Model za procjenu kritičnih informacijskih sustava primjenom višekriterijskoga odlučivanja s elementima za analizu i procjenu rizika u financijskim institucijama

Maček, Davor

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Davor Maček

MODEL ZA PROCJENU KRITIČNIH INFORMACIJSKIH SUSTAVA PRIMJENOM VIŠEKRITERIJSKOGA ODLUČIVANJA S ELEMENTIMA ZA ANALIZU I PROCJENU RIZIKA U FINANCIJSKIM INSTITUCIJAMA

DOKTORSKI RAD

Varaždin, 2021

Sveučilište u Zagrebu

Fakultet organizacije i informatike

Davor Maček

MODEL ZA PROCJENU KRITIČNIH INFORMACIJSKIH SUSTAVA PRIMJENOM VIŠEKRITERIJSKOGA ODLUČIVANJA S ELEMENTIMA ZA ANALIZU I PROCJENU RIZIKA U FINANCIJSKIM INSTITUCIJAMA

DOKTORSKI RAD

Mentori:

Izv.prof.dr.sc. Ivan Magdalenić

Prof.dr.sc. Nina Begičević Ređep

Varaždin, 2021

University of Zagreb

Faculty of Organization and Informatics

Davor Maček

A MODEL FOR THE EVALUATION OF CRITICAL INFORMATION SYSTEMS USING MULTICRITERIA DECISION-MAKING WITH ELEMENTS FOR RISK ANALYSIS AND ASSESSMENT IN FINANCIAL INSTITUTIONS

DOCTORAL THESIS

Supervisors:

Ivan Magdalenić, Ph.D., associate professor

Nina Begičević Ređep, Ph.D., full professor

Varaždin, 2021

PODACI O DOKTORSKOM RADU

I. AUTOR

Ime i prezime	Davor Maček
Datum i mjesto rođenja	16. lipnja 1982., Zagreb
Naziv fakulteta i datum diplomiranja na VII/I stupnju	Fakultet organizacije i informatike, Varaždin, Sveučilište u Zagrebu, 09. ožujka 2007.
Naziv fakulteta i datum diplomiranja na VII/II stupnju	Fakultet organizacije i informatike, Varaždin, Sveučilište u Zagrebu, 01. ožujka 2011.
Sadašnje zaposlenje	UniCredit Services GmbH, Wien, Austrija

II. DOKTORSKI RAD

Naslov	Model za procjenu kritičnih informacijskih sustava primjenom višekriterijskoga odlučivanja s elementima za analizu i procjenu rizika u financijskim institucijama
Broj stranica, slika, tablica, priloga, bibliografskih podataka	163 stranice, 38 slika, 47 tablica, 10 priloga, 165 bibliografskih podataka
Znanstveno područje i polje iz kojeg je postignut akademski stupanj	Znanstveno područje društvenih znanosti, znanstveno polje informacijske i komunikacijske znanosti
Mentori i voditelji rada	Izv.prof.dr.sc. Ivan Magdalenić Prof.dr.sc. Nina Begičević Ređep
Oznaka i redni broj rada	162

III. OCJENA I OBRANA

Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena tema	21. srpnja 2020.
Datum predaje rada	10. lipnja 2021.
Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena pozitivna ocjena rada	21. listopada 2021.
Sastav povjerenstva koje je rad ocijenilo	Doc.dr.sc. Nikola Ivković, predsjednik Prof.dr.sc. Marin Golub, član Doc.dr.sc. Nikola Kadoić, član
Datum obrane doktorskog rada	15. studenoga 2021.
Sastav Povjerenstva pred kojim je rad obranjen	Doc.dr.sc. Nikola Ivković, predsjednik Prof.dr.sc. Marin Golub, član Doc.dr.sc. Nikola Kadoić, član
Datum promocije	

Informacije o mentorima

Izv. prof. dr. sc. Ivan Magdalenić rođen je 17. travnja 1977. godine u Čakovcu. Po završetku prirodoslovno-matematičke gimnazije 1995. godine upisuje diplomski studij na Fakultetu elektrotehnike i računarstva (FER) Sveučilišta u Zagrebu. Na FER-u je diplomirao 2000. godine na smjeru Telekomunikacije i informatika te magistrirao na istom fakultetu 2003. godine s temom "Elektronička razmjena poslovnih dokumenata". Od 2000. do 2004. godine radi kao znanstveni novak na FER-u, a od 2004. godine radi kao asistent na Fakultetu organizacije i informatike (FOI) Sveučilišta u Zagrebu. Doktorirao je na Fakultetu elektrotehnike i računarstva u znanstvenom polju Računarstvo s temom doktorske disertacije "Dinamičko generiranje ontološki podržanih usluga Weba za dohvat podataka". U znanstveno-nastavno zvanje docent izabran je 2012. godine, a u znanstveno-nastavno zvanje izvanredni profesor 2018. godine.

Područje znanstvenog istraživanja prof. Magdalenića uključuje automatsko i generativno programiranje, elektroničko poslovanje, semantički web i druge napredne web tehnologije. Ivan Magdalenić je autor sveučilišnog udžbenika, objavio je poglavlje u znanstvenoj knjizi te je autor brojnih radova objavljenih u znanstvenim časopisima te na međunarodnim konferencijama.

Ivan Magdalenić aktivno sudjeluje u znanstvenim i stručnim projektima uvođenja elektroničkog poslovanja u Republici Hrvatskoj. Obnašao je dužnost pročelnika Katedre za informatičke tehnologije i računarstvo na Fakultetu organizacije i informatike Sveučilišta u Zagrebu u razdoblju od 2013–2017. Na preddiplomskom, diplomskom i specijalističkom poslijediplomskom studiju Fakulteta organizacije i informatike nositelj je brojnih kolegija kao što su Arhitektura računalnih sustava, Mreže računala, Operacijski sustavi, Sigurnost operacijskih sustava, Sigurnost umreženih računalnih sustava, itd.

Dobitnik je nagrade za mladog znanstvenika na Fakultetu organizacije i informatike 2012. godine.

Prof. dr. sc. Nina Begičević Ređep je diplomirala na Fakultetu organizacije i informatike (FOI) Sveučilišta u Zagrebu 2003. godine te se iste godine i zapošljava na tom Fakultetu. Godine 2005. završava poslijediplomski znanstveni magistarski studij "Menadžment poslovnih sustava" na FOI-ju. Bila je stipendistica američke Vlade te joj je dodijeljena JFDP (Junior Faculty Development Program) stipendija za usavršavanje na University of Pittsburgh – Katz

Graduate School of Business, u okviru koje je pripremala doktorsku disertaciju. U prosincu 2008. godine brani doktorsku disertaciju pod nazivom "Višekriterijski modeli odlučivanja u strateškom planiranju uvođenja e-učenja".

U 2018. godini izabrana je u znanstveno zvanje znanstvenog savjetnika, a u 2020. godini u znanstveno-nastavno zvanje redovne profesorice. Obavljala je funkciju prodekanice za poslovanje u dva mandata, te prodekanice za znanost u dva mandata, a trenutno je dekanica Fakulteta organizacije i informatike.

Sudjelovala je kao voditeljica/suvoditeljica/suradnica na više od dvadeset domaćih i međunarodnih znanstvenih i stručnih projekata (Horizon 2020, INTERREG, Erasmus, HRZZ, Tempus, ESF, IPA, LLP, EUREKA i dr.). Trenutno vodi projekt Hrvatske zaklade za znanost pod nazivom "Podizanje zrelosti visokih učilišta za implementaciju analitika učenja – HELA", a sudjeluje i na projektu e-škole u okviru kojeg vodi tim za razvoj Okvira digitalne zrelosti škola kao i provođenje vrednovanja digitalne zrelosti škola.

Predaje predmete Poslovno odlučivanje, Analiza poslovnih odluka te Teorija odlučivanja. Projektno te znanstveno-istraživački bavi se poslovnim odlučivanjem, višekriterijskim odlučivanjem, edukacijskim tehnologijama, e-učenjem te digitalnom transformacijom u području obrazovanja.

U 2018. godini osnovala je Laboratorij za strateško planiranje i odlučivanje čija je voditeljica.

Voditeljica je i suvoditeljica više radionica i stručnih usavršavanja s fokusom na strateško planiranje i odlučivanje o uvođenju IKT-a u obrazovanje.

Suautorica je sveučilišnog udžbenika Poslovno odlučivanje, više poglavlja knjiga te monografija te je autorica više od 70 znanstvenih članaka.

U uredništvu je više međunarodnih časopisa (IJAHP, JIOS, CrORR) te programskom odboru konferencija SYMORG, CECIIS, MIPRO, EDT, IFIP DSS. Članica je Hrvatskog društva za operacijska istraživanja. Također je članica U.S. Alumnia i U.S. Affiliates Community-ja.

Sažetak

Financijske institucije, posebno banke, izrazito su važne za stabilnost i funkcioniranje gospodarstva svake zemlje, ali i cjelokupne svjetske ekonomije. Problemi u poslovanju neke od banaka, pogotovo onih sistemski važnih, mogu imati značajne posljedice po funkcioniranje kako nacionalnih tako i svjetske ekonomije. Neki od gorućih problema s kojima se banke danas suočavaju jesu učestali kibernetički napadi na njihovu infrastrukturu i informacijske sustave te ozbiljne posljedice koje takvi napadu uzrokuju. S obzirom kako se današnje poslovanje banaka gotovo u potpunosti oslanja na komunikaciju preko interneta sa drugim poslovnim entitetima, tako su banke sve izloženije brojnim sigurnosnim prijetnjama i neizostavnim rizicima.

Zbog nedostatka svih relevantnih informacija te vremenskih i ostalih resursnih ograničenja, često nije moguće prikupiti i obraditi sve neophodne informacije o nekom informacijskom sustavu kako bi se isti moglo adekvatno procijeniti u prihvatljivom roku, a što organizaciju stavlja u stanje povećanog sigurnosnog rizika. Proučavanjem relevantne literature te postojećih modela i tehnika koji se koriste u praksi, utvrđeno je kako ne postoji rješenje za navedeni problem višekriterijskog odlučivanja u uvjetima rizika u domeni informacijske sigurnosti za kritične poslovne IT sustave.

Tako je predložen model za učinkovitije donošenje informirane odluke o stanju sigurnosti nekog kritičnog informacijskog sustava odabirom odgovarajućeg IT rješenja. Model je razvijen primjenom istraživačke metodologije znanstvenog dizajna (eng. *Design Science Research Methodology*, DSRM) koja se koristi u inženjerstvu i informacijskim znanostima u svrhu izrade odgovarajućih artefakta. Pri tome su se najznačajniji elementi za analizu i procjenu rizika informacijske sigurnosti integrirali u višekriterijski model odlučivanja. Generički elementi za analizu i procjenu rizika korišteni su kao evaluacijski kriteriji u višekriterijskom modelu u svrhu procjene, rangiranja i odabira kritičnih poslovnih informacijskih sustava. Glavni znanstveni doprinos višekriterijskog modela uz omogućavanje učinkovitijeg donošenja odluke o stanju sigurnosti kritičnih IT sustava očituje se i u tome da omogućava organizaciji kvalitetniju reakciju na brojne sigurnosne prijetnje i rizike. Dodatni doprinos postignut je i u sistematizaciji znanja i koncepata o metodama za višekriterijsko odlučivanje pogodnih za primjenu u domeni informacijske sigurnosti zajedno sa metodama za analizu i procjenu rizika.

Ključne riječi: Informacijska sigurnost, procjena rizika, višekriterijsko odlučivanje, kritični IT sustavi, financijske institucije, sustavni pregled literature, utjecaji, zavisnosti, hibridni model

Extended abstract

Financial institutions, peculiarly banks, are extremely important for the stability and functioning of the economy of each country, but also of the entire global economy. Problems in the operations of some banks, especially those of systemic importance, can have significant consequences for the functioning of both, the national and world economies. Some of the vital problems that the banks face today are frequent cyber attacks on their infrastructure and information systems, and the serious consequences caused by such attacks. Given that today's banking business relies heavily on Internet communication with other business entities, banks are increasingly exposed to numerous security threats and imminent risks.

Due to the lack of all relevant information and time and other resource constraints, it is often not possible to collect and process all the necessary information about an information system so that it can be adequately evaluated within an acceptable timeframe, which puts the organization into a state of increased security risk. So, one of the research questions defined was how to enable more efficient (in terms of cost and time) decision-making on the security status and selection of appropriate critical information systems in a financial institution?

By studying the relevant literature and the existing models and techniques used in practice, it was found that there is no solution to the stated problem of multicriteria decision-making in conditions of risk in the domain of information security for business critical IT systems. Thus, a model was proposed for more efficient decision-making on the security status of a critical information system by selecting the appropriate IT solution. The model was developed using the *Design Science Research Methodology* (DSRM).

In order to create a new model, first, it was necessary to conduct a systematic literature review (SLR) of papers on the applicability of multicriteria decision-making (MCDM) methods in a domain of information security risk assessment. Such SLR was conducted with very rigorous inclusion and exclusion criteria. By discovering which MCDM methods are suitable for creation of a new model, it was necessary to conduct the next research phase in order to identify all the information security risk assessment (ISRA) criteria that are relevant for integration into a new hybrid MCDM model. The *Delphi* technique was used to conduct the research by examining relevant information security experts from various financial institutions. Upon receipt of appropriate feedback on ISRA criteria, it was necessary to conduct another research in order to discover mutual influences and dependencies between those ISRA elements. That was one of the crucial research phases in order to get criteria weights of ISRA

elements. So, the most important elements for the analysis and assessment of information security risks were integrated into adequate methods for multicriteria decision-making. Generic criteria for risk analysis and assessment were used as evaluation criteria in the new multicriteria model for the purpose of evaluation, ranking and selection of critical business information systems. The model was validated in relevant case studies. By confirming hypotheses, the main goal of the research, i.e. making an informed decision on the security status of critical information systems in a financial institution and increasing the efficiency and quality of the assessment process and selection of such systems, was successfully achieved.

Keywords: Information security, risk assessment, multicriteria decision-making, critical IT systems, financial institutions, influences, dependencies, systematic literature review (SLR), hybrid model

"Lovely Jubbly!"

-- Delboy Trotter, *Only Fools and Horses*

"*Ako kaniš pobijediti, ne smiješ izgubiti*"

-- Broj Jedan, strip Alan Ford

"*Bilo je i većih problema pa ih nismo riješili*"

-- Grunf, strip Alan Ford

Mojoj obitelji

Sadržaj

Popis slika

Popis tablica

Popis kratica

AHP	Analitički hijerarhijski proces (eng. *Analytic Hierarchy Process*)
ALE	Očekivani godišnji gubitak (eng. *Annual Loss Expectancy*)
ANP	Analitički mrežni proces (eng. *Analytic Network Process*)
APT	Stalna napredna prijetnja (eng. *Advanced Persistent Threat*)
ARO	Godišnja vjerojatnost pojave negativnog događaja (eng. *Annualized Rate of Occurrence*)
AV	Vrijednost imovine (eng. *Asset Value*)
BN	Bayesove mreže (eng. *Bayesian networks*)
BCM	Upravljanje neprekidnošću poslovanja (eng. *Business Continuity Management*)
BIA	Analiza utjecaja na poslovanje (eng. *Business Impact Analysis*)
CBA	Analiza isplativosti (eng. *Cost-Benefit Analysis*)
CC	eng. *Common Criteria for Information Technology Security Evaluation*
CIA	Povjerljivost, cjelovitost, dostupnost (eng. *Confidentiality, Integrity, Availability*)
COSO	Odbor sponzorskih organizacija Povjerenstva Treadway (eng. *Committee of Sponsoring Organizations of the Treadway Commission*)
CR	Omjer konzistentnosti (eng. *Consistency Ratio*)
CSA	Savez za sigurnost u oblaku (eng. *Cloud Security Alliance*)
DEMATEL	Laboratorij za ispitivanje i ocjenjivanje donošenja odluka (eng. *DEcision MAking Trial and Evaluation Laboratory*)
DS	Znanstveni dizajn (eng. *Design Science*)
DSRM	Istraživačka metodologija znanstvenog dizajna (eng. *Design Science Research Methodology*)
EF	Faktor izloženosti (eng. *Exposure Factor*)
ELECTRE	eng. *ELimination Et Choice Translating REality*
ENISA	Europska agencija za mrežnu i informacijsku sigurnost (eng. *European Network and Information Security Agency*)
FAHP	Neizraziti analitički hijerarhijski proces (eng. *Fuzzy Analytic Hierarchy Process*)
FEDS	Okvir za evaluaciju u istraživanju znanosti o dizajnu (eng. *Framework for Evaluation in Design Science Research*)
FOS	Sustav za podršku platnih usluga klijentima (eng. *Front Office Payment System*)

FTE	Ekvivalent punog radnog vremena (eng. *Full-time equivalent*)
GDPR	Opća uredba o zaštiti osobnih podataka (eng. *General Data Protection Regulation*)
IOT	Internet stvari (eng. *Internet of Things*)
ISMS	Sustav upravljanja informacijskom sigurnošću (eng. *Information Security Management System*)
ISO	Međunarodna organizacija za standardizaciju (eng. *International Organization for Standardization*)
ISRA	Procjena rizika informacijske sigurnosti (eng. *Information Security Risk Assessment*)
ISRM	Upravljanje rizicima informacijske sigurnosti (eng. *Information Security Risk Management*)
IT	Informacijska tehnologija (eng. *Information technology*)
MADM	Višeatributno odlučivanje (eng. *Multi-attribute Decision Making*)
MCDA	Višekriterijska analiza (eng. *Multiple-criteria Decision Analysis*)
MCDM	Višekriterijsko odlučivanje (eng. *Multicriteria Decision Making*)
NIST	Nacionalni institut za standarde i tehnologiju (eng. *National Institute of Standards and Technology*)
NRM	Mapa mrežnih odnosa (eng. *Network relations map*)
OCTAVE	eng. *Operationally Critical Threat, Asset, and Vulnerability Evaluation*
OWASP	Otvoreni projekt sigurnosti web aplikacija (eng. *Open Web Application Security Project*)
PCI DSS	Standard zaštite podataka industrije platnih kartica (eng. *Payment Card Industry Data Security Standard*)
POS	Prodajno mjesto (eng. *Point of Sale*)
PROMETHEE	eng. *Preference Ranking Organization METHod for Enrichment of Evaluations*
RM	Upravljanje rizicima (eng. *Risk Management*)
SANS	Administrator sustava, revizija, umrežavanje i sigurnost (eng. *SysAdmin, Audit, Networking, and Security*)
SDLC	Životni ciklus razvoja sustava (eng. *Systems Development Life Cycle*)
SEPA	Jedinstveno područje plaćanja u eurima (eng. *Single Euro Payments Area*)
SLE	Očekivani pojedinačni gubitak (eng. *Single Loss Expectancy*)
SLR	Sustavni pregled literature (eng. *Systematic Literature Review*)

SMART	Posebno, mjerljivo, ostvarivo, bitno, vremenski ovisno (eng. *Specific*, *Measurable*, *Attainable*, *Relevant*, *Time-dependent*)
SNAP	Analitički proces socijalne mreže (eng. *Social Network Analytic Process*)
SQLi	SQL ubacivanje (eng. *SQL injection*)
SV	Vrijednost sigurnosne protumjere (eng. *Safeguard Value*)
SWIFT	Udruženje za svjetske međubankarske financijske telekomunikacije (eng. *Society for Worldwide Interbank Financial Telecommunication*)
TFN	Trosložni neizraziti broj (eng. *Triangular Fuzzy Number*)
TOE	Cilj procjene (eng. *Target of Evaluation*)
TOPSIS	Tehnika za redoslijed preferencija po sličnosti prema idealnom rješenju (eng. *Technique for Order of Preference by Similarity to Ideal Solution*)
VIKOR	*VIseKriterijumska Optimizacija I Kompromisno Rešenje*
XSS	Unakrsno skriptiranje (eng. *Cross-site scripting*)

1. Uvod

Financijske institucije, posebno banke, izrazito su važne za stabilnost i funkcioniranje gospodarstva gotovo svake zemlje, ali i cjelokupne svjetske ekonomije. Problemi u poslovanju neke od banaka, pogotovo onih sistemski važnih [1, 2], mogu imati značajne posljedice po funkcioniranje kako nacionalnih tako i svjetske ekonomije [3], ovisno o veličini i stupnju značaja pojedine banke u financijskom okruženju. Neki od gorućih problema s kojima se banke danas suočavaju jesu napadi na njihovu infrastrukturu i informacijske sustave te ozbiljne posljedice koje takvi napadu uzrokuju [4, 5, 6, 7], poput WannaCry i Petya napada [8, 9, 58], proboj u informacijski sustav tvrtke Equifax [10], pojava kritičnih Spectre/Meltdown ranjivosti [11] koje razni napadi pokušavaju iskoristiti, zatim uspješno ostvaren napad na SWIFT bankarsku mrežu [52] koji se svakako smatra dijelom kritične infrastrukture vezano uz međubankarska plaćanja, itd. Prema Međunarodnom monetarnom fondu [148], rizik kibernetičkog napada prepoznat je kao najznačajnija vrsta rizika u financijskom sektoru.

S obzirom kako se današnje poslovanje banaka uvelike oslanja na tzv. direktne kanale (internet i mobilno bankarstvo, elektronička trgovina i bankomatska mreža) i ostalu komunikaciju preko interneta s drugim poslovnim entitetima (npr. Reuters, Bloomberg, burza, centralna banka, POS[1] sustavi, itd.), tako su banke sve izloženije brojnim sigurnosnim prijetnjama i neizostavnim rizicima. Procjena i upravljanje IT sigurnosnim rizicima predstavlja kritičan proces, tj. skup povezanih aktivnosti za kontrolu i ovladavanje rizicima po informacijski sustav, a osnovni cilj tog procesa je da se rizici svedu na prihvatljivu razinu [12], [13], ovisno o razini apetita za rizik koji je menadžment organizacije spreman prihvatiti [14]. Upravo je zadatak sigurnosnih stručnjaka da omoguće poslovanje organizacije u takvim uvjetima neizvjesnosti odnosno rizika.

Jedan od temeljnih načina za adekvatno upravljanje rizicima jest odgovarajuća procjena i odabir prikladnog IT rješenja u svrhu zadovoljenja prvenstveno poslovnih, ali nužno i brojnih regulatornih te sigurnosnih zahtjeva. No, donošenje odluke o stanju sigurnosti i odabiru prikladnog IT rješenja u organizaciji je složen, dugotrajan i troškovno zahtjevan proces. Zbog brzo rastućeg trenda povećanja broja sigurnosnih prijetnji i novotkrivenih ranjivosti te vrlo često nedovoljne količine vremena i resursa u organizacijama kako bi se učinkovito odgovorilo na rizike koji se javljaju po informacijske sustave, adresiranje onih najkritičnijih rizika te

[1] *Point of Sale (POS)* terminal – Uređaj namijenjen elektroničkom plaćanju roba i usluga putem bankovne kartice na prodajnim mjestima.

posljedično procjena sigurnosnih protumjera, kontrola i/ili kritičnih IT sustava postaje suštinski problem. Tako se ovo istraživanje bavi načinom odlučivanja i rješavanja problema informacijske sigurnosti u uvjetima rizika u domeni kritičnih informacijskih sustava u financijskoj instituciji.

Ovaj rad organiziran je na način da slijedi korake znanstvenog dizajna (eng. *Design Science,* DS) [15, 16], istraživačkoj paradigmi koja je korištena prilikom provođenja istraživanja:

- Uočavanje problema i motivacija
- Predstavljanje područja istraživanja
- Definiranje ciljeva i istraživačkih pitanja, hipoteza i metrika te predstavljanje metodologije istraživanja i istraživačkih metoda
- Izrada baze znanja
- Dizajn i razvoj modela
- Demonstracija modela, tj. prikaz rješenja
- Vrednovanje
- Zaključak i komunikacija.

Kroz korake metodologije znanstvenog dizajna opisane su i sve znanstvene metode korištene u istraživačkom procesu.

2. Uočavanje problema i motivacija

Glavni cilj informacijske sigurnosti i svih donositelja poslovnih odluka u domeni informacijske sigurnosti je zaštita organizacije i sposobnost zaštite pripadajuće IT imovine, kao i osiguranje povjerljivosti (eng. *confidentiality*), cjelovitosti (eng. *integrity*) i dostupnosti (eng. *availability*) informacija i informacijskih sustava koji takve informacije dohvaćaju, obrađuju, pohranjuju i distribuiraju te osiguranje odgovornosti (eng. *accountability*) za resurse organizacije [17].

Poslovno odlučivanje dosta često predstavlja vrlo složen i dinamičan kognitivni proces koji u pravilu zahtijeva značajno vrijeme u kojemu je nužno izabrati između dvije ili više alternativa sa svrhom kako bi se najbolja alternativa sprovela i nastojao riješiti određeni problem. Odluka zapravo predstavlja krajnji rezultat procesa odlučivanja. Prema [18], vrste odluka s obzirom na važnost odnosno značenje odluka za neku organizaciju mogu se podijeliti na strateške, taktičke i operativne odluke, ovisno o razini menadžmenta u organizaciji koji je zadužen za donošenje odluka na temelju raspoloživih informacija.

Slika 2.1: Vrste odluka prema razinama menadžmenta [18]

Na Slici 2.1 prikazane su vrste odluka koje se donose ovisno o pojedinim razinama menadžmenta koji je odgovoran za donošenje istih. Operativne i rutinske (dnevne) odluke donosi najniža razina rukovodstva, dok najviša razina menadžmenta odlučuje o strateškim pitanjima u organizaciji.

Tablica 2.1: Obilježja odluka [18]

Vrste odluka / Obilježja odluka	Vrijeme	Priroda rizika	Strukturiranost	Kontrola
Strateške	dugoročne	visok	slabo definirane	iskustvena
Taktičke	srednje	umjeren	promjenjive	kvalitativna
Operativne	kratkoročne	nizak	dobro definirane	kvantitativna

Iz Tablice 2.1 mogu se vidjeti razlike prema najznačajnijim elementima između strateških, taktičkih i operativnih vrsta odluka.

Holistička zaštita informacijskog sustava odabirom adekvatnog IT rješenja može se prema svojim značajkama smatrati strateškom odlukom čije karakteristike su sljedeće:

- Značajnost: strateške odluke su svakako najvažnije odluke u organizaciji. Takvim odlukama se određuju strategija i ciljevi organizacije u budućnosti. Također, strateške odluke definiraju okvir unutar kojeg se moraju donositi taktičke odluke. Npr., promjena centralnog bankovnog sustava (eng. *core banking system*) unutar organizacije je strateška odluka koja implicira mnoge druge promjene na taktičkoj i operativnoj razini, uključujući moguće promjene poslovnih procesa, kao i sigurnosne aspekte te troškove.
- Dugoročnost: strateška odluka odnosi se na dugoročno razdoblje, uglavnom minimalno dvije, a ponekad pet ili više godina za neki IT sustav (pogotovo kritični).
- Složenost: strateške odluke su složene, obuhvaćaju veliki broj faktora koji se mogu izražavati kroz brojne kvantitativne i kvalitativne pokazatelje.
- Nesigurnost/rizik: strateške odluke su nesigurne i rizične jer njihov konačan rezultat ovisi o velikom broju faktora i događaja nad kojima ne postoji dovoljna razina kontrole. Pogrešna strateška odluka o nekom IT sustavu može imati dalekosežne i često negativne posljedice po organizaciju zbog čega se i postavlja velika odgovornost za donositelje takve vrste odluka.
- Resursna zahtjevnost: vrijeme, ljudi, novac, informacije i tehnologija su potrebni kako bi se moglo procijeniti i odabrati odgovarajući IT sustav u svrhu zadovoljenja određenih poslovnih ciljeva koji proizlaze kao rezultat strateške odluke.

Iz navedenih karakteristika strateškog odlučivanja proizlazi kako donošenje takvih vrsta odluka nikako nije jednostavno pa su stoga potrebne odgovarajuće metode i tehnike za modeliranje svih komponenti odlučivanja kako bi se odabrala najbolja alternativa s obzirom na definirani cilj.

Različiti čimbenici poput ljudskog faktora, organizacijske kulture, obrazovanja i tehnologije utječu i dodaju razinu složenosti u procese informacijske sigurnosti te posljedično i donošenje odluka. Rizici informacijske sigurnosti mogu se pojaviti u obliku tehničkog kvara, sistemskih ili aplikativnih ranjivosti, ljudske greške, prijevare ili vanjskog događaja. Tako razvoj i implementacija odgovarajućih sustava informacijske sigurnosti za zaštitu

povjerljivosti, cjelovitosti i dostupnosti informacijske imovine postaje ujedno i strateški cilj svake organizacije [19]. Stručnjaci za informacijsku sigurnost zapravo potiču svoje organizacije na provođenje procesa procjene rizika informacijske sigurnosti (eng. *Information Security Risk Assessment*, ISRA) kako bi se zaštitila imovina organizacije te pomoglo u ostvarenju poslovnih ciljeva [20]. Zbog velike složenosti u današnjim organizacijama, pogotovo velikim korporacijama poput financijskih institucija, analiza rizika je postao među-funkcionalni (eng. *cross-functional*) proces odlučivanja koji zahtijeva izrazito mnogo resursa (prvenstveno ljudi i vremena) iz raznih organizacijskih jedinica. Tako se prema [24] ujedno i sam postupak procjene rizika informacijske sigurnosti smatra složenim i višekriterijskim sustavom evaluacije.

Glavni motiv za ovo istraživanje pronađen je u praksi na temelju uočenog problema nepostojanja resursno učinkovite (troškovno i vremenski) metode odnosno modela za procjenu kritičnih informacijskih sustava u financijskoj instituciji kako bi se kvalitetnije postupalo sa sigurnosnim prijetnjama i rizicima po sam informacijski sustav te omogućilo donošenje odgovarajuće (informirane) odluke o stanju sigurnosti promatranog IT sustava (i posljedično odabiru adekvatnog rješenja), a što je uočeno i u nekim dosadašnjim istraživanjima [21], [22], [23], [24].

Iako postoji relativno značajan broj relevantnih znanstvenih radova i stručnih publikacija o prijetnjama, ranjivostima i povezanim rizicima u domeni višekriterijskog odlučivanja, ipak još uvijek ne postoji model temeljen na znanstvenim osnovama za procjenu i rangiranje kritičnih informacijskih sustava. Temeljem analize literature, uočeno je kako postoji niz znanstvenih radova na temu informacijske sigurnosti, međutim nije pronađen rad u kojemu je predstavljen model za procjenu, rangiranje i odabir kritičnih IT sustava primjenom višekriterijskog odlučivanja s generičkim kriterijima za analizu i procjenu rizika.

Prilikom odabira i uvođenja novih ili nadogradnje postojećih poslovnih rješenja ili sustava nužno je voditi posebnu brigu oko njihovih sigurnosnih značajki i sigurnosnih kontrola kako se rizik po informacijski sustav i cjelokupnu organizaciju ne bi povećao uslijed implementacije ili održavanja IT sustava. To je bitno kako zbog učinkovitog operativnog upravljanja novim sustavom tako i zbog činjenice da se novim sustavom ili rješenjem povećava složenost postojećeg informacijskog sustava, a time potencijalno povećava i sigurnosni rizik [25]. Tako je zadatak sigurnosnih stručnjaka analizirati, procijeniti i rangirati rizike koje novi sustav ili rješenje mogu imati na postojeći informacijski sustav organizacije te odabrati primjerene kontrole zaštite IS-a ili predložiti neko drugo rješenje (alternativu) za smanjenje sigurnosnih rizika. No, kako bi se donijelo ispravnu odluku potrebno je znati svrhu odnosno kontekst određenog sustava ili aplikacije te detalje o promatranom sustavu da bi se isti moglo

evaluirati, a to je vrlo teško kako zbog nedostatka svih relevantnih informacija tako i zbog vremenskog i resursnog ograničenja kako bi se neophodne informacije prikupilo i obradilo u prihvatljivom roku. S obzirom kako postoji jako mnogo elemenata koji utječu na donošenje konačne odluke o nekom IT rješenju pri čemu vremenska i resursna ograničenja postaju ključni izazovi, tako možemo reći da je zapravo prepoznat i identificiran složeni problem višekriterijskog odlučivanja u uvjetima rizika u domeni informacijske sigurnosti.

Motivacija za daljnje istraživanje područja upravljanja rizicima informacijske sigurnosti primjenom metoda višekriterijskog odlučivanja proizlazi iz činjenice kako istraživač, kao zaposlenik financijske institucije u kojoj je zadužen za procjenu rizika i evaluaciju sigurnosnih IT rješenja te predlaganje odgovarajućih mjera zaštite, želi dodatno produbiti saznanja o navedenim područjima te otkriti mogućnosti za učinkovitije donošenje prikladne (informirane) odluke o nekom kritičnom informacijskom sustavu uz nužno smanjenje rizika po organizaciju. Analiza specifičnih problema vezano uz odabir određenog sigurnosnog IT rješenja, kritičnog elementa informacijskog sustava ili specifičnog sklopovskog modula u uvjetima rizika dovodi do potrebe za učinkovitijim načinom rješavanja takvih problema, tj. nekim generičkim višekriterijskim modelom.

3. Područja istraživanja

Ovo poglavlje predstavit će područja znanstvenog istraživanja koje je interdisciplinarno i od intrinzičnog interesa za istraživača pa tako obuhvaća upravljanje sigurnošću i rizike informacijske sigurnosti, višekriterijsko (višeatributno) odlučivanje te kritične poslovne informacijske sustave.

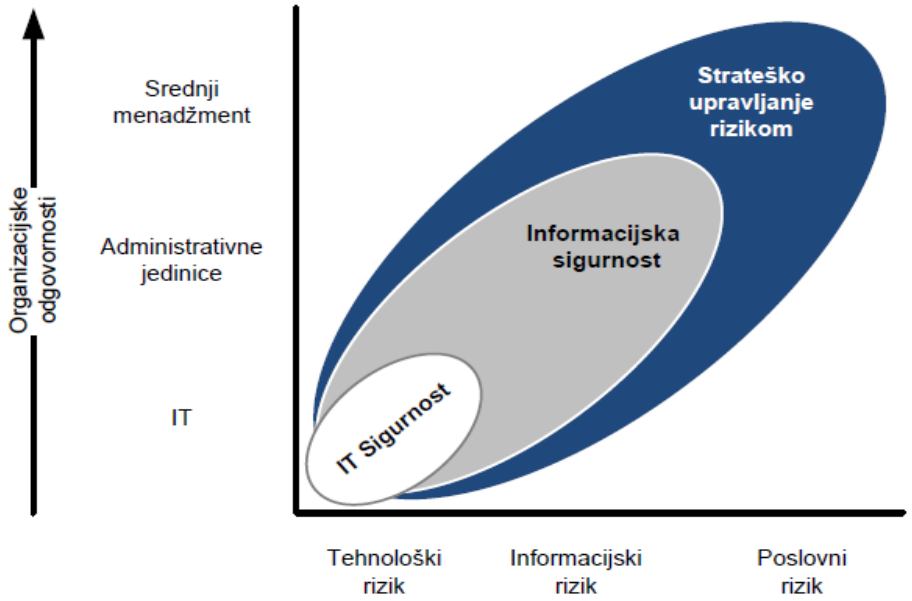
Slika 3.1: Područja obuhvaćena istraživanjem

Na Slici 3.1 prikazane su glavne domene odnosno područja obuhvaćena istraživanjem. U dijelu presjeka djelovanja tih područja smješten je uočeni istraživački problem za koji je potrebno dati odgovarajući prijedlog rješenja.

3.1. Rizici informacijske sigurnosti

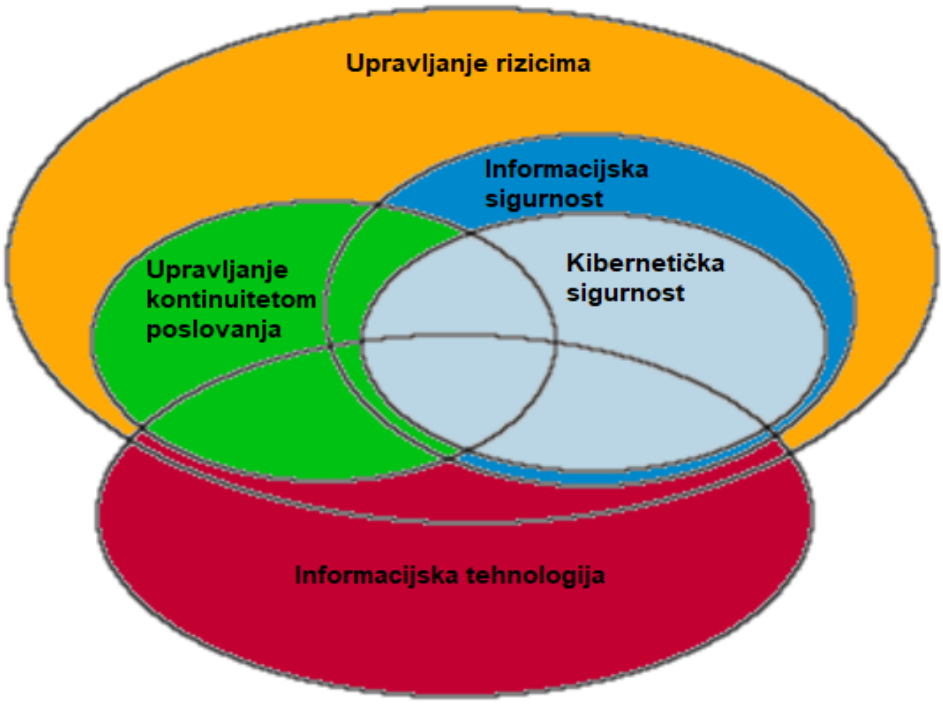
Rizici imaju različite dimenzije i učinke s mogućnošću pojavljivanja na različitim razinama i zahtijevaju vlastite specifične preventivne mjere na bilo kojoj razini [49]. Postoji mnoštvo različitih rizika u poslovnom sustavu, npr. zakonodavni, regulatorni, financijski, reputacijski, itd. Ali, kada se radi o slučaju ugrožavanja sigurnosti informacija, koje se smatra najvažnijom imovinom svake organizacije, tada se radi o rizicima informacijske sigurnosti. IT rizici su sastavni dio svake kategorije poslovnih rizika, a poslovne odluke ne mogu se donositi bez odgovarajućih informacija pri čemu izvori informacija o nekom poslovnom sustavu dolaze iz informacijskog sustava sa strukturiranim bazama podataka. Jedan od najvažnijih procesa u svakoj organizaciji vezano uz upravljanje informacijskom sigurnošću, a s obzirom na organizacijske zahtjeve i ciljeve, odnosi se na upravljanje sigurnosnim rizicima. S obzirom kako su informacijski sustavi temeljeni na IT podršci te da zapravo svi kritični poslovni procesi u bankama danas u potpunosti ovise o IT infrastrukturi, tako područje IT-a predstavlja uistinu veliki rizik za svaku organizaciju, a posebno banke. Jedan od takvih rizika je svakako evaluacija

i odabir adekvatnog IT rješenja u domeni kritičnih poslovnih informacijskih i sigurnosnih sustava za financijsku instituciju u uvjetima resursnog ograničenja, a što podrazumijeva prvenstveno vrijeme, kvalificirane stručnjake, relevantne informacije, tehnologiju i budžet.



Slika 3.2: Položaj IT rizika u ukupnom upravljanju rizicima poslovnog sustava [33]

Sa Slike 3.2 može se vidjeti položaj tehnoloških i informacijskih rizika u ukupnom (strateškom) upravljanju rizicima nekog poslovnog sustava.



Slika 3.3: Upravljanje rizicima i sigurnosne IT domene [156]

Dodatno, Slika 3.3 prikazuje široko područje kritičnog procesa upravljanja rizicima kao i pojedine sigurnosne IT domene obuhvaćene tim procesom. Pri tome treba napomenuti kako se kibernetička sigurnost i informacijska sigurnost u praksi koriste za opis procesa vezano uz zaštitu od gubitka, neovlaštene promjene i nedostupnost podataka i informacija. No, razlika je u tome što se kibernetička sigurnost odnosi samo na računalno (digitalno) područje, dok je domena informacijske sigurnosti šira te obuhvaća područja i fizičke i računalne sigurnosti.

Među najznačajnijim rizicima kojima su danas banke izložene su IT operativni rizici koji nastaju zbog neadekvatno uspostavljenih internih procesa, ljudi i sustava, ili zbog negativnih vanjskih događaja [30], npr. elementarna nepogoda ili računalni napad na resurse. IT operativni rizici su vrlo bitni zbog činjenice kako u određenim slučajevima njihovog ostvarenja takvi rizici mogu utjecati na pojavu drugih rizika poput pravnog, regulatornog (financijskog) i izrazito značajnog reputacijskog rizika, jer reputacija je ključna imovina za svaku tvrtku čiji su poslovni odnosi, kao kod banaka, zasnovani na povjerenju [31]. Primijećen je trend u povećanju broja sigurnosnih prijetnji i kibernetičkih napada na financijske institucije, gdje prema istraživanjima [32] proboj u informacijske sustave trenutno predstavlja vrlo značajnu prijetnju po organizacije, od čega je čak 86% takvih proboja financijski motivirano, što je posebno značajno upravo za bankarski sektor koji je izložen stalnim naprednim prijetnjama (eng. *advanced persistent threat*, APT). Dodatno, broj ICT sigurnosnih prijetnji i kibernetičkih napada je značajno povećan i tijekom COVID-19 pandemije [149, 150].

Prema smjernicama za implementaciju sustava za upravljanje informacijskom sigurnošću (eng. *Information Security Management System*, ISMS) [26], samo planiranje ISMS-a sastoji se od 5 faza: definiranje opsega, analiza nedostataka (eng. *gap analysis*), provođenje procesa procjene rizika (eng. *risk assessment*), definiranje kontrola i ciljeva te određivanje politike i procedure za ISMS. Upravo se faza procjene rizika smatra najvažnijom i najkritičnijom.

Postoji više definicija rizika iz različitih izora:

- ISO Guide 73:2009: Rizik je kombinacija vjerojatnosti pojave nekog događaja te posljedica koju takav događaj može izazvati [34].
- ISO Guide 73:2009: Rizik predstavlja neizvjesnost za postizanje ciljeva [34].
- AS/NZS 4360:2004: Rizik je šansa da će se dogoditi nešto što će imati utjecaj na ciljeve [35].
- COSO Enterprise Risk Management Framework: Rizik je mogućnost da će se događaj pojaviti i utjecati na ostvarenje strategije i poslovnih ciljeva [37].

