0,904	1,000	0,990
1,000	1,000	1,000	1,000	1,000

12.10. Rezultati analize složene orijentirane strukture 2 s jednakim težinama u svim grana

Shema zadane strukture je prikazana na slici 7.26.

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,000	0,000	0,000	0,000	0,000
0,010	0,000	0,000	0,096	0,010
0,020	0,001	0,000	0,183	0,020
0,030	0,002	0,000	0,263	0,030
0,040	0,003	0,000	0,335	0,040
0,050	0,005	0,000	0,401	0,050
0,060	0,007	0,000	0,461	0,060
0,070	0,010	0,000	0,516	0,070
0,080	0,013	0,000	0,566	0,080
0,090	0,017	0,000	0,611	0,090
0,100	0,021	0,000	0,651	0,100
0,110	0,025	0,000	0,688	0,110
0,120	0,030	0,000	0,721	0,120
0,130	0,036	0,000	0,752	0,130
0,140	0,041	0,000	0,779	0,140
0,150	0,048	0,000	0,803	0,150
0,160	0,054	0,000	0,825	0,160
0,170	0,062	0,000	0,845	0,170
0,180	0,069	0,000	0,863	0,180
0,190	0,077	0,000	0,878	0,190
0,200	0,086	0,000	0,893	0,200
0,210	0,095	0,000	0,905	0,210
0,220	0,104	0,000	0,917	0,220
0,230	0,114	0,000	0,927	0,230
0,240	0,124	0,000	0,936	0,240
0,250	0,135	0,000	0,944	0,250
0,260	0,146	0,000	0,951	0,260
0,270	0,157	0,000	0,957	0,270
0,280	0,169	0,000	0,963	0,280
0,290	0,182	0,000	0,967	0,290
0,300	0,194	0,000	0,972	0,300
0,310	0,207	0,000	0,976	0,310
0,320	0,221	0,000	0,979	0,320
0,330	0,234	0,000	0,982	0,330
0,340	0,249	0,000	0,984	0,340
0,350	0,263	0,000	0,987	0,350
0,360	0,278	0,000	0,988	0,360

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,370	0,293	0,000	0,990	0,370
0,380	0,308	0,000	0,992	0,380
0,390	0,324	0,000	0,993	0,390
0,400	0,340	0,000	0,994	0,400
0,410	0,356	0,000	0,995	0,410
0,420	0,372	0,000	0,996	0,420
0,430	0,388	0,000	0,996	0,430
0,440	0,405	0,000	0,997	0,440
0,450	0,422	0,000	0,997	0,450
0,460	0,439	0,000	0,998	0,460
0,470	0,456	0,001	0,998	0,470
0,480	0,473	0,001	0,999	0,480
0,490	0,490	0,001	0,999	0,490
0,500	0,508	0,001	0,999	0,500
0,510	0,525	0,001	0,999	0,510
0,520	0,543	0,001	0,999	0,520
0,530	0,560	0,002	0,999	0,530
0,540	0,577	0,002	1,000	0,540
0,550	0,594	0,003	1,000	0,550
0,560	0,612	0,003	1,000	0,560
0,570	0,629	0,004	1,000	0,570
0,580	0,646	0,004	1,000	0,580
0,590	0,662	0,005	1,000	0,590
0,600	0,679	0,006	1,000	0,600
0,610	0,695	0,007	1,000	0,610
0,620	0,711	0,008	1,000	0,620
0,630	0,727	0,010	1,000	0,630
0,640	0,743	0,012	1,000	0,640
0,650	0,758	0,013	1,000	0,650
0,660	0,773	0,016	1,000	0,660
0,670	0,788	0,018	1,000	0,670
0,680	0,802	0,021	1,000	0,680
0,690	0,816	0,024	1,000	0,690
0,700	0,829	0,028	1,000	0,700
0,710	0,842	0,033	1,000	0,710
0,720	0,855	0,037	1,000	0,720
0,730	0,867	0,043	1,000	0,730