- ISO/IEC 27005:2018: Rizik je kombinacija posljedice koja proizlazi iz pojave neželjenog događaja i vjerojatnosti pojave takvog događaja [28].
- NIST SP 800-30: Rizik je mjera u kojoj je subjekt ugrožen potencijalnom okolnošću ili događajem, te je obično funkcija: (*i*) nepovoljnih utjecaja koji bi nastali ako se ta okolnost ili događaj dogodi; i (*ii*) vjerojatnosti pojave. Rizici informacijske sigurnosti su oni rizici koji proizlaze iz gubitka povjerljivosti, cjelovitosti ili dostupnosti informacija ili informacijskih sustava i odražavaju potencijalne negativne učinke na organizacijske operacije (tj. misiju, funkcije, ugled ili reputaciju), imovinu organizacije, pojedince, druge organizacije i naciju [13].

Vidljivo je kako su sve definicije rizika relativno jednostavne i međusobno slične, a razlika je uglavnom u interpretaciji. S obzirom kako postoji više definicija rizika, tako postoji i više definicija vezano za upravljanje rizicima:

- NIST SP 800-39: Upravljanje rizikom je složena višestruka aktivnost koja zahtijeva uključenost cijele organizacije – od viših rukovoditelja koji osiguravaju stratešku viziju i ciljeve najviše razine za organizaciju; do rukovoditelja srednje razine koji planiraju izvršavaju i upravljaju projektima; pa do pojedinaca na operativnoj razini koji upravljaju informacijskim sustavom koji podržava misiju i poslovne funkcije organizacije. Upravljanje rizikom je sveobuhvatan proces koji zahtijeva od organizacije: (*i*) formuliranje rizika (tj. da se utvrdi kontekst za odluke temeljene na riziku); (*ii*) procjenu rizika; (*iii*) odgovor na na rizik kad se isti utvrdi; te (*iv*) kontinuirani nadzor rizika. Upravljanje rizicima provodi se kao holistička aktivnost na razini cijele organizacije koja se bavi rizikom od strateške do taktičke razine, osiguravajući da je donošenje odluka temeljeno na riziku integrirano u svako stajalište organizacije [36].
- COSO Enterprise Risk Management Framework: Upravljanje rizikom poslovanja je proces koji provodi upravni odbor subjekta, rukovodstvo i drugo osoblje, koji se primjenjuje u postavljanju strategije i na razini cijelog poduzeća, a koji je dizajniran za identifikaciju potencijalnih događaja koji mogu utjecati na subjekt te da upravljanje rizikom bude u okviru svoje sklonosti riziku (eng. *risk appetite*), kako bi se pružilo razumno jamstvo vezano uz postizanje ciljeva subjekta [37].
- NIST SP 800-37 Risk Management Framework (RMF): Upravljanje rizikom je holistička akvitnost koja utječe na svaki aspekt organizacije, uključujući aktivnosti misije i poslovnog planiranja, arhitekturu poslovnog sustava, SDLC (Systems

development life cycle) procese i aktivnosti inženjeringa sustava koji su sastavni dio procesa životnog ciklusa sustava [39].

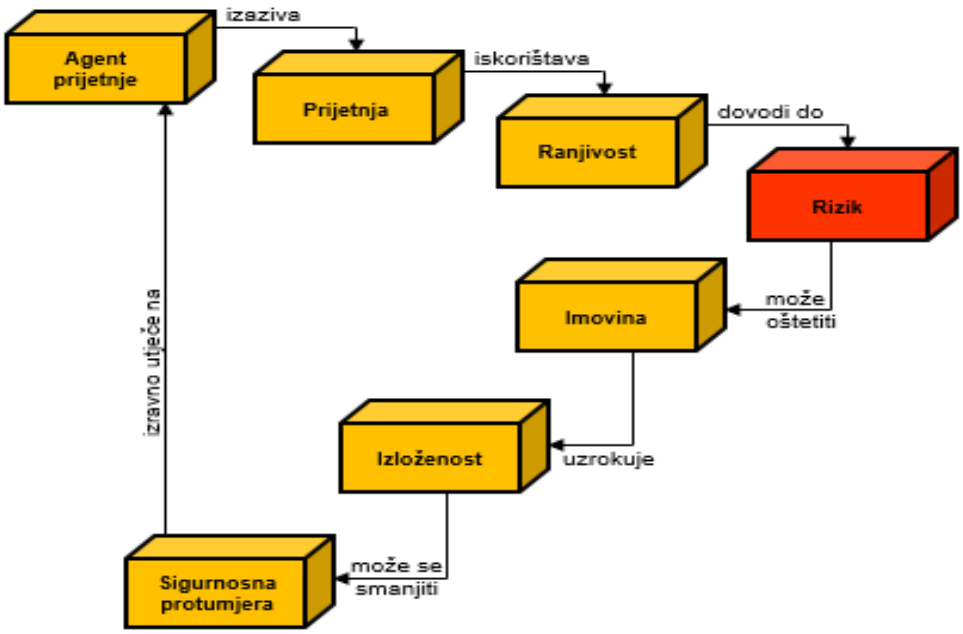
- ISO/IEC 27005:2018: Upravljanje rizicima informacijske sigurnosti treba biti integralni dio svih aktivnosti vezano u upravljanje informacijskom sigurnošću te se treba primijeniti na implementaciju i tekuće operacije ISMS-a. Upravljanje rizicima informacijske sigurnosti treba biti kontinuirani proces tijekom kojeg je uspostavljen kontekst, procijenjeni su rizici te da se s rizicima postupa na temelju plana za tretman rizika kako bi se implementiralo preporuke i odluke. Upravljanje rizicima analizira što se može dogoditi i koje su moguće posljedice, prije donošenja odluke što i kada je potrebno napraviti, kako bi se smanjilo rizik na prihvatljivu razinu [28].
- NIST SP 800-30: Upravljanje rizicima je proces identifikacije rizika, procjene rizika i poduzimanja radnji za smanjenje rizika na prihvatljivu razinu [13].
- ISO 31000:2018: Upravljanje rizikom predstavlja koordinirani skup aktivnosti za usmjeravanje i nadzor organizacije s obzirom na rizik [38].

Dodatno, treba naglasiti kako ISO 31000:2018 definira 5 temeljnih principa za upravljanje rizicima:

- Srazmjerno (eng. *Proportionate*): Aktivnosti upravljanja rizicima moraju biti proporcionalne razini rizika s kojima se suočava organizacija.
- Usklađeno (eng. *Aligned*): Aktivnosti upravljanja rizicima trebaju biti usklađene s ostalim aktivnostima u organizaciji.
- Sveobuhvatno (eng. *Comprehensive*): Kako bi bio potpuno učinkovit, pristup upravljanju rizicima mora biti sveobuhvatan.
- Ugrađeno (eng. *Embedded*): Aktivnosti upravljanja rizicima moraju biti ugrađene u organizaciju.
- Dinamično (eng. *Dynamic*): Aktivnosti upravljanja rizicima moraju biti dinamične i osjetljive na nove i promjenjive rizike.

Vidljivo je kako postoje mnoge definicije koje opisuju upravljanje rizicima, ali općenito može se reći kako je upravljanje rizicima informacijske sigurnosti sistematičan, analitički i ponavljajući proces identifikacije, procjene i rangiranja rizika, implementacije protumjera za smanjenje rizika te nadzor rizika pri čemu se rizik može definirati kao mogućnost da neka prijetnja iskoristi određenu ranjivost informacijskog sustava te uzrokuje štetu ili gubitak informacijske imovine.

Tu dolazi do potrebe da se definiraju različiti sigurnosni koncepti te njihovi međusobni odnosi kako bi se vidjelo kontekst u kojemu nastaju i djeluju rizici po informacijski sustav.



Slika 3.4: Veze između različitih sigurnosnih koncepata [53]

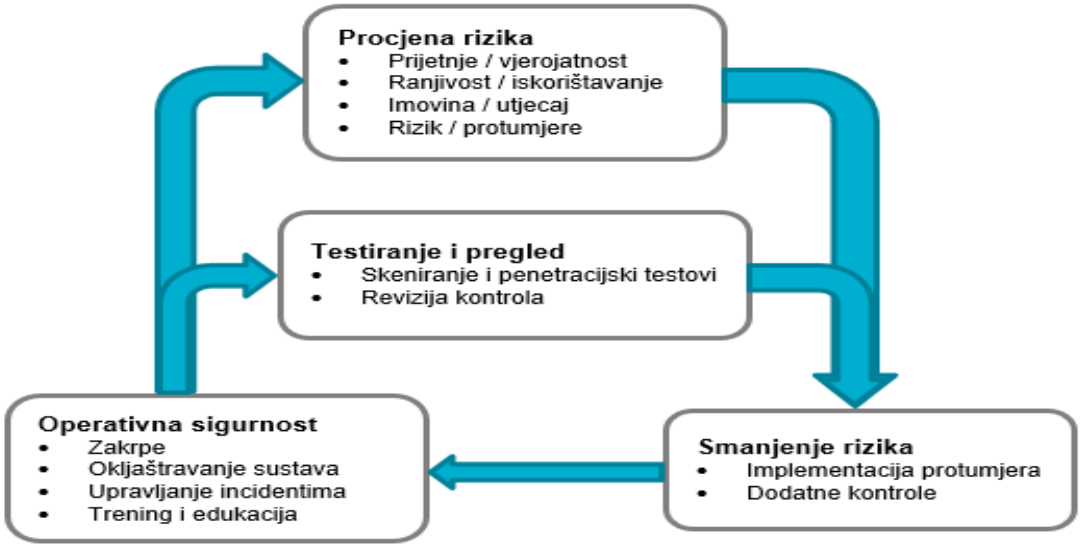
- Prijetnja – Bilo koja potencijalna opasnost povezana s iskorištavanjem ranjivosti, npr. zloćudni softver ili lažne e-mail poruke.
- Agent prijetnje – Entitet koji iskorištava ranjivost, to može biti napadač na računalnu mrežu ili proces koji pristupa podacima na način nedozvoljen sigurnosnom politikom.
- Ranjivost – Nedostatak sigurnosne protumjere ili slabost prisutna u informacijskoj imovini, npr. to može biti nežurirani antivirusni softver ili operacijski sustav na računalu ili mobilnom uređaju, otvoreni port na vatrozidu, nezaštićena bežična pristupna točka (eng. *wireless access point*), itd.
- Rizik – Vjerojatnost da će agent prijetnje iskoristiti ranjivost sustava i time napraviti određeni negativni utjecaj na poslovno okruženje.
- Izloženost – Instanca izložena gubicima. Ranjivost izlaže organizaciju mogućim gubicima. Ako se lozinkama slabo upravlja i ako se pravila za lozinke ne provode, organizacija je tada izložena mogućnosti da se lozinke dohvate i koriste na neovlašteni način.
- Sigurnosna protumjera ili kontrola – Postavlja se kako bi se smanjio potencijalni rizik. Ta sigurnosna protumjera može biti softverska konfiguracija, sklopovski uređaj ili procedura koja eliminira ranjivost ili smanjuje vjerojatnost da će agent

prijetnje biti u mogućnosti iskoristiti ranjivost. Primjeri sigurnosnih protumjera su primjena jakih lozinki (najmanje 8 znakova uključujući složenost), vatrozid, mehanizmi kontrole pristupa, enkripcija podataka, antivirusni softver, itd.

Shvaćanje ovih osnovnih sigurnosnih koncepata i njihovih međusobnih veza je nužno kako bi se moglo dublje ulaziti i analizirati problematiku rizika informacijske sigurnosti.

3.1.1. Analiza i procjena rizika informacijske sigurnosti

Procjena rizika smatra se najvažnijom i najkritičnijom fazom u procesu upravljanja rizicima koji osigurava da su rizici u prihvatljivim granicama s obzirom na razinu apetita za rizik definiranog od strane nadležnog višeg (eng. *senior*) menadžmenta. Procjena rizika je vrlo važan mehanizam odlučivanja koji identificira informacijsku imovinu koja je ranjiva na prijetnje, izračunava kvantitativnu ili kvalitativnu vrijednost rizika (ili očekivani gubitak) te prioritizira incidente rizika.



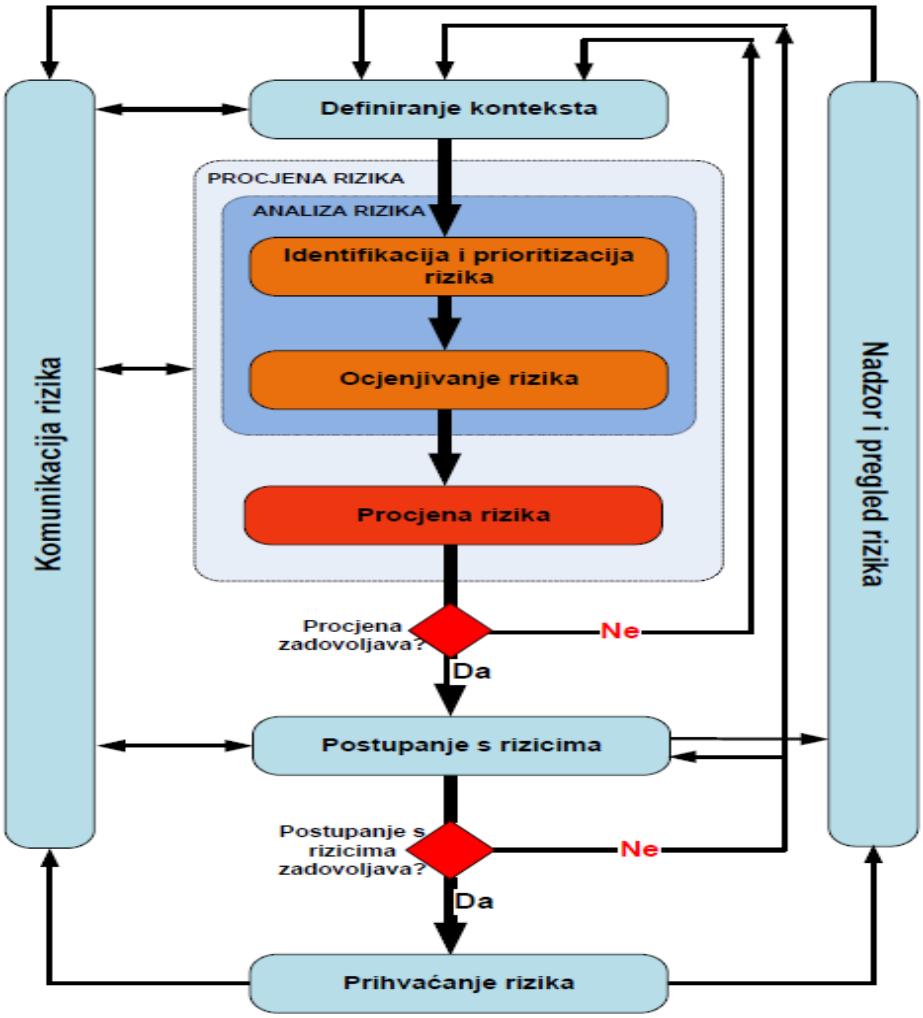
Slika 3.5: Proces upravljanja sigurnosnim rizicima [51]

Na Slici 3.5 mogu se vidjeti faze procesa upravljanja sigurnosnim rizicima te ključna uloga procjene rizika informacijske sigurnosti jer dobavlja informacije o prijetnjama, imovini i cjelokupnim rizicima u organizaciji.

Proces procjene informacijskih rizika sastoji se od tri temeljne faze, a to su uspostava konteksta, identifikacija rizika i njihova analiza te posljedično tretman uočenih rizika [27], [28], [29]. Prema ISO 31000, procjena rizika je sveobuhvatni proces identifikacije, analize i evaluacije rizika [38]. Dodatno, prema [46], [47], procjena rizika je proces identifikacije sigurnosnih rizika na sustavu te određivanje vjerojatnosti njihove pojave, utjecaja i sigurnosnih

protumjera kako bi se smanjilo eventualni negativni utjecaj. Glavni cilj procjene rizika je odrediti odgovarajuće kontrole za smanjenje ili eliminaciju tih rizika, a koraci su sljedeći [134]:

1. Identifikacija prijetnji. Ovaj prvi korak identificira sve potencijalne prijetnje po sustav. Omogućava identifikaciju potencijalnih izvora prijetnji i razvija popis izjava o prijetnjama koje su potencijalni izvori prijetnji koji su primjenjivi na informacijski sustav.
2. Identifikacija ranjivosti. U drugom koraku, cilj identifikacije ranjivosti je razviti popis ranjivosti informacijskog sustava (nedostataka ili slabosti) koje bi mogli biti iskorišteni od strane potencijalnih izvora prijetnji.
3. Određivanje rizika. U trećem koraku, svrha određivanja rizika je procijeniti razinu rizika po informacijski sustav.
4. Preporuka kontrola. U četvrtom koraku, cilj je odrediti kontrole koje bi mogle ublažiti ili eliminirati uočene rizike, a prema potrebama organizacije. Cilj preporučenih kontrola je smanjiti razinu rizika po informacijski sustav.



Slika 3.6: Proces procjene rizika [28]

Na Slici 3.6 prikazan je cjelokupni proces procjene rizika informacijske sigurnosti – preuzeto iz norme ISO/IEC 27005:2018 [28], koji se zapravo smatra najznačajnijim i najčešće korištenim standardom za područje rizika informacijske sigurnosti.

Prema ISO 27005:2018, procjena rizika određuje vrijednost informacijske imovine, identificira primjenjive prijetnje i ranjivosti koje postoje (ili bi mogle postojati), identificira postojeće kontrole i njihov utjecaj na identificirani rizik, određuje potencijalne posljedice i konačno daje prioritet izvedenim rizicima i rangira ih u odnosu na kriterije za procjenu rizika definirane tijekom faze uspostave konteksta [28]. Temeljem rezultata procjene rizika može se razumjeti stanje sigurnosti promatranog informacijskog sustava te poduzeti ciljane sigurnosne protumjere koje kontroliraju rizik na prihvatljivoj razini.

Treba napomenuti kako se termini procjena rizika i analiza rizika u praksi najčešće koriste naizmjenično za istu svrhu, ali u suštini se razlikuju po tome što procjena rizika predstavlja proces prikupljanja podataka, dok je analiza rizika proces u kojemu se ispituju i obrađuju prikupljeni podaci sa svrhom kako bi se dobilo određene rezultate na temelju kojih se može donijeti adekvatna odluka o postupanju s uočenim informacijskim rizicima.

Prvi korak prilikom procesa provedbe procjene rizika informacijske sigurnosti je jasno definiranje i razumijevanje pristupa koji će se koristiti tijekom tog procesa. Postoje mnogi pristupi koji se razlikuju u kontekstu analize, mjerenja, korištenja alata, itd. Jedna od najznačajnijih razlika između ISRA tehnika jest način na koji se određuju i izračunavaju tzv. varijable za odluku o riziku (eng. *risk decision variables*). Svaka varijabla odnosno element za odluku o riziku može se odrediti pomoću složenih izračuna ili preko subjektivnih prosudbi pa tako postoje kvantitativna i kvalitativna analiza rizika [51].

3.1.2. Kvantitativna i kvalitativna analiza rizika

Kvantitativna analiza rizika se koristi za dodjeljivanje novčanih i brojčanih vrijednosti svim elementima procesa analize rizika. Svi elementi unutar analize su kvantificirani i uneseni u jednadžbu kako bi se odredilo ukupni rizik (eng. *total risk*) i preostali rizik (eng. *residual risk*). Takav pristup analizi rizika smatra se više znanstvenim ili matematičkim u usporedbi s kvalitativnim pristupom. Prema [53], elementi za analizu rizika su sljedeći:

- Vrijednost imovine (eng. *Asset Value*)
- Učestalost prijetnji (eng. *Threat Frequency*)

- Težina ranjivosti (eng. *Severity of Vulnerability*)
- Utjecaj štete (eng. *Impact Damage*)
- Cijena protumjera (eng. *Safeguard Costs*)
- Učinkovitost protumjera (eng. *Safeguard Effectiveness*)
- Nesigurnost/neizrazitost (eng. *Uncertainty*)
- Vjerojatnosti (eng. *Probability Items*).

Postoji nekoliko formula koje se uobičajeno koriste u kvantitativnoj analizi sigurnosnih rizika pri čemu te formule pokrivaju očekivani gubitak za određene rizike i vrijednost sigurnosnih protumjera za smanjenje rizika. Formule[1] su sljedeće:

ALE = SLE * ARO

SLE = AV * EF

- **ARO**: Vrijednost koja predstavlja procijenjenu učestalost da će se određena prijetnja ostvariti unutar jednogodišnjeg razdoblja. Raspon vrijednosti može biti od 0.0 (nikad) do 1.0 (jednog godišnje), ili čak vrijednost i veća od 1 (npr. nekoliko puta godišnje).
- **EF**: Predstavlja postotak mogućeg gubitka za određenu imovinu u slučaju da se prijetnja ostvari (za jedan incident po informacijskoj imovini).
- **AV**: Vrijednost informacijske imovine koja se izražava novčano ($).
- **SLE**: Očekivani novčani ($) gubitak za tvrtku u slučaju ostvarenja jednog negativnog događaja odnosno pojave sigurnosnog incidenta.
- **ALE**: Očekivani godišnji novčani ($) gubitak po tvrtku u slučaju ostvarenja određenih prijetnji po informacijsku imovinu. Očekivani gubitak je zapravo vrlo koristan koncept jer se u kontekstu rizika ne radi o izvjesnosti nego o vjerojatnosti.
- **SV**: Vrijednost sigurnosne protumjere (izražena novčano, $) nakon implementacije iste u informacijskom sustavu na godišnjoj razini.

Uz navedene formule, postoji još jedan ključan element za istaknuti, a to je protumjera (eng. *countermeasure*). Protumjera je bilo koji administrativni, fizički ili tehnički sigurnosni mehanizam pomoću kojeg se smanjuje rizik po imovinu organizacije [51]. Nijedna protumjera ne može u potpunosti eliminirati rizik po imovinu organizacije, već protumjera može smanjiti

[1] ALE (eng. *Annual Loss Expectancy*) – očekivani godišnji gubitak
ARO (eng. *Annualized Rate of Occurrence*) – godišnja vjerojatnost pojave negativnog događaja
SLE (eng. *Single Loss Expectancy*) – očekivani pojedinačni gubitak
AV (eng. *Asset Value*) – vrijednost informacijske imovine
EF (eng. *Exposure Factor*) – faktor izloženosti
SV (eng. *Safeguard Value*) – vrijednost sigurnosne protumjere

rizik po imovinu organizacije smanjenjem SLE i/ili ALE vrijednosti. Implementacija svake protumjere iziskuje određene novčane troškove, a može se prikazati sljedećom formulom:

SV = (ALE prije – ALE poslije) – Godišnji trošak sigurnosne protumjere

U poslovnoj praksi vrijednost sigurnosne protumjere (SV) za organizaciju najčešće ne smije biti veća od ALE vrijednosti, osim ako nije riječ o određenim zakonodavnim ili regulatornim odredbama, npr. ako se radi o nacionalnoj kritičnoj infrastrukturi.

Kvalitativna analiza rizika temelji se na subjektivnim prosudbama članova tima za procjenu sigurnosnih rizika kako bi se odredio ukupni rizik po informacijski sustav. Kod kvalitativnih metoda prolazi se kroz različite scenarije za vjerojatnosti rizika i rangiranje ozbiljnosti prijetnji te vrednovanje mogućih protumjera. Kvalitativne metode uključuju prosudbe, najbolju praksu, znanje i iskustvo procjenitelja. Primjeri kvalitativnih tehnika za prikupljanje podataka su *Delphi*, *brainstorming*, fokus grupe, ankete, upitnici, liste za provjeru, izravni pojedinačni sastanci i intervjui. Tim za analizu rizika odabire najbolju tehniku za prijetnje koje treba procijeniti. U svrhu ovog istraživanja odabrana je *Delphi* tehnika za prikupljanje mišljenja od strane sigurnosnih stručnjaka o najznačajnijim elementima za analizu i procjenu rizika koji se namjeravaju koristiti u svrhu procjene, rangiranja i odabira IT rješenja primjenom višekriterijskoga odlučivanja.

Kod kvalitativne analize rizika koriste se isti elementi kao i u kvantitativnoj analizi, ali bez brojčanih vrijednosti za rizik te se pritom koristi opisna hijerarhijska skala za rizik, npr.:

Kritičan (eng. ***C**ritical*) > Visok (eng. ***H**igh*) > Srednji (eng. ***M**edium*) > Nizak (eng. ***L**ow*)

No, kvalitativne vrijednosti rizika se također izračunavaju i to u pravilu prema sljedećoj jednostavnoj formuli:

Rizik = Vjerojatnost * Posljedica

Pri tome se uobičajeno definira i sljedeća tablica rizika:

Tablica 3.1: Matrica rizika [29]

Vjerojatnost	Posljedica			
	Niska	Srednja	Visoka	Teška
Visoka	M	H	H	C
Srednja	M	M	H	H
Niska	L	M	M	H

Razlog zbog kojeg organizacije implementiraju sigurnosne protumjere jest smanjiti rizik na prihvatljivu razinu (eng. *risk tolerance*). Niti jedan informacijski sustav nije u potpunosti siguran, što znači kako kako uvijek postoji određeni preostali rizik s kojim se treba baviti, a zove se **rezidualni rizik** (eng. *residual risk*). Taj preostali rizik razlikuje se od ukupnog

rizika s kojim se suočava organizacija u slučaju odabira strategije da ne implementira bilo kakve sigurnosne protumjere. Organizacija može odabrati pristup za ukupni rizik ako CBA[2] pokaže da je to najbolji način djelovanja. Npr., ako postoji vrlo mala vjerojatnost da web poslužitelj organizacije može biti kompromitiran i ako je trošak potrebnih protumjera veći od potencijalnog gubitka, tada organizaciji ostaje logičniji izbor ne implementirati sigurnosne protumjere odabirući strategiju za ukupni rizik. Tako imamo sljedeće jednostavne formule [53]:

Ukupni rizik = Prijetnje * Ranjivost * Vrijednost imovine

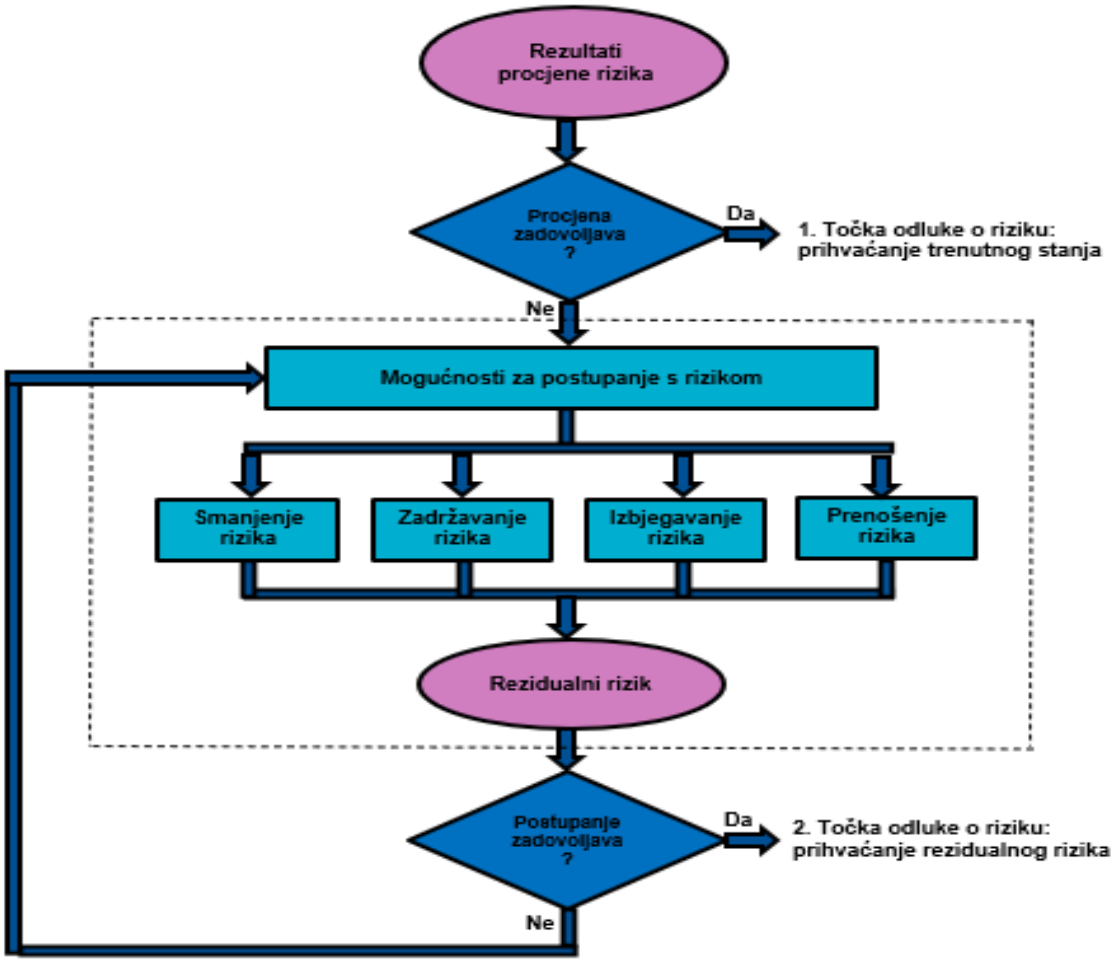
Rezidualni rizik = (Prijetnje * Ranjivost * Vrijednost imovine) * Nedostatak kontrola

Može se pojaviti i sljedeći koncept:

Rezidualni rizik = Ukupni rizik – Sigurnosne protumjere

Tijekom procesa procjene rizika identificirane su prijetnje i ranjivosti. Vjerojatnost da će neka prijetnja iskoristiti ranjivost je pomnožena sa vrijednosti imovine koja se procjenjuje, a što rezultira ukupnim rizikom. Kad se uračuna i nedostatak kontrola, rezultat je rezidualni rizik. Implementacija sigurnosnih protumjera predstavlja jedan od načina za smanjenje rizika. Po dobivanju rezultata o riziku (ukupni i rezidualni) na temelju izračuna i definirane matrice rizika te ovisno o razini kritičnosti promatranog IT sustava, organizacija tada izrađuje plan aktivnosti za postupanje s rizikom (Slika 3.7).

[2] *Cost-Benefit Analysis* (CBA) – Metoda ekonomske analize kojom se uspoređuju i vrednuju sve prednosti i nedostaci nekog projekta analizom troškova (eng. *cost*) i koristi (eng. *benefit*)



Slika 3.7: Aktivnosti za postupanje s rizikom [28]

Sa Slike 3.7 vidljivo je kako postoje 4 osnovna načina za postupanje s rizikom:

- Prenošenje rizika (eng. *Risk Transfer*): Dijeljenje rizika s trećom (vanjskom) stranom. Ovaj pristup može izazvati nove rizike ili promijeniti postojeće identificirane rizike pa je tako moguće da bude potrebno provesti i dodatni tretman rizika. Prijenos se može obaviti putem ugovaranja police osiguranja. Treba reći kako je moguće prenijeti zaduženje za upravljanje rizikom, ali nije moguće prenijeti odgovornost za posljedicu. U slučaju nekog negativnog događaja klijenti obično pripisuju krivnju na organizaciju s kojom imaju ugovornu obvezu, npr. to je posebno karakteristično za bankarstvo.
- Izbjegavanje rizika (eng. *Risk Avoidance*): Kada je identificirani rizik previsok ili ako troškovi implementacije drugih opcija za tretman rizika premašuju koristi, odluka organizacije može biti ukidanje aktivnosti koje donose rizik. Npr., obustavljanje rada nekog web servisa.
- Smanjenje rizika (eng. *Risk Mitigation*): Razina rizika se smanjuje odabirom odgovarajućih i opravdanih kontrola tako da rezidualni rizik može biti ponovno

procijenjen kao prihvatljiv. Kontrole se odabiru tako da zadovoljavaju zahtjeve identificirane procesima procjene i tretmana rizika pri čemu se moraju uzimati u obzir kriteriji za procjenu rizika te zakonodavni, regulatorni i ugovorni zahtjevi. Također, odabir kontrola mora uzeti u obzir troškove i vrijeme potrebno za implementaciju kontrola kao i tehničke, kulturalne i aspekte okruženja. Često je moguće smanjiti ukupni trošak vlasništva nad informacijskim sustavom sa pravilno odabranim kontrolama za zaštitu informacijskog sustava. Općenito, kontrole omogućavaju sljedeće vrste zaštita: ispravak, uklanjanje, sprečavanje, smanjenje utjecaja, odvraćanje, otkrivanje, oporavak, praćenje i svijest. Tijekom postupka odabira kontrola bitno je odvagati troškove nabave, implementacije, administracije, rada, nadzora i održavanja kontrola u odnosu na vrijednost imovine koja se štiti. Rezultat aktivnosti je lista mogućih kontrola sa pripadajućim troškovima, koristima i prioritetom za implementaciju.

- Prihvaćanje rizika (eng. *Risk Acceptance*): Odluka o zadržavanju odnosno prihvaćanju rizika bez dodatnih akcija treba se donijeti na temelju evaluacije rizika. Ako razina rizika zadovoljava kriterije za prihvaćanje rizika, tada nema potrebe za implementacijom dodatnih kontrola pa se takav rizik može zadržati.

Treba napomenuti kako svaka odluka o postupanju s rizikom sa sobom nosi i određeni oportunitetni trošak što zapravo predstavlja cijenu donesene odluke jer se izborom jedne opcije propuštaju neke druge prilike. Svaki od navedenih pristupa za analizu i procjenu rizika ima svojih prednosti i nedostataka pa su tako karakteristike kvalitativnih i kvantitativnih ISRA metoda prikazane u Tablici 3.2:

Tablica 3.2: Usporedba kvalitativnih i kvantitativnih ISRA metoda [51], [53], [58]

	Kvantitativne metode	**Kvalitativne metode**
Prednosti	• Omogućavaju kvantitativno definiranje posljedice (u novčanim vrijednostima) za pojavu incidenata • Vrijednosti imovine i sigurnosne protumjere iskazuju se novčano ($$) • Koriste nezavisne metrike koje su provjerljive i objektivne • Omogućavaju CBA tijekom odabira zaštitnih mjera • Daju precizniju i vjerodostojnu sliku promatranog rizika • Pokazuju jasne novčane gubitke koji mogu nastati u roku od jedne godine	• Omogućavaju određivanje područja većeg rizika u kraćem vremenskom razdoblju te bez većih troškova • Koriste se jednostavnije metrike • Analiza rizika je relativno jednostavna i jeftinija

	• Podržavaju procjenu budžeta za projekte • Omogućavaju praćenje uspješnosti upravljanja rizicima informacijske sigurnosti (osnova za definiranje KPI[3] parametara)	
Nedostaci	• Izračuni mogu biti jako složeni • Ovise o opsegu i točnosti definirane mjerne skale • Potrebno je mnogo pripremnog rada za dohvaćanje svih detaljnih i relevantnih informacija o okruženju • Rezultati analize mogu biti netočni i nejasni – daju lažan osjećaj točnosti • Nužno je analizu dodatno obogatiti kvalitativnim opisima • Analize su općenito značajnije skuplje te zahtijevaju znatno veće iskustvo i napredne alate	• Vrijednost imovine je subjektivna jer se određuje iskustvenom metodom • Ne omogućavaju određivanje vjerojatnosti i rezultata korištenjem numeričkih vrijednosti – teško je izraditi budžet za sigurnost jer nema definiranih novčanih vrijednosti • CBA je svakako teže izvediva tijekom postupka odabira zaštitnih mjera • Procjena i dobiveni rezultati su subjektivni, imaju općeniti karakter i približne vrijednosti • Otežano praćenje uspješnosti sigurnosnih programa

Tim za analizu rizika, menadžment, alati za analizu rizika i organizacijska kultura određuju koji od navedenih ISRA pristupa će se primijeniti. Cilj bilo koje metode je procijeniti stvarni rizik po organizaciju te rangirati prijetnje po težinama tako da se odgovarajuće kontrole mogu planirati i primijeniti.

S obzirom da je gotovo nemoguće provesti čistu kvantitativnu procjenu rizika te kako čisti kvalitativni proces ne daje dovoljno statističkih podataka za financijske odluke, u praksi se stoga najčešće ova dva pristupa za analizu i procjenu rizika koriste u hibridnom modelu. Kvantitativna evaluacija se može koristiti za materijalnu informacijsku imovinu (novčane vrijednosti), dok se kvalitativna procjena može koristiti za nematerijalnu imovinu (vrijednosti prioriteta).

Istraživanje područja procjene rizika dobiva sve veću pozornost kako poslovnog svijeta tako i akademske zajednice [48]. Što se tiče ovog istraživanja u kontekstu rizika informacijskih sustava, najvažniji dio odnosi se na elemente za analizu i procjenu rizika unutar faze procjene rizika gdje se namjeravaju identificirati oni najznačajniji (generički) elementi kako bi se isti integrirali u višekriterijski model sa svrhom učinkovitije evaluacije kritičnih IT rješenja upravo prema identificiranim elementima za analizu i procjenu rizika.

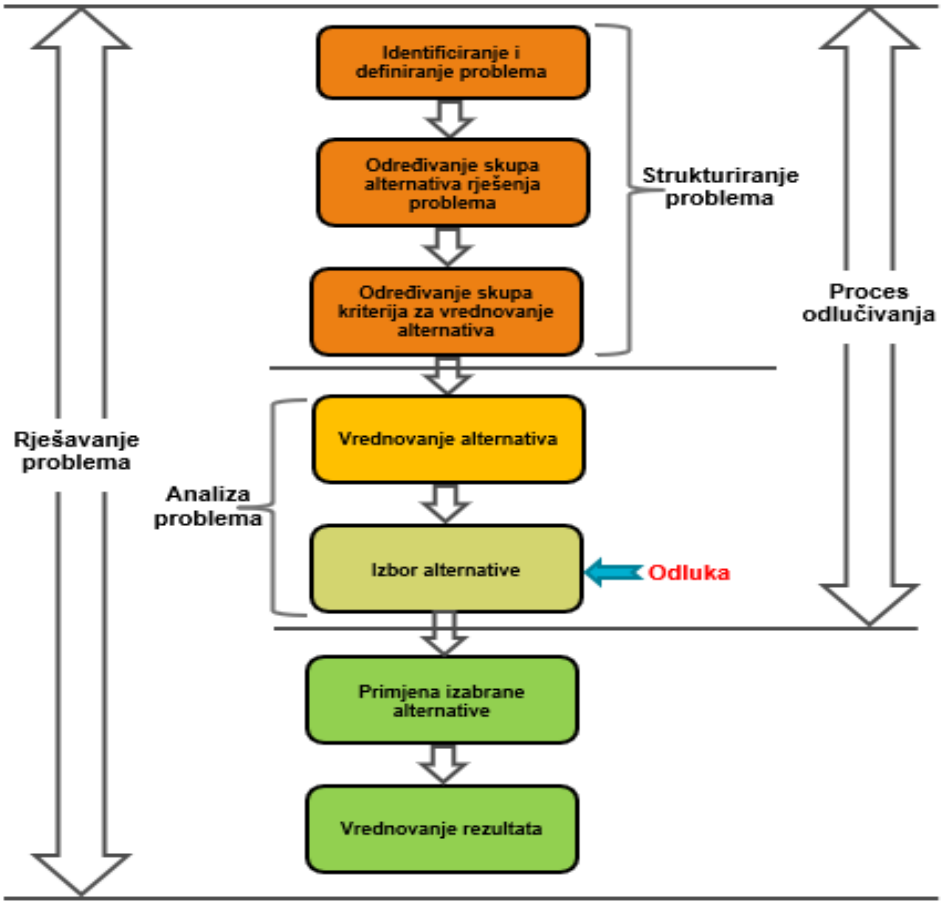
[3] *Key Performance Indicators* (KPI) – Ključni pokazatelji učinaka, služe za mjerenje uspješnosti organizacije ili određene projektne aktivnosti

3.2. Višekriterijsko odlučivanje

Proces donošenja odluka uključuje niz slijednih koraka: identifikacija problema, izrada pretpostavki odnosno preferencija, zatim evaluacija alternativa i konačno određivanje najbolje alternative [40]. Rješavanje problema je proces identifikacije razlike između stvarnog stanja nekog sustava i poželjnog stanja te posljedično poduzimanje određenih aktivnosti za smanjenje ili uklanjanje uočenih razlika [18, 41, 50].

Složenost procesa odlučivanja ovisi o složenosti definiranog problema. Donošenje odluka je vrlo jednostavno u slučaju problema s jednim kriterijem pri čemu je potrebno samo odabrati alternativu s najvišom ocjenom preferencije. No, kada odlučivanje za evaluaciju alternativa uzima više kriterija kao što su težine kriterija (eng. *criteria weights*), ovisnosti (eng. *dependencies*) između preferenci i konflikti između kriterija, tada je potrebno koristiti određene sofisticirane metode za rješavanje problema.

Prema [18], svaki složeni proces rješavanja bilo kojeg problema odlučivanja nužno sadržava korake prikazane na Slici 3.8:



Slika 3.8: Koraci procesa odlučivanja i rješavanja problema [18]

Na Slici 3.8 prikazani su svi nužni koraci u cjelokupnom procesu odlučivanja i rješavanja problema. Također, na Slici 3.8 vidljivo je kako se i sam proces odlučivanja može dodatno raščlaniti na dva dijela: strukturiranje problema i analiza problema. Svrha podjele jest odvojiti postupak strukturiranja problema koji je od velike važnosti i u kojem se mogu koristiti različite metode kako bi se što bolje strukturiralo problem, a za što dosta često nema dovoljno vremena ili resursa – to je posebno slučaj kod analize IT poslovnih ili IT sigurnosnih rješenja zbog čega se i javljaju rizici.

Tipovi metoda za odlučivanje, a vezano uz postojanje određenih formalnih proceduralnih ograničenja, mogu se podijeliti na heurističke i analitičke metode odlučivanja. Formalna proceduralna ograničenja najčešće se pojavljuju u obliku zahtjeva da se u postupku donošenja odluke koriste samo kvantitativni podaci pa se u tom slučaju traži optimalno rješenje. Ključni kriterij za osnovnu podjelu metoda je taj da li se sama metoda temelji na iskustvu ili matematičkome modelu. Glavna razlika između heurističkih i analitičkih metoda odlučivanja jest u samoj kvaliteti rješenja i troškovima. Heurističke metode daju zadovoljavajuća rješenja uz niže troškove, a analitičke metode se temelje na analizi kvantitativnih podataka i daju optimalna rješenja uz veće troškove [18, 50].

Donositelju odluke ponekad nije jednostavno izabrati odgovarajuću metodu odlučivanja, ali postoje nužni uvjeti koje treba zadovoljiti kako bi se moglo primijeniti analitički postupak odnosno kvantitativnu metodu:

- Zadovoljenje svih formalnih uvjeta koji omogućuju izgradnju matematičkog modela za identifikaciju optimalnog rješenja – predstavlja najvažniji uvjet odnosno element
- Problem sadržava samo kvantitativne aspekte
- Definirana su pravila koja ukazuju je li rješenje problema prihvatljivo
- Analitička procedura je dostupna i primjenjiva
- Problem je dobro definiran i dobro strukturiran.

Ako su ispunjeni svi navedeni uvjeti tada je moguća primjena kvantitativne metode za analizu odluke. S obzirom kako se u ovom istraživanju radi o složenom problemu odlučivanja koji je važan zbog svojih mogućih sigurnosnih i ekonomskih posljedica po financijsku instituciju, problem je nov i ne postoji zadovoljavajuće iskustvo s rješavanjem istoga te je problem ujedno i ponavljajući. Tako će se u radu obrađivati i primjenjivati različite kvantitativne metode za analizu odluke. Te metode za analizu složenih odluka su izrazito bitne pri čemu su najznačajnija obilježja takvih odluka postojanje više ciljeva koji se namjeravaju ostvariti te rizik. Kada je potrebno uskladiti više ciljeva javlja se problem konflikta između tih

ciljeva i dolazi do potrebe za procjenom kompenzacijskih efekata – povećanje vrijednosti jednog cilja nužno vodi smanjenju vrijednosti nekog drugog cilja. Tako zbog različitih važnosti ciljeva koji se žele postići donošenjem neke odluke svi kriteriji za procjenu inačica nemaju jednaku važnost. Metode koje se primjenjuju za rješavanje takvih složenih problema odlučivanja zovu se metode višekriterijskog ili višeatributnog odlučivanja [18, 41, 50].

Kako bi se primijenila određena metoda višekriterijskog odlučivanja, prvi korak je identificirati problem odlučivanja. Nakon toga potrebno je odrediti preferencije odlučivanja. Daljnji korak je određivanje skupa mogućih alternativa ili strategija kako bi se jamčilo da će cilj biti postignut, tj. radi se evaluacija alternativa. Idući korak je odabir odgovarajuće metode za evaluaciju, nadmašivanje (eng. *outranking*) ili poboljšanje alternativa ili strategija odnosno pronalazak i određivanje najbolje alternative.

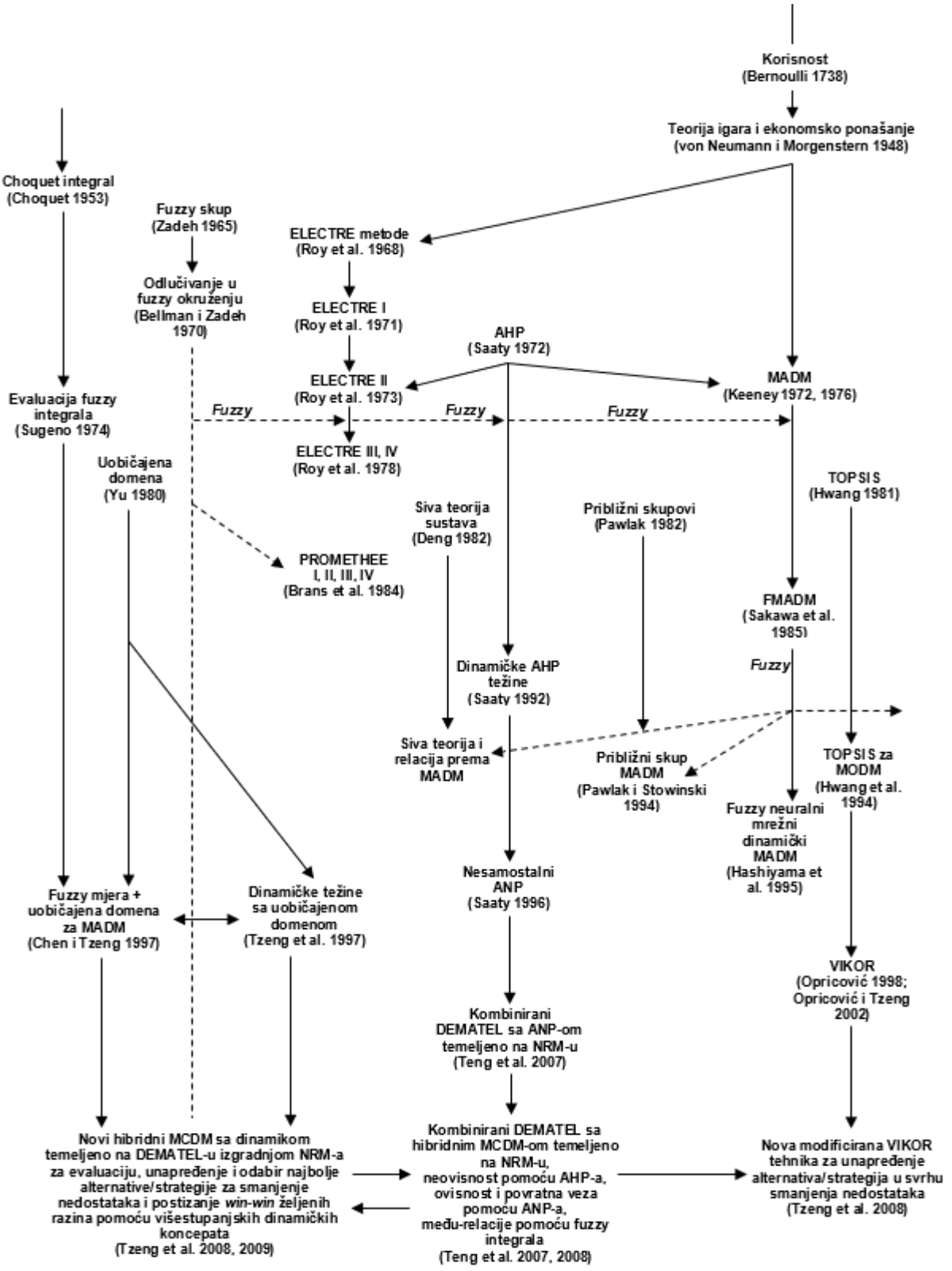
MCDM (eng. *Multicriteria Decision Making*) metode se primjenjuju u kontekstu ocjenjivanja, a što je najčešće povezano s ograničenim brojem unaprijed određenih alternativa i diskretnim ocjenama preferencija. Konvencionalne MCDM metode razmatraju samo oštre, tj. jasne probleme odlučivanja i nemaju opću paradigmu za specifične probleme iz stvarnog svijeta. Stoga se većina MCDM problema u stvarnom svijetu treba smatrati nejasnim ili neizrazitim (eng. *fuzzy*) MCDM problemima, a koji se sastoje od ciljeva, aspekata ili dimenzija, atributa odnosno kriterija i mogućih alternativa (ili strategija) [41].

Višekriterijsko odlučivanje naziva se još i više atributno odlučivanje (eng. *Multi-attribute Decision Making*, MADM). Povijesno gledajući, MADM problematika seže sve do pojave St. Petersburg paradoksa (naziva se još i St. Petersburg lutrija) koji je vezan uz vjerojatnost i teoriju odlučivanja u ekonomiji. To je igra na sreću gdje je jedan igrač kockar koji želi osvojiti neku nagradu, dok je drugi igrač banka koja kockaru nudi priliku za igranje i isplaćuje nagradu. Na početku igre se igrači dogovore o iznosu uloga potrebnog za sudjelovanje u igri te svaki krug započinje na način da kockar plati banci taj dogovoreni iznos. Igra se odvija bacanjem poštenog novčića, pri čemu je jednaka vjerojatnost pojavljivanja pisma i glave, sve dok dođe do kraja, tj. kada padne glava prestaje bacanje novčića i kockaru banka isplaćuje nagradu, a ukupan broj bacanja određuje nagradu koja je jednaka $\$2^n$. Problem koji se pritom javlja je sljedeći: koliko ste spremni platiti za ovu igru? Prema teoriji očekivane vrijednosti (eng. *expected value theory*), može se izračunati $EV = \sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n * 2^n$, pri čemu očekivana vrijednost zapravo ide u beskonačnost. Međutim, krajnji rezultat očito je drugačiji (tj. suprotan) od uobičajenog ljudskog ponašanja jer nitko nije spreman platiti više od 1000 dolara za ovu igru [42]. St. Petersburg paradoks je situacija u kojoj naivni kriterij odlučivanja, a koji uzima u

obzir samo očekivanu vrijednost, predviđa akcije za koje se ipak pretpostavlja kako osobe u realnom (stvarnom) životu ne bi poduzele.

Ovdje se neće ulaziti u detalje rasprave o rješenju koje je predstavio švicarski matematičar Daniel Bernoulli pri čemu je proveo detaljno istraživanje vezano uz navedenu problematiku te iz čega i proizlazi njegovo djelo o teoriji mjerenja rizika [43], nego je fokus na zaključku kako ljudi donose odluke ne na temelju očekivane vrijednosti nego na temelju očekivane korisnosti. Implikacija očekivane korisnosti je u tome što ljudi biraju alternativu s najvećom vrijednosti pretpostavljene korisnosti pri suočavanju s problemima višekriterijskog odlučivanja.

Autori von Neumann i Morgenstern su 1947. godine objavili svoju slavnu knjigu *Teorija igara i ekonomsko ponašanje* [44], kako bi se detaljno shvatilo matematičku teoriju ekonomske i društvene organizacije temeljeno na teoriji igara. Njihov značajan istraživački rad potaknuo je ekspanziju daljnjih istraživanja vezano uz ekonomsko ponašanje ljudi za MADM probleme. Tako se u nastavku opisuje i prikazuje povijesni razvoj MADM metoda, što je i prikazano na Slici 3.9.



Slika 3.9: Razvoj MADM tehnika [41]

Na Slici 3.9 može se vidjeti povijesni razvoj MADM metoda i tehnika, počevši od Bernoullijeve teorije korisnosti, preko razvoja ELECTRE i PROMETHEE metoda za nadmašivanje (eng. *outranking*), zatim slijedi razvoj AHP (*Analytic Hierarchy Process*) metode

i ANP (*Analytic Network Process*) metode, potom paralelni razvoj TOPSIS metode i unapređenje u vidu razvoja VIKOR metode za rješavanje problema odlučivanja sa konfliktnim i nemjerljivim kriterijima te konačno u novije vrijeme izrada hibridnih modela integracijom DEMATEL (*Decision-Making Trial and Evaulation Laboratory*) i ANP metoda pri čemu se uzimaju u obzir međusobne ovisnosti odnosno utjecaji među elementima za evaluaciju alternativa.

Autori Dobois i Prade u svom su radu predstavili generalizaciju MADM procedure u 5 glavnih koraka [45]:

1. korak: Definicija prirode problema

2. korak: Izrada hijerarhijskog sustava za njegovu evaluaciju

3. korak: Odabir odgovarajućeg modela za evaluaciju

4. korak: Dobivanje relativnih težina i ocjena performansi za svaki atribut u odnosu na svaku alternativu

5. korak: Određivanje najbolje alternative prema sintetičkim vrijednostima korisnosti, a koje su agregacijska vrijednost relativnih težina i ocjene performansi koje odgovaraju alternativama.

Ako su ukupne ocjene alternativa ipak nejasne (neizrazite), autori Tzeng i Huang [41] predlažu dodatno i 6. korak kako bi se rangiralo alternative u svrhu odabira one najbolje:

6. korak: nadmašivanje alternativa koje se odnose na njihove sintetičke neizrazite korisnosti iz koraka 5.

Dodatno, treba naglasiti kako se prema [62] sljedećih 5 principa svakako mora slijediti prilikom formuliranja evaluacijskih kriterija: cjelovitost (eng. *completeness*), operativnost (eng. *operationality*), razgradivost (eng. *decomposability*), bez redundantnosti (eng. *non-redundancy*) i najmanja veličina (eng. *minimum size*).

Analiza najznačajnijih metoda za višekriterijsko odlučivanje te odabir onih koje su primijenjene u razvoju modela za procjenu kritičnih informacijskih sustava detaljno su opisani u poglavlju *5.2 Metode za višekriterijsko odlučivanje*.

3.3. Kritični informacijski sustavi

Kritičnim sustavima smatraju se svi oni sustavi kod kojih pogreška u radu sustava može rezultirati značajnim financijskim gubicima, fizičkim oštećenjima opreme, objekata ili okoliša, kao i prijetnjama nacionalnoj sigurnosti i ljudskom životu, te gospodarskoj, ekonomskoj, socijalnoj i zdravstvenoj skrbi neke zemlje, ovisno o kojoj vrsti promatranog sustava je riječ. Tako u Republici Hrvatskoj postoje *Zakon o kritičnim infrastrukturama* [55] i *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga* [56] kojim su definirani sektori nacionalnih kritičnih infrastruktura (npr. energetika, komunikacijska i informacijska tehnologija, zdravstvo, financije, itd.), definirani su također i analiza rizika za identifikaciju kritičnih infrastruktura, postupanje s osjetljivim podacima, postupanje s incidentima, itd.

U ovom radu osvrt na kritične infrastrukture bit će prvenstveno u domeni informacijskih sustava i servisa koji se koriste u financijskim institucijama (bankama), a imaju značajan utjecaj na poslovanje banke, druge financijske institucije (ukoliko se radi o međusobno ovisnim i povezanim servisima) te stabilnosti čitavog financijskog ekosustava. Radi je zapravo o tzv. poslovnim kritičnim informacijskim sustavima [57].

Odluka o tome je li neki informacijski sustav kritičan ili nije za organizaciju prvenstveno je određena iz podrške tog sustava poslovnim ciljevima odnosno iz analize utjecaja na poslovanje (eng. *Business Impact Analysis*, BIA). Kritični sustavi su oni sustavi koji automatiziraju kritične poslovne funkcije. BIA se smatra funkcionalnom analizom pri čemu tim ljudi prikuplja podatke na način da intervjuira vlasnike informacijske imovine i poslovnih procesa te iz dostupne dokumentacije o istima. Zatim se dokumentiraju poslovne funkcije, aktivnosti i transakcije, izrađuje se hijerarhija poslovnih funkcija te se na kraju primjenjuje klasifikacijska shema kako bi se označilo razinu kritičnosti za svaku pojedinu poslovnu funkciju i informacijsku imovinu. BIA je usko povezana sa procesima upravljanja kontinuitetom poslovanja (eng. *Business Continuity Management*, BCM). Tako BIA omogućava procjenu mjerljivog utjecaja na poslovne operacije u slučaju katastrofe. Kritični informacijski sustavi moraju se identificirati i promatrati nezavisno s obzirom kako imaju jedinstvenu funkciju, podatke, korisnike i vlasnike podataka, iako postoji mogućnost preklapanja takvih sustava u nekim aspektima. Npr., može postojati jedan vlasnik podataka za dva ili više sustava koji podržavaju neku poslovnu funkciju.

Primjeri kritičnih okolina u bankama i općenito financijskim institucijama su mrežna sigurnosna rješenja, kriptografski sustavi, PCI DSS[4] okolina, sustavi za identifikaciju, autentikaciju i autorizaciju te posebno kritični bankovni poslovni sustavi poput transakcijskih sustava (internet i mobilno bankarstvo, platni promet) i osnovnog bankovnog sustava (eng. *core banking system*). Upravo će kritični poslovni informacijski sustavi biti predmetom ovog istraživanja prilikom testiranja i validacije novog hibridnog višekriterijskoga modela.

[4] *Payment Card Industry Data Security Standard (PCI DSS)* – Globalni standard informacijske sigurnosti za organizacije koje prenose, obrađuju i pohranjuju kartične podatke

4. Ciljevi, istraživačka pitanja, hipoteze i metodologija istraživanja

U ovom poglavlju predstavit će se svi najvažniji aspekti znanstvenog istraživanja, a koji nužno uključuju ciljeve planiranog istraživanja, istraživačka pitanja, znanstvene hipoteze, metrike te metodologiju provedbe istraživanja.

4.1. Ciljevi istraživanja

Znanstveno istraživanje u ovom radu ima nekoliko ciljeva te ih se može podijeliti na glavni (općeniti) cilj i specifične ciljeve.

Glavni cilj:

(1) Donošenje informirane odluke o stanju sigurnosti i odabiru kritičnog poslovnog informacijskog sustava kako bi se povećalo učinkovitost i kvaliteta procesa procjene takvih sustava u financijskoj instituciji.

Specifični ciljevi:

- **C1**: Provesti detaljan i sustavan pregled područja kako bi se utvrdilo koje metode i tehnike za procjenu rizika i višekriterijsko odlučivanje se trenutno koriste za procjenu, rangiranje i odabir informacijskih sustava.
- **C2**: Razviti hibridni model s relevantnim elementima za analizu i procjenu rizika informacijske sigurnosti u svrhu procjene, rangiranja i odabira kritičnih poslovnih informacijskih sustava primjenom metoda za višekriterijsko odlučivanje.
- **C3**: Provjeriti primjenjivost, valjanost i učinkovitost (validacija) novog višekriterijskog modela međusobnom usporedbom rezultata sa studije slučaja za generičke i inherentne kriterije promatranog kritičnog poslovnog informacijskog sustava.

4.2. Istraživačka pitanja

Nastavno na ciljeve istraživanja, postavljena su sljedeća istraživačka pitanja:

- **P1**: Kako omogućiti učinkovitije donošenje informirane odluke o stanju sigurnosti i odabiru kritičnih poslovnih informacijskih sustava u financijskoj instituciji?
- **P2**: Koji sve elementi za analizu i procjenu sigurnosnih rizika su prikladni i relevantni za izradu hibridnog višekriterijskoga modela za procjenu, rangiranje i odabir kritičnih informacijskih sustava u svrhu učinkovitijeg donošenja informirane odluke o promatranom kritičnom IT sustavu u financijskoj instituciji?
- **P3**: Za koje sve poslovne informacijske sustave je hibridni višekriterijski model primjenjiv i validan?

4.3. Znanstvene hipoteze

Postavljene su dvije znanstvene hipoteze:

- **H1**: *Višekriterijski model za procjenu, rangiranje i odabir kritičnih poslovnih informacijskih sustava s generičkim kriterijima za analizu i procjenu rizika je valjan*.

  Ova hipoteza vezana je uz ostvarenje specifičnog cilja **C2** te daje odgovor na postavljeno istraživačko pitanje **P1** gdje se za rješenje uočenog problema predlaže razvoj višekriterijskoga modela za evaluaciju, rangiranje i odabir kritičnih poslovnih IT sustava s generičkim kriterijima. Valjanost modela utvrđuje se procesom validacije na studiji slučaja primjenom definirane metrike **M1** čime se ostvaruje specifični cilj **C3** te daje odgovor na postavljeno istraživačko pitanje **P3**. Također, izradom višekriterijskoga modela s odgovarajućim elementima za analizu i procjenu rizika daje se odgovor na istraživačko pitanje **P2**.

- **H2**: *Višekriterijski model s generičkim kriterijima u procesu donošenju odluka je učinkovitiji od modela s inherentnim atributima*.

  Ova hipoteza izravno je vezana za ostvarenje specifičnog cilja **C3** (validacija novog modela) te daje odgovor na postavljeno istraživačko pitanje **P3** o primjenjivosti i

valjanosti modela. Učinkovitost modela utvrđuje se procesom validacije na studiji slučaja primjenom definirane metrike **M2**.

4.4. Metrike

Metrika predstavlja jedinicu mjere koja je osmišljena kako bi se olakšalo donošenje odluke te poboljšalo učinkovitost i odgovornost kroz prikupljanje, analizu i izvještavanje relevantnih podataka. Prema SANS-ovom vodiču za sigurnosne metrike [54], dobre metrike su one koje su pametne (eng. **SMART**), tj. posebne (eng. *Specific*), mjerljive (eng. *Measurable*), ostvarive (eng. *Attainable*), bitne (eng. *Relevant*) i vremenski ovisne (eng. *Time-dependent*). Stvarno korisne metrike pokazuju stupanj ispunjenja sigurnosnih ciljeva, kao što je povjerljivost podataka, te pokreću mjere poduzete za poboljšanje cjelokupnog sigurnosnog programa organizacije.

Metrike koje su primijenjene u istraživanju tijekom procesa validacije sa svrhom ostvarenja glavnog cilja, a to je učinkovitije donošenje informirane odluke o stanju sigurnosti i odabiru kritičnog informacijskog sustava u financijskoj instituciji, su sljedeće:

- **M1**: Odstupanje u rangu rješenja za rezultate dobivene novim hibridnim modelom s generičkim kriterijima u odnosu na rang dobiven korištenjem inherentnih atributa promatranog poslovnog informacijskog sustava iz studije slučaja tijekom procesa validacije.
- **M2**: Razlika u broju FTE-a (eng. *Full-time equivalent*, Ekvivalent punog radnog vremena) potrebnih za procjenu kritičnog poslovnog informacijskog sustava prema novom predloženom hibridnom višekriterijskom modelu s generičkim kriterijima u odnosu na procjenu poslovnih IT sustava s inherentnim kriterijima.

Ako novi višekriterijski model pokaže na isti rang rješenja (informacijskih sustava) kao u slučaju kada se koriste inherentni atributi za promatrano IT rješenje ili kritični sustav koristeći neku od metoda za višekriterijsko odlučivanje, a pritom se utroši manje vremena i resursa, tada je zadani cilj ispunjen.

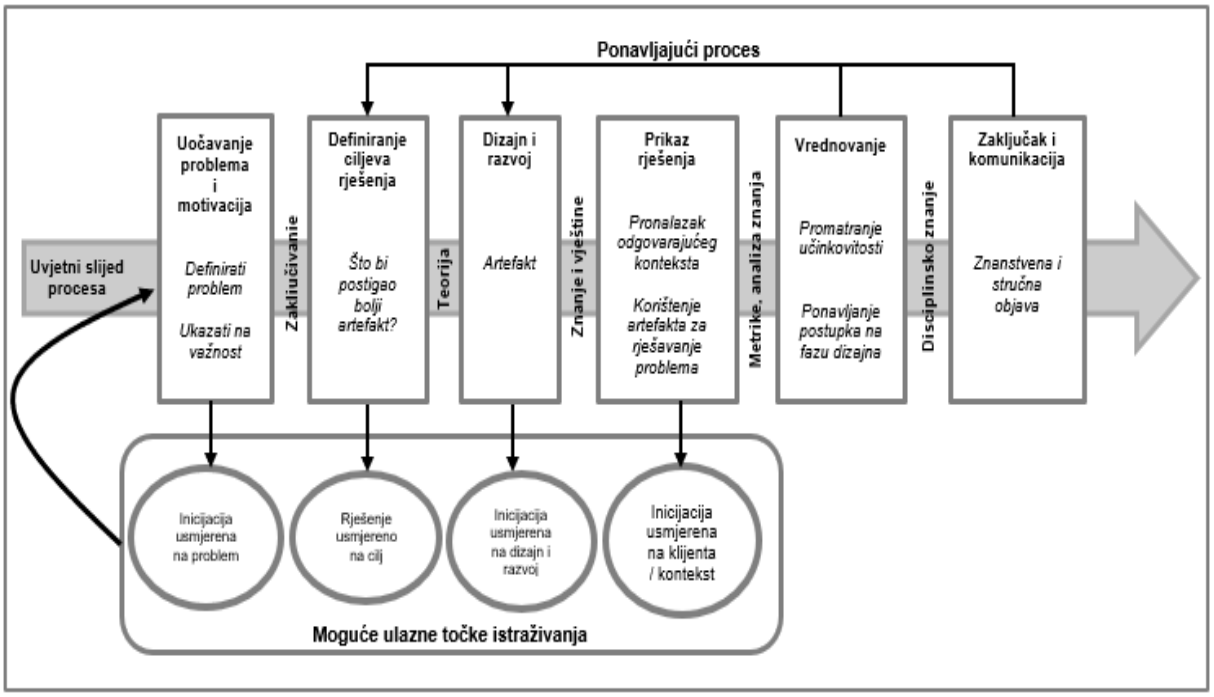
4.5. Metodologija istraživanja

4.5.1. Znanstveni dizajn

Kao metodološki pristup u ovom istraživanju korištena je paradigma znanstveni dizajn (eng. *Design Science*) koja se koristi za potrebe istraživanja ponajprije u inženjerstvu, ali u novije vrijeme i u informacijskim znanostima, te nudi specifične smjernice za procjenu i ponavljanja unutar istraživačkih projekata [15], [16]. Svaki dizajn se prvenstveno bavi sintezom, gdje dizajner kombinira različite dijelove, elemente, koncepte i procese kako bi definirao novu cjelinu, pri čemu je naglasak na pronalasku adekvatnog uređenja dijelova iako određeni elementi mogu već postojati. Artefakti su krajnji proizvodi aktivnosti u dizajnu odnosno projektiranju.

Istraživanje korištenjem ove paradigme uključuje stvaranje novih znanja projektiranjem novih ili inovativnih artefakta (stvari ili procesa) te analizom korištenja i/ili izvedbe takvih artefakta – kako bi se poboljšalo i razumjelo ponašanje aspekata informacijskog sustava. Artefakti mogu uključivati, ali nisu limitirani, algoritme (npr. za dohvaćanje informacija), računalna sučelja te sistemski dizajn metodologija ili programskih jezika. Istraživači znanosti o dizajnu mogu se pronaći u mnogim disciplinama i područjima, posebno u inženjerstvu i računalnim znanostima, pri čemu se koriste različiti pristupi, metode i tehnike [16].

Osnovni tipovi artefakta su konstrukti, modeli, metode i implementacije. Kao i u prirodnim znanostima, postoji potreba za osnovnim jezičnim konceptima, tj. konstruktima pomoću kojih bi se okarakteriziralo pojave. Osnovni konstrukti se mogu formirati u konstrukte višeg reda koji se nazivaju modelima, a koriste se za opis zadataka, situacija ili artefakta. Dizajnom se mogu razvijati i metode koje predstavljaju skupove slijednih koraka za obavljanje određenih aktivnosti u svrhu postizanja definiranih ciljeva. Svi navedeni tipovi artefakta mogu se implementirati s ciljem izvođenja određenih zadataka ili primjene artefakta u nekom okruženju. Istraživači koji koriste metodologiju znanstvenog dizajna nastoje izraditi modele, metode i implementacije koje su inovativne i vrijedne. Znanstveni dizajn se sastoji od dvije osnovne aktivnosti: kreiranje i vrednovanje. Kreiranje je proces izrade artefakta za specifičnu svrhu, a vrednovanje je proces u kojemu se određuje uspješnost artefakta [59].



Slika 4.1: Procesni model istraživačke paradigme znanstveni dizajn [15]

Metodologija znanstvenog dizajna sastoji se od šest slijednih procesnih faza (Slika 4.1), koje su sljedeće [15]:

1. *Uočavanje problema i motivacija*: Definira se specifični istraživački problem i opravdava vrijednost rješenja. Budući da se definicija problema u kasnijoj fazi istraživanja koristi za razvoj artefakta koji bi trebao pružiti učinkovito rješenje, korisno je konceptualizirati problem tako da rješenje obuhvaća njegovu složenost i moguća ograničenja (predstavljeno u poglavlju *6.1.1. Konceptualni model*). Obrazloženje vrijednosti rješenja motivira istraživača da nastavi potragu za rješenjem i prihvati rezultate te pomaže razumijevanju zaključaka istraživanja. Resursi potrebni za ovu aktivnost uključuju poznavanje stanja problema i važnost rješenja istoga.
2. *Definiranje ciljeva istraživanja*: Ciljevi istraživanja se utvrđuju iz definicije problema i znanja o tome što je moguće i izvedivo. Ciljevi mogu biti kvantitativni ili kvalitativni i trebali bi biti racionalno izvedeni iz specifikacije problema. Resursi potrebni za ovu fazu uključuju poznavanje stanja problema i trenutna rješenja, ako ih ima, te njihovu učinkovitost.
3. *Dizajn i razvoj*: Izrada novog artefakta, npr. novi konstrukti, modeli, metode ili instance. Artefakt istraživanja može biti bilo koji dizajnirani objekt u kojem je doprinos istraživanja ugrađen u dizajn. Ova aktivnost uključuje određivanje željene

funkcionalnosti i arhitekture artefakta te zatim i kreiranje stvarnog artefakta. Potrebni su resursi za dizajn i razvoj te teorijsko znanje koje se može pretvoriti u konačno rješenje.

4. *Prikaz rješenja*: Prikaz uporabe artefakta za rješavanje jednog ili više slučajeva problema. To može uključivati njegovu upotrebu u eksperimentiranju, simulaciji, studiji slučaja, dokazima ili drugim odgovarajućim aktivnostima. Resursi potrebni za demonstraciju uključuju učinkovito znanje o tome kako koristiti artefakt za rješavanje problema.
5. *Vrednovanje*: Promatranje i mjerenje koliko dobro artefakt podržava rješenje problema. Ova aktivnost uključuje usporedbu ciljeva rješenja sa stvarnim promatranim rezultatima korištenja artefakta u demonstraciji. To zahtijeva poznavanje relevantnih metrika i tehnika analize. Ovisno o prirodi problema i artefakta, evaluacija može imati različite oblike pa tako može uključivati stavke kao što su usporedba funkcionalnosti artefakta s ciljevima rješenja ili mjerenje performansi (npr. vrijeme odziva ili dostupnost). Konceptualno, takva procjena može uključivati bilo koji odgovarajući empirijski ili logički dokaz. Na kraju ove aktivnosti istraživači odlučuju hoće li se vratiti na treći korak (*Dizajn i razvoj*) kako bi poboljšali učinkovitost artefakta ili će prijeći na fazu komunikacije i ostaviti daljnja poboljšanja za buduća istraživanja ili projekte. Priroda konkretnog istraživanja može uvjetovati je li takva iteracija izvediva ili ne.
6. *Zaključak i komunikacija*: Komunikacija problema i njegove važnosti te artefakta i njegove korisnosti, inovativnosti, strogosti dizajna i učinkovitosti ostalim istraživačima i zainteresiranoj publici. U znanstvenim istraživačkim publikacijama, istraživači mogu koristiti strukturu ovog procesa za strukturiranje svojih radova, baš kao što je i nominalna struktura empirijskog istraživačkog procesa (definiranje problema, pregled literature, razvoj hipoteza, prikupljanje podataka, analiza, rezultati, rasprava i zaključak) uobičajena struktura za empirijska istraživanja.

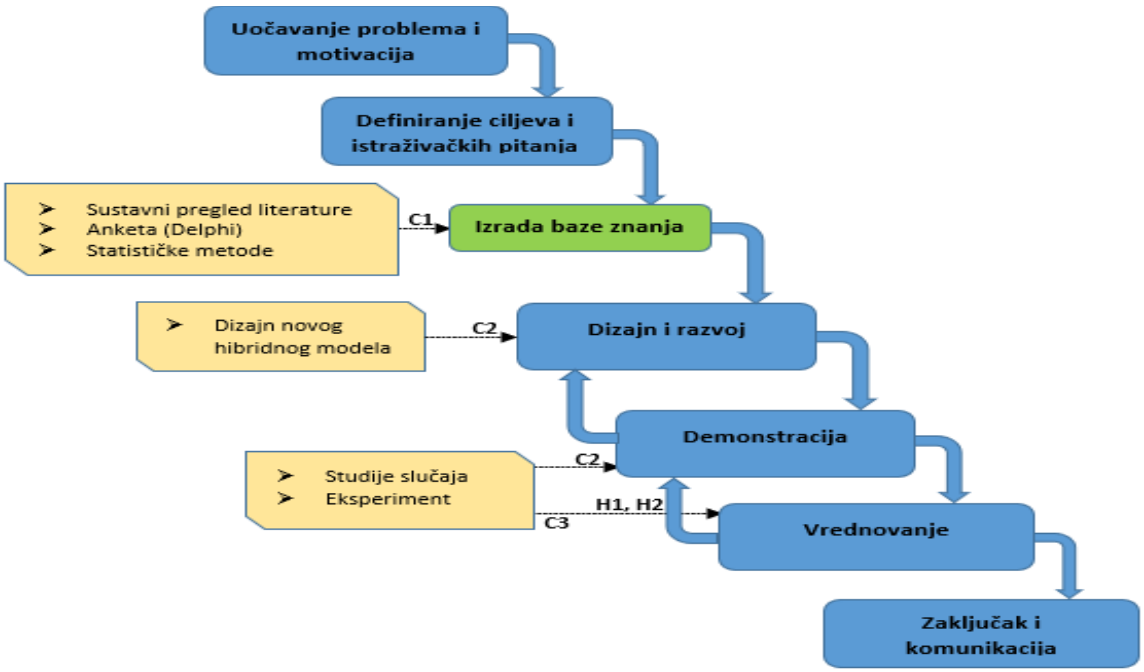
Osim prema opisanoj paradigmi znanstvenog dizajna, istraživanje u sklopu ovog doktorskog rada napravljeno je i prema određenim smjernicama za provedbu istraživanja temeljenog na dizajnu [60].

Tablica 4.1: Smjernice za istraživanje temeljeno na dizajnu [60]

Smjernica	Opis
1. Dizajn kao artefakt	Istraživanje temeljeno na dizajnu mora proizvesti održiv artefakt u obliku konstrukta, modela, metode ili instance.
2. Relevantnost problema	Cilj istraživanja temeljenog na dizajnu je razvoj tehnoloških rješenja za važne i relevantne poslovne probleme.
3. Evaluacija dizajna	Korisnost, kvaliteta i učinkovitost artefakta moraju se strogo dokazati dobro provedenim metodama evaluacije.
4. Doprinos istraživanja	Učinkovito istraživanje u području znanstvenog dizajna mora pružiti jasne i provjerljive doprinose u područjima dizajna artefakta, dizajnerskih osnova i/ili metodologije dizajna.
5. Istraživački zahtjevi	Istraživanje temeljeno na dizajnu oslanja se na primjenu strogih metoda u konstrukciji i procjeni artefakta dizajna.
6. Dizajn kao istraživački proces	Potraga za učinkovitim artefaktom zahtijeva korištenje dostupnih sredstava i načina za postizanje željenih ciljeva uz zadovoljavanje zakona u problemskom okruženju.
7. Komunikacija istraživanja	Istraživanje temeljeno na dizajnu mora se učinkovito predstaviti publici orijentiranoj prema tehnologiji kao i publici orijentiranoj na menadžment.

4.5.2. Faze, metode, tijek i opseg istraživanja

Prema smjernicama za provedbu istraživanja temeljenog na dizajnu [60], planirana je i provedena dodatna aktivnost u istraživačkoj metodologiji, a riječ je o izradi baze znanja (eng. *knowledge base*) [61], gdje je cilj obaviti detaljan pregled istraživačkih područja i pokazati kako trenutno nema rješenja za uočeni istraživački problem. Tako je definiran konačni skup svih istraživačkih aktivnosti koje su provedene u sklopu izrade ovog doktorskog rada:



Slika 4.2: Istraživački proces i znanstvene metode

Sa Slike 4.2 jasno se mogu vidjeti sve istraživačke faze kao i znanstvene metode koje su korištene u svrhu ovog istraživanja i izrade doktorskog rada. Također, prikazani su i ciljevi koji se ostvaruju pojedinim znanstvenim metodama unutar svake faze te hipoteze.

1. faza: *Uočavanje problema i motivacija*: Problem zapravo proizlazi iz prakse, a to je nepostojanje resursno učinkovite (troškovno i vremenski) metode ili modela za procjenu kritičnih informacijskih sustava u financijskoj instituciji u svrhu donošenja prikladne odluke o odabiru adekvatnog IT rješenja. Svrha istraživanja i motivacija već su detaljnije predstavljeni u poglavlju *2. Uočavanje problema i motivacija*.
2. faza: *Definiranje ciljeva i istraživačkih pitanja*: U poglavlju *4.1. Ciljevi istraživanja,* već je predstavljen općeniti odnosno glavni cilj istraživanja (učinkovitije donošenje informirane odluke o odabiru i implementaciji te stanju sigurnosti kritičnog informacijskog sustava u financijskoj instituciji izradom novog hibridnog modela) kao i specifični ciljevi. U poglavlju *4.2. Istraživačka pitanja,* definirana su ukupno 3 istraživačka pitanja.
3. faza: *Izrada baze znanja*: Provedena je primjenom metode sustavnog pregleda literature i *Delphi* istraživačke tehnike. Te metode su korištene kao sredstvo vrednovanja i tumačenja dostupnih istraživanja iz definiranih istraživačkih domena. Baza znanja služi kao referentna točka za višekriterijski model. Metoda sustavnog pregleda literature i *Delphi* tehnika kao i dobiveni rezultati detaljno su predstavljeni u poglavlju *5. Izrada baze znanja*.
4. faza: *Dizajn i razvoj*: Ova faza započinje izradom konceptualnog modela pri čemu se prikazuje generalizacija rješenja uočenog problema. Nakon toga prelazi se na fazu razvoja novog višekriterijskoga modela pri čemu se definiraju pretpostavke i ograničenja istoga. Ulazni parametri (tj. elementi za analizu i procjenu rizika) za novi model dobiveni su *Delphi* istraživačkom tehnikom, što je također zapisano u bazu znanja. *Dizajn i razvoj* je najvažnija faza istraživanja gdje se nastoje ostvariti istraživački cilj **C2**, a način provedbe i dobiveni rezultati predstavljeni su u poglavlju *6.1 Dizajn i razvoj modela*.
5. faza: *Demonstracija*: Kreirani artefakt (tj. novi hibridni višekriterijski model) predstavljen je pomoću komponenti (tj. razvojnih faza) više razine višekriterijskog modela, zatim kroz hijerarhijski prikaz modela s generičkim ISRA elementima za procjenu kritičnih IT sustava te preko mrežnog prikaza modela pomoću klastera.
6. faza: *Vrednovanje*: Kreirani artefakt evaluiran je kroz identične studije slučaja kao i u fazi demonstracije kako bi se moglo vršiti procjenu novog modela na temelju

definiranih metrika **M1** i **M2**. U ovoj fazi se postavljene hipoteze **H1** i **H2** potvrđuju ili odbacuju.

7. faza: *Zaključak i komunikacija*: Određeni dijelovi istraživanja napravljeni u sklopu izrade ovog doktorskog rada objavljeni su u relevantnim znanstvenim časopisima na engleskom jeziku. Cilj je predstaviti rezultate istraživanja kao i otvorena pitanja za moguća buduća istraživanja široj znanstvenoj i stručnoj javnosti.

4.5.3. Očekivani znanstveni doprinos

Istraživanje temeljeno na DSRM metodologiji zahtijeva upotrebu strogih znanstvenih metoda prilikom izrade i vrednovanja artefakta. Učinkovita primjena baze znanja te odgovarajućih razvojih metoda osigurava kvalitetan znanstveni doprinos. Očekivani znanstveni doprinos koji proizlazi iz prethodno definiranih ciljeva, istraživačkih hipoteza i korištenih znanstvenih metoda je sljedeći:

- **D1**: Model s generičkim elementima za analizu i procjenu rizika primjenom višekriterijskog odlučivanja omogućava učinkovitije donošenje informirane odluke o stanju sigurnosti nekog kritičnog IT sustava te na taj način posljedično daje mogućnost financijskoj instituciji da kvalitetnije odgovori na sigurnosne prijetnje i rizike odabirom adekvatnog IT rješenja.
- **D2**: Sistematizacija znanja i koncepata o metodama za višekriterijsko odlučivanje pogodnih za primjenu u domeni informacijske sigurnosti zajedno sa metodama za analizu i procjenu rizika.

Uz očekivani znanstveni doprinos, novi višekriterijski model bi trebao biti uistinu i praktično primjenjiv u financijskoj industriji (banci) za stručnjake iz domene informacijske sigurnosti te posebno za donosioce odluka s ciljem olakšavanja i automatizacije procesa donošenja i vrednovanja informirane odluke, a što zapravo predstavlja i širi društveni doprinos.

5. Izrada baze znanja

Aktivnost izrade baze znanja ima za cilj obaviti detaljan pregled promatranih istraživačkih područja i pokazati kako trenutno ne postoji adekvatno rješenje za problem kojim se predloženo istraživanje bavi. U ovom poglavlju rezultati dobiveni istraživačkim metodama sustavnog pregleda literature i *Delphi* anketnom tehnikom predstavljaju osnovu za izradu baze znanja sa svrhom kako bi se u narednoj istraživačkoj fazi *Dizajn i razvoj* moglo konačno kreirati ciljani višekriterijski model za procjenu kritičnih informacijskih sustava. U ovom poglavlju predstavit će se i prethodna relevantna istraživanja autora vezano uz ISRA i MCDM domene.

5.1. Sustavni pregled literature

Istraživanja većinom započinju nekim oblikom pregleda literature. Tako se pregled literature mora obaviti temeljito i nepristrano kako bi se dobilo određenu znanstvenu vrijednost. Ovo poglavlje daje pregled relevantne i recentne literature iz obje istraživačke domene, a to su upravljanje ricizima informacijske sigurnosti i problematika višekriterijskog odlučivanja, pri čemu su identificirani standardi, metode, tehnike i alati koji se smatraju najznačajnijima u promatranim istraživačkim područjima.

5.1.1. Metodologija za pregled literature

Pregledu literature iz znanstvenih bibliografskih baza pristupilo se primjenom smjernica za sustavni pregled literature (eng. *Systematic Literature Review*, SLR) u programskom inženjerstvu autora B. Kitchenham i S. Charters [73]. SLR predstavlja formaliziran i ponovljiv postupak za dokumentiranje relevantnog znanja u određenom istraživačkom području. To je zapravo oblik sekundarnog istraživanja koji koristi dobro definiranu metodologiju za identifikaciju, analizu i tumačenje svih dostupnih dokaza povezanih sa određenim istraživačkim pitanjem na način koji je nepristran i (u određenoj mjeri) ponovljiv. Glavni cilj istraživanja SLR postupkom je pronaći ISRA i MCDM standarde, metode i tehnike koji se zajedno koriste rješavajući višekriterijski problem vezano uz procjenu i rangiranje sigurnosnih rizika informacijskih sustava. Sustavni pregled literature kao i pripadajući rezultati su, u skladu s

metodologijom istraživanja i izrade ovog doktorskog rada, objavljeni u znanstvenom časopisu s međunarodnom recenzijom [142].