Težina grana strukture	UKUPNA TEŽINA STRUKTURE			
	Zadana struktura	Serijska struktura	Paralelna struktura	Jedna grana
0,740	0,878	0,049	1,000	0,740
0,750	0,889	0,056	1,000	0,750
0,760	0,900	0,064	1,000	0,760
0,770	0,910	0,073	1,000	0,770
0,780	0,919	0,083	1,000	0,780
0,790	0,928	0,095	1,000	0,790
0,800	0,937	0,107	1,000	0,800
0,810	0,945	0,122	1,000	0,810
0,820	0,952	0,137	1,000	0,820
0,830	0,959	0,155	1,000	0,830
0,840	0,965	0,175	1,000	0,840
0,850	0,970	0,197	1,000	0,850
0,860	0,975	0,221	1,000	0,860
0,870	0,980	0,248	1,000	0,870
0,880	0,984	0,279	1,000	0,880
0,890	0,987	0,312	1,000	0,890
0,900	0,990	0,349	1,000	0,900
0,910	0,993	0,389	1,000	0,910
0,920	0,995	0,434	1,000	0,920
0,930	0,996	0,484	1,000	0,930
0,940	0,998	0,539	1,000	0,940
0,950	0,999	0,599	1,000	0,950
0,960	0,999	0,665	1,000	0,960
0,970	1,000	0,737	1,000	0,970
0,980	1,000	0,817	1,000	0,980
0,990	1,000	0,904	1,000	0,990
1,000	1,000	1,000	1,000	1,000

13. REFERENCE I LITERATURA

[1] ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[2] ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems —Requirements

[3] ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management

[4] ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance

[5] ISO/IEC 27004:2009, Information technology — Security techniques — Information security management — Measurement

[6] ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management

[7] ISO 31000:2009, Risk management — Principles and guidelines

[8] Advanced Topics In Information Resources Management (Advanced Topics In Information Resources Management Series), 2004, IGI Global, ISBM 1591402530

[9] The Analytics Of Risk Model Validation (Quantitative Finance) (Quantitative Finance), 2007, Academic Press, ISBN 978-0-7506-8158-2

[10] Annals Of Cases On Information Technology (Cases On Information Technology Series), 2003, IGI Global, ISBN 1591400619

[11] Are You Being Served?: New Tools For Measuring Service Delivery, 2007 World Bank Publications, ISBN 978-0-8213-7185-5

[12] Asset Protection And Security Management Handbook 2002 AUERBACH 0-8493-1603-0

[13] Business Process Management Workshops: Bpm 2007 International Workshops, Bpi, Bpd, Cbp, Prohealth,

[14] Refmod, Semantics4ws, Brisbane, Australia, September ... Papers (Lecture Notes In Computer Science) 2008 Springer 3-540-78237-0

[15] Catastrophe Modeling: A New Approach To Managing Risk (Huebner International Series On Risk, Insurance And Economic Security) 2004 Springer 0-387-23082-3

[16] CompTIA's IT Project+ certification exam Computer Security In The 21st Century 2005 Springer 0-387-24005-5

[17] Corporate Governance In Banking 2007 Edward Elgar Publishing 9781845429409

[18] Digital Communities In A Networked Society: E-Commerce, E-Business And E-Government (Ifip International Federation For Information Processing) 2004 Springer 1-4020-7795-5

[19] Distance Learning And University Effectiveness: Changing Educational Paradigms For Online Learning 2003 Information Science Publishing 1-59140-178-X

[20] The Economics Of Risk 2003 W. E. Upjohn Institute 0-88099-268-9

[21] Encyclopedia Of Information Science And Technology 2005 Idea Group Reference 1-59140-553-X

[22] Frontiers Of Evolutionary Computation (Genetic Algorithms And Evolutionary Computation) 2004 Springer 1-4020-7524-3

[23] Hacker's Challenge 2001 McGraw-Hill Osborne Media 0-07-219384-0
[24] Handbook Of Research On Wireless Security 2008 Information Science Reference 978-1-59904-899-4
[25] Handbook On Architectures Of Information Systems (International Handbooks On Information Systems) 2005 Springer 3-540-25472-2
[26] Information Management Information Quality Management: Theory And Applications (Information Quality Management) 2006 IGI Global 1-59904-024-7
[27] Information Security Management Handbook, Fifth Edition 2003 AUERBACH 0-8493-1997-8
[28] Information Security Policies And Actions In Modern Integrated Systems 2004 IGI Global 1591401860
[29] Internal Audit Handbook: Management With The Sap®-Audit Roadmap 2007 Springer 978-3-540-70886-5
[30] International Convergence Of Capital Measurement And Capital Standards 2004 Bank for Internat. Settlements 92-9131-669-5
[31] ISQ Handbook 2003: An In-Depth Coverage Of Vendor And Vendor- Neutral Qualifications 2003 Forschungsstelle für Sicherheitspolitik ETH Zürich 3905641917
[32] IT Baseline Protection Manual Learning Design: A Handbook On Modelling And Delivering Networked Education And Training 2005 Springer 3-540-22814-4
[33] Managing Business Risk: A Practical Guide To Protecting Your Business 2008 Kogan Page 978-0-7494-5059-5
[34] Managing Downside Risk In Financial Markets (With- Cd-Rom) (Quantitative Finance) 2001 Butterworth-Heinemann 0750648635
[35] Monte Carlo And Quasi-Monte Carlo Methods 2004 2006 Springer 3-540-25541-9
[36] The Portable Mba In Project Management 2003 Wiley 0-471-26899-2
[37] The Professional Handbook Of Financial Risk Management 2000 Butterworth-Heinemann 0750641118
[38] Project And Program Risk Management: A Guide To Managing Project Risks And Opportunities (Pmbok Handbooks) 1992 Project Management Institute 1-880410-06-0
[39] Project Management: Basic, Second Edition 2004 Course Technology Risk In Social Science 2006 Oxford University Press, USA 0199285950
[40] Risk Management Guide For Small Business 2005
[41] Global Risk Alliance and the NSW Dept. of State and Regional Development 0731332490
[42] The Secure Online Business Handbook: E-Commerce, It Functionality And Business Continuity 2005 Kogan Page 0-7494-4425-8
[43] Springer Handbook Of Engineering Statistics 2006 Springer 1-85233-806-7
[44] Strategic Knowledge Management Technology 2004 Idea Group Publishing 1591403367
[45] Technologies For Business Information Systems 2007 Springer 1-4020-5633-8
[46] Web And Information Security 2005 IRM Press 1-59140-588-2
[47] Rath & Strong Rath & Strong's Six Sigma Team Pocket Guide 2003 McGraw-Hill 0071417567