Sustavni pregled literature odrađen je u 3 slijedne faze:

1. Pregled primjene najznačajnijih ISRA/ISRM metoda i standarda
2. Pregled primjene najznačajnijih MCDA/MCDM metoda i tehnika
3. Pregled literature vezano uz primjenu MCDM metoda u području IT sigurnosnih rizika.

SLR proces je pokrenut identifikacijom odgovarajućeg istraživačkog pitanja u svakoj od tri definirane faze. Odluka je bila da se SLR istraživanje treba usredotočiti na znanstvene bibliografske citatne baze umjesto na specifične knjige ili znanstvene časopise. Tako je SLR proveden primjenom sljedeće strategije i pravila na definiranim citatnim bazama u sve tri faze. Strategija i kriteriji provedbe SLR-a prikazani su u Tablici 5.1:

Tablica 5.1: Strategija i kriteriji provedbe SLR-a

Izvor podataka:	Elektroničke znanstvene citatne baze podataka
Imena pretraživanih baza i kriteriji pretraživanja:	• **Web of Science Core Collection**, https://www.webofknowledge.com/ ○ Kategorije pretraživanja po fazama: ▪ Faza 1: računalne znanosti (eng. *Computer Science*), informacijski sustavi (eng. *Information Systems*) i telekomunikacije (eng. *Telecommunications*) ▪ Faza 2: operacijska istraživanja (eng. *Operations Research*), primijenjena matematika (eng. *Applied Mathematics*) i menadžment (eng. *Management*) ▪ Faza 3: operacijska istraživanja, primijenjena matematika, menadžment, računalne zananosti i telekomunikacije ○ Vrste dokumenata: članak (eng. *Article*), rad iz zbornika (eng. *Proceedings paper*) ○ Ograničenje: prvih 10 stranica rezultata (10 rezultata po stranici) ○ Odvajanje (eng. *sort*): po važnosti (eng. *by relevance*) • **IEEE Xplore Digital Library**, https://ieeexplore.ieee.org/ ○ Vrsta sadržaja: konferencije, časopisi ○ Ograničenje: prvih 4 stranice rezultata (25 rezultata po stranici) ○ Odvajanje: po važnosti • **ScienceDirect**, https://www.sciencedirect.com/ ○ Vrsta članka: istraživački članci (eng. *Research Articles*) ○ Ograničenje: prvih 4 stranice rezultata (25 rezultata po stranici) ○ Odvajanje: po važnosti • **Google Scholar**, https://scholar.google.com/ ○ Ograničenje: prvih 10 stranica rezultata (10 rezultata po stranici) ○ Odvajanje: po važnosti • **SpringerLink**, https://link.springer.com/ ○ Vrsta sadržaja: radovi s konferencija, članci ○ Disciplina: računalne znanosti ○ Ograničenje: prvih 5 stranica rezultata (20 rezultata po stranici) ○ Odvajanje: po važnosti

Strategija pretraživanja te kriteriji uključivanja i isključivanja znanstvenih radova:	• Pretraživački upit napravljen koristeći Boole-ovu algebru (AND i OR operatori) u svakoj od faza pretraživanja: ▪ Faza 1: *("Information Security Risk") AND ("Management" OR "Assessment" OR "Analysis") AND ("Standards" OR "Methods" OR "Methodology" OR "List" OR "Comparisons")* ▪ Faza 2: *("Multiple-criteria") AND ("Decision") AND ("Making" OR "Method" OR "Technique" OR "Analysis" OR "Comparison")* ▪ Faza 3: *("Information" OR "Security") AND ("Risk Management" OR "Risk Assessment") AND ("AHP" OR "ANP" OR "TOPSIS" OR "VIKOR" OR "ELECTRE" OR "PROMETHEE")* • Uključeni radovi isključivo na engleskom jeziku koji su objavljeni u znanstvenom časopisu ili prezentirani na znanstvenoj konferenciji (zbornici radova) • Radovi se nužno moraju odnositi na istraživačko pitanje definirano unutar pojedine SLR faze • Poglavlja iz knjiga, enciklopedije, patenti, vijesti, rasprave, kratka priopćenja, softverske publikacije, video zapisi i ostale vrste članaka su isključeni • Naglasak je stavljen na izvorne istraživačke radove te su prema tome isključeni ostali pregledni radovi • Duplicirani radovi pronađeni u više od jedne citatne baze brojali su se samo jednom kod računanja pojavnosti odnosno zastupljenosti pojedine ISRA ili MCDM metode/standarda/tehnike • Radovi koji nisu izričito vezani uz tematiku analize, procjene i tretmana rizika informacijske sigurnosti te u kojima nije analizirana ili primijenjena neka od ISRA i/ili MCDM metoda su isključeni • U radovima u kojima se analiziralo ili koristilo više ISRA ili MCDM metoda, za svaku metodu se posebno bilježila pojavnost • Radovi za koje je pronađena obavijest o povlačenju (eng. *Notice of Retraction*) nisu analizirani • Ključan kriterij za uključivanje radova u pregled i statistiku: stvarna analiza ili primjena ISRA ili MCDM metode je nužna, a ne samo referenca u tekstu prema ISRA ili MCDM metodi • Vremenski okvir objave radova za SLR analizu: o Faza 1 i faza 2: 2006 – 2018 o Faza 3: 2012 – 2018. Razlog skraćivanja vremenskog razdoblja objavljenih članaka u trećoj SLR fazi je taj kako se želi pronaći samo najnovije radove u kojima se MCDM metode primjenjuju u svrhu analize i procjene rizika informacijske sigurnosti. • Kako bi određeni rad bio odabran, isti mora zadovoljiti sve navedene kriterije uključivanja odnosno isključivanja
Datum pretraživanja:	16.01.2019.- 29.03.2019.

Navedene citatne baze su odabrane zbog njihove mogućnosti pribavljanja radova iz značajnih i cjelovitih časopisa i zbornika konferencija. Odabrane znanstvene baze podataka imaju vrlo dobro pokrivanje radova vezanih uz ISRA i MCDM teme.

Jedna od poteškoća na koju se naišlo u ovom istraživanju vezano uz primjenu ISRA i MCDM metoda bila je potreba da se u cijelosti i detaljno provjeri velika većina radova pronađenih pretraživanjem znanstvenih citatnih baza kako bi se mogli napraviti relevantni statistički podaci i zaključci. Stoga su se svi radovi pronađeni tijekom istraživanja morali detaljno analizirati s obzirom kako osnovni pregled naslova, sažetka, ključnih riječi i zaključka nisu bili dovoljni da bi se otkrilo koje su točno ISRA i MCDM metode, tehnike i standardi

stvarno korišteni i analizirani u pojedinom znanstvenom članku. Glavni nedostatak SLR istraživanja je taj što zahtijeva izrazito mnogo vremena i resursa kako bi se samo istraživanje provelo u potpunosti. Također, ograničenje SLR metodologije leži u njenoj strogosti pa tako neka od obećavajućih istraživanja ipak nisu odabrana u završnu analizu i statistiku iz razloga jer svi strogo postavljeni SLR kriteriji nisu bili u potpunosti zadovoljeni. Prema analizi SLR metodologije u programskom inženjerstvu [141], SLR se smatra vrlo korisnim i može se upotrijebiti za smanjenje pristranosti i povećanje kvalitete recenzije znanstvenih radova.

5.1.2. Pregled metoda za analizu i procjenu rizika informacijske sigurnosti

Cilj prve SLR faze je pokazati primjenu ISRA metoda i standarda u znanstvenim istraživanjima, a ne samo praktičnu uporabu u IT industriji.

Pitanje koje se postavlja temeljem definiranog specifičnog istraživačkog cilja **C1**, a vezano uz pregled literature za ISRA/ISRM standarde, metode i alate, jest sljedeće:

- *Koje metode i standardi za analizu i procjenu rizika informacijske sigurnosti su najznačajniji te najčešće evaluirani i primijenjeni u znanstvenim istraživanjima?*

Tako se istraživanju pristupilo na sljedeći način:

1. Pregled najznačajnijih industrijskih standarda i metoda iz područja upravljanja rizicima informacijske sigurnosti.
2. Pregled znanstvene literature iz relevantnih baza na temu procjene i upravljanja rizicima informacijske sigurnosti.

Kao polazna osnova za pregled relevantnih ISRA standarda, metoda i alata korištena je ENISA[5] dokumentacija [63], [64] temeljena na istraživanju do tada poznatih metoda i standarda za upravljanje i procjenu rizika informacijske sigurnosti. ENISA je kao polazna točka istraživanja ISRA metoda korištena i u nekim drugim istraživanjima [65], [66] te se svakako može smatrati vrlo relevantnim izvorom. Svrha ENISA-ina istraživanja bila je identificirati otvorene probleme u području upravljanja rizicima informacijske sigurnosti te pružiti putokaz za rješavanje daljnjih otvorenih pitanja na europskoj razini.

Treba dodati kako na ENISA-inim web stranicama postoji mogućnost međusobne usporedbe mnogih ISRA/ISRM standarda, metoda i alata [67] prema određenim zajedničkim kriterijima i karakteristikama, čime se zapravo na vrlo jednostavan i učinkovit način mogu

[5] *European Network and Information Security Agency (ENISA)* – Europska agencija za mrežnu i informacijsku sigurnost

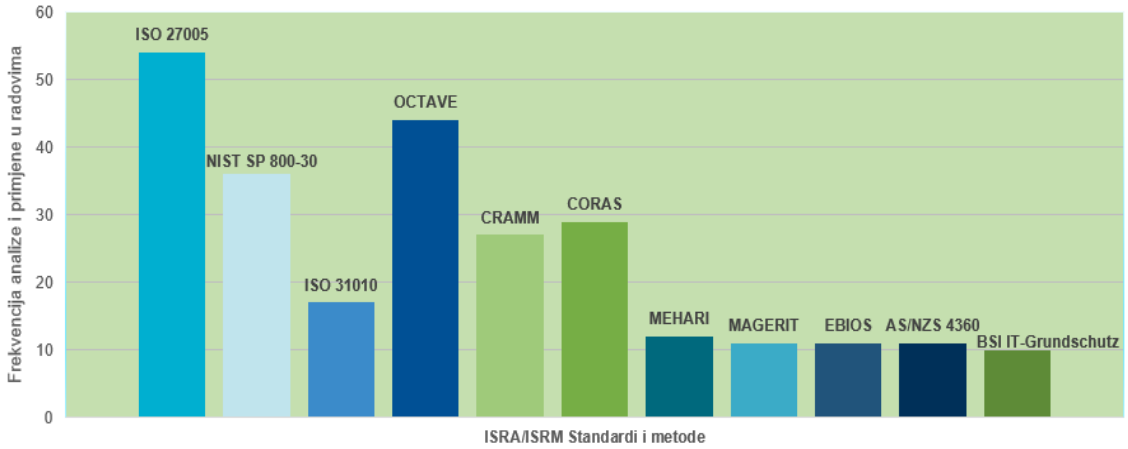
identificirati prednosti i nedostaci svake od njih te na temelju toga svaka organizacija može izabrati metodu koja najviše odgovara njenim potrebama i poslovnim ciljevima. ENISA repozitorij tako predstavlja najznačajniju referentnu točku pri analizi ISRA metoda.

Kao ostali relevantni izvori znanja o ISRA metodama i tehnikama uzeti su sljedeći znanstveni radovi iz časopisa:

- *Taxonomy of information security risk assessment (ISRA)* [68]: Napravljena je taksonomija za procjenu rizika informacijske sigurnosti iz čak 125 radova objavljenih od 1995. do svibnja 2014. godine. ISRA metode su podijeljene na profesionalne organizacije s jedne strane te istraživačke projekte s druge strane.
- *A Systematic Review of Information Security Risk Assessment* [69]: Napravljen je sustavni pregled literature s 80-ak pronađenih radova na temu rizika informacijske sigurnosti u razdoblju 2004-2014. Pri tome je napravljena klasifikacija radova i ISRA metoda.
- *Risk Management in Information Security: A Systematic Review* [70]: Napravljen je sistematski pregled glavnih bibliografskih baza s postavljenim istraživačkim pitanjem *Koje su najznačajnije metodologije i metode za upravljanje rizicima informacijske sigurnosti?*

Potom je uslijedilo provođenje sustavnog pregleda literature za ISRA metode i standarde na način definiran u Tablici 5.1.

Istraživanje u ovoj prvoj SLR fazi je pokazalo kako trenutno postoji izrazito veliki broj metoda, tehnika i alata te relativno mali broj industrijskih standarda za analizu, procjenu i upravljanje rizicima informacijske sigurnosti. Tako je s obzirom na definiranu strategiju pretraživanja te parametre uključivosti i isključivosti pronađeno ukupno 91 relevantnih radova na temu analize, procjene i upravljana rizicima informacijske sigurnosti.



Slika 5.1: Primjena ISRA metoda i standarda (izvor: autorov izračun)

Istraživanjem je uočeno (Slika 5.1) kako je dominantno analiziran i korišten međunarodni industrijski standard ISO/IEC 27005 (s različitim godištima izdanja) za potrebe analize, procjene, tretmana i upravljanja rizicima informacijske sigurnosti.

Treba napomenuti kako se radovi u kojima se spominjao standard ISO/IEC 27001 u kontekstu metode za analizu i procjenu rizika nisu uzimali u obzir za brojenje pojavnosti tog standarda jer se ISO/IEC 27001 ipak primarno koristi za izgradnju sustava za upravljanje informacijskom sigurnošću (eng. *Information Security Management System*, ISMS), dok je standard ISO/IEC 27005 iz serije ISO 2700x posebno namijenjen za analizu, procjenu, postupanje i upravljanje rizicima informacijske sigurnosti. Također, u ranije objavljenim znanstvenim radovima gdje se analiziralo ili referenciralo na ISO/IEC 13335-1 standard iz 2004., pojavnost se ipak računala za ISO/IEC 27005 s obzirom kako je ISO/IEC 13335-1 zamijenjen upravo navedenim novijim standardom iz serije ISO 2700x.

Osim nabrojanih standarda i metoda za analizu i procjenu rizika informacijske sigurnosti, pretragom se pronašlo i neke druge ISRA metode korištene u pojedinim radovima, ali s malom učestalošću primjene. Npr., OWASP metodologija za ocjenu rizika, CobIT 5 for Risk, FAIR, FMEA, TARA, MITRE, Microsoft vodič za upravljanje sigurnosnim rizicima, itd. Ove spomenute ISRA metode su također vrlo cijenjene i korisne u svijetu informacijske sigurnosti.

Također, uočeno je kako postoji određeni trend povećanja broja radova na temu upravljanja rizicima informacijske sigurnosti za definirani vremenski okvir pretraživanja radova u odnosu na godine unutar promatranog razdoblja, a što je zapravo i očekivano s obzirom na sve veću pojavu raznih oblika prijetnji te mnoštva pronađenih ranjivosti u informacijskim sustavima.

S obzirom na dominantnu zastupljenost standarda ISO/IEC 27005 u znanstvenim radovima te u praksi (uz određene prilagodbe za potrebe svake organizacije), logično je kako se kao osnova za definiranje skupa kriterija za analizu i procjenu rizika potrebnih za procjenu nekog kritičnog informacijskog sustava koristilo upravo funkciju rizika iz navedenog međunarodnog standarda.

5.1.3. Pregled metoda za višekriterijsko odlučivanje

Prema [71], metode za potporu odlučivanju (eng. *Decision-Making*, DM) mogu se identificirati prema 3 perspektive:

1. Višekriterijsko odlučivanje (eng. *Multicriteria decision making*, MCDM)
2. Matematičko programiranje (eng. *Mathematical programming*, MP)
3. Umjetna inteligencija (eng. *Artificial intelligence*, AI).

S obzirom na definiranu problematiku znanstvenog istraživanja i ciljeva koji su se namjeravali ispuniti, u ovom radu opisane su samo MCDM metode koje se prema istim autorima [71] mogu klasificirati u 4 kategorije:

(1) Metode s korištenjem više atributa (eng. *multiattribute utility methods*, MAUT), npr. AHP i ANP
(2) Metode nadmašivanja odnosno eliminacije (eng. *outranking methods*), npr. ELECTRE, PROMETHEE i QUALIFLEX
(3) Metode nagodbe (eng. *compromise methods*), npr. TOPSIS i VIKOR
(4) Ostale (jednostavne) MCDM tehnike, npr. SMART, DEMATEL i SAW.

Pitanje koje se postavlja temeljem definiranog specifičnog istraživačkog cilja **C1**, a vezano uz pregled literature za MCDA/MCDM metode, tehnike i alate, jest sljedeće:

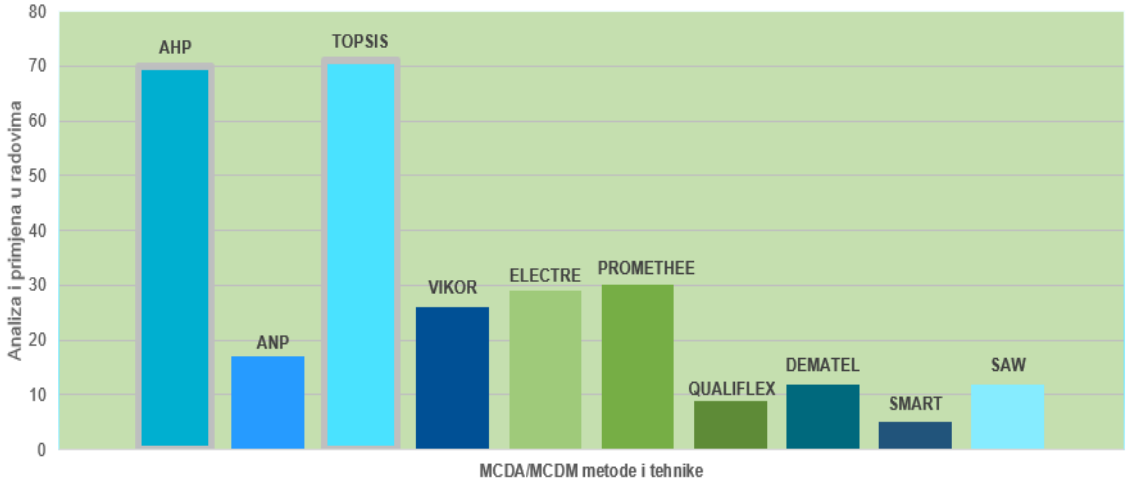
- *Koje metode, tehnike i alati za rješavanje problema višekriterijskog odlučivanja su najzastupljenije odnosno najčešće korištene u znanstvenim istraživanjima?*

Kao inicijalni relevantni izvori znanja o MCDM metodama, tehnikama i alatima korišteni su sljedeći znanstveni radovi i knjige:

- *Mathematical foundations of the methods for multicriterial decision making* [72]: Ovaj znanstveni rad opisuje matematičke osnove najznačajnijih metoda za višekriterijsko odlučivanje.
- *Application of decision-making techniques in supplier selection: A systematic review of literature* [71]: Rad daje sustavni pregled tehnika za potporu odlučivanju te njihovu (prethodno spomenutu) klasifikaciju.
- *Multiple Attribute Decision Making: Methods and Applications* [41]: U ovoj knjizi autori detaljno objašnjavaju problematiku višekriterijskog odlučivanja kao i najznačajnije metode te njihovu primjenu.
- *Poslovno odlučivanje* [18]: Autori pokušavaju odgovoriti na sva relevantna pitanja teorije i prakse poslovnog odlučivanja s konkretnim primjerima.

Potom je uslijedilo provođenje sustavnog pregleda literature za MCDM metode i tehnike na način definiran u Tablici 5.1.

Istraživanje u ovoj drugoj SLR fazi je pokazalo kako postoji značajan skup metoda, tehnika i alata koji se koriste kod rješavanja problema višekriterijskog odlučivanja, pri čemu je uočeno dominantno korištenje AHP i TOPSIS metoda i njihovih neizrazitih (eng. *fuzzy*) inačica, pri čemu su te dvije metode podjednako zastupljene, a što je vidi na Slici 5.2.



Slika 5.2: Primjena MCDM metoda i tehnika – faza 2 (izvor: autorov izračun za objavljene znanstvene radove u razdoblju 2006-2018)

Tako je, s obzirom na definirane parametre uključivosti i isključivosti radova te strategiju pretraživanja, pronađeno ukupno čak 140 relevantnih radova iz citatnih baza vezano uz problematiku višekriterijskog odlučivanja na relativno malom uzorku (prvih 100 izlistanih radova pretrage iz svake od 5 indeksnih baza citata). Svakako je jako važno napomenuti kako se kod pojave podkategorija pojedine MCDM tehnike korištene u nekim istraživanjima sama pojavnost brojala za glavnu tehniku unutar MCDM familije. Npr., tako se za neizrazite (eng. *fuzzy*) AHP i TOPSIS metode, proširenu neizrazitu (eng. *fuzzy extended*) AHP metodu (FEAHP) te ELECTRE i PROMETHEE inačice nije radila zasebna statistika već se tehnike grupiralo prema pripadajućoj krovnoj generaciji MCDM tehnika.

Istraživanjem je uočeno kako su se u pojedinim radovima istraživale i primjenjivale još neke druge MCDM tehnike, ali s vrlo malom zastupljenošću, kao što su agregacijske metode (ARAS, WASPAS, SWARA, MOORA, MULTIMOORA i COPRAS), SC (eng. *Social Choice*), metoda eliminacije GAIA (eng. *Geometric Alanalysis for Interactive Aid*), MACBETH kao metoda s korištenjem više atributa te LINMAP metoda za višeatributno grupno odlučivanje.

5.1.4. Primjena MCDM metoda u svrhu procjene rizika informacijske sigurnosti

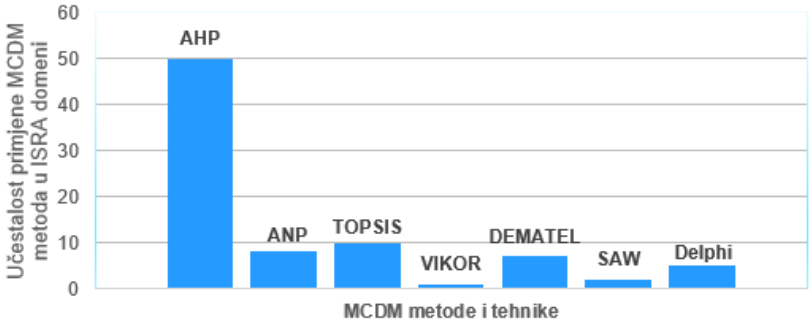
Treća faza istraživanja literature zapravo je i najvažnija jer se integriraju saznanja iz prethodne dvije faze kako bi se dobilo presjek primjena odnosno kombinacija ISRA i MCDM standarda, metoda i tehnika. U ovoj fazi istraživanja literature cilj je bio dobiti presjek istraživačkih područja, odnosno vidjeti na koji način se najznačajnije metode i tehnike za višekriterijsko odlučivanje koriste u svrhu analize, procjene, tretmana i generalno upravljanja sigurnosnim rizicima.

Istraživačko pitanje koje se postavlja u ovoj trećoj SLR fazi kako bi se konačno zadovoljilo ostvarenje specifičnog istraživačkog cilja **C1**, a vezano uz primjenu MCDM metoda u svrhu procjene rizika informacijske sigurnosti te na kraju ciljane procjene kritičnih IT sustava (ulazni parametri za ostvarenje specifičnog cilja **C2**), jest sljedeće:

- *Koje metode, tehnike i alati za rješavanje problema višekriterijskog odlučivanja se najviše primjenjuju u znanstvenim istraživanjima u svrhu procjene i upravljanja rizikom informacijske sigurnosti*?

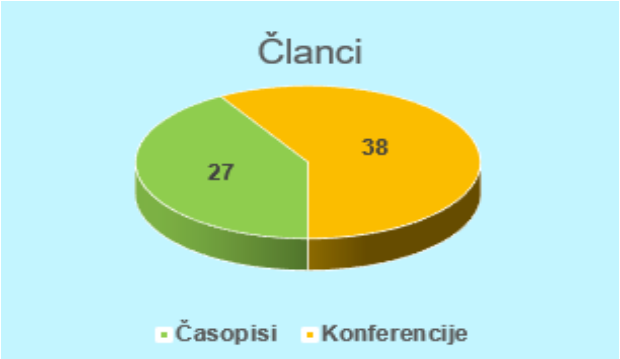
S obzirom na dobivene rezultate iz prethodnih faza pregleda relevantne literature, u skladu s tim je definiran i pretraživački upit na indeksne baze citata te je istraživanje provedeno na način definiran u Tablici 5.1. U ovoj zadnjoj SLR istraživačkoj fazi, dodatno je uključena i *ACM Digital Library* citatna baza kako bi istraživanje bilo još cjelovitije i preciznije. Tako su u *ACM Digital Library* bazi pronađena samo dva relevantna rada, a koji nisu pronađeni u ostalim pregledanim bazama.

Pregledom literature uočeno je kako postoji značajna primjena relevantnih MCDM metoda i tehnika u kontekstu procjene rizika za razna društvena, inženjerska ili medicinska područja. Npr., rizici softverskih projekata [74, 75, 76], rizici odabira servisa u oblaku, upravljanja odnosima s klijentima (eng. *Customer Relationship Management*, CRM), građevinskih projekata, odabira raznih dobavljača, zatim željezničkih, pomorskih i transportnih sustava, sigurnosti vodoopskrbnog sustava, nuklearnih elektrana, zdravstvenih sustava, eksternalizacije usluga za e-nabavu, kreditni rizici, itd. Ali, relativno manji broj pronađenih radova odnosi se konkretno na analizu i procjenu rizika informacijske sigurnosti ili evaluaciju IT sigurnosnih ili drugih poslovnih rješenja pomoću MCDM metoda u kombinaciji sa nekim ISRA standardom (metodom) ili njegovim elementima.



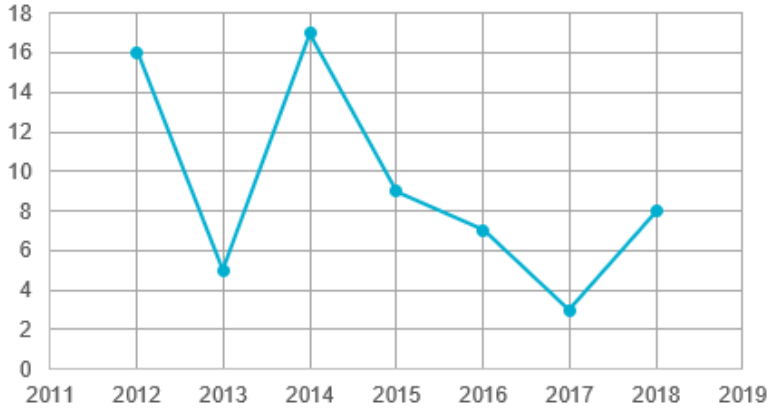
Slika 5.3: Korištenje MCDM tehnika u svrhu analize i procjene rizika po informacijski sustav ili odabira adekvatnog IT rješenja – faza 3

Na Slici 5.3 vidi se kako je izrazito dominantno korištena AHP metoda, a što se može pripisati relativnoj jednostavnosti primjene AHP metode te njenoj popularnosti među istraživačima. Izvor za određivanje broja korištenja MCDM tehnika su znanstveni radovi objavljeni u razdoblju 2012-2018. Pretraživanjem je pronađeno ukupno 65 relevantnih radova objavljenih na konferencijama ili u znanstvenim časopisima koji zadovoljavaju kriterije pretraživanja te daju odgovor na postavljeno istraživačko pitanje.



Slika 5.4: Raspodjela radova s kombinacijom ISRA i MCDM (autorov izračun za razdoblje 2012-2018)

Može se vidjeti na Slici 5.4 kako je nešto veći broj radova ipak prezentirano na konferencijama u odnosu na objave u znanstvenim časopisima.



Slika 5.5: Raspodjela radova po broju i godini izdanja (izvor: autorov izračun)

Na Slici 5.5 može se vidjeti trend objavljivanja znanstvenih radova po godinama. Više od 60 relevantnih radova pronađenih SLR pregledom uz vrlo strogo definirane kriterije pokazuje određenu popularnost primjene MCDM metoda u svrhu analize i procjene rizika informacijske sigurnosti, uz predviđanje daljnjeg rasta u budućim istraživanjima.

Završetkom treće faze sustavnog pregleda literature uspješno je ostvaren zadani specifični istraživački cilj **C1**.

5.1.5. Analiza radova i rasprava

U nastavku, prema SLR smjernicama, bit će predstavljeni i ukratko analizirani najznačajniji radovi identificirani pretraživanjem relevantne literature gdje je uočena primjena MCDM metoda u svrhu procjene rizika informacijske sigurnosti i procjene IT rješenja. Također, raspravit će se prednosti i nedostaci provedenog istraživanja, predstavit će se značaj nalaza za planirano istraživanje te će se prikazati strukturirane preporuke za primjenu MCDM metoda u polju upravljanja rizicima informacijske sigurnosti.

5.1.5.1. Analiza radova

Do radova za analizu došlo se detaljnim pregledom svakog znanstvenog rada tijekom SLR procesa pri čemu su za konkretnu analizu odabrani oni radovi koji su imali određeni značaj u vidu smjernica za razvoj novog višekriterijskoga modela. Npr., primjena određenih MCDM metoda u domeni rizika informacijske sigurnosti ili računanje utjecaja i zavisnosti između evaluacijskih elemenata. U analizi koja slijedi, najznačajniji radovi su grupirani i analizirani prema određenim tematskim cjelinama, npr. modeli za sigurnosne kontrole, sigurnost u oblaku, BCM, kritične IT sustave, sigurnosne incidente, itd.

- Predloženi modeli napravljeni za djelovanje sa sigurnosnim ICT kontrolama su sljedeći:
  Prema radu [78] predlaže se hibridna procedura za učinkovitiju evaluaciju razine rizika na informacijske sustave uzimajući u obzir isprepletene međuovisnosti između sigurnosnih kontrola primjenom DEMATEL i ANP metoda, a što je svakako vrlo važan indikator za tematiku ovog doktorskog rada u kontekstu međuovisnosti i utjecaja između elemenata za analizu i procjenu rizika informacijske sigurnosti.
  Yang et al. [92] predlažu hibridni model za procjenu performansi kontrola rizika informacijske sigurnosti (eng. *Information Security Risk-Control Assessment Model*,

ISRCAM) koji kombinira čak 3 MCDM metode (VIKOR, ANP i DEMATEL) u svrhu rješavanja problema konfliktnih kriterija s međusobnom ovisnošću i povratnim vezama. Taj model bi mogao pomoći IT i sigurnosnim menadžerima u razumijevanju kontrolnih područja ili ciljeva koje treba unaprijediti kako bi se uskladilo sa prihvatljivom razinom rizika (rezidualni rizik) po organizaciju. Korištenjem DEMATEL tehnike za izradu mape mrežnih odnosa (eng. *network relations map*, NRM) predloženi model može pomoći u analizi zašto određene sigurnosne kontrole imaju više manjkavosti (ranjivosti). Model upravljanja rizicima je nužno kontinuirani proces koji se temelji na PDCA (eng. *Plan-Do-Check-Act*) strategiji pa tako u ovoj studiji predloženi ISRCAM model ispituje učinkovitost kontrola u tzv. "Check" fazi.

Autori *N. Al-Safwani et al.* u svojim istraživanjima kombiniraju ISRA standard ISO/IEC 27005 sa TOPSIS metodom u svrhu poboljšanja procjene implementiranih kontrola informacijske sigurnosti [90] te predlažu ISCP (eng. *Information Security Control Prioritization*) model za odabir kritičnih sigurnosnih kontrola [91]. TOPSIS metoda se integrirala u koraku Identifikacija postojećih kontrola (eng. *Identification of Existing Controls*) tijekom procesa analize i identifikacije rizika unutar ISO/IEC 27005 okvira za upravljanje rizicima. Pritom se TOPSIS metoda zapravo koristila za određivanje i rangiranje kritičnih i ranjivih kontrola informacijske sigurnosti (tehničke kontrole) unutar IT odjela jedne tvrtke na temelju 5 evaluacijskih kriterija, a to su poznate ranjivosti (eng. *known vulnerabilities*), važeće ranjivosti (eng. *valid vulnerabilities*), vrsta napada (eng. *attack class*), ozbiljnost napada (eng. *severity of attacks*) i razina napora potrebnog za sanaciju (eng. *remediation effort level*). Kritične kontrole prema navedenim kriterijima su evaluirane od strane stručnjaka za procjenu i ispitivanje ranjivosti sustava (*Vulnerability Assessment and Penetration Testing*). Glavni cilj modela je zapravo smanjiti preveliko trošenje resursa u vidu troškova i vremena te optimizirati procjenu sigurnosnih kontrola.

- U sljedećim radovima predstavljeni su modeli koji upotrebljavaju standardne faktore za procjenu rizika:

  U radu [79] jasno su naznačena 4 faktora za procjenu rizika, a to su informacijska imovina, prijetnja po imovinu, ranjivost te postojeće (implementirane) sigurnosne protumjere. Također, predstavljen je AHP model za klasifikaciju informacijske imovine pri čemu su kao evaluacijski kriteriji uzeti već navedeni faktori za procjenu rizika, no u radu se ipak ne precizira na koje točno informacijske sustave bi se model primijenio te

nema definiranih nužnih (inherentnih) međuovisnosti između faktora za procjenu rizika (a što je zapravo ipak logično s obzirom kako je AHP model hijerarhijski i ne modelira zavisnosti između elemenata). Autor M.C. Lee [80] predlaže identične faktore za analizu rizika kao i u radu [79] s razlikom što su za svaki od 4 kriterija u AHP metodi dodatno definirani i pripadajući podkriteriji, npr. C-I-A[6] atributi za imovinu, okruženje i ljudski čimbenici za prijetnje, itd. Također, u radu [81] jasno su definirani osnovni elementi za procjenu rizika (imovina, prijetnja, ranjivost) zajedno sa pripadajućim kategorijama (npr. podaci, softver, sklopovlje, napadi na mrežnu okolinu, itd.), ali za razliku od [79, 80] uzimajući u obzir i odnose utjecaja između elemenata procjene rizika i neizvjesnost koja se stvara u procesu procjene rizika sigurnosti i privatnosti, te se predlaže novi model procjene rizika sigurnosti i privatnosti za informacijski sustav koji se temelji na DEMATEL-ANP kombinaciji sa teorijom sivog sustava (eng. *grey system theory*). U radu [82] na sličan način kao i u radu [79] definirani su osnovni elementi rizika pri čemu je analizirana njihova međusobna ovisnost, ali u kontekstu predviđanja rizika a ne procjene rizika informacijske sigurnosti temeljeno na ANP metodi u kombinaciji sa teorijom sivog sustava.

- Sljedeći paragraf prikazuje značajne radove vezane uz upravljanje kontinuitetom poslovanja, a što je jedna od najvažnijih sigurnosnih domena:
  Autori *Hiete et al.* [84] koriste DEMATEL tehniku u svrhu analize strukture složenih uzročno-posljedičnih veza između podindikatora ranjivosti o katastrofi (eng. *disaster vulnerability*). Ovaj rad je važan u kontekstu utjecaja moguće katastrofe na informacijski sustav i prvenstveno otpornosti (eng. *resilience*) na katastrofu što implicira na razinu dostupnosti (eng. *availability*) IS-a kao jednog od tri najvažnija atributa sigurnosti (C-I-A trojstvo). Element otpornosti je dosta često zapostavljen te nije dovoljno naglašena njegova važnost kod procjene stanja sigurnosti nekog informacijskog sustava pa iz toga zapravo i proizlazi značajnost navedenog istraživanja.
  Autori K.Y. Kim i K.S. Na u svom radu [85] predlažu TOPSIS metodu za sustavnu procjenu rizika s intervalnim podacima za rješavanje problema oporavka kritičnih poslovnih procesa, tj. njihovu prioritizaciju tijekom incidenta prekida poslovanja, a u svrhu upravljanja kontinuitetom poslovanja (eng. *Business Continuity Management*, BCM). Pritom su kao evaluacijski kriteriji korišteni učestalost pristupa (eng. *access*

[6] ***C****onfidentiality* – povjerljivost, ***I****ntegrity* – cjelovitost, ***A****vailability* – dostupnost informacijskog sustava

frequency), vrijeme pristupa (eng. *access time*), alternativno vrijeme rada (eng. *alternative work time*), RTO[7] (*Recovery Time Objective*) i iznos gubitka (eng. *loss amount*).

- U sljedećim predloženim modelima, najznačajniji atributi sigurnosti informacijskih sustava (C-I-A) korišteni su kao evaluacijski kriteriji:
  U radovima [86, 87], AHP metoda se koristila za procjenu rizika sa dvo-razinskim kriterijima za evaluaciju alternativa pri čemu se kao kriteriji prve razine koriste C-I-A sigurnosni atributi kao temeljni faktori utjecaja na kriterije druge razine za evaluaciju alternativa. H.J. Kim [88] predlaže AHP model također s C-I-A kriterijima za evaluaciju i rangiranje sigurnosnih kontrola definiranih prema standardu NIST SP 800-53 [89], a koje su nužne za implementaciju u svrhu procjene sigurnosnog rizika i adekvatne zaštite sustava socijalne mreže (Facebook, Twitter, LinkedIn, itd.).

- Sljedeći predloženi modeli i metode odnose se na računalne sustave u oblaku:
  Autori Li i Bardi [95] predlažu model za evaluaciju 4 karakteristična faktora utjecaja koji induciraju rizik za računarstvo u oblaku (eng. *Cloud Computing*), a to su imovina, ranjivost, prijetnja i kontrolne mjere, a koji su evaluirani korištenjem AHP metode i višerazinskog neizrazitog ocjenjivanja (eng. *multi-level fuzzy evalution*). Autori *Ruo-xin et al*. [96] dodatno predlažu holistički višerazinski model indeksnog sustava za procjenu sigurnosti računalstva u oblaku pri čemu su korišteni *Delphi* tehnika i AHP metoda. Dodatno, u radu [97] predlaže se strategija za procjenu rizika računalstva u oblaku primjenom *Delphi* tehnike za strukturiranje ključnih faktora (kriterija) rizika te ANP metode za definiranje međuovisnosti i utjecaja između definiranih kriterija i podkriterija kao i neophodni izračuni njihovih težina. Pri tome je privatnost (eng. *privacy*) naznačena kao najznačajniji faktor rizika. S druge strane, u radu [98] predlaže se metoda za dinamičku federaciju entiteta u oblaku temeljeno na procjeni rizika korištenjem AHP metode, gdje je osnovna ideja izbjeći potrebu za inicijalnom uspostavom povjerenja (eng. *trust*) između različitih entiteta koji se žele udružiti s ciljem lakšeg (*ad-hoc*) stupanja u federaciju. Metoda se čini dosta revolucionarnom, ali i teško primjenjivom u korporativnom okruženju (posebno financijskim institucijama) zbog konteksta računalstva u oblaku koje za jednu od svojih osnovnih karakteristika

[7] ***R**ecovery **T**ime **O**bjective* (*RTO*) – najduže moguće vrijeme tijekom kojeg poslovni proces može biti nedostupan prije nego što se ponovo uspostavi, tj. oporavi.

vezano uz dijeljenje resursa od strane više entiteta (eng. *multitenancy*) sa sobom nosi inherentne faktore rizika, kao što su prvenstveno regulatorni, jurisdikcija i privatnost (eng. *privacy*).

- Radovi koji se odnose se na kreirane AHP modele za kritične elektroenergetske sustave: Autori *Farzan et al.* [100] predlažu metodologiju za identifikaciju kritičnih podcentrala i procjenu kibernetičkih rizika u električnoj mreži (eng. *power grid*). U prvoj fazi predložene metodologije identificira se najkritičnija podcentrala unutar električne mreže koristeći AHP metodu i (*N-1*) simulacijsku analizu kako bi se izračunao indeks rizika za podcentrale unutar električne mreže. Druga faza metodologije se odvija na razini podcentrale kako bi se identificiralo njene najkritičnije komponente. Nakon toga slijedi popravak (tretman) najkritičnijih ranjivosti električne podcentrale s ciljem optimizacije investicija (troška) i smanjenja sigurnosnih rizika s obzirom na sveprisutne prijetnje kibernetičih napada od strane malicioznih hakera. Autori *Y. Ru et al.* Također se bave problematikom procjene rizika informacijskog sustava električne mreže, ali u kontekstu mogućeg kibernetičkog napada na sâm SCADA sustav [101]. U ovom slučaju metoda za kvantitativnu procjenu rizika se temelji na modelu stabla napada (eng. *attack tree*) i AHP metodi. Pritom su se za kvantifikaciju indeksa rizika u AHP-u koristili sljedeći atributi: gubitak paketa (eng. *Loss of data packets*), kašnjenje u komunikaciji (eng. *Communication delay*), šteta po sekundarnu opremu (eng. *Harm to the secondary equipment*), utjecaj na rad mreže (eng. *Influence on grid operation*) i ekonomski gubici (eng. *Economic losses*). Nedostatak ovog pristupa je taj što se ne uzimaju u obzir međusobne ovisnosti i povratne veze između navedenih elemenata, već se pretpostavlja njihova relativna međusobna neovisnost.

- U sljedećem paragrafu analizirani radovi su grupirani prema korištenju Bayesove teorije vjerojatnosti zajedno s MCDM metodama u složenim modelima u svrhu procjene rizika informacijske sigurnosti:

  U radu [102], predlaže se Bayesova procedura prioritizacije (eng. *Bayesian prioritization procedure*, BPP) za potporu AHP grupnom odlučivanju (eng. AHP *Group Decision Making*, AHP-GDM) za procjenu rizika informacijske sigurnosti kod pojave nekompletnih informacija. MCDM metode se uglavnom temelje na pretpostavci da se dostavljaju potpuni podaci o svim parametrima modela (rezultati, težine atributa), a to u praksi vrlo često nije moguće pa tako donositelji odluka ne mogu izraziti $n \times (n-1)/2$

mogućih prosudbi u recipročnoj matrici usporedbi u parovima ili izražavaju nekonzistentne prosudbe. Upravo Bayesove metode omogućavaju tretman nepotpunih informacija koristeći tehnike povećanja podataka. Z. Tan i P. Li u svom radu [103] za potrebe procjene rizika informacijskih sustava također predlažu grupni AHP model odlučivanja čiji je cilj određivanje važnosti faktora rizika u kojemu su kao kriteriji evaluacije definirani vjerojatnost, utjecaj i neupravljivost (eng. *uncontrolability*), a predložene alternative su napadi na povjerljivost (eng. *confidentiality attacks*), uništenje cjelovitosti (eng. *integrity destruction*), napadi lažnog predstavljanja (eng. *impersonation attacks*), neautorizirani pristup (eng. *unauthorized access*) i uskraćenje usluge (eng. *denial of service*). Prema definiranim kriterijima rizičnosti evaluiraju se najznačajnije sigurnosne prijetnje po informacijski sustav kroz grupno odlučivanje kako bi se smanjio subjektivni utjecaj osobnih preferencija tijekom procesa evaluacije. Autori Wu i Zhao predlažu generički model procjene rizika za sigurnost privatnosti (eng. *privacy security*) u internetu stvari (eng. *Internet of Things*, IoT) na temelju Bayesovih mreža (eng. *Bayesian Networks*, BN) i DEMATEL tehnike za višekriterijsko odlučivanje [104]. Sigurnosni analitičar u ovom modelu koristi BN kako bi strukturirao mrežu širenja rizika (eng. *risk propagation network*) i generirao vjerojatnost pojave rizika na temelju zaključka o dokazima (eng. *evidence inference*). Tako donositelji odluka mogu lako pronaći relevantan put širenja (eng. *propagation path*) koji utječe na mnoge čimbenike rizika po imovinu. Prema zaključivanju u Bayesovim mrežama, može se također izračunati vjerojatnost svakog puta širenja. DEMATEL tehnika se pritom koristi za izračun težina utjecaja (eng. *influence weights*) za put širenja koji podržava učinkovito donošenje odluka o upravljanju rizikom za IoT sustave. To je zapravo model za rješavanje vjerojatnosne uzročnosti (eng. *probabilistic causality*) evaluacijskih faktora i dobivanje težina za odnose utjecaja (eng. *influence-relation*) na puteve širenja (eng. *propagation paths*). Model preuzima zaključivanje na temelju vjerojatnosti (eng. *probabilistic inference*) i generira vrijednosti za vjerojatnosti rizika za imovinu i puteve širenja pomoću Bayesove uzročno relacijske mreže i prethodne vjerojatnosti.

- Sljedeći radovi se odnose na modele napravljene za rješavanje sigurnosnih incidenata: Autori *Anuar et al.* [83] su kreirali vlastiti model rizika RIM (*Risk Index Model*) za ocjenu i rangiranje IT sigurnosnih incidenata korištenjem AHP metode pri čemu su dva glavna kriterija odlučivanja bili vjerojatnost pojave događaja i posljedica istoga od kojih je svaki od tih kriterija imao dodatno po 5 zasebnih neizvjesnih (eng. *uncertain*)

indikatora, npr. kritičnost imovine, kontrola, težina utjecaja, učestalost, osjetljivost, itd. Kombinacijom elemenata i indikatora za procjenu rizika zajedno sa AHP metodom, indeks rizika za svaki indikator je kvantitativno razvrstan i rangiran. Prema dobivenim rezultatima, novi model smanjuje broj incidenata i omogućava sigurnosnim analitičarima da se usredotoče isključivo na manji broj onih stvarnih i kritičnih incidenata čime se posljedično smanjuje utrošak vremena i resursa.

U članku [105], predložen je novi algoritam za rangiranje kibernetičkih sigurnosnih upozorenja (eng. *cyber security alerts*) za baze podataka. Cilj je bio razviti AHP model za prioritizaciju koji može rangirati upozorenja na razini rizika kojeg predstavlja transakcija olakšavajući tako sigurnosnim stručnjacima da usmjere svoje vrijeme i napore na najvažnija upozorenja. Predloženi *CyberRank* model je vrlo važan korak u smjeru korištenja neke MCDM metode sa uzorcima podataka sigurnosnog rizika kako bi se rangiralo određene alternative (u ovom slučaju sigurnosna upozorenja) kada postoji nesigurnost uzrokovana nedostatkom informacija, vremena i resursa. Podatkovni uzorci i Python skripte korišteni u ovom istraživanju su dostupni na *GitHub* repozitoriju za *CyberRank*[8] model.

- U zadnjem paragrafu analize znanstvenih radova predstavljeni su još neki važni pojedinačni radovi koji se nisu mogli svrstati u određeno istraživačko područje zbog nedostatka većeg broja radova iz tog područja:

  Članak [77] prikazuje primjenu kvantitativnog hibridnog modela dobivenog metodama modeliranja i sinteze u svrhu ocjenjivanja rizika informacijske sigurnosti kombinacijom FAHP i TOPSIS metoda pri čemu takav novi model, prema rezultatima autora rada, daje točnije rezultate s manjim postotkom pogreške u odnosu na neizrazitu (eng. *fuzzy*) FAHP metodu. Cilj je bio napraviti novi hibridni FAHP-TOPSIS model koji minimizira broj međusobnih usporedbi koje nužno proizlaze korištenjem AHP metode, a kako bi se dobilo veću točnost u procjenama odnosno niži koeficijent varijacije u odnosu na standardnu FAHP metodu. Stoga je napravljen *t-test* nezavisnih uzoraka za istraživanje razlike između FAHP metode i predloženog hibridnog modela te je novi predloženi model imao manji koeficijent varijacije što upućuje na manji postotak pogreške novog modela. Iako se u radu prilikom evaluacije spominje korištenje 3 razine kriterija rizika

[8] ***https://github.com/hagitGC/CyberRank***

informacijske sigurnosti, ipak se ne navodi koji su to točno kriteriji kao niti njihove izračunate težine, što je svakako manjkavost u ovom radu.

Autori Moeti i Kalema u svom su radu [94] identificirali metrike potrebne za izradu okvira za upravljanje informacijskom sigurnošću te ih klasificirali po kategorijama pri čemu je validacija metrika napravljena pomoću AHP metode. Rezultati studije upućuju na to kako su metrike iz okoline (eng. *environmental metrics*) ključne za upravljanje informacijskom sigurnošću, pri čemu toj kategoriji pripadaju prijetnje malicioznog kôda, inherentne ranjivosti informacijskog sustava i mreža te regulatorni i pravni okvir. No, iznenađuje kako je kategorija upravljanje rizicima (eng. *Risk Management*) rangirana kao zadnja od svih grupa metrika, što svakako može ukazivati na nedovoljnu svijest o važnosti adekvatnog upravljanja i procjene rizika informacijske sigurnosti od strane ispitivača koji su validirali predloženi okvir za mjerenje informacijske sigurnosti u akademskoj instituciji.

Kako bi se preciznije kvantificiralo prijetnje po imovinu i povezane ranjivosti, autori *Su et al.* [99] predlažu metodologiju da se procjena rizika sigurnosti računalne mreže napravi korištenjem AHP metode i neuronske mreže. Pri tome je proces analize sigurnosnih rizika definiran tako da je identifikacija informacijske imovine napravljena kroz identifikaciju kritičnih poslovnih procesa, što je zapravo ključan korak jer je pretpostavka ako je poslovni proces siguran tada je analogno tome sigurna i informacijska mreža. Nakon toga se dalje nastavilo s aktivnostima identifikacije prijetnji po informacijsku imovinu, zatim identifikacija ranjivosti koju svaka prijetnja može iskoristiti, izračun rizika za svaku imovinu i konačno izračun sistemskog rizika čitave informacijske mreže.

Kako bi se ostvarila transformacija iz kvalitativne u kvantitativnu analizu u obliku dinamičkog ciklusa vezano uz procjenu rizika informacijske sigurnosti, Meng [93] tako predlaže primjenu AHP metode za dobivanje težina faktora rizika nakon čega je primijenjena PDCA ciklička metoda u svrhu upravljanja rizicima za definirane faktore rizika (korišteni dvo-razinski evaluacijski faktori rizika IT sigurnosti s razinom kriterija te indeksnom podrazinom). Istraživanje je pokazalo kako su najznačajniji indeksni faktori rizika vezani uz sigurnost operacijskih sustava i sigurnost mreže.

5.1.5.2. Rasprava i preporuke

Sustavnim pregledom literature je uočeno kako se u gotovo svim istraživanjima želi napraviti određena kvantifikacija vezano uz procjenu i rangiranje sigurnosnih rizika, faktora koji utječu na rizik ili softverskih rješenja, a za što je potrebno koristiti neku od kvantitativnih MCDM metoda i tehnika. Takav pristup je vrlo cijenjen i predstavlja snagu istraživačkog polja jer MCDM metode imaju čvrste matematičke osnove, pri čemu je danas neophodna kvantifikacija razine rizika kojem su izloženi informacijski sustavi (u smislu novčanih vrijednosti) kako bi se sami rizici mogli izmjeriti i pomoći najvišem rukovodstvu u organizaciji da donese odgovarajuće (informirane) odluke.

Temeljem rezultata istraživanja jasno je kako postoje razni pristupi i metode za rangiranje rizika informacijske sigurnosti primjenom neke od kvantitativnih metoda za višekriterijsko odlučivanje te kako se u iznimno malom broju studija nastojalo integrirati neke osnovne ISRA elemente ili C-I-A atribute u AHP, ANP, DEMATEL ili TOPSIS metode. Uočeno je kako usko polje metoda za procjenu rizika informacijske sigurnosti za specifičnu svrhu evaluacije kritičnih IT rješenja primjenom višekriterijskog odlučivanja nije dovoljno istraženo u znanstvenim radovima. To predstavlja određene nedostatke u istraživačkom polju, ali je isto tako i vrlo važan putokaz za daljnja istraživanja i mogućnosti da se osnovni ISRA elementi prošire, definira njihova međusobna ovisnost te napravi integracija sa nekom od MCDM metoda u svrhu konkretne evaluacije kritičnih informacijskih sustava. Stoga se javlja potreba za novim hibridnim modelom za učinkovitiju procjenu kritičnih IT rješenja primjenom višekriterijskog odlučivanja i integracijom elemenata za procjenu rizika. Takav novi model bude važan doprinos u području informacijske sigurnosti, posebno u domeni rizika. Prema tome, već navedena i opisana istraživanja, posebno radovi [79, 81, 84, 92], su predstavljali okosnicu za daljnja istraživanja u svrhu izrade ovog doktorskog rada.

Također, istraživanjem literature uočeno je kako postoji trend izrade hibridnih modela za analizu i procjenu rizika i donošenje odluke o stanju sigurnosti ili odabiru prikladnog informacijskog sustava primjenom višekriterijskog odlučivanja (posebno naznačeno u radovima [78, 80]), a što je zapravo i logična pojava interdisciplinarnosti u istraživanjima s obzirom kako se upravljanje rizicima informacijske sigurnosti nužno integrira u druge poslovne domene te tako postaje jedna od prioritetnih aktivnosti u zaštiti imovine i poslovanja svake moderne organizacije.

Na temelju detaljno pregledanih 65 znanstvenih radova tijekom SLR istraživačkog procesa s ciljem otkrivanja primjene višekriterijskih modela u domeni upravljanja rizicima i

procjene rizika informacijske sigurnosti, u Tablici 5.2 daju se i određene preporuke za korištenje MCDM metoda za MCDM problem u domeni rizika informacijske sigurnosti. Tablica 5.2 zapravo predstavlja autorov doprinos u domeni rizika informacijske sigurnosti temeljeno na provedenom sustavnom pregledu literature dajući sistematizaciju preporučene primjene MCDM metoda za navedenu domenu sigurnosnih IT rizika.

Tablica 5.2: Preporuke za korištenje MCDM metoda u domeni rizika informacijske sigurnosti

MCDM metoda	MCDM problem
AHP	Preporučuje se za rješavanje problema kada ne postoje zavisnosti između kriterija procjene, npr.: • kada se koriste C-I-A atributi kao evaluacijski kriteriji za rangiranje i procjenu IT sigurnosnih incidenata • kada su samo vjerojatnost i posljedica definirani kao evaluacijski kriteriji • za rangiranje upozorenja o kibernetičkoj sigurnosti (eng. *cyber security alerts*).
ANP i DEMATEL	Preporučuje se snažno kada su kriteriji za procjenu rizika međusobno ovisni i utječu jedni na druge, te kada je potrebno izraditi mapu mrežnog odnosa (eng. *Network Relationship Map*, NRM) uz neophodan izračun težina kriterija.
TOPSIS	Metoda prikladna za rješavanje BCM problema i rangiranja kritičnih i ranjivih kontrola informacijske sigurnosti kada su kriteriji za procjenu međusobno neovisni.

Treba dodati kako je SLR istraživanjem uočeno da se uz navedene MCDM metode često koristilo i Delphi tehniku prikupljanja anonimnih mišljenja unutar grupe profesionalaca kao početni korak u istraživanju prije primjene određenih MCDM metoda. Npr., kao upitnik za strukturiranje i definiranje ključnih faktora (kriterija) rizika.

5.1.6. Pregled integracije ISRA metoda s MCDM tehnikama koje su prethodile istraživanju doktorske disertacije

Najznačajnija istraživanja provedena od strane autora ovog doktorskog rada vezano uz mogućnosti integracije ISRA metoda sa MCDM tehnikama, a koja su prethodila istraživanju doktorske disertacije, proizlaze iz sljedećih znanstvenih radova:

- *Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard* [106]: Napravljena je integracija VECTOR metode za procjenu rizika informacijske sigurnosti sa AHP metodom pri čemu su VECTOR atributi

korišteni kao evaluacijski kriteriji kako bi se dobilo koji od PCI DSS[9] zahtjeva je najkritičniji te bi u skladu s dobivenim rezultatima takav kritični zahtjev trebalo i najprije adresirati. Nakon identificiranja najkritičnijeg PCI DSS zahtjeva pomoću predloženg hibridnog modela, formalna procjena rizika za identificirani zahtjev te predlaganje tretmana za uočeni rizik napravljeni su pomoću OCTAVE (eng. *Operationally Critical Threat, Asset, and Vulnerability Evaluation*) metode za procjenu rizika. OCTAVE metoda se pokazala kao komplementarna za cjelovito rješavanje uočenog problema. VECTOR matrica je otvorena i relativno jednostavna kvalitativna metoda za procjenu rizika informacijske sigurnosti kreirana kako bi se pomoglo poslovnim sustavima u definiranju prioriteta kritičnih rizika. Ta metoda omogućava da se jednostavno kvantificiraju i vizualno predstave svi mogući aspekti rizika informacijske sigurnosti za neki poslovni sustav. VECTOR metoda dolazi od akronima sljedećih engleskih riječi:

V = *Vulnerability* (ranjivost): To je karakteristika imovine ili poslovnog procesa koja upućuje na neki nedostatak koji bi se mogao iskoristiti određenom vrstom napada. Ranjivost je usko povezana s prijetnjom koja istu iskorištava te ranjivost nužno mora imati smisla za određenu vrstu prijetnje kako bi se ranjivost zaista smatralo relevantnim elementom rizika.

E = *Ease of Execution* (jednostavnost izvršenja): To je parametar koji opisuje razinu znanja, stručnosti, naprednih treninga, specijalnih alata i opreme te vremena potrebnih napadaču kako bi uspješno izvršio napad na određeni informacijski sustav. Niska razina jednostavnosti izvršenja znači kako napadač mora učiniti značajne napore kako bi uspješno napravio proboj u inforamcijski sustav. S druge strane, visoka razina jednostavnosti izvršenja znači kako napadač ne mora uložiti značajan nego minimalan trud za uspješan i neovlašteni proboj u informacijski sustav neke organizacije.

C = *Consequence* (posljedica): Predstavlja gubitak neke ekonomske, simboličke ili psihološke vrijednosti za organizaciju, npr. reputacijski rizik za banku u slučaju gubitka ili krađe podataka, nedostupnosti određenih dijelova informacijskog sustava, smanjene razine kvalitete usluge, itd.

T = *Threat* (prijetnja): Predstavlja vjerojatnost nekog događaja u kojemu će napadač napraviti štetu na određenom informacijskom sustavu. Analiza prijetnji je zapravo

[9] ***P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard* (*PCI DSS*) – sigurnosni standard za zaštitu kartičnih podataka

prvi korak koji je potrebno napraviti u procesu analize i procjene rizika. Postoje različiti izvori i oblici prijetnji, a neki od najvažnijih po financijske institucije su neautorizirani pristup, maliciozni programi (posebno tzv. *ransomware*[10]), objava povjerljivih i osobnih podataka (izrazito značajno zbog GDPR[11] regulacije) ili uskraćivanje usluge servisima (eng. *Denial of Service*, DoS) koji moraju klijentima biti 24x7 dostupni (npr. mobilno bankarstvo, internet bankarstvo, e-commerce). Upravo se ovi navedeni korisnički *online* sustavi smatraju vrlo kritičnima te su u kontekstu financijskih, regulatornih i reputacijskih rizika osjetljivi na najznačajnije aplikativne IT rizike adresirane od strane OWASP Top 10 projekta [108]. Prijetnje za koje ne postoji evidentirana ranjivost nemaju utjecaja na informacijski sustav niti na rezultat rizika. Prijetnje za koje postoji uočena ranjivost, ali još ne postoji mogućnost iskorištavanja ranjivosti (tzv. *exploit*[12]) svakako utječe na konačni rezultat rizika, pogotovo za kritične ranjivosti jer za iste postoji velika vjerojatnost kako će napadač (eng. *threat actor*) napisati maliciozni kôd kako bi se pokušalo izvršiti proboj u informacijski sustav.

O = *Operational Importance* (operativna važnost): To je mjera važnosti koju određena imovina ima u cjelokupnoj misiji organizacije. Imovina odnosno informacijski sustavi s većom vrijednosti smatraju se kritičnima pa ako su takvi sustavi zastali s radom, tada se može dogoditi zaustavljanje i svih drugih ovisnih operacija. Redundantni sustavi mogu smanjiti razinu operativne važnosti za pojedine kritične sustave i aplikacije.

R = *Resiliency* (otpornost): Otpornost ili elastičnost je brzina kojom se organizacija može uspješno oporaviti, reorganizirati i pripremiti za nastavak operacija nakon značajnog ispada informacijskog sustava. Ocjenjivanje rizika za ovaj kriterij temelji se na inverznom odnosu. Velika razina otpornosti (npr. brzi oporavak s minimalnim vremenom ispada) rezultira s malom razinom ocjene rizika. S druge strane, kad informacijska imovima ima nisku razinu otpornosti (npr. nepostojanje redundantnog

[10] *Ransomware* – Tzv. ucjenjivački softver, to je vrsta malicioznog softvera koja korisniku uskraćuje pristup računalnim resursima i ujedno zahtijeva plaćanje otkupnine (u pravilu korištenjem kriptovalute) za uklanjanje ograničenja. Pojedini oblici ransomwarea kriptiraju datoteke dok drugi zaključavaju sustav, gdje se korisniku prilikom pokušaja pristupa pojavljuje poruka u kojoj se zahtijeva nužno plaćanje otkupnine.

[11] *General Data Protection Regulation (GDPR)* – Opća Uredba o zaštiti osobnih podataka. To je zakon koji regulira zaštitu osobnih podataka građana Europske unije. Primjenjuje se na sve države članice Europske Unije bez uvođenja u nacionalno zakonodavstvo te se primjenjuje i na sve pravne subjekte koji rade s podacima građana EU-a.

[12] *Exploit* – Komad malicioznog softvera, skup podataka ili sekvenca naredbi koji je u stanju iskoristiti grešku ili ranjivost informacijskog sustava s ciljem neovlaštenog proboja u isti.

sustava, rezervnih kopija, rezervne lokacije, itd.), tada je ocjena rizika vrlo visoka za ovaj kriterij.

VECTOR metoda za procjenu rizika informacijske imovine ima vrlo jednostavnu skalu za procjenu koja je za svaki VECTOR element sljedeća:

1 - 4 **nizak** rizik, 5 - 7 **srednji** rizik, 8 - 10 **visok** rizik.

Ovaj rad predstavlja značajan korak u integraciji ISRA i MCDM domena sa svrhom učinkovitije procjene sigurnosnih zahtjeva i politika. Također, spoznaje dobivene istraživanjem i prezentirane u radu svakako mogu biti od značajne koristi za financijsku industriju u vidu boljeg fokusa na zaštitu korisničkih kartičnih podataka kao kritične informacijske imovine kako bi se zadovoljili zahtjevi PCI DSS standarda te izbjegli potencijalni financijski gubici u slučaju neusklađenosti.

- *Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique* [107]: Rad predlaže i opisuje metodu za evaluaciju kritičnih (i visokorizičnih) informacijskih sustava pri čemu se VECTOR matrica kao metoda za prioritizaciju kritične imovine i kritičnih rizika integrirala u AHP metodu. Kritični sustavi koji su se pritom procjenjivali i međusobno uspoređivali su trenutno najzastupljeniji *online* transakcijski sustavi: internet bankarstvo, mobilno bankarstvo, *e-commerce* (tj. elektronička trgovina na internetu) i Bitcoin kriptosustav. Istraživanjem se htjelo vidjeti stanje sigurnosti Bitcoin sustava u odnosu na druge značajne korisničke *online* transakcijske sustave primjenom hibridnog modela u kombinaciji ISRA i MCDM metoda.

Ovi radovi predstavljaju važne pokazatelje i smjernice o mogućnosti integracije ISRA i MCDM metoda u svrhu evaluacije određenih informacijskih sustava i sigurnosnih standarda, ali i nedostatke provedenih istraživanja. Hibridni AHP model s VECTOR elementima zapravo daje prijedlog kako riješiti određene probleme u IT sigurnosnom (i poslovnom) okruženju prilikom pojave problema višekriterijskog odlučivanja vezano uz vremenska i resursna ograničenja te neizvjesnost. Jedan od uočenih nedostataka u radovima je svakako nepostojanje čvrstih znanstvenih osnova vezano uz odabir VECTOR matrice kao i pitanje da li su elementi te jednostavne metode za procjenu i rangiranje rizika sveobuhvatni i dostatni za primjenu u kontekstu evaluacije kritičnih informacijskih sustava. Nedostatak je i nepostojanje referentnog modela kako bi se moglo vršiti usporedbe i validirati predloženi hibridni model sa VECTOR elementima u AHP metodi. Osim toga, odabir AHP-a kao metode za višekriterijsko odlučivanje

je potrebno dodatno analizirati i vidjeti postoji li neka prikladnija metoda u koju bi se mogli integrirati elementi za analizu i procjenu rizika s ciljem dobivanja preciznijih rezultata uz manji utrošak resursa. Stoga će istraživanje u svrhu izrade ovog doktorskog rada pokušati odgovoriti na uočene nedostatke ranijih istraživanja te predložiti adekvatan model temeljen na metodama za višekriterijsko odlučivanje s elementima za analizu i procjenu rizika za potrebe učinkovitije evaluacije kritičnih informacijskih sustava.

5.2. Metode za višekriterijsko odlučivanje

Na temelju rezultata proizašlih sustavnim pregledom literature te prethodnim istraživanjima autora, a u svrhu razvoja hibridnog višekriterijskoga modela za procjenu kritičnih poslovnih informacijskih sustava, predstavit će se najznačajnije metode i tehnike važne za izradu višekriterijskoga modela (AHP, ANP i DEMATEL), dok ostale metode identificirane sustavnim pregledom literature (npr. TOPSIS ili VIKOR) koje nisu korištene za izradu modela neće biti predmetom detaljnog razmatranja.

5.2.1. Analitički hijerarhijski proces (AHP)

Analitički hijerarhijski proces (eng. *Analytic Hierarchy Process*, AHP) je strukturirana metoda za strukturiranje problema, analizu i donošenje složenih odluka temeljeno na matematici i psihologiji. AHP je pristup za rješavanje problema višekriterijskog odlučivanja koji je predložio T.L. Saaty [109, 110, 162]. To je zapravo metoda za potporu odlučivanju koja se može koristiti za rješavanje složenih problema odlučivanja na način da se njenom primjenom temeljem procjena eksperata izračunavaju težine kriterija te prioriteti alternativa. Problem se strukturira u hijerarhijsku strukturu ciljeva, kriterija, podkriterija i alternativa. Relevantni podaci dobivaju se pomoću usporedbi u parovima od strane stručnjaka tj. donositelja odluke. Takve usporedbe se koriste za dobivanje težinskih vrijednosti za kriterije odlučivanja i mjerenje relativnih performansi alternativa u smislu svakog pojedinačnog kriterija odlučivanja.

Prema [72, 123, 162, 163], osnovni koraci u razvoju AHP modela su sljedeći:

(1) Dekompozicija problema odlučivanja u hijerarhijsku strukturu

Prilikom rješavanja nekih složenih problema, čovjek nastoji grupirati elemente uočenog problema po sličnosti njihova utjecaja na proces na koji taj problem djeluje,

tj. na ciljeve koji se žele postići. Prirodan način na koji čovjek strukturira složene probleme i potom ih analizira jest hijerarhijska struktura, tj. raščlanjivanje problema na jednostavnije dijelove. Rješavanje složenih problema odlučivanja metodom AHP temelji se upravo na njihovoj dekompoziciji u hijerarhiju pri čemu osnovni hijerarhijski AHP model uključuje cilj, kriterije (moguće i podkriterije) i alternative. Dakle, hijerarhija je prva faza razvoja AHP modela. Cilj odlučivanja nalazi se na vrhu hijerarhije, dok su kriteriji i alternative na nižim razinama. Postoje razne metode i pristupi koji mogu pomoći prilikom strukturiranja problema odlučivanja i izrade hijerarhije, npr. pregled literature o relevantnim problemima koji su prethodno riješeni u nekoj problemskoj domeni, intervjui sa stručnjacima iz određene problemske domene, zatim *Delphi* tehnika koja se konkretno u ovom radu koristila za potrebe istraživanja i usuglašavanja oko evaluacijskih kriterija (elementi za analizu i procjenu rizika) za kritična IT rješenja, itd.

(2) Izvršenje prosudbi kako bi se dobili prioriteti za elemenate u hijerarhiji

Nakon izrade AHP hijerarhije dalje je potrebno napraviti prosudbe kako bi se dobilo prioritete za elemente na svakoj razini hijerarhijske strukture. Kako bi se moglo raditi usporedbe, potrebno je imati skalu brojeva koja pokazuje koliko je puta važniji ili dominantniji jedan element nad drugim elementom s obzirom na kriterij ili svojstvo u odnosu na koji se sami elementi uspoređuju. Prosudbe donositelja odluka o relativnoj važnosti između dva elementa na istoj razini hijerarhije izražavaju se pomoću sljedeće ljestvice intenziteta (Tablica 5.3):

Tablica 5.3: Temeljna skala relativnih važnosti [109, 162]

Intenzitet važnosti	Definicija	Objašnjenje
1	Jednako važno	Dva kriterija jednako doprinose cilju
3	Umjereno važnije	Iskustvo i procjena daju umjerenu prednost jednom kriteriju u odnosu na drugi kriterij
5	Strogo važnije	Iskustvo i procjena strogo favoriziraju jedan kriterij u odnosu na drugi kriterij
7	Vrlo stroga dokazana važnost	Jedan evaluacijski kriterij izrazito značajno se favorizira u odnosu na drugi kriterij, njegova dominacija dokazana je u praksi
9	Ekstremna važnost	Dokazi na temelju kojih se favorizira jedan kriterij u odnosu na drugi kriterij potvrđeni su s najvećom mogućom razinom
2, 4, 6, 8	Međuvrijednosti	
Reciprociteti	$j = \frac{1}{i}$	Ako kriterij i ima jedan od gore spomenutih ne-nula brojeva koji su mu dodijeljeni prilikom usporedbe s kriterijem j, tada kriterij j ima recipročnu vrijednost prilikom usporedbe s kriterijem i.

Prilikom uspoređivanja u parovima nužno je imati konzistentnost u usporedbama. Konzistentnost se odnosi na svojstvo tranzitivnosti, npr. ako alternativa *a1* po određenom kriteriju *k1* ima veću težinu od alternative *a2*, i ako *a2* ima veću težinu od *a3* po istom kriteriju evaluacije, tada nužno slijedi kako *a1* nadmašuje *a3* po definiranom kriteriju *k1*.

(3) Sinteza modela

Izračunavaju se prioriteti alternativa i težine kriterija na temelju definiranog skupa matrica za usporedbu u parovima. Na temelju procjena relativnih važnosti elemenata (atributa) odgovarajuće razine hijerarhije problema koji se rješava pomoću matematičkog modela izračunavaju se lokalni prioriteti (težine) definiranih kriterija, podkriterija i alternativa koji se zatim sintetiziraju u ukupne prioritete alternativa. Ukupni prioritet pojedine alternative izračunava se tako da se zbrajaju lokalni prioriteti alternative koji su ponderirani s težinama elemanata (kriterija) više razine.

(4) Provođenje analize osjetljivosti.

Ovaj korak predstavlja ispitivanje osjetljivosti izlaznih varijabli (tj. prioriteta alternativa) na temelju promjena ulaznih varijabli (težine evaluacijskih kriterija) i odgovarajućih usporedbi. Tu se ispituje da li mala promjena ulaznih procjena (težine evaluacijskih kriterija) utječe na prioritete i rangiranje alternativa te u kojoj mjeri. U slučaju da neka manja promjena kod ulaznih procjena utječe na promjenu ranga alternativa, tada je potrebno provesti dodatnu analizu.

Druga važna osnova AHP metode je **matematički model** pomoću kojeg se računaju prioriteti (tj. težine) elemenata hijerarhijske strukture koji pripadaju istoj grani. Pomoću matematičkog modela se težine elemenata računaju iz procjena njihovih omjera koji se daju za svaki par elemenata koji se uspoređuje. Pritom se koristi Saatyjeva ljestvica relativnih važnosti (Tablica 5.3). Ulazni podaci za AHP model su procjene omjera važnosti kriterija i prioriteta alternativa. Donositelj odluke uspoređuje međusobno u parovima glavne kriterije u odnosu na njihovu važnost za mjerenje postizanja cilja. Ako postoje definirani i podkriteriji nekog glavnog kriterija za procjenu, tada se u parovima procjenjuju omjeri težina tih podkriterija u odnosu na to koliko su pojedinačni aspekti koji se mjere tim podkriterijima važni za cijeli aspekt zastupljen odgovarajućim glavnim kriterijem. Npr., za slučaj odabira mrežnog vatrozida nove generacije (eng. *next generation firewall*, NGFW) jedan od glavnih kiterija bi svakako bio *performanse* dok bi relevantni podkriteriji mogli biti *propusnost FW-a, propusnost IPS-a* i *max. br. konekcija*. Kako bi se odredile težine ovih podkriterija, u parovima se procjenjuju njihove

relativne važnosti s aspekta njihova doprinosa za ukupne performanse mrežnog vatrozida, dakle u odnosu na granu hijerarhijske strukture kojoj pripadaju određeni podkriteriji. Nakon što se ovim postupkom odrede težine svih kriterija (i mogućih podkriterija) u AHP modelu, alternative problema odlučivanja uspoređuju se u parovima po svakom od izlaznih čvorova (grana) hijerarhije kriterija. To znači kako u slučaju dekompozicije kriterija *performanse* na već spomenute podkriterije, definirane alternative se tada ne bi uspoređivale u parovima direktno u odnosu na taj kriterij *performanse*, nego bi se uspoređivale u odnosu na svaki od definiranih podkriterija (*propusnost FW-a*, *propusnost IPS-a* i *max. br. konekcija*). Iz tih usporedbi proizlaze njihovi lokalni prioriteti koji se potom ponderiranjem i zbrajanjem sintetiziraju u prioritete alternativa prema kriteriju *performanse*.

Prilikom procesa provođenja usporedbi u parovima, potrebno je uzeti u obzir sljedeće važne aksiomime[13] na kojima se temelji AHP metoda [18, 110]:

- Aksiom 1 – *Reciprocitet*: Prilikom usporedbe u parovima, ako element *i* dominira nad elementom *j* intenzitetom *x* (prema definiranoj Saatyjevoj ljestvici), tada vrijedi da *j* dominira nad *i* intenzitetom $\frac{1}{x}$.
- Aksiom 2 – *Homogenost*: Usporedba u parovima ima smisla jedino ako su elementi međusobno usporedivi odnosno dovoljno srodni za usporedbu prema Saatyjevoj ljestvici.
- Aksiom 3 – *Zavisnost*: Usporedba elemenata u parovima iz jedne hijerarhijske razine moguća je samo u odnosu na elemente više razine hijerarhije.
- Aksiom 4 – *Očekivanje*: Bilo koja promjena u hijerarhijskoj strukturi AHP modela zahtijeva ponovni izračun prioriteta u novoj hijerarhiji.

Slijedi opis postupka usporedbi u parovima i dobivanje konzistentnosti pomoću srodnog matematičkog modela [18, 72]. Postupak izračuna težina kriterija i prioriteta alternativa iz njihovih usporedbi u parovima sastoji se od tri koraka:

(1) Definiranje matrice omjera prioriteta (težina)

(2) Normalizacija matrice omjera

(3) Izračun težina kriterija i prioriteta alternativa.

[13] *Aksiom* ili *postulat* – Temeljna istina koja se ne dokazuje i služi kao osnova neke matematičke ili logičke teorije. Smislenost aksioma se ocjenjuje prema teoriji koja se iz njega izvodi.

Postupak izračuna težina (prioriteta) iz omjera njihovih vrijednosti temelji se na teoremima iz linearne algebre. Nakon što su sve prosudbe izvršene, iste su sintetizirane pomoću srodnog matematičkog modela [72, 109, 162]:

$$Aw = nw$$

- Ako je n broj kriterija (ili alternativa) za koje je potrebno pronaći težine w_i, i
- Ako $a_{ij} = \frac{w_i}{w_j}$, pri čemu je w_i težina *i*-tog kriterija (ili prioritet *i*-te alternative), bude element matrice **A**, tada matrica **A** usporedbi u parovima i vektor $w = (w_1, w_2, ..., w_n)$ zadovoljavaju navedenu jednadžbu. Tako je definirana **matrica A omjera relativnih važnosti**:

$$A = \begin{bmatrix} a_{11} a_{12} \ldots a_{1n} \\ a_{21} a_{22} \ldots a_{2n} \\ \ldots\ldots\ldots\ldots \\ a_{n1} a_{n2} \ldots a_{nn} \end{bmatrix} = \begin{bmatrix} \frac{w_1}{w_1} \frac{w_1}{w_2} \ldots \frac{w_1}{w_n} \\ \frac{w_2}{w_1} \frac{w_2}{w_2} \ldots \frac{w_2}{w_n} \\ \ldots\ldots\ldots\ldots \\ \frac{w_n}{w_1} \frac{w_n}{w_2} \ldots \frac{w_n}{w_n} \end{bmatrix}$$

Iz navedene matrice **A** za slučaj konzistentnih procjena za koje vrijedi $a_{ij} = a_{ik} \cdot a_{kj}, i, j, k \in \{1,2,...,n\}$, matrica **A** zadovoljava matričnu jednadžbu $Aw = nw$, pri čemu je *w* vektor (jednostupčana matrica) prioriteta kriterija.

$$\begin{bmatrix} \frac{w_1}{w_1} \frac{w_1}{w_2} \ldots \frac{w_1}{w_n} \\ \frac{w_2}{w_1} \frac{w_2}{w_2} \ldots \frac{w_2}{w_n} \\ \ldots\ldots\ldots\ldots \\ \frac{w_n}{w_1} \frac{w_n}{w_2} \ldots \frac{w_n}{w_n} \end{bmatrix} \cdot \begin{bmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{bmatrix} = n \cdot \begin{bmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{bmatrix}$$

Usporedbom u parovima dobiva se vektor prioriteta, a što je zapravo glavni svojstveni vektor (*eigenvector*) matrice **A**. Taj vektor daje relativni prioritet kriterijima izračunatima prema omjernoj Saatyjevoj skali (Tablica 5.3). S obzirom na specijalni oblik matrice **A** (svaki redak je višestruka konstanta od prvog retka, svi elementi su pozitivni te $a_{ij} = \frac{1}{a_{ji}}$), rang matrice **A** je 1, sve svojstvene vrijednosti (eng. *eigenvalues*) su 0 osim jedne i ta ne-nulta svojstvena vrijednost ima vrijednost *n*.

Ako matrica **A** sadrži nekonzistentnosti, tada se vektor $w = (w_1, w_2, ..., w_n)$ za težine može dobiti koristeći sljedeće jednadžbe:

$$(A - \lambda_{max} I)w = 0$$

$$\Sigma w_i = 1$$

Pri tome je λ_{max} najveća svojstvena vrijednost matrice **A**. Treba još napomenuti kako navedeni sustav jednadžbi $(A - \lambda I)w = 0$, uz uvjet da $\sum_{i=1}^{n} w_i = 1$, u općenitom slučaju nije moguće sasvim točno riješiti bez posebnog računalnog softvera, a najčešće je algoritam za rješavanje tog sustava uključen u programske alate koji podržavaju AHP metodu (npr. *ExpertChoice*, *TransparentChoice*, *SuperDecisions*, *DecisionLens*, itd.). S obzirom na karakteristike matrice **A**, izrazi $\lambda_{max} \geq n$ i razlika $\lambda_{max} - n$ mogu se koristiti za mjerenje (ne)konzistentnosti procjena. Indeks konzistentnosti (eng. *consistency index*, CI) daje relaciju

$$CI = \frac{\lambda_{max} - n}{n - 1}$$

Tako je omjer konzistentnosti definiran kao $\boldsymbol{CR = \frac{CI}{RI}}$, gdje je *RI* nasumični indeks (eng. *random index*, *RI*). Nasumični indeks *RI* je zapravo indeks konzistentnosti mnogih slučajno generiranih matrica za usporedbu u parovima veličine *n*, te se primjenjuje samo ako je $n \geq 3$.

Tablica 5.4: Vrijednosti slučajnih indeksa [18]

N	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,52	0,89	1,11	1,25	1,35	1,4	1,45	1,49

Ako je $CR \leq 0.1$, tada se usporedbe u parovima smatraju prihvatljivima. Postoji više mogućih uzroka za pojavu nekonzistentnosti u procjenama, npr.:

- Pomanjkanje koncentracije zbog umora ili nezainteresiranosti procjenitelja
- Administrativna pogreška prilikom unosa vrijednosti omjera kriterija (npr. kod unosa inverzne vrijednosti)
- Inherentna nelogičnost u stvarnom problemu koji se modelira
- Neadekvatna struktura modela
- Nedostatak pravih informacija za procjenitelja, npr. neodgovarajuće upute od strane meoderatora.

Tablica 5.5: Prednosti i nedostaci AHP metode [18, 123, 144, 163]

Prednosti AHP metode	Nedostaci AHP metode
Donositelj odluke uključen je u sve faze strukturiranja i analize problema odlučivanja	Nedovoljna veličina Saatyjeve ljestvice relativnih važnosti za usporedbu elemenata kod nekih problema odlučivanja
Metoda AHP omogućuje integraciju kvalitativnih i kvantitativnih faktora u odlučivanje na intuitivan način za donositelja odluke, bez potrebe dubinskog razumijevanja matematičkih osnova te metode	Potrebno provođenje velikog broja usporedbi u parovima kod složenijih problema odlučivanja
Kontrola konzistentnosti temeljem indeksa konzistentnosti (CI) te analiza nekonzistentnosti	Otežano postizanje prihvatljivog omjera konzistentnosti kod određenih problema odlučivanja
Zbog redundantnosti usporedbi u parovima, metoda AHP je manje osjetljiva na pogreške u procjenjivanju	Aksiomi na kojima se temelji AHP metoda ne dozvoljavaju neusporedivost inačica
Metoda AHP je pogodna za grupno odlučivanje jer omogućava učinkovitu medijaciju u procesu odlučivanja. Kombinacija prezentacijskih alata i programske podrške za AHP metodu značajno poboljšava komunikaciju među članovima grupe i utječe na učinkovitost. Pojedini napredniji softverski alati za AHP metodu imaju dodatne module za podršku grupnom odlučivanju, čime se smanjuje rizik nekvalitetnih odluka karakterističnih za grupno odlučivanje te omogućavaju kontroliranu integraciju individualnih procjena u grupnu procjenu.	Ne uzimaju se u obzir utjecaji (zavisnosti) među kriterijima za procjenu
Procesom odlučivanja primjenom AHP metode dolazi se do približnog rješenja problema većom brzinom nego na grupnim sastancima uz manje troškove prilikom procesa donošenja odluke.	
Rezultati odlučivanja AHP metodom omogućavaju rang ljestvicu alternativa te ujedno daju i vrijedne informacije o težinama kriterija u odnosu na cilj, a što omogućava kvalitetnu analizu osjetljivosti.	

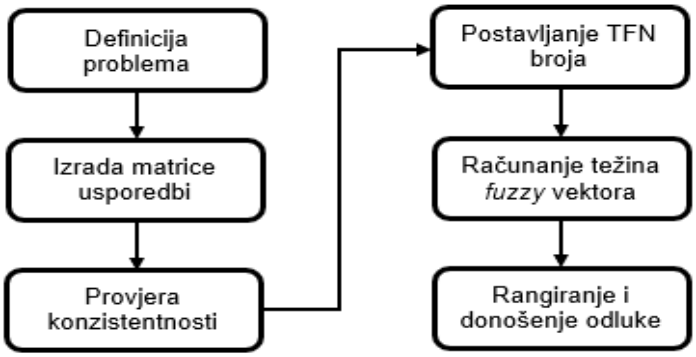
Tablicom 5.5 strukturirano su prikazane identificirane prednosti i nedostaci AHP metode.

Općenito, za AHP se može reći kako je to vrlo korisna i iznimno široko rasprostranjena metoda višekriterijskog odlučivanja kada su višestruki troškovi i koristi relevantni za određivanje prioriteta alternativa. Dodatno, treba naglasiti kako je metoda AHP značajno korištena i analizirana u brojnim znanstvenim istraživanjima kao najdominantnija metoda za višekriterijsko odlučivanje, a što se i pokazalo sustavnim pregledom literature.