[48] Rob Addy Effective It Service Management: To Itil And Beyond! 2007 Springer 978-3-540-73197-9
[49] Dennis M. Ahern; Aaron Clouse; Richard Turner Cmmi Distilled: A Practical Introduction To Integrated Process Improvement (3rd Edition) (The Sei Series In Software Engineering) 2008 Addison-Wesley Professional 978-0-321-46108-7
[50] A.Kaufmann, D.Grouchko, R.Croun, Mathematical Models for the Study of the Reliability of Systems, 1977, Academic Press, 0-12-402370-3
[51] Dennis M. Ahern; Aaron Clouse; Richard Turner Cmmi(R) Distilled: A Practical Introduction To Integrated Process Improvement (2nd Edition) (The Sei Series In Software Engineering) 2003 Addison-Wesley Professional 0-321-18613-3
[52] F. Alan Goodman Defining And Deploying Software Processes 2005 AUERBACH 0-8493-9845-2
[53] Joyce Fortune, Geoff Peters, Information Systems Achieving Success by Avoiding Failure, 2005, John Wiley & Sons Ltd, 0-470-86255-6
[54] Claudio Albanese; Giuseppe Campolieti Advanced Derivatives Pricing And Risk Management: Theory, Tools, And Hands-On Programming Applications (Academic Press Advanced Finance
[55] Series) (Academic Press Advanced Finance Series) 2005 Academic Press 0-12-047682-7
[56] Jason Albanese; Wes Sonnenreich Network Security Illustrated 2003 McGraw-Hill Professional 0-07-141504-1
[57] Christopher Alberts; Audrey Dorofee Managing Information Security Risks: The Octave (Sm) Approach (The Sei Series In Software Engineering) 2002 Addison-Wesley Professional 0-321-11886-3
[58] Zee B. Alfassi Statistical Treatment Of Analytical Data 2004 WileyBlackwell 0-632-05367-4
[59] Theodore T. Allen Introduction To Engineering Statistics And Six Sigma: Statistical Quality Control And Design Of Experiments And Systems 2006 Springer 1-85233-955-1
[60] Inteaz Alli Food Quality Assurance: Principles And Practices 2003 CRC 1-56676-930-2
[61] Amanda Andress Surviving Security: How To Integrate People, Process, And Technology, Second Edition 2003 AUERBACH 0849320429
[62] Asqc The Quality Auditor's Haccp Handbook 2001 ASQ Quality Press 0-87389-496-0
[63] Claudia M. Baca; Patti M. Jansen; Claudia Baca; Patti Jansen Pmp: Project Management ProfessionalWorkbook 2003 Sybex 0782142400
[64] Kenneth R. Bainey Integrated It Project Management: A Model-Centric Approach (Artech House Project Management Library) 2004 Artech House Publishers 1-58053-828-2
[65] Robert M. Losee, A Discipline Independent Definition of Information, J. of the American Society for Information Science 48(3) 1997, 254-269.
[66] Erik Banks Alternative Risk Transfer: Integrated Risk Management Through Insurance, Reinsurance, And The Capital Markets (TheWiley Finance Series) 2004 Wiley 0-470-85745-5
[67] Erik Banks; Richard Dunn Practical Risk Management 2003 Wiley 0-470-84967-3