5.2.2. Neizraziti AHP

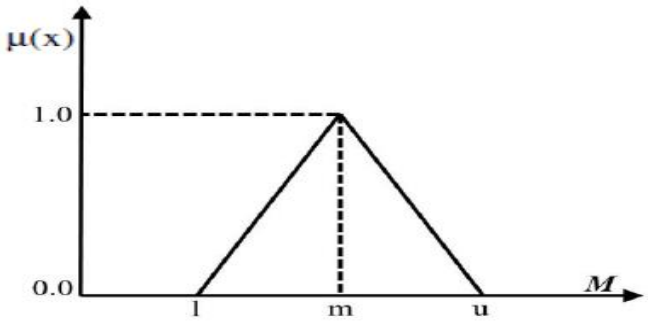
Neizrazita (eng. *fuzzy*) AHP metoda proširuje Saatyjevu originalnu AHP metodu tako što se kombinira sa teorijom neizrazitog skupa (eng. *Fuzzy Set Theory*, FST) kako bi se odgovorilo na pojavu neizvjesnosti u procesu donošenja odluka kroz jezičnu terminologiju i stupanj pripadnosti [137]. Glavni doprinos teorije neizrazitih skupova je njezina sposobnost predstavljanja nejasnih ili dvosmislenih podataka. U AHP metodi, dvije alternative se međusobno uspoređuju pri čemu se dodjeljuje numerička vrijednost kako bi se označilo razinu važnosti između promatranih alternativa. Kod F-AHP metode, prioritet je okarakteriziran pomoću intervala koji se međusobno presijecaju, što poboljšava preciznost konačne odluke [138] zbog smanjenja subjektivnosti koja je inherentna ljudskoj prirodi prilikom donošenja odluke.

U *fuzzy* AHP metodi, skale neizrazitih omjera se koriste za označavanje relativne važnosti faktora u odgovarajućim kriterijima [135].



Slika 5.6: Blok dijagram faza F-AHP procesa [136]

Na Slici 5.6 vidi se kako postupak u F-AHP metodi počinje identično kao i kod tradicionalne (originalne) AHP metode, ali s bitnom razlikom što se nakon provjere konzistentnosti pojavljuje korak za izračun trosložnog neizrazitog broja (eng. *Triangular Fuzzy Number*, TFN). Alternative se procjenjuju i prioritiziraju pomoću TFN-a.



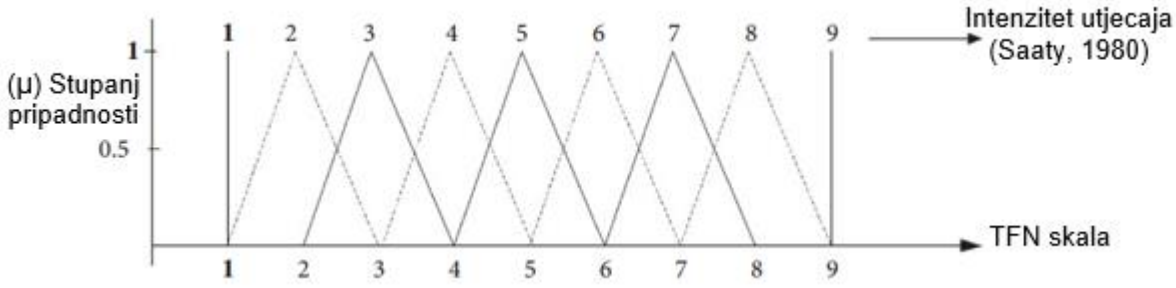
Slika 5.7: Trosložni neizraziti broj [138]

TFN se jednostavno označava kao $M = (l, m, u)$.

- l: označava najmanju moguću vrijednost
- m: označava najbližu vrijednost
- u: označava najveću moguću vrijednost

Funkcija pripadnosti opisuje se na sljedeći način:

$$\mu(\overline{M}) = \begin{cases} 0, x < l \\ \dfrac{x-l}{m-l}, l \le x \le m \\ \dfrac{u-x}{u-m}, m \le x \le u \\ 0, x > u \end{cases}$$



Slika 5.8: Graf neizrazitog trosložnog skupa [136]

Ako su $M_1 = (l_1, m_1, u_1)$ i $M_2 = (l_2, m_2, u_2)$ dva TFN-a, tada imamo sljedeće relacije i matematičke operacije nad njima, a koje se koriste u F-AHP metodi:

(1) Zbrajanje

$$(l_1, m_1, u_1) + (l_2, m_2, u_2) = (l_1 + l_2, m_1 + m_2, u_1 + u_2)$$

(2) Umnožak

$$(l_1, m_1, u_1) * (l_2, m_2, u_2) = (l_1 * l_2, m_1 * m_2, u_1 * u_2)$$

(3) Inverz

$$(l_1, m_1, u_1)^{-1} = \left(\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}\right)$$

Pretpostavimo da je $X = \{x_1, x_2, x_3 \dots x_n\}$ neki objektni skup, a postavljeni cilj $G = \{g_1, g_2, g_3 \dots g_n\}$. Svaki objekt se uzima s popisa objekata i na svakom objektu se provodi proširena analiza za svaki cilj. Nakon implementacije proširene analize, m vrijednost proširene analize za svaki objekt može se dobiti pomoću sljedećih TFN-a:

$$M_{gi}^1, M_{gi}^2 \dots M_{gi}^m, i = 1,2,3 \dots n$$

Nakon što se vrijednosti usporedbe dobivene AHP metodom transformiraju u F-AHP vrijednosnu skalu, izračunava se neizrazita vrijednost sinteze. Proces dobivanja neizrazite vrijednosti sinteze prikazan je sljedećom formulom:

$$S_i = \sum_{j=1}^{m} M_{gi}^{j} * \left[\sum_{i=1}^{n} \sum_{j=1}^{m} M_{gi}^{j} \right]^{-1}, \text{ pri čemu}$$

- S_i = neizrazita vrijednost sinteze
- $\sum_{j=1}^{m} M_{gi}^{j}$ = zbroj vrijednosti ćelije u stupcu počevši od stupca 1 u svakom retku matrice
- i = red
- j = stupac

Kako bi se dobilo $\sum_{j=1}^{m} M_{gi}^{j}$, provodi se *fuzzy* operacija zbrajanja nad *m* povrh vrijednosti proširene analize za određenu matricu pomoću sljedeće relacije:

$$\sum_{j=1}^{m} M_{gi}^{j} = \left(\sum_{j=1}^{n} l_j, \sum_{j=1}^{n} m_j, \sum_{j=1}^{n} u_j\right)$$

Nakon određivanja S_i vrijednosti (l, m, u), sljedeći korak je odrediti razinu mogućnosti svakog kriterija i alternativa, gdje za $M_2 = (l_2, m_2, u_2) \geq M_1 = (l_1, m_1, u_1)$ vrijedi sljedeće:

$$V(M_2 \geq M_1) = \sup_{y \geq x} \left[\min\left(\mu_{M_1}(x), \mu_{M_2}(y)\right)\right],$$

a što je jednako izrazu

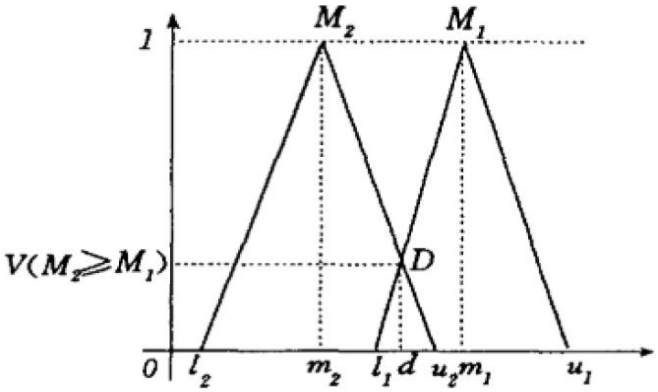
$V(M_2 \geq M_1) = hgt(M_1 \cap M_2) = \mu_{M_2}(d)$,

odnosno

$$\begin{cases} 1, & \text{ako je } m_2 \geq m_1 \\ 0, & \text{ako je } l_2 \geq l_1 \\ \dfrac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)} & \text{inače} \end{cases}$$

pri čemu je d ordinata najviše točke presjeka D koja se nalazi između μ_{M_1} i μ_{M_2}, a što je prikazano Slikom 5.9.

Izraz *hgt* je visina neizrazitih brojeva na presjeku M_1 i M_2.



Slika 5.9: Presjek između M_1 i M_2 [151]

Sljedeći korak je dobiti namanju razinu mogućnosti za svaki kriterij i svaku alternativu. Kako bi se dobilo najmanje moguće vrijednosti za $M_2 \geq M_1$, sve neizrazite vrijednosti $M_i = (1,2,\dots,k)$ moraju se usporediti koristeći sljedeći izraz:

$$V(M \geq M_1, M_2, \dots, M_k) = minV(M \geq M_i), (i = 1,2,3, \dots, k)$$

Pretpostavimo kako je $d'(A_i) = minV(S_i \geq S_k)$; za $k = 1,2,3, \dots, n$; težinski vektori su izračunati na sljedeći način:

$$W' = (d'(A_1), d'(A_2), \dots, d'(A_n))^T$$

gdje $A_i = (i = 1,2, \dots, n)$ predstavlja n elemenata.

Sljedeći korak je normalizacija matrice usporedbi i dobivanje težinskog vektora. Tako normalizirani težinski vektor je definiran kao:

$$W = (d(A_1), d(A_2), \dots, d(A_n))^T$$

pri čemu je W ne-*fuzzy* broj. Tu se zapravo radi postupak defazifikacije ordinalne vrijednosti (d').

Završni korak kod F-AHP je identičan kao kod standardne AHP metode gdje se izračunavaju relativne težine i rangiraju alternative na temelju performansi relativnih težina mogućih alternativa.

Korištenje F-AHP metode može pomoći u donošenju efikasnijih, fleksibilnijih i realnijih odluka na temelju raspoloživih kriterija i alternativa te se u istraživanjima koristi kako bi se uključilo neizvjesnosti i smanjilo nepreciznosti prilikom davanja usporedbi u parovima u odnosu na konvencionalnu AHP metodu. Ipak, postoje i značajni problemi prilikom korištenja F-AHP metode:

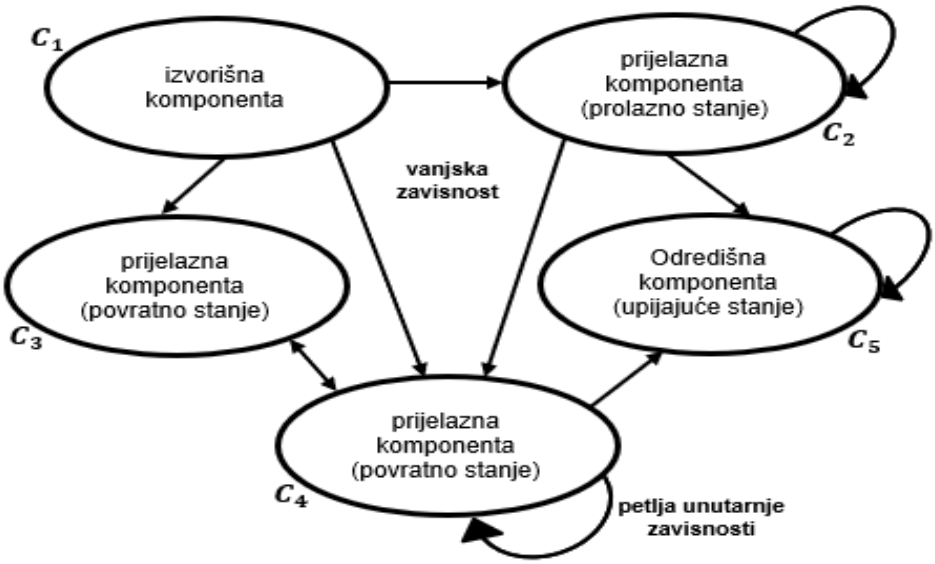
- Značajno se povećava složenost i vrijeme potrebno za dobivanje svih izračuna
- Ograničena softverska podrška
- Nepostojanje standardne (jedinstvene) TFN skale [151].

5.2.3. Analitički mrežni proces (ANP)

Analitički mrežni proces (eng. *Analytic Network Process*, ANP) je novija metoda za višekriterijsko odlučivanje koja omogućava modeliranje utjecaja (zavisnosti) između elemenata hijerarhije te uključuje određenu nadogradnju u odnosu na AHP metodu [164]. Mnogi problemi odlučivanja ne mogu se strukturirati pomoću hijerarhije jer uključuju interakciju i zavisnost elemenata (kriterija) više razine hijerarhije sa elementima niže razine. ANP metoda omogućava modeliranje funkcionalne interakcije kriterija i alternativa u nekom modelu, pri čemu se postiže veća stabilnost rezultata [163]. Stoga je predložena ANP metoda koja omogućava mrežu umjesto hijerarhije koja je omogućena AHP metodom [111, 113, 127, 164, 165].

Struktura povratnih veza (eng. *feedback*) koja postoji u ANP-u nema formu hijerarhije, već više podsjeća na mrežu s krugovima (ciklusima) koji spajaju komponente svojih elemenata (zato se više ne mogu zvati razinama) i petljama koje spajaju određenu komponentu odnosno klaster prema samima sebi. Kada se radi o hijerarhiji, težine kriterija služe za vrednovanje alternativa te da bi se odredili prioriteti tih alternativa. S druge strane, u mreži može svaka komponenta zavisiti o nekoj drugoj mrežnoj komponenti.

Vrste komponenti u ANP mreži prikazane su na Slici 5.10., kao i njihove veze.

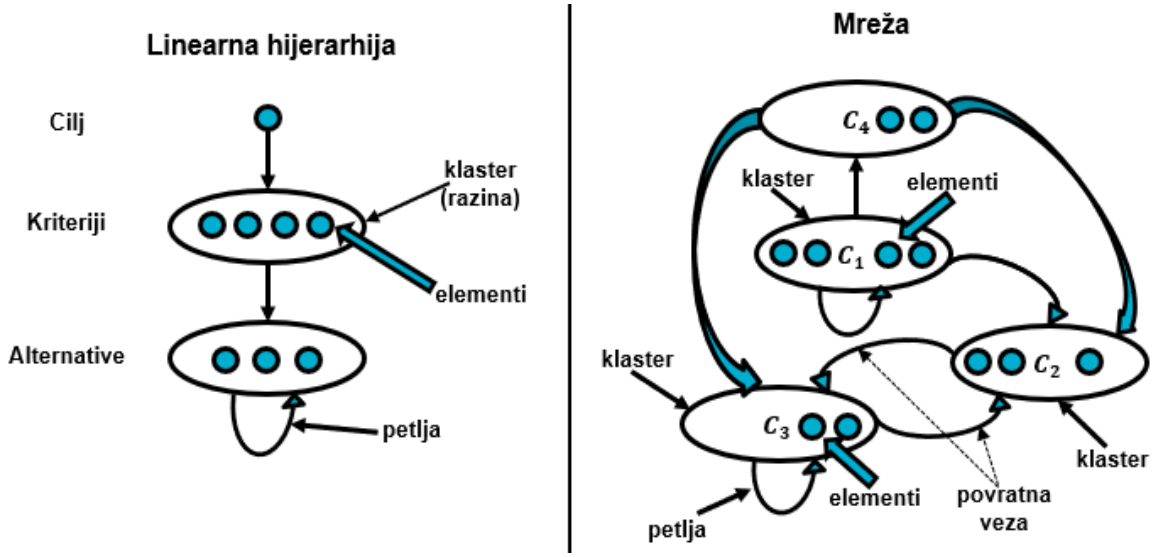


Slika 5.10: Komponente i konekcije u ANP mreži [165]

Mreža se sastoji od klastera (tj. komponenti) u kojima su kao čvorovi smješteni cilj, kriteriji i alternative. Upravo je klaster osnovni element ANP mreže, a klasteri se sastoje od čvorova koji se međusobno povezuju ovisno o njihovoj zavisnosti (utjecaju). U ANP mreži postoje izvorišni (eng. *sources*) i odredišni (eng. *sinks*) čvorovi. Zavisnosti se prikazuju vezom između dva čvora kad među njima postoji utjecaj. Ako čvorovi međusobno utječu jedan na drugog, tada se takva veza naziva povratna veza. Izvorišni čvor je izvor za putanje utjecaja

(važnosti), ali nikad nije odredište takvih putanja. To znači da elementi izvorišnog klastera zavise o elementima drugih klastera, a niti jedan element nekog drugog klastera ne zavisi o nekom elementu izvorišnog klastera. Izvorišni klaster sadrži izvorišne čvorove, a primjer takvog klastera je cilj. Cilj utječe na komponente niže razine, ali niti jedna komponenta ne utječe na cilj. Odredišni čvor je odredište za putanje utjecaja, ali nikad nije izvor takvih putanja. To znači da elementi odredišnog klastera utječu na elemente nekih drugih klastera (ili čak istog klastera), ali niti jedan element odredišnog klastera ne zavisi o nekom elementu bilo kojeg drugog klastera. Postoji i prijelazni klaster čiji elementi zavise o elementima drugih klastera, ali i elementi nekih drugih klastera ovise o elementima tog prijelaznog klastera. Primjer prijelaznog klastera je klaster s kriterijima. Kriteriji najčešće utječu na cilj, te zavise i utječu na alternative, tako da je to zapravo ključan klaster [111, 113, 164, 165].

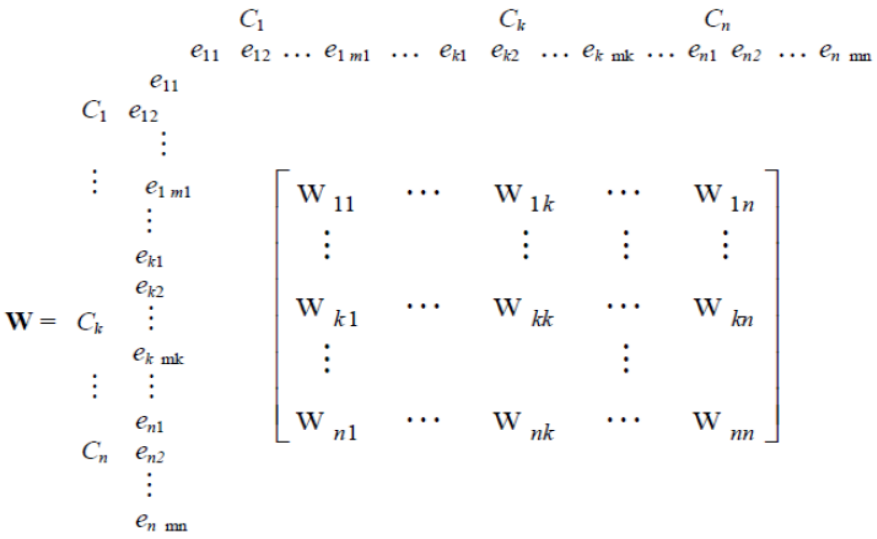
Problem odlučivanja koji uključuje povratne veze najčešće proizlazi iz prakse i pritom je veliki izazov odrediti prioritete (tj. težine) elemenata u mreži i posebno alternative odluke, a još više opravdati valjanost ishoda odlučivanja. S obzirom da povratne informacije uključuju cikluse, a mrežni ciklusi su zapravo beskonačan proces, operacije potrebne za dobivanje prioriteta postaju značajno zahtjevnije nego što je to bilo u slučaju AHP metode s hijerarhijom. Hijerarhija je zapravo specijalni slučaj mreže gdje veze idu samo prema jednom smjeru – prema elementima niže razine [111, 113, 163, 164, 165]. Osnovna razlika između AHP i ANP metoda je ta što se u AHP-u određuju prioriteti alternativa s obzirom na važnost kriterija, dok u ANP-u kriteriji utječu na važnost alternativa te dodatno važnost alternativa utječe na određivanje težina evaluacijskih kriterija [163].



Slika 5.11: Usporedba između hijerarhije i mreže [111, 165]

Na Slici 5.11 prikazana je usporedba hijerarhijske i mrežne strukture. Vidljivo je kako razine u hijerarhiji odgovaraju klasterima u mreži. Mreža se sastoji od klastera koji sadrže određene elemente (kriterije) gdje su elementi iz jednog klastera povezani sa elementima iz drugog klastera (vanjska zavisnost, eng. *outer dependence*) ili unutar samog klastera (unutarnja zavisnost, eng. *inner dependence*) ili petlja (eng. *loop*). Vanjska zavisnost ukazuje da barem jedan element klastera zavisi o najmanje jednom elementu nekog drugog klastera (npr. ako imamo klaster *rizik* i klaster *otpornost*, tada istoimeni element iz klastera *otpornost* može ovisiti o elementu *prijetnja* iz klastera *rizik*). Unutarnja zavisnost ukazuje da barem jedan element klastera zavisi o barem jednom elementu unutar istog klastera. Petlja u hijerarhiji ukazuje da svaki element ovisi samo o sebi, nema drugih zavisnosti i takav element ne utječe na druge elemente niti oni utječu na njega. U mreži su kao čvorovi smješteni cilj, kriteriji i alternative. Postoje dvije vrste utjecaja: vanjski i unutarnji. Kod vanjskog utjecaja se uspoređuje utjecaj elemenata iz jednog klastera na elemente drugog klastera u odnosu na kontrolni kriterij (ako je isti definiran). Kod unutarnjeg utjecaja se uspoređuje međusobni utjecaj elemenata u grupi, tj. klasteru. Petlja u klasteru označava unutarnju zavisnost između elemenata tog klastera u odnosu na zajedničko svojstvo (npr. element *prijetnja* ovisi o elementu *ranjivost* unutar klastera *rizik*). Veza od klastera C_4 prema klasteru C_2 upućuje na vanjsku zavisnost elemenata iz klastera C_2 prema elementima klastera C_4, a u odnosu na neko zajedničko svojstvo. Svakako treba istaknuti kako je koncept zavisnosti suprotan (inverzan) konceptu utjecaja.

Nakon što su identificirani klasteri s elementima, potrebno je napraviti usporedbe u parovima, tj. usporedbe klastera i usporedbe pojedinih elemenata u klasterima. Takvi prioriteti dobiveni usporedbom u parovima matrica unose se kao dijelovi stupaca supermatrice. Supermatrica predstavlja prioritet utjecaja elementa na lijevoj strani matrice u odnosu na element na vrhu matrice, a s obzirom na određeni kontrolni kriterij. Dakle, kako bi se dobilo globalne prioritete u sustavu sa međuzavisnim utjecajima, vektori lokalnih prioriteta unose se u odgovarajuće stupce matrice. Kao rezultat, supermatrica je zapravo particionirana matrica gdje svaki segment matrice predstavlja vezu između dva čvora (elemenata ili klastera) u sustavu. Standardni oblik supermatrice mreže prikazan je sljedećim izrazom [164, 165]:



Pri tome je:

m – broj klastera

C_k – komponente (klasteri) sustava odlučivanja, $k = 1,2, \dots, n$

m_k – broj elemenata unutar k-tog klastera

$e_{k\,mk}$ – element sustava.

Znači, komponente sustava odlučivanja su C_k i svaka komponenta k ima m_k elemenata koji se označavaju kao $e_{k1}, e_{k2}, \dots, e_{k\,mk}$. Vektori lokalnih prioriteta dobiveni usporedbom u parovima se grupiraju i smještaju na odgovarajuće pozicije unutar supermatrice na temelju protoka utjecaja iz jedne komponente u drugu komponentu ili iz komponente u samu sebe kao u petlji.

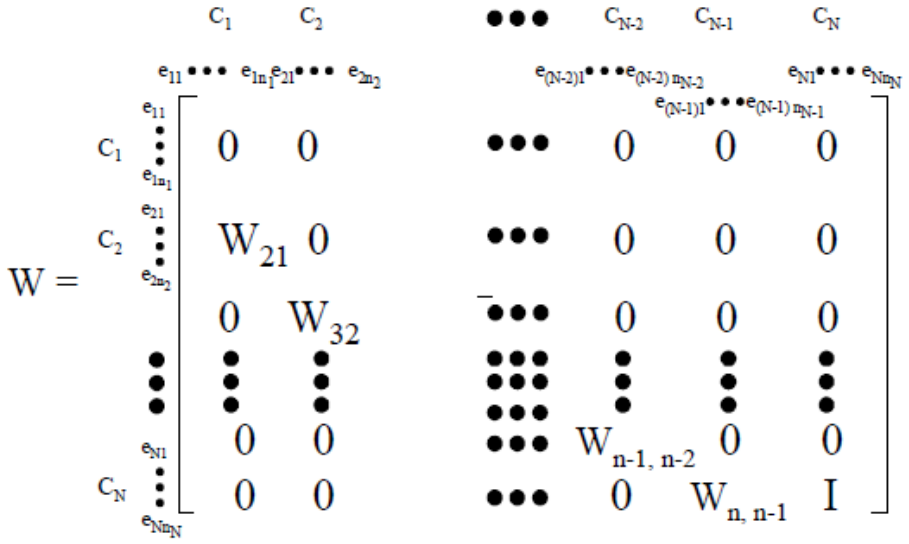
Uobičajeni element u supermatici je blok (komponenta) W_{ij} supermatrice mreže što je prikazano sljedećim izrazom [111, 113, 164, 165]:

$$W_{ij} = \begin{bmatrix} W_{i1}^{(j_1)} & W_{i1}^{(j_2)} & \bullet\bullet\bullet & W_{i1}^{(jn_j)} \\ W_{i2}^{(j_1)} & W_{i2}^{(j_2)} & \bullet\bullet\bullet & W_{i2}^{(jn_j)} \\ \vdots & \vdots & & \vdots \\ W_{in_i}^{(j_1)} & W_{in_i}^{(j_2)} & \bullet\bullet\bullet & W_{in_i}^{(jn_j)} \end{bmatrix}$$

Svaki stupac bloka supermatrice je vektor vlastite vrijednosti koji predstavlja utjecaj (tj. važnost) elementa u i-toj komponenti ANP mreže na element u j-toj komponenti mreže. Pojedini ulazi unutar bloka supermatrice mogu imati vrijednost 0, što znači da takvi elementi nemaju međusobne zavisnosti. Kada se rade procjene kako bi se dobilo vrijednosti svojstvenih

vektora, ne moraju se raditi usporedbe svih elemenata nego samo onih koji između sebe imaju definirane zavisnosti.

Sljedeći izraz predstavlja hijerarhiju supermatrice od *m* razina [165]:



Osnovni element supermatrice hijerarhije je blok W_{ij} pozicioniran na mjestu gdje je *i*-ta razina (lijeva strana matrice) povezana i utječe na *j*-tu razinu (vrh matrice). Ulaz u zadnjem retku i stupcu supermatrice hijerarhije je jedinična matrica *I*, a koja korespondira petlji u donjoj razini hijerarhije te označava da svaki element ovisi isključivo o sebi [163].

Kako bi se iz supermatrice u kojoj je zbroj stupca najčešće veći od 1 moglo dobiti granične prioritete utjecaja elemenata, supermatrica se najprije mora transformirati u tzv. stohastičnu matricu za koju vrijedi da je zbroj elemenata svakog njenog stupca jednak 1. Komponente se međusobno uspoređuju s obzirom na postojeću zavisnost te u odnosu na kontrolni kriterij više razine (ako je isti definiran). Tako se dobivaju vektori težina koji uključuju utjecaje komponenti na lijevoj strani supermatrice na komponente s vrha matrice. Postupak se ponavlja s obzirom na broj komponenti, a rezultat je tzv. ponderirana matrica koja je stohastična [163].

Sljedeći korak je računanje granične supermatrice hijerarhije [165]:

$$W^k = \begin{bmatrix} 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots\vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 \\ W_{n,n-1}W_{n-1,n-2}\dots W_{32}W_{21} & W_{n,n-1}W_{n-1,n-2}\dots W_{32} & \dots W_{n,n-1}W_{n-1,n-2} & W_{n,n-1} & I \end{bmatrix}$$

Najvažnije pitanje u ANP-u je kako integrirati sve postojeće tranzitivnosti u završne prioritete elemenata [163]. Ako je matrica stohastična, prioriteti elemenata ili alternativa (dobiveni preko izračuna granične supermatrice) zavise o tome je li matrica reducibilna (svodiva, moguće ju je smanjiti) ili nije. Ako je matrica svodiva, nakon potenciranja te matrice k puta (što je vezano uz strukturu matrice i međusobne zavisnosti elemenata), dobivaju se traženi prioriteti elemenata. Ako matrica nije svodiva, tada se koristi Cezarova suma kako bi se odredili prioriteti za sve tranzitivnosti različitih duljina. Neka je W supermatrica od n elemenata u problemu odlučivanja. Ukupna dominacija $w(A_i)$ za alternativu A_i na sve ostale alternative preko putanja različitih duljina dana je sljedećim beskonačnim nizom [165]:

$$w(A_i) = \sum_{k=1}^{\infty} \frac{\sum_{j=1}^{n} a_{ij}^{(k)}}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{(k)}}$$

čiji zbroj je Cezarova suma:

$$\lim_{M\to\infty} \frac{1}{M} \sum_{k=1}^{M} \frac{\sum_{j=1}^{n} a_{ij}^{(k)}}{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{(k)}}$$

Dodatno, problem donošenja odluke u ANP mreži može zahtijevati i analizu odluke prema 4 principa odnosno kontrolna kriterija [111, 127, 163, 164]:

- Prednosti (eng. *Benefits*, **B**) – dobre stvari koje bi proizašle donošenjem odluke
- Mogućnosti (eng. *Opportunities*, **O**) – potencijalno dobre stvari (prilike) koje mogu rezultirati u budućnosti donošenjem odluke
- Troškovi (eng. *Costs*, **C**) – određena razočaranja i gubici koji bi mogli nastati donošenjem odluke
- Rizici (eng. *Risks*, **R**) – potencijalna razočaranja i gubici koji mogu nastati donošenjem odluke.

Koristi i mogućnosti predstavljaju pozitivne čimbenike, dok su troškovi i rizici negativni čimbenici pri čemu svaki od njih na određeni način doprinosi donošenju odluke. Potrebno je odrediti najbolji ishod za svaki navedeni kontrolni kriterij pa se kombiniraju

alternative u onome što je poznato kao idealni oblik za sve kontrolne kriterije za svako **BOCR** svojstvo. Tada se uzima najbolja alternativa pod **B** i koristi se za promišljanje o prednostima te se uzima i ona alternativa najbolja ispod **O**, a koja može biti drugačija od one ispod **C**, i koristi se za promišljanje o prilikama, i tako dalje se nastavlja postupak za troškove i rizike. Na kraju, moraju se ocijeniti ova četiri svojstva s obzirom na strateške kriterije (to su kriteriji koji podliježu ocjeni osnovanosti svih odluka koje se donose) koristeći način ocjenjivanja u AHP-u za dobivanje prioritetnih ocjena za B, O, C i R kontrolne kriterije. Potom se normaliziraju (iako nije obavezno, ali se svakako preporučuje) i koriste tako dobiveni ponderi (tj. vrijednosti) za kombiniranje četiri vektora ishoda svake alternative po BOCR-u kako bi se dobilo ukupne prioritete. Sinteza modela radi se korištenjem $\frac{BO}{CR}$ omjera pri čemu alternativa s najvećim omjerom zapravo postaje sama odluka.

Tablica 5.6: Prednosti i nedostaci ANP metode [111, 123, 163, 164]:

Prednosti ANP metode	Nedostaci ANP metode
Podrška za strukturiranje složenih problema odlučivanja	Veliki broj koraka, tj. usporedbi u parovima
Podrška višestrukih kriterija, uključujući i kontrolne BOCR kriterije	Dugo trajanje procesa implementacije metode ANP zbog prevelike složenosti
Modeliranje utjecaja (zavisnosti) među kriterijima	Neodvojivost, tj. međusobna zavisnost alternativa i kriterija
Podrška za kvalitativne i kvantitativne skale kriterija	Usporedbe u parovima s obzirom na cilj odlučivanja nemaju nikakav utjecaj na ukupne težine evaluacijskih kriterija
Grupno odlučivanje	Nedovoljna veličina Saatyjeve ljestvice relativnih važnosti za usporedbu elemenata
Analiza osjetljivosti	Pri strukturiranju problema odlučivanja nije sasvim jasna primjena svojstva refleksivnosti, tj. je li na glavnoj dijagonali supermatrice potrebno postaviti vrijednosti 0 ili 1, ili je to ovisno o promatranom kriteriju

Tablica 5.6 strukturirano prikazuje uočene prednosti kao i glavne nedostatke ANP metode za višekriterijsko odlučivanje.

Sažeto, može se reći kako se izračun težina kriterija u ANP mreži odvija prema sljedećim koracima [164]:

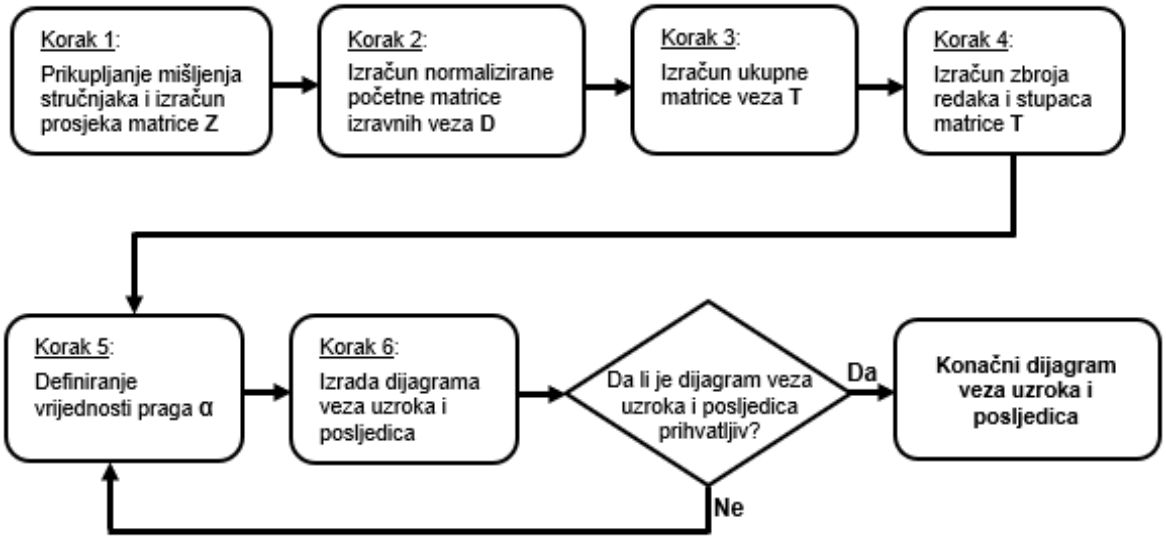
1. Identifikacija klastera s pripadajućim kriterijima
2. Izrada matrice utjecaja između kriterija unutar svakog klastera
3. Izrada matrice utjecaja između klastera.

Detaljne aktivnosti za svaki od ovih koraka prikazane su prilikom izračunavanja težina generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti (poglavlje 6.1.4) te izračunavanja težina svojstvenih (inherentnih) kriterija u studijama slučaja prilikom procesa validacije višekriterijskog modela (poglavlje *6.3 Vrednovanje višekriterijskoga modela*).

Može se reći kako mrežna zavisnost elemenata doprinosi boljem modeliranju realnih i složenih problema odlučivanja jer većina problema koja proizlazi iz realnog svijeta je nelinearna, dok povratne veze omogućavaju preciznije određivanje prioriteta elemenata (kriterija) te donošenje kvalitetnije odluke o nekom problemu.

5.2.4. DEMATEL metoda

Razvoj DEMATEL (eng. *Decision-Making Trial and Evaulation Laboratory*) metode započinje 1972. godine [116]. Metoda je vrlo prihvaćena od strane istraživača u svrhu rješavanja višekriterijskog problema odlučivanja kada postoje međusobne veze odnosno utjecaji i zavisnosti (eng. *feedback*) između kriterija koje treba analizirati i definirati, tj. odrediti težinu njihove međusobne zavisnosti [117]. Metoda DEMATEL se temelji na teoriji grafova te omogućava vizualno planiranje i rješavanje složenih problema odlučivanja, a sastoji se od sljedećih koraka [117, 118, 119]:



Slika 5.12: Proces metode DEMATEL

U nastavku slijedi prikaz i objašnjenje svih koraka DEMATEL metode.

Korak 1: Prikupljanje mišljenja stručnjaka i izračun prosjeka matrice $\boldsymbol{Z}$.

Skup od *m* stručnjaka i *n* faktora (kriterija) se koriste u ovom koraku. Od svakog stručnjaka se traži da ocijeni stupanj izravnog utjecaja između dva kriterija na temelju usporedbe u parovima. Stupanj do kojeg je stručnjak percipirao utjecaj kriterija *i* na kriterij *j* se označava kao x_{ij} pri čemu se koristi skala cijelih brojeva od 0 – 4:

- 0 – nema utjecaja (eng. *no influence*)
- 1 – nizak utjecaj (eng. *low influence*)
- 2 – srednji utjecaj (eng. *medium influence*)
- 3 – visok utjecaj (eng. *high influence*)
- 4 – vrlo visok utjecaj (eng. *very high influence*)

Tom prilikom se za svakog pojedinog stručnjaka kreira *n x n* ne-negativna matrica kao $X^k = [x_{ij}^k]$, gdje je *k* broj pojedinog stručnjaka koji sudjeluje u evaluacijskom procesu pri čemu $1 \leq k \leq m$. Tako su $X^1, X^2, X^3, ..., X^m$ matrice od *m* stručnjaka. Kako bi se agregiralo sve prosudbe prikupljene od *m* stručnjaka, prosječna matrica $Z = [z_{ij}]$ ima sljedeći izraz:

$$z_{ij} = \frac{1}{m} \sum_{k=1}^{m} x_{ij}^k$$

Korak 2: Izračun normalizirane početne matrice izravnih veza ***D***.

Normalizirana početna matrica izravne veze $D = [d_{ij}]$, pri čemu je vrijednost svakog elementa u matrici ***D*** u rasponu [0, 1].

$\boldsymbol{D} = \lambda * \boldsymbol{Z}$ ili $[d_{ij}]_{nxn} = \lambda [z_{ij}]_{nxn}$, pri čemu

$$\lambda = \min\left[\frac{1}{\max 1 \leq i \leq n \sum_{j=1}^{n} |z_{ij}|}, \frac{1}{\max 1 \leq i \leq n \sum_{i=1}^{n} |z_{ij}|}\right]$$

Na temelju teorije Markovljevih lanaca, $\boldsymbol{D^m}$ je potencija matrice ***D***, npr. $\boldsymbol{D^2}$, $\boldsymbol{D^3}$,..., $\boldsymbol{D^\infty}$ osigurava konvergentno rješenje za inverznu matricu: $\lim_{m \to \infty} D^m = [0]_{nxn}$.

Korak 3: Izračun ukupne matrice veza ***T***.

Matrica ukupnog utjecaja ***T*** dobiva se pomoću sljedeće formule: $\boldsymbol{T} = \boldsymbol{D}(\boldsymbol{I} - \boldsymbol{D})^{-1}$, gdje ***I*** predstavlja $n\ x\ n$ jediničnu matricu identiteta. Element t_{ij} predstavlja neizravan utjecaj koji je faktor *i* imao nad faktorom *j*, te tada matrica ***T*** reflektira ukupne veze između svih parova sistemskih faktora.

Korak 4: Izračun zbroja redaka i stupaca matrice ***T***.

U matrici ukupnog utjecaja ***T*** potrebno je zbrojiti retke (*r*) i stupce (*c*) kako bi se dobili traženi vektori. Zbroj nekog retka (r_i) označava ukupni utjecaj koji određeni kriterij ima na druge kriterije. Zbroj nekog stupca (c_j) označava ukupni utjecaj koji određeni kriterij prima od svih ostalih kriterija. Ako *j=i*, tada vrijednost ($r_i + c_i$) predstavlja ukupan utjecaj kojeg neki kriterij *i* ima na druge kriterije te ujedno i prima od drugih kriterija. Vrijednost ($r_i - c_i$) pokazuje utjecaj koji kriterij *i* ima na sustav. Kada je vrijednost ($r_i - c_i$) pozitivna, kriterij *i* je uzrok u mreži, a kada je vrijednost ($r_i - c_i$) negativna znači da je kriterij *i* bio primatelj u mreži.

Korak 5: Definiranje vrijednosti praga α.

Vrijednost praga α dobije se izračunom prosjeka elemenata iz matrice ***T*** pomoću sljedeće formule: $\alpha = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} [t_{ij}]}{N}$, gdje je *N* ukupni broj elemenata u matrici ***T***.

Korak 6: Izrada dijagrama veza uzroka i posljedica.

Izrađuje se NRM (eng. *Network Relationship Map*) u koordinatnom sustavu mapiranjem svih skupova koordinata ($r_i + c_i$, $r_i - c_i$) kako bi se predstavilo složene zavisnosti između kriterija i pružilo informacije za prosudbu o tome koji su najvažniji kriteriji i kako isti utječu na druge kriterije u sustavu. Kriteriji čiji t_{ij} u matrici ***T*** je veći od vrijednosti praga α su iscrtani strelicama utjecaja na grafu.

5.3. Identifikacija elemenata za analizu i procjenu rizika

U ovom poglavlju opisan je način provođenja empirijskog istraživanja kojim su prikupljeni podaci od strane stručnjaka za informacijsku sigurnost vezano uz identifikaciju najznačajnijih (kritičnih) elemenata za analizu i procjenu rizika informacijske sigurnosti. Empirijski podaci prikupljeni su provođenjem *Delphi* istraživačke tehnike.

Ranije spomenuta međunarodna norma IEC 31010:2019 za upravljanje rizicima predlaže mnoštvo metoda, alata i tehnika za identifikaciju, analizu i procjenu rizika informacijske sigurnosti pa su tako između ostalog prepoznate i MCDA metode te *Delphi* tehnika [29]. S obzirom kako je u trećoj fazi istraživanja literature (*5.1.4. Primjena MCDM metoda u svrhu procjene rizika informacijske sigurnosti*), gdje se tražilo presjek korištenja MCDM metoda s metodama za analizu i procjenu rizika, proizašla i *Delphi* kao jedna od učestalijih tehnika koja se može koristiti u procesu odlučivanja, tako je i ta tehnika korištena u

skladu sa svojim karakteristikama te vrstom problema u daljnjem istraživanju. Konkretno, *Delphi* tehnika je odabrana za potrebe identifikacije najznačajnijih elemenata za analizu i procjenu rizika koji tvore višekriterijski model u svrhu procjene, rangiranja i odabira kritičnih informacijskih sustava.

Delphi tehnika predstavlja način kombiniranja stručnog (profesionalnog) mišljenja koji može podržati izvor i utjecati na identifikaciju, procjenu vjerojatnosti i utjecaja (posljedice) te evaluaciju rizika. To je tehnika suradnje za postizanje konsenzusa među stručnjacima [29]. Dakle, *Delphi* predstavlja tehniku grupnog odlučivanja gdje je idealno da članovima skupine (stručnjacima) nije poznato tko je sve uključen u rad (ili istraživanje) pri čemu sudionici izražavaju svoje mišljenje iskreno, individualno, nezavisno i anonimno uz eventualnu mogućnost kasnijeg uvida u tuđa mišljenja (ali bez stvarnog znanja o tome tko su drugi ispitanici). Primjenjuje se kada treba ispitati više osoba nego što ih može direktno međusobno komunicirati (npr. zbog geografske dislociranosti) i kada se obavezno želi izbjeći mogući dominantan utjecaj jednog stručnjaka. *Delphi*, u odnosu na druge tehnike za prikupljanje i analizu podataka, zahtijeva više iteracija kako bi se postigao konsenzus mišljenja o određenoj temi dok se postizanje sporazuma, tj. konsenzusa oko konačne odluke stručnjaka i donositelja odluke provodi uporabom upitnika.

Iteracije se odnose na proces dobivanja povratnih informacija. Proces je promatran kao niz rundi (krugova); u svakom krugu je svaki sudionik ispunio upitnik koji je vraćen istraživaču, a koji je potom prikupio, uredio i vratio nazad svakom sudioniku izjavu o položaju cijele grupe te o vlastitom položaju. Sažetak komentara je svakog sudionika obavijestio o rasponu mišljenja i razlozima na kojima ta mišljenja počivaju. *Delphi* tehnika može se koristiti za postizanje sljedećih ciljeva [112]:

1. Odrediti ili razviti niz mogućih programskih alternativa;
2. Istražiti temeljne pretpostavke ili informacije koje vode do različitih prosudbi;
3. Tražiti informacije koje mogu stvoriti konsenzus u dijelu skupine ispitanika;
4. Uskladiti informirane prosudbe o temi koja se odnosi na širok raspon disciplina;
5. Educirati grupu ispitanika o raznolikim i međusobno povezanim aspektima teme.

Koraci u *Delphi* tehnici su sljedeći [112]:

- Predstavljanje problema i strukturiranje upitnika
- Testiranje upitnika
- Popunjavanje upitnika od strane stručnjaka (1. krug)

- Analiza prikupljenih podataka i distribucija rezultata dionicima istraživanja
- Popunjavanje drugog (i idućeg) upitnika – moguće više iteracija
- Konsenzus (opća suglasnost).

Delphi je široko rasprostranjena i prihvaćena tehnika za prikupljanje podataka od ispitanika u okviru njihovih domena stručnosti. *Delphi* tehnika je dizajnirana kao grupni komunikacijski proces koji ima za cilj konvergiranje mišljenja odnosno dobivanje odgovora na specifična pitanja [114] koja se za potrebe ovog istraživanja postavljaju u svrhu identifikacije ključnih elemenata za analizu i procjenu rizika informacijske sigurnosti te kasnije definiranja njihovih međusobnih utjecaja odnosno zavisnosti.

Odabir istraživačke teme, vremenski okviri za provođenje i dovršenje studije, mogućnost niske stope odgovora i nenamjerno usmjeravanje povratnih informacija od skupine ispitanika su elementi koje treba uzeti u obzir prilikom izrade i provedbe *Delphi* studije. Tako su identificirane sljedeće prednosti i nedostaci *Delphi* tehnike:

Tablica 5.7: Prednosti i nedostaci Delphi tehnike

Prednosti Delphi metode	Nedostaci Delphi metode
Izražavanje nepopularnih stavova je vjerojatnije zbog anonimnosti	Radno intenzivan i dugotrajan postupak, posebno za moderatora
Svi stavovi imaju jednaku težinu, čime se izbjegava problem dominantnih osobnosti	Sudionici moraju biti u stanju jasno izraziti svoje mišljenje u pisanom obliku
Ispitanik ostvaruje vlasništvo nad dobivenim rezultatima	Uspjeh metode ovisi isključivo o sudionicima (ispitanicima) istraživanja, odnosno njihovim razinama kompetencija za promatrani problem
Ispitanici se ne moraju okupiti na jednoj lokaciji istovremeno kako bi se usuglasili	Relativno složen postupak provođenja istraživanja
Mogućnost provođenja korištenjem *online* alata, npr. e-mail ili GoogleForms	
Izbjegava se problem prerane evaluacije ili odabira rješenja	

Treba istaknuti kako prema normi IEC 31010:2019, *Delphi* tehnika podržava samo prvi korak u procesu procjene rizika, a to je identifikacija rizika dok ostali koraci (analiza i evaluacija rizika) nisu podržani. No, u ovoj istraživačkoj fazi prikupljanja podataka o ISRA elementima smatra se sasvim dovoljnim.

Dodatno, treba naglasiti kako se provođenjem istraživanja *Delphi* tehnikom željelo prikupiti objektivne informacije o najznačajnijim elementima za analizu i procjenu rizika informacijske sigurnosti. Upitnik je putem elektroničke pošte odaslan stručnjacima za informacijsku sigurnost u različitim financijskim institucijama (većinom bankama) i *FinTech* tvrtkama u Europi zbog čega je izvorno i napisan na engleskom jeziku. Elementi za analizu i

procjenu rizika informacijske sigurnosti koji su ušli u prvu iteraciju *Delphi* istraživanja su sljedeći:

- Prijetnja (T)
- Ranjivost (V)
- Vjerojatnost (P)
- Posljedica (C)
- Otpornost (R)

Osnova za definiranje upravo ovih pet ISRA elemenata u inicijalnom *Delphi* upitniku proizlazi iz standarda ISO/IEC 27005 koji je identificiran sustavnim pregledom literature kao najznačajnija ISRA metoda [142]. Također, identificiran je i element otpornost u radu [84] vezano uz upravljanje kontinuitetom poslovanja gdje se DEMATEL metoda koristi u svrhu analize strukture složenih uzročno-posljedičnih veza između podindikatora ranjivosti o katastrofi (eng. *disaster vulnerability*). Iako ISO/IEC 27005 standard u funkciji rizika obavezno definira i element *imovina* (eng. *Asset*), taj element nije definiran u inicijalnom upitniku s obzirom na prirodu istraživanja i željenog višekriterijskog modela gdje je element imovina zapravo zamišljen kao cilj, odnosno najpovoljnija odabrana alternativa (tj. kritični poslovni IT sustav).

Konkretni upitnik (Excel dokument) napravljen je u obliku tablice čiji potpuni izgled i sadržaj je prikazan u Prilogu A i Prilogu B na kraju ovog rada. Iz upitnika je jasno kako se od sigurnosnih stručnjaka nisu tražili osjetljivi ili povjerljivi podaci, npr. podaci podložni GDPR[14] (eng. *General Data Protection Regulation*) regulaciji, određeni financijski podaci ili poslovne tajne. Ponuđeni odgovori vezani uz mjerenje stavova za kritične elemente za analizu i procjenu rizika informacijske sigurnosti oblikovani su kao semantičke ordinalne skale Likertova tipa te su korištene dobre prakse pri sastavljanju pitanja [114]. Uz svako pitanje dodatno je napisano i detaljno objašnjenje ISRA elemenata te što bi trebalo uzeti u obzir prilikom izražavanja vlastitog stava (npr. *vulnerability* i *threat agent* faktori za element *vjerojatnost* prema OWASP metodologiji za ocjenu rizika [120]) kako bi se osiguralo ujednačeno shvaćanje te posljedično i usporedivost odgovora. S obzirom na specifičnost istraživačkog problema te kako bi se prikupilo što više informacija od strane stručnjaka za informacijsku sigurnost o kritičnim elementima za analizu i procjenu rizika, ispitanicima je omogućen unos komentara za svako postavljeno pitanje. Ispitanici su morali nužno odgovoriti na svako postavljeno pitanje kako bi se mišljenje svakog pojedinog stručnjaka moglo provjeriti, evaluirati i usporediti. Skup

[14] ***G**eneral **D**ata **P**rotection **R**egulation* (*GDPR*) – Opća uredba o zaštiti osobnih podataka

individualnih pitanja (nevezano direktno uz elemente za analizu i procjenu rizika) napravljen je iz razloga kako bi se uvidjelo razinu kompetencija ispitanika koji su zaduženi za analizu i procjenu rizika, evaluaciju IT rješenja te konačno i najvažnije, a to je donošenje odluka u financijskim institucijama vezano uz informacijsku sigurnost. Također, prilikom slanja upitnika prema IT sigurnosnim stručnjacima predstavljeno je detaljno objašnjenje te je navedena svrha istraživanja. Anketni upitnik je pregledan i odobren od strane oba mentora ovog doktorskog rada.

Inicijalno, anketni upitnik je odaslan ukupno na 78 stručnjaka i menadžera informacijske sigurnosti, a relevantne odgovore je poslalo 38 osoba (48,72%). Prema istraživanim studijama o *Delphi* tehnici [115], u velikoj većini takvih studija za koje su dobiveni relevantni rezultati sudjelovalo je do 30 ispitanika tako da se broj od 38 odgovora ispitanika za prvu iteraciju *Delphi* tehnike ovog istraživanja može smatrati dovoljnim za statističku pouzdanost. Nakon prikupljenih podataka od ispitanika iz prvog kruga *Delphi* metode započelo se s procesom obrade podataka. Iako još uvijek ne postoji jasno definiran pristup oko mjerenja konsenzusa vezano za obradu podataka prikupljenih *Delphi* metodom [115], najčešće se kao statističke metode koriste mjere centralne tendencije (aritmetička sredina, medijan i mod) i razine disperzije (interkvartilni raspon, standardna devijacija i koeficijent varijacije) [112]. Tako su u svrhu ovog istraživanja za svaki od elemenata za analizu i procjenu rizika koji su evaluirani od strane stručnjaka za računalnu sigurnost izračunati mod, aritmetička sredina (*M*) i standardna devijacija (*SD*) na temelju pristiglih odgovora. Iako je medijan kao mjera centralne tendencije manje osjetljiv na ekstremne vrijednosti od aritmetičke sredine i vjernije prikazuje stvarno stanje u određenim situacijama (npr. kod velike razlike u plaćama između običnih radnika i menadžmenta), u ovom slučaju zbog skale za izražavanje stavova o elementima za analizu i procjenu rizika od samo 5 razina nije imalo previše smisla računanje medijan vrijednosti.

Tablica 5.8: Rezultati istraživanja dobiveni Delphi tehnikom

***Delphi* runda**	**Početni broj ispitanika**	**Broj dobivenih odgovora**	**Kriterij**	**Mod**		**Aritmetička sredina ($\bar{x}$)**	**Standardna devijacija (SD)**
				Vrijednost na Likert ljestvici	**Pojavnost**		
1	78	38	Prijetnja (T)	5-Potpuno se slažem	24	4,55	0,6857
			Ranjivost (V)	5-Potpuno se slažem	23	4,53	0,6872
			Vjerojatnost (P)	5-Potpuno se slažem	21	4,34	0,8785
			Posljedica (C)	5-Potpuno se slažem	25	4,63	0,5413
			Otpornost (R)	5-Potpuno se slažem	16	4,13	0,9056

2	38	33	Prijetnja (T)	5-Potpuno se slažem	25	4,70	0,5855
			Ranjivost (V)	5-Potpuno se slažem	23	4,70	0,5855
			Vjerojatnost (P)	5-Potpuno se slažem	19	4,52	0,6185
			Posljedica (C)	5-Potpuno se slažem	23	4,67	0,5401
			Otpornost (R)	5-Potpuno se slažem	11	3,91	0,9799
				4-Slažem se	11		
			Iskoristivost (E)	3-Neutralno	16	2,97	0,9515

Za drugi krug *Delphi* tehnike istraživački upitnik je pripremljen tako da je ponovno traženo mišljenje odnosno stav eksperata o istih pet elemenata za analizu i procjenu rizika na istoj mjernoj skali uz dostavljene podatke o modu, aritmetičkoj sredini (*M*) i standardnoj devijaciji (*SD*) za svaki od ranije evaluiranih elemenata iz prve *Delphi* iteracije. Osim toga, na temelju dobivenih komentara na otvoreno pitanje iz prvog kruga uvršten je i dodatni element, a to je iskoristivost (eng. *exploitability*, ***E***) mogućeg hakerskog napada odnosno iskoristivost poznate ranjivosti IT sustava. U svojim komentarima vezano uz element iskoristivosti kolege stručnjaci za računalnu sigurnost su se uglavnom referencirali na Microsoft STRIDE i DREAD modele [124] za rangiranje sigurnosnih prijetnji i procjenu rizika. Element iskoristivost ima za pitanje otkriti koliko jednostavno se može pokrenuti kibernetički napad i iskoristiti postojeća ranjivost nekog informacijskog sustava.

Standardna devijacija (SD[15]) izračunata je prema sljedećoj formuli:

$$s = \sqrt{\frac{(x_1 - \bar{x})^2 + (x_2 - \bar{x})^2 + \cdots + (x_n - \bar{x})^2}{n - 1}}$$

pri čemu je:

$\bar{x}$ – aritmetička sredina

n – broj elemenata nekog skupa

Treba samo napomenuti kako se ovdje zapravo radi o korigiranoj standardnoj devijaciji s obzirom kako se u naziviku ukupan broj elemenata n umanjuje za 1.

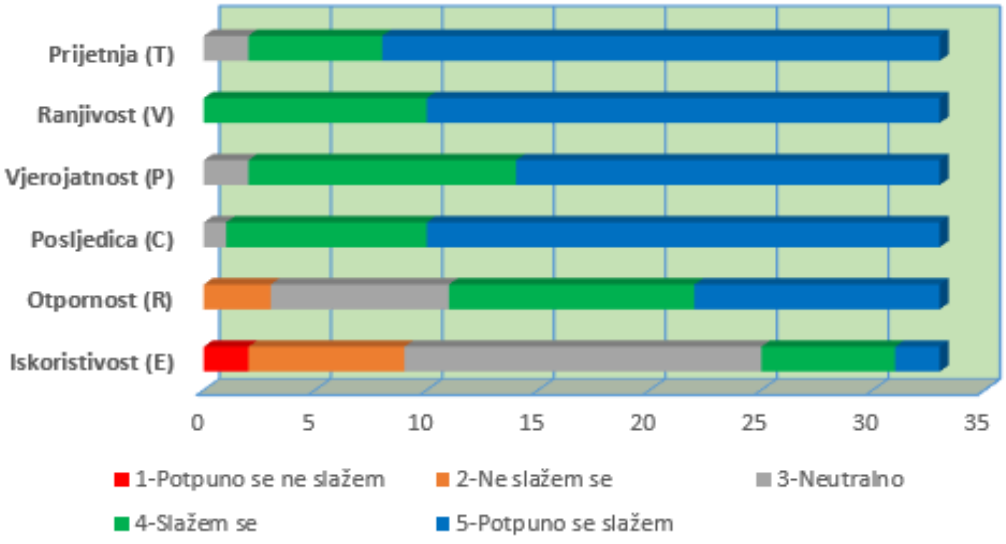
Prema [115], konsenzus u *Delphi* tehnici je postignut ako su zadovoljeni sljedeći uvjeti:

- Vrijednost standardne devijacije manja od 1,5
- Preko 51% ispitanika za pojedini element izjasnilo se za vrijednosti između 8-10 na skali vrijednosti 1-10, a što bi zapravo odgovaralo vrijednosti *5-Potpuno*

[15] *Standardna devijacija (SD)* – Statistički pojam koji označava mjeru raspršenosti podataka u nekom skupu. Interpretira se kao prosječno kvadratno odstupanje numeričkih vrijednosti od aritmetičke sredine i to u apsolutnom iznosu. Koristi se kao standard za mjerenje varijabilnosti niza. Ako je standardna devijacija mala, tada aritmetička sredina adekvatno predstavlja rezultate.

se slažem i *4-Slažem se* na skali od 5 razina. Ovih 51% se može shvatiti i kako je za prihvaćanje mod[16] (eng. *mode*) vrijednosti nužno da preko polovice odgovora za svaki kriterij bude vrednovano s ocjenom *5-Potpuno se slažem* i *4-Slažem se* ili *1-Potpuno se ne slažem* i *2-Ne slažem se*, ovisno je li mišljenje o nekom pojmu ili promatranoj pojavi afirmativno ili negativno.

Iz Tablice 5.8 vidljivo je kako je u obje iteracije standardna devijacija značajno ispod granične vrijednosti od 1,5 za svaki promatrani kriterij. Također, *mod* vrijednost za svaki element iz prve iteracije je *5-Potpuno se slažem*, dok je u drugoj rundi istraživanja *Delphi* tehnikom za istih 5 elemenata stav ispitanika također bio takav da je *mod* vrijednost *5-Potpuno se slažem*, a za dodatni element iskoristivost (predložen od strane manjeg broja ispitanika u otvorenom pitanju iz prve iteracije) *mod* vrijednost je *3-Neutralno*. S obzirom na mišljenje većine eksperata vezano uz element *iskoristivost*, a čije objašnjenje izraženo u komentarima u ispunjenom upitniku glasi kako je taj element dijelom redundantan sa elementima vjerojatnost i ranjivost i da je zapravo konceptualno dio vjerojatnosti, tako element iskoristivost neće biti uključen u konačni višekriterijski model. Iskoristivost će se pri evaluaciji IT rješenja označiti kao jedan od faktora ranjivosti (prema OWASP metodologiji za ocjenu rizika [120]) koji svakako treba uzeti u obzir prilikom procjena utjecaja između kriterija za analizu i procjenu rizika. Također, dio eksperata je u svojim komentarima naznačio kako bi uvođenje dodatnog (i dijelom redundantnog) elementa povećalo složenost novog modela, a što je svakako cilj izbjeći s obzirom na definiranu hipotezu **H2** o većoj učinkovitosti novog višekriterijskog modela.



Slika 5.13: Stavovi ispitanika o kriterijima za analizu i procjenu rizika

[16] *Mod* – Vrijednost podatka koja se najčešće ponavlja u nekom promatranom skupu, to je dominantna vrijednost.

Sa Slike 5.13 mogu se vidjeti proporcije odgovora odnosno stavova ispitanika o važnosti svakog promatranog kriterija za analizu i procjenu rizika informacijske sigurnosti iz druge iteracije *Delphi* tehnike.

Završetkom prikupljanja podataka *Delphi* tehnikom od relevantnih stručnjaka za informacijsku sigurnost te analizom istih, dobivena je ključna informacija o najznačajnijim ISRA elementima koji su integrirani u hibridni višekriterijski model za evaluaciju kritičnih IT rješenja. Time je dobiven odgovor na postavljeno istraživačko pitanje **P2** te su ostvareni preduvjeti za prelazak na sljedeću istraživačku fazu prema metodologiji znanstvenog dizajna, a to je *Dizajn i razvoj*.

6. Model za procjenu kritičnih informacijskih sustava

Ovo poglavlje daje prikaz ciljanog modela za procjenu kritičnih poslovnih informacijskih sustava kroz preostale faze metodologije znanstvenog dizajna, a što uključuje dizajn i ravoj modela, prikaz rješenja, vrednovanje i komunikaciju.

6.1. Dizajn i razvoj modela

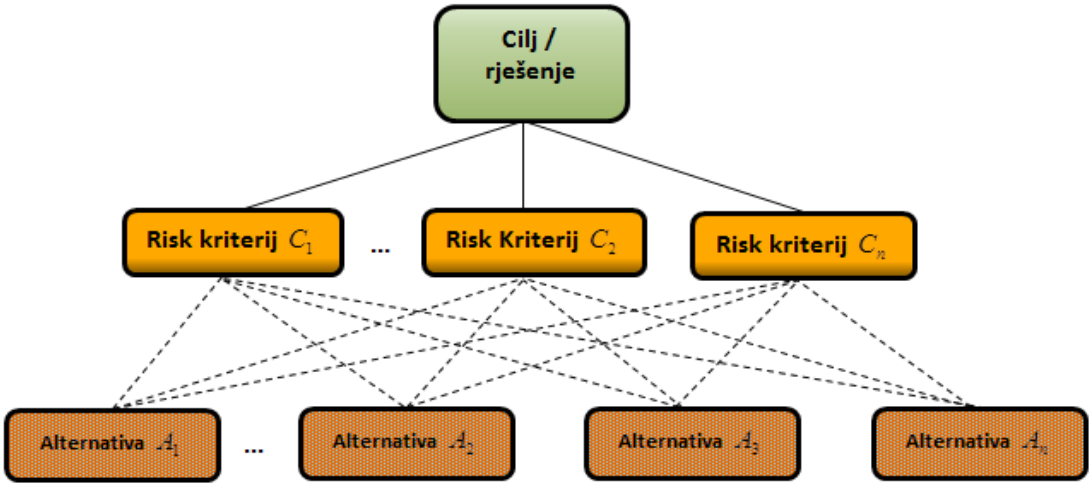
Istraživačka faza *Dizajn i razvoj* predstavlja najvažniju (kritičnu) fazu znanstvenog dizajna pa tako i ovog istraživanja jer predstavlja rezultate te faze odnosno sintezu novih spoznaja tijekom koje su razvijeni glavni doprinosi i ciljevi istraživanja (što je u konačnici izrada višekriterijskoga modela za procjenu kritičnih poslovnih informacijskih sustava), a u svrhu izrade doktorske disertacije.

Prilikom dizajna i razvoja novog modela, glavne znanstvene metode koje su korištene su konceptualno modeliranje i sinteza dosadašnjih spoznaja dobivenih kroz sustavno istraživanje literature, provođenje *Delphi* istraživačke tehnike i anketno ispitivanje, te zatim mjerenje, uspoređivanje i validacija uz korištenje određenih statističkih metoda. Na temelju prethodnih saznanja i definiranjem neophodne baze znanja prelazi se na dizajn i razvoj višekriterijskoga modela za učinkovitije donošenje informirane odluke o stanju sigurnosti i implementaciji nekog kritičnog poslovnog IT rješenja u financijskoj instituciji. Dizajn predstavlja inovativnu metodu za pronalazak učinkovitog rješenja za zadani problem pri čemu je nužno ovladati određenim organizacijskim i tehničkim znanjima i vještinama.

6.1.1. Konceptualni model

Nakon što su definirani ciljevi istraživanja potrebno je dizajnirati određeni konceptualni odnosno metamodel kako bi se novi višekriterijski model uopće mogao razviti, testirati i validirati. To je svakako bilo nužno napraviti prije izrade završnog modela za procjenu kritičnih informacijskih sustava na temelju rezultata istraživanja ISRA i MCDM metoda, tehnika i alata, kao i kritičnih ISRA elemenata *Delphi* tehnikom. Zapravo, nužno je prikazati generalizaciju mogućeg rješenja uočenog problema (preporuka za prvu fazu *Uočavanje problema i motivacija*

prema metodologiji znanstvenog dizajna [15]). Sama generalizacija modela je neophodna kako bi se dobilo kvalitetniju predodžbu što se zapravo želi napraviti i uz koje sastavne elemente odnosno komponente modela.



Slika 6.1: Generički konceptualni model

Na Slici 6.1 prikazan je konceptualni model koji opisuje kako je prilikom evaluacije alternativa (tj. kritičnih IT sustava za neku poslovnu svrhu) glavni cilj pronaći i odabrati odgovarajući IT sustav odnosno poslovno rješenje na temelju stručne procjene koristeći pritom generičke kriterije za analizu i procjenu rizika primjenom višekriterijskoga odlučivanja. Za ovu svrhu je generički konceptualni model prikazan u obliku hijerarhije zbog pojednostavljenja i lakšeg razumijevanja problematike.

6.1.2. Razvoj višekriterijskoga modela odlučivanja

Nakon predstavljanja konceptualnog modela s prikazanom generalizacijom mogućeg rješenja istraživačkog problema, prelazi se na fazu konkretnog razvoja modela. U toj fazi nužno je definirati određene preduvjete i ukazati na pretpostavljena ograničenja novog modela:

- *Komplementarnost*: Odabir prikladnih odnosno komplementarnih metoda i tehnika za procjenu rizika informacijske sigurnosti i višekriterijsko odlučivanje. S obzirom na brojnost postojećih metoda, tehnika i alata u obje promatrane istraživačke domene, izazov je svakako pronaći upravo one komplementarne metode (tj. njihove elemente) koje rješavaju uočeni složeni problem na najučinkovitiji mogući način, a

u čiju svrhu je i proveden sustavni pregled literature te je kreirana i baza znanja prema smjernicama za provedbu istraživanja temeljenog na dizajnu [60, 61].

- *Sveobuhvatnost* i *minimalnost*: Model mora sadržavati sve najznačajnije elemente (atribute) za analizu i procjenu rizika informacijske sigurnosti koji će se koristiti kao evaluacijski kriteriji u nekoj od MCDM metoda kako bi se adekvatno moglo procijeniti, rangirati i odabrati odgovarajući kritični IT sustav. No, isto tako, višekriterijski model ne smije sadržavati preveliki broj kriterija za procjenu kako bi se izbjeglo preklapanje evaluacijskih kriterija te time negativno utjecalo na traženu učinkovitost novog modela.
- *Generički atributi*: Kako bi se dobilo standardan višekriterijski model koji omogućava učinkovitije (troškovno i vremenski) rješavanje uočenog složenog problema, upravo generički elementi odnosno kriteriji za procjenu kritičnih IT sustava predstavljaju i ograničenje u vidu fleksibilnosti modela te njegovu primjenu na samo određene segmente u domeni poslovnih IT sustava u financijskom sektoru. Koji su to sve prikladni segmenti odnosno IT rješenja pokazano je provedene kroz studije slučaja.
- *Složenost*: Novi model za procjenu kritičnih IT sustava nužno mora imati nižu razinu složenosti (jednostavnije ze korisnika) u odnosu na postojeće modele i tehnike ili referentni model kako bi bio učinkovitiji te samim time potencijalno prihvaćeniji u praksi s obzirom na prepoznati deficit resursa.
- MCDM metoda za procjenu kritičnih IT sustava obavezno mora imati odnosno omogućavati sljedeća svojstva:
    - Strukturiranje problema odlučivanja (podrška za složene probleme odlučivanja)
    - Podrška za više kriterija (utjecaj većeg broja faktora na cilj odlučivanja)
    - Podrška za kvantitativne skale kriterija
    - Grupno odlučivanje
    - Analiza osjetljivosti
    - Modeliranje rizika tijekom procesa donošenja odluke
    - Pri računanju težina evaluacijskih kriterija za analizu i procjenu rizika, novi višekriterijski model mora uzimati u obzir dvije dimenzije za svaki promatrani ISRA kriterij [118]: važnost odnosno usporedbe kriterija s

obzirom na cilj odlučivanja te međusobne utjecaje i zavisnosti (eng. *feedback*) između definiranih kriterija

- Izračunavanje težina kriterija bez zavisnosti o alternativama.

Treba napomenuti da svako donošenje odluke implicira određene rizike pa tako i MCDM tehnika mora biti u mogućnosti modelirati rizike. No, s obzirom na specifičnost problema pri čemu se elementi za analizu i procjenu rizika integriraju u MCDM metodu, navedeni zahtjev se zapravo implicitno rješava preko ISRA kriterija.

Prema definiranim pretpostavkama i ograničenjima modela potrebno je odabrati prikladne elemente za analizu i procjenu rizika te odgovarajuću MCDM tehniku (ili više njih) unutar koje će se sami elementi integrirati te po kojima će se evaluirati alternative (kritična poslovna IT rješenja). Iako je u pojedinim istraživanjima [123] jedna od traženih karakteristika za MCDM metodu navedena i mogućnost modeliranja rizika prilikom odlučivanja, s obzirom na prirodu i ciljeve ovog istraživanja to ipak nije obavezan zahtjev za MCDM metodu jer je zapravo sam rizik modeliran preko ISRA elemenata.

Na temelju rezultata dobivenih istraživanjem pomoću *Delphi* tehnike (prikazano u poglavlju *5.3. Identifikacija elemenata za analizu i procjenu rizika*), elementi za analizu i procjenu rizika informacijske sigurnosti koji su postali cjelovitim dijelom novog višekriterijskoga modela su sljedeći:

- Prijetnja (eng. *Threat*, **T**)
- Ranjivost (eng. *Vulnerability*, **V**)
- Vjerojatnost (eng. *Probability*, **P**)
- Posljedica (eng. *Consequence*, **C**)
- Otpornost (eng. *Resilience*, **R**).

Za navedene elemente, tj. generičke kriterije potrebno je odrediti težine. Kako bi se dobilo neophodne težine kriterija, tj. elemenata za analizu i procjenu rizika koji se integriraju u odgovarajuću MCDM metoda u svrhu evaluacije kritičnih IT sustava, potrebno je provesti dodatno istraživanje ispitivanjem stručnjaka za računalnu sigurnost kako bi dali svoj stav o utjecajima i zavisnostima između tih elemenata koristeći standardnu DEMATEL skalu (0-4) [118]. Tom prilikom su Microsoft STRIDE i DREAD sigurnosni modeli [124] korišteni i naglašeni kao vrlo važni ulazni parametri odnosno faktori koje su ispitanici obavezno trebali uzeti u obzir prilikom procjene utjecaja između pojedinih kriterija za analizu i procjenu rizika informacijske sigurnosti. U nastavku slijedi opis STRIDE i DREAD sigurnosnih modela.

STRIDE: Mnemonički model sigurnosnih prijetnji koji služi kao pomoć u pronalasku prijetnji na informacijski sustav pri čemu svaka prijetnja predstavlja negativno odstupanje od željenog svojstva ili stanja nekog informacijskog sustava.

Tablica 6.1: Prijetnje i željena svojstva informacijskog sustava

Prijetnja	Željeno svojstvo
Lažiranje (eng. *Spoofing*, **S**)	Vjerodostojnost (eng. *Authenticity*)
Neovlaštena izmjena (eng. *Tampering*, **T**)	Cjelovitost (eng. *Integrity*)
Poricanje (eng. *Repudiation*, **R**)	Neporecivost (eng. *Non-repudiation*)
Objava informacija (eng. *Information disclosure*, **I**)	Povjerljivost (eng. *Confidentiality*)
Nedostupnost servisa (eng. *Denial of Service*, **D**)	Dostupnost (eng. *Availability*)
Podizanje ovlaštenja (eng. *Elevation of Privilege*, **E**)	Dozvola (eng. *Authorization*)

DREAD: Mnemonički model za procjenu rizika.

- Šteta (eng. *Damage,* **D**) – koliko opasan može biti napad na informacijski sustav? Npr., u kontekstu procjene elementa *posljedica* (eng. *consequence*).
- Ponovljivost (eng. *Reproducibility,* **R**) – koliko jednostavno se napad na informacijski sustav može ponoviti? Npr., u kontekstu procjene elemenata *vjerojatnosti* i *otpornosti*.
- Iskoristivost (eng. *Exploitability,* **E**) – koliko napora (vremena, novca i resursa) je potrebno za uspješan napad na informacijski sustav? Npr., u kontekstu procjene elemenata *ranjivosti* i *otpornosti*.
- Pogođeni korisnici (eng. *Affected users,* **A**) – koliko korisnika će biti pogođeno? Npr., u kontekstu procjene elemenata *prijetnje* i *posljedice*.
- Mogućnost otkrivanja (eng. *Discoverability*, **D**) – koliko je jednostavno otkriti određene prijetnje i postojanje ranjivosti u nekom sustavu? Npr., u kontekstu procjene elemenata *vjerojatnosti, prijetnje* i *ranjivosti*.

Microsoft STRIDE i DREAD modeli su vrlo važni kao ulazni faktori jer omogućavaju dodanu vrijednost i pojašnjenje ispitanicima prilikom definiranja utjecaja između elemenata za analizu i procjenu rizika.

Također, prema definiranim pretpostavkama i ograničenjima modela bilo je potrebno osim relevantnih ISRA elemenata odabrati i odgovarajuću MCDM metodu (ili više njih) unutar

koje su ISRA elementi (kriteriji) integrirani kako bi se moglo evaluirati alternative (kritične IT sustave).

S obzirom na definiciju uočenog problema gdje se na učinkovitiji način želi omogućiti donošenje prikladne (informirane) odluke o odabiru nekog kritičnog informacijskog sustava gdje se elementi za analizu i procjenu rizika integriraju u MCDM metodu pri čemu se uzima u obzir važnost kriterija s obzirom na cilj odlučivanja, a sami ISRA elementi su međusobno zavisni, tako je nužno upotrijebiti upravo onu MCDM metodu (ili više njih) koja uzima u obzir važnost ISRA kriterija te omogućava modeliranje utjecaja i zavisnosti između pojedinih ISRA evaluacijskih kriterija. U nastavku slijedi racionalizacija odluke o odabiru prikladne MCDM metode u svrhu rješavanja identificiranog istraživačkog problema.

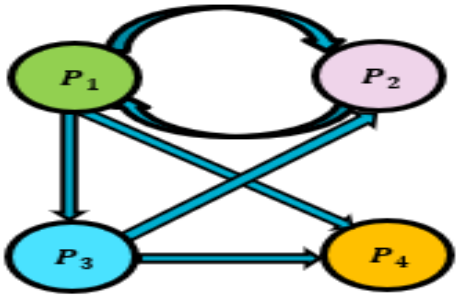
Metoda AHP svakako uzima u obzir važnost kriterija u odnosu na cilj odlučivanja, a metoda ANP uzima u obzir utjecaje (zavisnosti) između kriterija. Sustavnim pregledom literature pokazana je određena razina korištenja ANP metode unatoč složenosti primjene (često u kombinaciji sa DEMATEL metodom [117, 119]) te kako se u metodi ANP može uvesti klaster cilja. No, detaljna analiza metode ANP napravljena u radu (disertaciji) [123] pokazala je kako usporedbe kriterija s obzirom na cilj nemaju nikakve utjecaje na konačne težine evaluacijskih kriterija te samim time vrlo složeni i dugotrajni izračuni postaju nepotrebni. Osim toga, u metodi ANP su kriteriji i alternative međusobno zavisni, a što nije cilj novog modela te također predstavlja određeno ograničenje za izradu novog višekriterijskoga modela za evaluaciju kritičnih IT sustava. Zbog svega navedenog, jasno je kako najčešće korištene MCDM metode kao što su AHP, ANP, TOPSIS ili VIKOR (dobiveno na temelju rezultata sustavnog pregleda literature) nisu sasvim pogodne za rješavanje identificiranog složenog istraživačkog problema gdje se obavezno zahtijeva da novi višekriterijski model mora uzimati u obzir dvije dimenzije za svaki promatrani ISRA kriterij, a to su usporedbe evaluacijskih kriterija s obzirom na cilj odlučivanja te međusobni utjecaji i zavisnosti između definiranih kriterija. Dodatno, zahtjev je i da se težine kriterija računaju bez zavisnosti o alternativama. S obzirom kako AHP i ANP metode ne udovoljavaju ovim zahtjevima, prijedlog je da se kao MCDM metoda koja najbolje odgovara traženim svojstvima za razvoj višekriterijskog modela koristi SNAP (eng. *Social Network Analytic Process*) metoda. Do SNAP metode kao mogućeg rješenja koje najbolje odgovara traženim svojstvima za MCDM metodu došlo se dodatnim istraživanjem literature te konzultacijama s mentorima i autorom SNAP metode. U sljedećem poglavlju slijedi objašnjenje SNAP metode kao i razlozi odabira iste u svrhu razvoja višekriterijskoga modela za procjenu kritičnih IT sustava.

6.1.3. SNAP metoda

SNAP [121] je sasvim nova metoda za višekriterijsko odlučivanje razvijena za potrebe analize i rješavanja složenih problema odlučivanja temeljena na analitičkom mrežnom procesu (ANP) i mjerama centraliteta preuzetih iz metode za analizu društvenih mreža (eng. *Social Network Analysis*, SNA). U disertaciji [123], dokazano je kako SNAP metoda nema ograničenja koje imaju metode AHP (nepostojanje utjecaja/zavisnosti između kriterija) ili ANP (zanemarena važnost kriterija s obzirom na cilj, međusobna zavisnost kriterija i alternativa, kao i izrazito velika korisnička složenost zbog brojnih ponavljajućih usporedbi u parovima), te je pokazana značajnija jednostavnost korištenja SNAP metode u odnosu na ANP metodu. To su ključni razlozi odabira SNAP metode za razvoj višekriterijskoga modela.

Mjere centraliteta u metodi SNAP koriste se za izračun težina kriterija, a najvažnije mjere su stupanj centraliteta (eng. *centrality degree*) i tzv. PageRank centralitet. Glavna razlika između ove dvije mjere centraliteta vezana je uz procjenu utjecaja između kriterija gdje ispitanici, ako procijene da postoji utjecaj između dva kriterija, mogu gledati samo izravan utjecaj neovisno o drugim kriterijima, ili uzimati u obzir ukupan utjecaj agregiran sa svim indirektnim utjecajima od strane ostalih kriterija. Ako se gleda samo izravni utjecaj između kriterija, tada se primjenjuje PageRank centralitet, a kada se gledaju i ostali (posredni) utjecaji koje određeni kriterij prima, tada se za izračun težina kriterija koristi stupanj centraliteta. Npr., kod usporedbe kriterija *posljedica* sa kriterijem *prijetnja* (**C->T**), svakako postoje i posredni utjecaji od strane ostalih kriterija kao što su ranjivost sustava, vjerojatnost iskorištavanja neke ranjivosti i otpornost na proboj u informacijski sustav. No, zbog prevelike složenosti i brojnosti faktora (parametara) utjecaja koje bi svaki ispitanik trebao promatrati prilikom procjene utjecaja te velike vjerojatnosti dobivanja nekonzistentnih rezultata u procjenama, tako je ispitanicima (sigurnosnim računalnim stručnjacima) tijekom istraživanja predana uputa da gledaju samo izravan utjecaj između dva elementa za analizu i procjenu rizika. Stoga je posljedično potrebno koristiti SNAP metodu koja se temelji na PageRank centralitetu za izračun težina kriterija (mreža kriterija je težinska mreža). Treba napomenuti kako koncept izravne utjecajnosti između kriterija nije nužno tranzitivna relacija, kao što je to slučaj kod koncepta važnosti između kriterija s obzirom na cilj odlučivanja [123]. Npr. ako kriterij *prijetnja* utječe na kriterij *vjerojatnost*, a *vjerojatnost* utječe na kriterij *posljedica*, tada ne mora nužno značiti da *prijetnja* direktno utječe *posljedicu* (ovisno jasno o problemu), već može utjecati posredno preko nekog drugog kriterija (npr. preko kriterija *ranjivost* ili *otpornost*).

PageRank je algoritam korišten od strane Google pretraživača (*Google Web Search*) kako bi se rangiralo web stranice dobivene temeljem rezultata pretrage. PageRank je način mjerenja važnosti web stranica. PageRank algoritam za računanje PageRank centraliteta temelji se na pretpostavci kako je relevantna ona web stranica na koju se referencira veliki broj ostalih web stranica pritom uzimajući u obzir relevantnost, važnost ili popularnost pojedine stranice. Tako PageRank algoritam relevantnost neke web stranice određuje na temelju relevantnosti onih web stranica koje imaju definirane poveznice na promatranu web stranicu. Relevantnije web stranice će tražilica staviti na vrh popisa, a one manje relevantne na dno popisa i time omogućiti korisniku brži dolazak do pravih i pouzdanih informacija [122].



Slika 6.2: Poveznice između web stranica [122]

Na Slici 6.2 prikazane su jednostavne poveznice između web stranica na temelju kojih se PageRank algoritmom izračunava njihova relevantnost.

U disertaciji [123], predstavljeno je ukupno 12 verzija SNAP metode, a najvažnije su SNAP1, SNAP2, SNAP11 i SNAP12. Prema radu [118], treba istaknuti kako su težine kriterija dvo-komponentna mjera, pri čemu je prva komponenta važnost kriterija s obzirom na cilj, a druga komponenta su težine faktora utjecaja. SNAP2 i SNAP12 verzije ne uključuju važnost kriterija s obzirom na cilj odlučivanja (zbog toga su te dvije verzije SNAP metode usporedive s ANP metodom), što zbog definicije samog problema i međusobne povezanosti ISRA elemenata i njihove presudne važnosti za cilj (odabir prikladnog IT rješenja) nije sasvim prihvatljiva metoda za ovo istraživanje. SNAP1 verzija u težinu kriterija svakako uključuje i važnost kriterija s obzirom na cilj čime se zadovoljava traženi uvjet za MCDM metodom. No, problematika kod SNAP1 verzije je ta kako je potrebno promatrati i indirektne utjecaje između elemenata prilikom davanja ocjena na DEMATEL skali, a što bi za veliku većinu ispitanika uključenih u rješavanje ovog realnog problema odlučivanja predstavljalo dodatni napor te rizik u vidu dobivanja nekonzistentnih rezultata, a samim time i mogućnost da dijagram veza uzroka i posljedica bude neprihvatljiv promatrajući logiku samog problema odlučivanja. Dakle, SNAP1 verzija bi svakako bila sasvim prihvatljiva metoda za rješavanje problema, ali nije

optimalna za korisnika (tj. ispitanika) zbog svoje velike složenosti vezano uz davanje ocjena na DEMATEL skali.

Iz svega navedenog proizlazi, a s obzirom na definirane zahtjeve za MCDM metodom, kako je najprikladnija SNAP11 metoda za rješenje uočenog problema, tj. integraciju definiranih kriterija za analizu i procjenu rizika informacijske sigurnosti, kako bi se moglo učinkovitije procijeniti kritična IT rješenja.