[68] Bruce T. Barkley Integrated Project Management 2006 McGraw-Hill Professional 0071466266
[69] Robert Barton Global It Management: A Practical Approach 2003 Wiley 0-470-85433-2
[70] Thomas L. Barton; William G. Shenkir; Paul L. Walker Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management (Financial Times Prentice Hall Books) 2002 FT Press 0-13-008754-8
[71] Gattiker, Urs E., The Information Security Dictionary: Defining The Terms That Define Security For E-Business, Internet, Information And Wireless Technology (The International ... Series In Engineering And Computer Science), 2004, Springer, 1-4020-7889-7
[72] Chris Bates Xml In Theory And Practice 2003 Wiley 0470843446
[73] Aaron W. Bayles; Chris Hurley; Johnny Long; Ed Brindley; James C. Foster; Christopher W. Klaus Infosec Career Hacking: Sell Your Skillz, Not Your Soul 2005 Syngress 1-597490-11-3
[74] Boris Beizer Software Testing Techniques 2e 1990 International Thomson Computer Press 1850328803
[75] Michael Bell Service-Oriented Modeling (Soa): Service Analysis, Design, And Architecture 2008 Wiley 978-0-470-14111-3
[76] Simon Bell; Trevor Wood-Harper How To Set Up Information Systems: A Non-Specialist's Guide To The Multiview Appproach 2003 Earthscan Publications Ltd. 1853839582
[77] Scott Berkun The Art Of Project Management (Theory In Practice (O'reilly)) 2005 O'Reilly Media, Inc. 0-596-00786-8
[78] Joël Bessis Risk Management In Banking, 2nd Edition 2002 Wiley 0-471-89336-6
[79] Elaine Biech The Business Of Consulting: The Basics And Beyond (Cd-Rom Included) (Essential Knowledge Resource) 2007 Pfeiffer 0787994642
[80] Paul P. Biemer; Lars E. Lyberg Introduction To Survey Quality (Wiley Series In Survey Methodology) 2003 Wiley-Interscience 0-471-19375-5
[81] Matt Bishop Computer Security: Art And Science 2002 Addison-Wesley Professional 0-201-44099-7
[82] Matt Bishop Introduction To Computer Security 2004 Addison-Wesley Professional 0-321-24744-2
[83] Rex Black Critical Testing Processes: Plan, Prepare, Perform, Perfect 2003 Addison-Wesley Professional 0-201-74868-1
[84] Tessa, Blakeley Silver Joomla! Template Design: Create Your Own Professional-Quality Templates With This Fast, Friendly Guide 2007 Packt Publishing 978-1-847191-44-1
[85] Thorsten Blecker; Gerhard Friedrich; Bernd Kaluza; Nizar Abdelkafi; Gerold Kreutler Information And Management Systems For Product Customization (Integrated Series In Information Systems) 2004 Springer 0-387-23347-4
[86] Stephen S. Bonham It Project Portfolio Management 2004 Artech House Publishers 1-58053-781-2
[87] Robert J. Brent Applied Cost-Benefit Analysis 2007 Edward Elgar Publishing 9781843768913

[88] J. Brian Heywood The Outsourcing Dilemma: The Search For Competitiveness 2001 Financial Times/Prentice Hall 0130351318
[89] Warren Brussee Statistics For Six Sigma Made Easy 2004 McGraw-Hill 0071433856
[90] Noel Bruton Managing The It Services Process (Computer Weekly Professional) (Computer Weekly Professional) 2003 Butterworth-Heinemann 0750657235
[91] Web Link: Princeton Univerity http://wordnet.princeton.edu/
[92] Web Link: Wikipedia http://en.wikipedia.org/wiki/Information
[93] Web Link: Web Dictionary of Cybernetics and Systems http://pespmc1.vub.ac.be/ASC/indexASC.html
[94] Web Link: WikiAnswers http://wiki.answers.com/Q/What_is_the_definition_of_information_system
[95] Web Link: UKAS http://www.ukas.com/
[96] Web Link: Encyclopedia Britanica http://www.britannica.com/EBchecked/topic/287895/information-system
[97] Web Link: AllWords http://www.allwords.com/word-information+system.html
[98] Web Link: BusinessDictionary http://www.businessdictionary.com/definition/information-system.html
[99] ISO 9001:2008 Quality management systems – Requirements
[100] Jessup, Leonard M.; Joseph S. Valacich (2008). *Information Systems Today* (3rd ed.). Pearson Publishing. p. 416
[101] Chorafas, Dimitris N. , Enterprise Architecture And New Generation Information Systems, CRC, 9781574443172, 2001
[102] Polack, Jennifer (December 2009). "Planning a CIS Education Within a CS Framework". Journal of Computing Sciences in Colleges 25 (2): 100–106. ISSN 1937-4771