Koraci metode SNAP11 su sljedeći [121, 123]:

1. Prvi ulazni element je matrica $\boldsymbol{Z}$ težinskih veza utjecaja (agregacija prikupljenih mišljenja stručnjaka i izračun prosjeka matrice $\boldsymbol{Z}$ – prvi korak u metodi DEMATEL)
2. Računanje zbrojeva stupaca i identifikacija stupca s najvećim zbrojem
3. Računanje normalizirane matrice $\boldsymbol{S}$ težinskih veza utjecaja na način da se svaki element iz matrice $\boldsymbol{Z}$ podijeli s vrijednošću identificiranog najvećeg zbroja stupca uvećanog za 1
4. Definiranje matrice $\boldsymbol{E}$ – matrica reda *n* koja ima sve vrijednosti jednake i iznosi $\frac{\mathbf{1}}{\boldsymbol{n}}$
5. Računanje matrice $\boldsymbol{G}$ po formuli $\boldsymbol{G} = (\mathbf{0,85} \cdot \boldsymbol{S}) + (\mathbf{0,15} \cdot \boldsymbol{E})$
   Razne studije su testirale različite faktore prigušenja (eng. *damping factors*), ali se općenito prema autorima Google PageRank algoritma [125] taj faktor kreće oko vrijednosti 0,85.
6. Računanje matrice $\boldsymbol{I} - \boldsymbol{G}$ ($\boldsymbol{I}$ predstavlja jediničnu matricu)
7. Računanje inverzne matrice $(\boldsymbol{I} - \boldsymbol{G})^{-\mathbf{1}}$
8. Množenje matrice $\boldsymbol{G}$ s inverznom matricom $(\boldsymbol{I} - \boldsymbol{G})^{-\mathbf{1}}$
9. Računanje vrijednosti $P_D O$, $P_D I$ i njihove razlike r (tj. $P_D O - P_D I$) za matricu iz prethodnog koraka, pri čemu je
   $P_D O$ – odlazni (eng. *outgoing*) centralitet, tj. zbroj redova u završnoj matrici
   $P_D I$ – dolazni (eng. *incoming*) centralitet, tj. zbroj stupaca u završnoj matrici
10. Dodavanje konstante *c* na razliku *r*, pri čemu je
    $c = \max_{i=1}^{n} \{P_D O(i) - P_D I(i)\} - \min_{i=1}^{n} \{P_D O(i) - P_D I(i)\}$
11. Računanje prosjeka dobivenih težina iz prethodnog koraka s težinama kriterija u odnosu na cilj odlučivanja.

Konačnim odabirom SNAP11 metode za izračun težina evaluacijskih kriterija, ostvareni su preduvjeti za prelazak na sljedeću aktivnost unutar faze dizajna i razvoja, a to je određivanje težina generičkih ISRA kriterija.

6.1.4. Određivanje težina generičkih kriterija za analizu i procjenu rizika

Metoda prikupljanja podataka od strane stručnjaka za informacijsku sigurnost, elementi (tj. evaluacijski kriteriji) koji ulaze u konačni model te faktori utjecaja na evaluacijske kriterije koje treba uzeti u obzir prilikom izražavanja stava o utjecajima između ISRA kriterija već su predstavljeni u poglavlju *6.1.2. Razvoj višekriterijskoga modela odlučivanja*.

Kako bi se moglo izračunati težine generičkih kriterija SNAP11 metodom, potrebne su dvije ulazne komponente: utjecaji (zavisnosti) između elemenata i težine kriterija u odnosu na cilj odlučivanja. Prikupljanje podataka je ponovno provedeno ispitivanjem stručnjaka za informacijsku sigurnost u dvije faze:

1. Faza: Stručnjaci su dodjeljivali ocjene na DEMATEL skali (0-4) o utjecajima (zavisnostima) između ranije identificiranih elemenata za analizu i procjenu rizika popunjavajući sljedeću tablicu:

   Tablica 6.2: Definiranje utjecaja (zavisnosti) između ISRA kriterija

Utjecaji između ISRA kriterija	T	V	P	C	R
Prijetnja (T)	0				
Ranjivost (V)		0			
Vjerojatnost (P)			0		
Posljedica (C)				0	
Otpornost (R)					0

   Na temelju dobivenih podataka (što je bio inicijalni ulaz u SNAP metodu) od stručnjaka za informacijsku sigurnost (dobiveno ukupno 23 odgovora) te provodeći cjelokupni postupak računanja utjecaja (zavisnosti) između ISRA kriterija SNAP metodom (predstavljeno u poglavlju *6.1.3. SNAP metoda*), dobivene su vrijednosti prikazane u Tablici 6.3.

   Tablica 6.3: Težine ISRA kriterija s obzirom na utjecaje (zavisnosti) između elemenata

Generički ISRA kriteriji	Težine ISRA kriterija (SNAP12)
Prijetnja (T)	0,198096379
Ranjivost (V)	0,318888835
Vjerojatnost (P)	0,143692265
Posljedica (C)	0,118888835
Otpornost (R)	0,220433685

   Dobivene težine kriterija iz Tablice 6.3 zapravo odgovaraju izračunima za SNAP12 metodu. Problem je što SNAP12 metoda ne razmatra kriterije odnosne njihove

vrijednosti s obzirom na cilj odlučivanja. Tako je s obzirom na uočenu i definiranu problematiku istraživanja potrebno dobiti i vrijednosti ISRA kriterija u odnosu na cilj kako bi se mogle izračunati konačne težine ISRA kriterija koristeći ciljanu SNAP11 metodu.

2. Faza: Stručnjaci su davali ocjene o važnosti kriterija u odnosu na cilj odlučivanja primjenom AHP metode. Identificirani ISRA kriteriji su podijeljeni u dva klastera: klaster **Rizik** (eng. *Risk*) koji sadrži 4 standardna kriterija za analizu i procjenu rizika (vjerojatnost, prijetnja, ranjivost i posljedica, prema međunarodnom standardu ISO/IEC 27005) i klaster **Otpornost** (eng. *Resiliency*). Tom prilikom koristila se standardna Saatyjeva skala [109] za usporedbu u parovima odnosno definiranje važnosti (dominacije) između ISRA kriterija. Stručnjaci su imali zadatak ispuniti sljedeće dvije tablice usporedbi (eng. ***C**omparisons **T**able*) u parovima, **CT1** i **CT2**.

Tablica 6.4: Usporedbe klastera za generičke kriterije

CT1	Otpornost	Rizik
Rizik	1	
Otpornost		1

Tablica **CT1** ima za cilj usporediti važnost (dominaciju) između klastera **Otpornost** i **Rizik**, tj. definirati koji kriterij odnosno klaster je važniji (kritičniji) u zaštiti vrijednosti IT imovine. Na glavnoj dijagonali vrijednosti su postavljene na 1 prema Saatyjevoj skali jer se međusobno uspoređuju isti elementi.

Tablica 6.5: Usporedbe kriterija unutar klastera Rizik

CT2	P	T	V	C
Vjerojatnost (P)	1			
Prijetnja (T)		1		
Ranjivost (T)			1	
Posljedica (C)				1

Tablica **CT2** ima za cilj usporediti važnost pojedinih kriterija unutar klastera **Rizik**. Za svaku usporedbu u paru potrebno je dati i odgovarajuću recipročnu vrijednost. Također je važno naglasiti da se u tom postupku treba poštivati pravilo tranzitivnosti. Npr., ako ranjivost (V) dominira u odnosu na prijetnju (T), a prijetnja dominira u odnosu na vjerojatnost (P), tada ujedno vrijedi kako ranjivost dominira nad kriterijem vjerojatnost. Ako pravilo tranzitivnosti nije ispoštovano, tada omjer

konzistentnosti (eng. *Consistency Ratio*, **CR**) raste što može dovesti do nezadovoljavajuće vrijednosti za CR, a koja mora biti ispod 0,1 (ali obavezno pozitivna) kako bi se prosudbe stručnjaka smatrale valjanima. Upitnik dostavljen stručnjacima za IT sigurnost prikazan je u Prilogu C u izvornom obliku. U ovoj podfazi dobiveno je ukupno 22 odgovora (pravilno ispunjene obje tablice) od strane ispitanika.

Težine kriterija s obzirom na cilj odlučivanja (međukorak za izračun SNAP11 kriterija) primjenom AHP metode prikazane su sljedećom tablicom:

Tablica 6.6: Težine ISRA kriterija s obzirom na cilj odlučivanja

Generički ISRA kriteriji	Težine ISRA kriterija (AHP)
Prijetnja (T)	0,105824012
Ranjivost (V)	0,186796789
Vjerojatnost (P)	0,057177557
Posljedica (C)	0,196417034
Otpornost (R)	0,453784608

Konačne težine generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti dobivene primjenom aritmetičke sredine na vrijednosti iz Tablice 6.3 i Tablice 6.6 prikazane su u Tablici 6.7.

Tablica 6.7: Težine kriterija za generičke ISRA elemente dobivene SNAP11 metodom

Generički ISRA kriteriji	Težine ISRA kriterija (SNAP11)
Prijetnja (T)	0,151960196
Ranjivost (V)	0,252842812
Vjerojatnost (P)	0,100434911
Posljedica (C)	0,157652935
Otpornost (R)	0,337109146

Dobivene težine generičkih ISRA kriterija iz Tablice 6.7 korištene su kao vektor za umnožak zajedno sa vrijednostima svojstvenih vektora (eng. *eigenvector*) dobivenih pri evaluaciji kritičnih poslovnih IT sustava prema ISRA kriterijima u istraživačkoj fazi vrednovanje (poglavlje *6.3. Vrednovanje višekriterijskoga modela*).

Cjelokupni postupak računanja težina generičkih kriterija za analizu i procjenu rizika SNAP11 metodom prikazan je u Prilogu D (agregacija individualnih procjena).

6.1.5. Odabir MCDM metode za evaluaciju alternativa

Nakon dobivanja težina evaluacijskih kriterija SNAP11 metodom, sljedeći korak je primijeniti odgovarajuću metodu za višekriterijsko odlučivanje kako bi se pomoću definiranih generičkih kriterija i pripadajućih težina moglo evaluirati alternative (tj. kritične IT sustave) u studijama slučaja.

B. Roy [128] ističe kako je odabir MCDA metode iznimno važan element u rješavanju problema odlučivanja, te da bi se dobilo odgovarajuće rješenje za neki problem isto tako donositelj odluke mora odabrati i primijeniti odgovarajuću metodu. Donositelji odluka često nisu u stanju opravdati svoj izbor metode koja je primijenjena za rješavanje određenih situacija odlučivanja i odabir MCDM metode je uglavnom napravljen proizvoljno te je motiviran znanjem samog donositelja odluke o odabranoj metodi ili dostupnosti softverske podrške za određenu metodu [131, 132]. Slični problemi postoje i kod odabira MCDM softvera pri čemu donositelji odluka najčešće biraju softver za podršku odlučivanju koji im je poznat [133] pa tako dolazi do situacije da određena MCDM metoda nije odabrana u svrhu rješavanja konkretnog problema nego je problem odlučivanja zapravo prilagođen odabranoj MCDM metodi i pripadajućem softveru. Problem odabira odgovarajuće MCDM metode za određenu situaciju odlučivanja je vidljiv u tome što razne metode mogu dati različite rezultate za istu promatranu situaciju. Znači, odabir MCDM metode ovisi o karakteristikama samog problema odlučivanja.

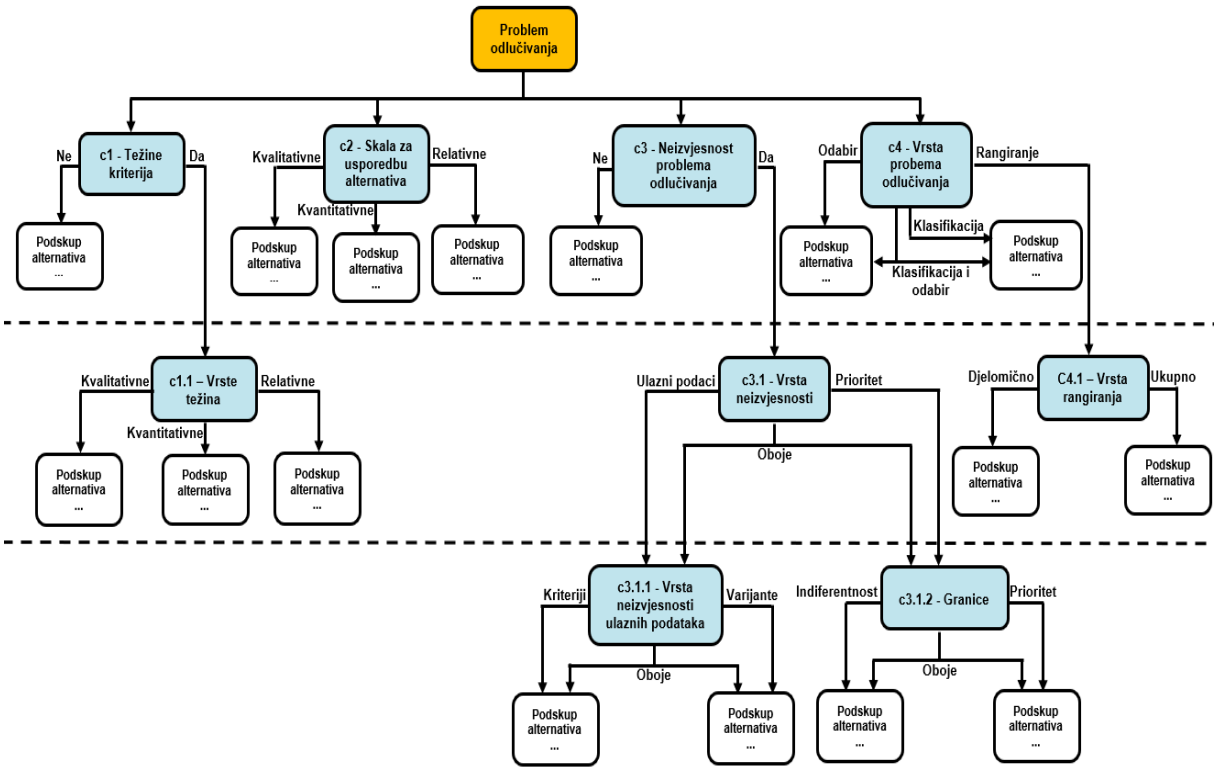
Tako je ovom prilikom bilo nužno provesti dodatno istraživanje kako bi se vidjelo postoji li definirana metodologija, okvir (eng. *framework*) ili određene upute za odabir adekvatne MCDM metode, a s obzirom na već definirane zahtjeve za MCDM-om (poglavlje *6.1.2. Razvoj višekriterijskoga modela odlučivanja*), kao i činjenicu da postoje izračunate težine generičkih ISRA kriterija dobivene SNAP11 metodom. Provedena je analiza literature te su identificirani značajni radovi koji se bave problemom odabira i sistematizacije MCDM metoda za određeni problem donošenja odluka [132]. Međutim, raspon ovih rješenja često je ograničen na nekoliko najpoznatijih MCDM metoda ili na jedno proizvoljno odabrano polje primjene. S obzirom na problemsku domenu ovog istraživanja te kako osim članka [130] nisu pronađena druga relevantna istraživanja vezano uz konkretan odabir adekvatne MCDM metode u kontekstu procjene stanja sigurnosti IS-a i/ili rizika informacijske sigurnosti, tako je kao polazna osnova za odabir relevantne MCDM metode korišten općeniti okvir za odabir MCDM metode koji je neovisan o problemskoj domeni [129]. Predloženi okvir temelji se na određivanju skupa karakteristika dostupnih MCDM metoda i karakteristika određenog

problema odlučivanja te predstavlja pokušaj rješavanja neizvjesnosti u procesu odabira MCDM metode. Valjanost okvira je potvrđena znanstvenim istraživanjem u kojemu su preporuke za upotrebu MCDM metoda predložene tim okvirom jednako konzistentne metodama korištenima od strane stručnjaka za rješavanje specifičnih problema u području održivosti transporta i logistike. Okvir u svom početku traži da donositelj odluke (eng. *Decision Maker*, DM) definira samo tzv. općenite deskriptore (*c*) problema odlučivanja. Predloženi deskriptori su sljedeći:

- c1 – da li će se koristiti težine pojedinačnih kriterija; mogućnosti: Da/Ne
- c2 – vrsta skale po kojoj će se evaluirati performanse alternativa u odnosu na definirane kriterije; mogućnosti: kvalitativna, kvantitativna ili relativna skala
- c3 – da li postoji neizvjesnost u problemu odlučivanja; mogućnosti: Da/Ne
- c4 – kakva je vrsta problema odlučivanja; mogućnosti: odabir, klasifikacija, rangiranje + odabir ili klasifikacija + odabir.

Treba svakako istaknuti da prema [129], navedeni deskriptori korespondiraju s karakteristikama MCDM metoda.

Sukladno navedenom, odabir prikladne MCDM metode može se prikazati i hijerarhijski u obliku stabla na Slici 6.3.



Slika 6.3: Stablo odluke za odabir prikladne MCDM metode na temelju deskriptora [129]

Na Slici 6.3 vide se mogućnosti grananja stabla u predloženom okviru za odabir MCDM metoda te kako za svaku opciju postoji određeni podskup alternativa. Stablo zapravo predstavlja problem odabira MCDM metode ovisno o informacijama o problemu odlučivanja koje su poznate donositelju odluke. U realnom svijetu, donositelj odluke često nema potpuno znanje o problemu odlučivanja te ne može jasno odrediti karakteristike (deskriptore) za svaku razinu hijerarhije, uvodeći tako neizvjesnost u odlučivanje. No, općeniti okvir je fleksibilan te se njegovom primjenom može doći do proširenog skupa MCDM metoda za potencijalno rješenje problema. S obzirom na karakteristike problema odlučivanja vezano uz procjenu, rangiranje i odabir kritičnog IT sustava primjenom višekriterijskoga odlučivanja s elementima za analizu i procjenu rizika, a koji je predmetom ovoga rada i istraživanja, ulazni parametri (tj. deskriptori) su sljedeći:

- c1 – Težine kriterija: **da**, postoje – izračunate SNAP11 metodom
    - c1.1 – Vrste težina kriterija: **relativne**.

      Kontekst: Iako postoje jasno izračunate težine kriterija za svaki atribut, tražene težine ipak se ne mogu smatrati egzaktnima već relativnima jer su ulazni parametri prikupljani od strane stručnjaka za informacijsku sigurnost koji mogu imati različite stavove o značaju atributa za analizu i procjenu rizika kao i znanja o MCDM metodama te usporedbi u parovima koje je bilo nužno provesti kako bi se dobilo ulazne parametre.
- c2 – Vrsta skale za evaluaciju alternativa: **relativna**.

  Kontekst: S obzirom kako su vrste težina kriterija definirane kao relativne, istom logikom se vodio i odabir vrste skale za evaluaciju alternativa kako bi se zadržalo konzistentnost vezano uz odabir deskriptora.
- c3 – Neizvjesnost problema odlučivanja: **ne**.

  Kontekst: Inicijalna neizvjesnost je svakako postojala vezano uz ulazne podatke u kontekstu težina kriterija za analizu i procjenu rizika. No, s obzirom na veličinu uzorka i razinu kompetencija ispitanih eksperata iz domene informacijske sigurnosti, njihovu geografsku rasprostranjenost i međusobnu neovisnost te relativnu konzistentnost u davanju procjena, neizvjesnost se u ovom slučaju ipak može zanemariti. Neizvjesnost vezano uz ulazne podatke o varijantama/alternativama koje se mogu procjenjivati (npr. m-banking aplikacija, napredni vatrozid, karakteristike poslužitelja, itd.) ne postoji jer svi podaci o kritičnom IT sustavu prilikom dostavljanja ponuda od strane dobavljača moraju biti jasno specificirani kako bi se uopće mogla raditi evaluacija istih.

- c4 – Vrsta problema odlučivanja: **rangiranje + odabir**.

  Kontekst: Cilj je odabrati poslovno IT rješenje s adekvatnim mjerama zaštite koje se uklapa u postojeći informacijski sustav financijske institucije, ali isto tako omogućiti i rangiranje alternativa kako bi se u slučaju utjecaja od strane nekih vanjskih (dodatnih) kriterija (npr. cijena ili podrška dobavljača) budući model mogao proširiti novim atributima (koji ipak nisu sigurnosni elementi) te tako odabrati prikladno rješenje. Znači, s deksriptorom **rangiranje + odabir** implicira se skalabilnost i modularnost novog višekriterijskoga modela za odabir kritičnih poslovnih IT sustava u svrhu budućih istraživanja.

  - c4.1 – Vrsta rangiranja: **potpuno**.

    Kontekst: Prema ISACA definiciji [134], rangiranje rizika izvodi se iz kombinacije svih komponenti rizika, uključujući prepoznavanje prijetnji i karakteristika izvora prijetnji, ozbiljnost ranjivosti, vjerojatnost uspjeha kibernetičkog napada uzimajući u obzir učinkovitost implementiranih kontrola te utjecaj na organizaciju u slučaju uspješnog napada. Tako i vrsta rangiranja postaje važna za ovaj problem odlučivanja, jer iako bi moguće i parcijalni rang u određenoj mjeri zadovoljio cilj da se odabere prikladno (najbolje) IT rješenje među promatranim alternativama, ipak se kompletni rang smatra cjelovitim pristupom s obzirom na kontekst samog problema odlučivanja pri čemu se u novi višekriterijski model integriraju generički kriteriji za analizu i procjenu rizika informacijske sigurnosti.

Primjenom karakteristika navedenih deskriptora u aplikativnu podršku[17] izrađenu za predloženi općeniti okvir [129], dobivaju se sljedeće mogućnosti za odabir MCDM metode:

AHP, ANP, MACBETH, DEMATEL i REMBRANDT.

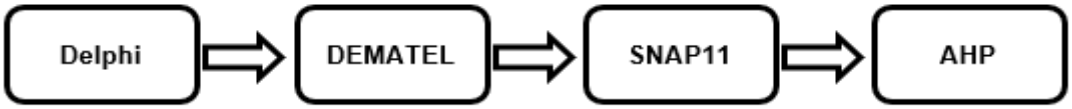
S obzirom na specifičnu problematiku odlučivanja i zahtjeve za evaluacijskim kriterijima gdje se moraju uzimati u obzir utjecaji i zavisnosti između kriterija kao i važnost kriterija s obzirom na cilj odlučivanja i da kriteriji moraju biti neovisni o alternativama, te na činjenicu kako je tijekom procesa izračuna težina generičkih kriterija već korištena AHP metoda (kao cjeloviti dio SNAP11 metode), odabir AHP-a kao metode za evaluaciju kritičnih IT sustava čini se sasvim opravdanim u odnosu na ostale predložene metode dobivene primjenom deskriptora iz općenitog okvira za odabir MCDM metode. Brojne prednosti i razlozi korištenja AHP metode već su prethodno detaljno opisani u Tablici 5.5.

[17] http://www.mcda.it/ – web platforma za podršku općenitom okviru za odabir MCDM metode

6.2. Prikaz rješenja (Demonstracija)

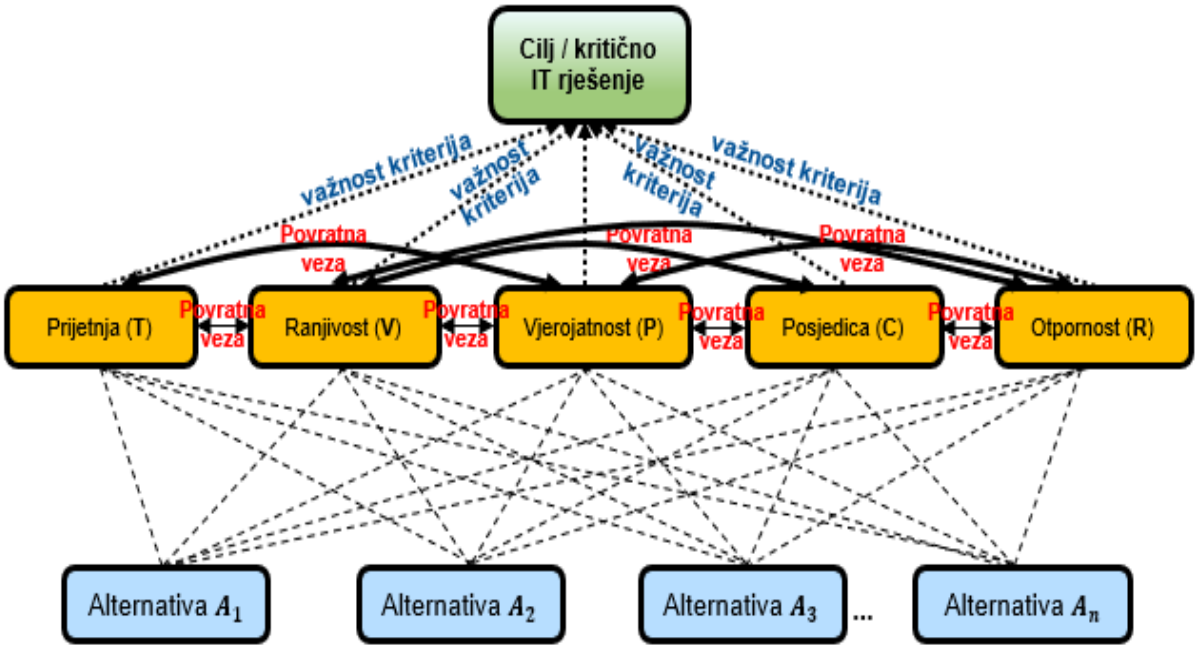
Na temelju rezultata istraživanja o najvažnijim elementima za analizu i procjenu rizika proizašlih provođenjem *Delphi* istraživačke tehnike, analizom MCDM metoda, identifikacijom veza između ISRA elemenata te definiranjem njihovih težinskih utjecaja, u ovom poglavlju prikazan je konačni model za procjenu kritičnih IT rješenja.

Najprije su prikazane komponente više razine kako bi se sumiralo istraživački postupak kojim se došlo do novog modela.



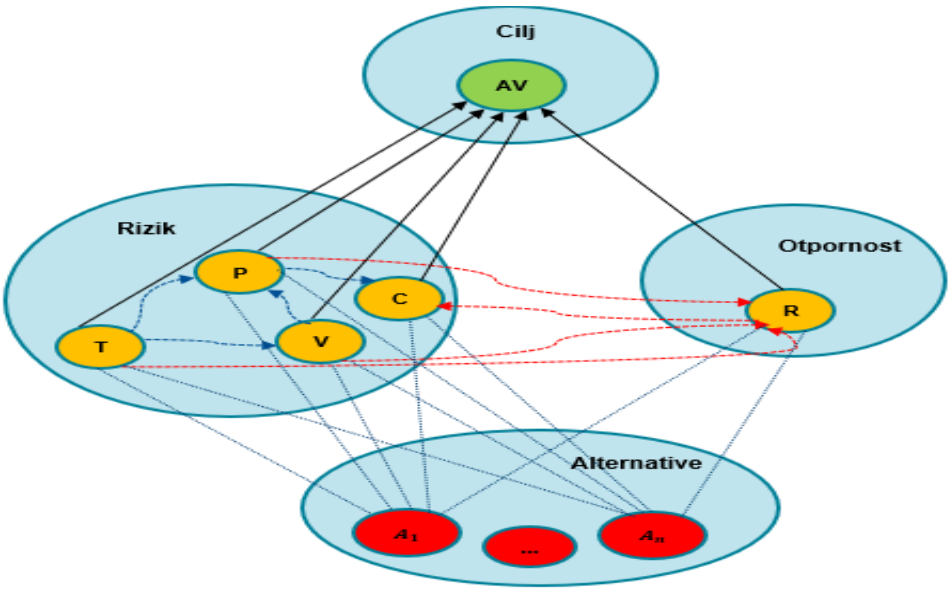
Slika 6.4: Komponente više razine hibridnog višekriterijskog modela

Na Slici 6.4 prikazane su glavne komponente više razine pomoću kojih se došlo do novog višekriterijskoga modela. Inicijalno, *Delphi* istraživačkom tehnikom prikupljeni su podaci o relevantnim kriterijima i pripadajućim faktorima utjecaja na kriterije za analizu i procjenu rizika informacijske sigurnosti, a što je bila prva faza istraživanja. Zatim se za takve identificirane ISRA elemente trebalo izračunati međusobne utjecaje i zavisnosti (eng. *feedback*) korištenjem inicijalno DEMATEL metode (druga faza istraživanja) te potom SNAP11 metode (treća faza istraživanja) kako bi se izračunalo težine generičkih kriterija u odnosu na cilj odlučivanja. Tako dobivene težine generičkih kriterija za analizu i procjenu rizika korištene su za potrebe procjene kritičnih informacijskih sustava u četvrtoj fazi istraživanja.



Slika 6.5: Višekriterijski model s generičkim ISRA elementima za procjenu IT kritičnih sustava

Novi hibridni višekriterijski model za procjenu kritičnih informacijskih sustava s generičkim ISRA atributima prikazan na Slici 6.5 korespondira konceptualnom modelu prikazanom na Slici 6.1 u poglavlju *6.1.1. Konceptualni model*.



Slika 6.6: Razvijeni višekriterijski model za procjenu kritičnih IT sustava – klasteri

Slika 6.6 prikazuje sve definirane klastere te utjecaje i zavisnosti između klastera kao i elemenata unutar klastera **Rizik**. Također, prikazana je i važnost evaluacijskih kriterija u odnosu na cilj odlučivanja (klaster vrijednost imovine, tj. traženi kritični IT sustav – eng. *Asset Value*, **AV**) što je važno zbog ciljane SNAP11 metode koja podržava taj zahtjev, te neovisnost kriterija u odnosu na moguće alternative (kritične IT sustave). Sve navedeno i prikazano Slikom 6.6 iznimno je bitno zbog zahtjeva i karakteristika traženih za MCDM metodu za procjenu kritičnih IT sustava (definirano u *6.1.2. Razvoj višekriterijskoga modela odlučivanja*), kao i navedeni mrežni prikaz definiranih klastera i pripadajućih elemenata te njihovih međusobnih odnosa (utjecaja i zavisnosti).

Predstavljanjem novog višekriterijskom modela u istraživačkoj fazi *Demonstracija* prema metodologiji znanstvenog dizajna, uspješno se ostvaruje definirani specifični istraživački cilj **C2**, čime se omogućuje prelazak na sljedeću istraživačku fazu vezano uz validaciju samog modela.

6.3. Vrednovanje višekriterijskoga modela

Proces vrednovanja, odnosno validacija, predstavlja centralni i ključan korak u istraživačkoj paradigmi znanstvenog dizajna [16, 59, 60] kako bi se uopće dobila informacija da li novokreirani artefakt daje očekivane (bolje) rezultate u odnosu na neki referentni model (ako takav postoji) te kako bi se osiguralo i ispoštovalo strogost (eng. *rigour*) zahtjeva znanstveno-istraživačkog procesa sa svrhom prikazivanja korisnosti, kvalitete i učinkovitosti dizajniranog artefakta korištenjem dobro izvedenih evaluacijskih metoda [60]. Znači, kako bi se novi DSR (eng. *Design Science Research*) artefakt mogao zaista klasificirati kao znanstveni, validacija mora biti stroga, releventna te znanstveno utemeljena.

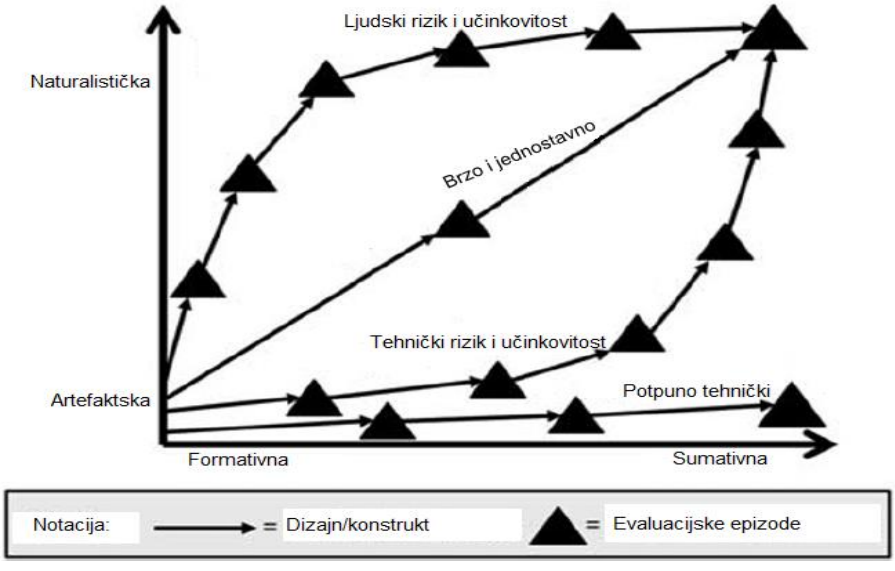
S obzirom kako je u ovom radu riječ o mješovitoj vrsti istraživanja (eng. *Mixed research*) što uključuje kombiniranje komplementarnih snaga i nepovezanih slabosti kvantitativnih i kvalitativnih metoda istraživanja, procjena valjanosti nalaza može biti posebno složena, a što dovodi do problema integracije. Validacija se u mješovitim istraživanjima naziva legitimacija [152], a što predstavlja proces koji je analitički, socijalni, estetski, politički i etički te koji mora uključivati zajednicu kvantitativnih i kvalitativnih znanstvenika koji su predani rješavanju višestrukih problema koji se mogu pojaviti u mješovitim istraživanjima. Prema [152], postoji ukupno 9 vrsta legitimacija u mješovitim istraživanjima, pri čemu se u ovom istraživanju koristi legitimacija umanjivanjem slabosti (eng. *Weakness minimization legitimation*). Mješovito istraživanje smatra se najpogodnijim za maksimiziranje ovog oblika legitimacije jer je istraživač u mogućnosti na sistematičan način dizajnirati studiju koja kombinira više metoda. Pri tome je ključno pažljivo procijeniti opseg u kojemu se slabosti jednog pristupa kompenziraju s prednostima drugog pristupa te potom planirati i dizajnirati studiju kako bi se ispunilo istraživački potencijal. Istraživač također mora koristiti ova znanja prilikom kombiniranja, ponderiranja i tumačenja rezultata.

Kao pristup za potporu legitimaciji umanjivanjem slabosti u ovom istraživanju koristi se FEDS okvir (eng. *Framework for Evaluation in Design Science Research*) [153]. FEDS okvir omogućava istraživačima izradu strategije za evaluaciju artefakta razvijenog temeljem DSR paradigme. FEDS strategija razmatra zašto, kada, kako i što zapravo treba vrednovati. FEDS okvir omogućava podršku za donošenje odluke o vrednovanju dizajna (artefakta) istraživanja povezujući evaluacijske ciljeve i evaluacijske strategije. Razlog odabira FEDS okvira za vrednovanje novog višekriterijskog modela je taj što mnoge druge poznate metode i paradigme za validaciju [15, 16, 59, 60, 154] ne daju dovoljno jasne smjernice za provedbu validacije ili izradu strategije za evaluaciju znanstvenog dizajna (kako, kada i što). FEDS je okvir za

vrednovanje posebno prikladan za uporabu u DSR-u. Važna značajka FEDS okvira je usredotočenost na dvije ključne svrhe validacije u DSR-u, pri čemu se validacija ne odnosi samo na aspekt korisnosti artefakta u okolini, već i na kvalitetu znanja pridonesenog izgradnjom artefakta. Kako bi se bolje postigle obje svrhe, istraživači mogu osmisliti strategiju procjene FEDS-a koja ne samo da odgovara ciljevima i postavkama DSR projekta, već održava i korisnost artefakta u njegovom okruženju i prijenos znanja ostalim zainteresiranima.

FEDS okvir sastoji se od dva aspekta odnosno dimenzije za vrednovanje znanstvenog dizajna:

- Funkcionalna svrha vrednovanja, a koja može biti tvorbena (eng. *formative*) ili sumarna (eng. *summative*). Ova dimenzija daje odgovor na pitanje zašto vrednovati. Formativna evaluacija je usmjerena na posljedice te podržava odluke kojima se želi poboljšati sam subjekt evaluacije (tj. novi artefakt). Sumarna evaluacija usredotočena je na značajnost te podržava vrste odluka kojima se želi utjecati na odabir artefakta za određenu primjenu.
- Paradigma vrednovanja studije, a koja može biti artefaktska (eng. *artificial*) ili prirodna (eng. *naturalistic*). Ova dimenzija daje odgovor na pitanje kako vrednovati. Artefaktska evaluacija uključuje laboratorijske pokuse, simulacije, analizu temeljenu na kriterijima, teorijske argumente i matematičke dokaze. Naturalistička evaluacija istražuje svojstva tehnološkog rješenja u stvarnom okruženju (npr. stvarni ljudi, sustavi i postavke). Naturalistička evaluacija je uvijek empirijska pri čemu znanstvene evaluacijske metode najčešće uključuju studije slučaja, terenske studije, terenske eksperimente i ankete.



Slika 6.7: FEDS okvir sa evaluacijskim strategijama [153]

Tijekom evaluacijskih epizoda u vrednovanju DSR projekta primjenom FEDS okvira, potrebno je odabrati i odgovarajuću strategiju. Na Slici 6.7 prikazane su ukupno četiri moguće strategije vrednovanja. No, kako bi se moglo primijeniti FEDS okvir, definiran je i proces za izradu specifične strategije u svrhu vrednovanja znanstvenog dizajna odnosno novog artefakta, a sastoji se od četiri slijedna koraka:

1. Objasniti ciljeve evaluacije

   Mogući su sljedeći konkurentski ciljevi u dizajniranju evaluacijske komponente DSR-a koje je svakako nužno razmotriti:

   - *Strogost*: Cilj evaluacije (u ovom slučaju sumarnog tipa) je provjeriti primjenjivost, valjanost i učinkovitost novog artefakta (višekriterijskoga modela) međusobnom usporedbom rezultata sa studije slučaja, pri čemu se uspoređuju rezultati dobiveni procjenom kritičnih poslovnih IT sustava koristeći generičke ISRA kriterije sa rezultatima dobivenima koristeći inherentne kriterije promatranog kritičnog informacijskog sustava u realnom okruženju (financijskoj instituciji).
   - *Neizvjesnost i smanjenje rizika*: Kako bi se smanjilo neizvjesnost i rizike tijekom DSR projekta, formativna evaluacija je zadovoljena izradom baze znanja. Inicijalno je napravljen sustavni pregled literature (SLR, [142]) za definirana istraživačka područja (rizici informacijske sigurnosti i višekriterijsko odlučivanje), a potom je napravljeno istraživanje provođenjem *Delphi* tehnike gdje se ispitivanjem relevantnih stručnjaka za informacijsku sigurnost iz više različitih europskih zemalja dobilo adekvatne informacije te identificiralo ključne elemente (evaluacijske atribute) za izradu novog višekriterijskoga modela. Odabrani stručnjaci za informacijsku sigurnost iz financijskih institucija i povezanih FinTech tvrtki su nužno morali zadovoljavati kriterije relevantnog iskustva rada u financijskim institucijama, akademski stupanj (min. bacc.), posjedovanje relevantnih industrijskih certifikata (CISSP, CISM, CRISC, CEH, itd.) te poznavanje domene upravljanja rizicima informacijske sigurnosti. Tako je baza znanja poslužila kao referentna točka za izradu novog višekriterijskog modela te istodobno i njegove inicijalne (*ex ante*) evaluacije. U kasnijoj, sumativnoj fazi evaluacije, strogost i smanjenje neizvjesnosti (rizika) su postignuti definiranjem referentnog modela za usporedbu s pripadajućim kriterijima inherentnima promatranom (evaluiranom) kritičnom poslovnom

informacijskom sustavu, pri čemu je korištena adekvatna znanstvena literatura kao referenca za odabir inherentnih kriterija.

- *Etika*: Tijekom evaluacije artefakta, ispitanicima je poslan materijal s detaljnim objašnjenjima problematike i ciljeva istraživanja, ali sami ispitanici nisu znali tko je sve uključen u istraživanje kako bi se osiguralo nepristranost. Također, ispitanicima je doznačeno kako njihovi osobni podaci neće biti nigdje objavljeni niti korišteni te da se na kraju radi agregacija svih pojedinačnih procjena (prema SNAP metodologiji).
- *Učinkovitost*: Evaluacija novog višekriterijskog modela za procjenu kritičnih informacijskih sustava je prema FEDS okviru vezano uz paradigmu vrednovanja zapravo naturalističkog tipa pri čemu se provodilo studije slučaja sa svrhom potvrđivanja hipoteze H1 (vezano uz valjanost novog modela) i hipoteze H2 (vezano uz potvrđivanje učinkovitosti modela). Naturalistička evaluacija sa provođenjem studije slučaja na stvarnim poslovnim IT sustavima i stvarnim ljudima (sigurnosnim stručnjacima iz financijskih institucija) uzrokovala je porast troškova ovog istraživanja (prvenstveno vremenski), ali isto tako nudi veću vrijednost te osigurava veću strogost u procjeni učinkovitosti višekriterijskog modela u odnosu na artefaktsku evaluaciju, a što je posebno važno u kontekstu potvrđivanja hipoteze H2.

2. Odabir evaluacijske strategije (ili više njih)

   Svaka strategija podrazumijeva odluku o tome zašto, kada i kako vrednovati. Pri odabiru evaluacijske strategije potrebno je razmotriti i određene heuristike:

   - Procijeniti i odrediti prioritete za rizike dizajna koji su shvaćeni kao mogući problemi s kojima se dizajn može suočiti. U kontekstu novog višekriterijskoga modela, glavni rizik dizajna je korisnički orijentiran, točnije (ne)poznavanje primjene metoda višekriterijskoga odlučivanja za potrebe procjene, rangiranja i odabira IT sustava.
   - Procijeniti troškove vrednovanja sa stvarnim korisnicima te stvarnim IT sustavima i stvarnim postavkama promatranih sustava. U kontekstu novog višekriterijskoga modela, bilo je relativno jednostavno i jeftino (u smislu vremenskih zahtjeva) angažirati relevantne sigurnosne IT stručnjake iz financijskih institucija u svrhu evaluacije samog modela na stvarnim IT sustavima. Ograničenje predstavlja što je takvih stručnjaka s adekvatnim

znanjima o rizicima informacijske sigurnosti te kritičnim bankovnim informacijskim sustavima relativno malo u području, ali su identificirani te su sudjelovali u evaluaciji novog višekriterijskoga modela.

- Procijeniti je li kreirani artefakt čisto tehnički (ne uključuje ljude) ili problem adresiran dizajnom zapravo već postoji ili će postojati u budućnosti. U kontekstu novog višekriterijskoga modela, problem adresiran dizajnom i razvojem već postoji u realnom okruženju, a što je zapravo bila i glavna motivacija za izradu novog modela koji nije isključivo tehnički već je namijenjen donositeljima odluka vezano uz kritične poslovne IT sustave u financijskim institucijama.
- Procijeniti veličinu i složenost konstrukcije dizajna novog artefakta. Novi višekriterijski model je razmjerno veliki te svakako vrlo složen u svom dizajnu jer uključuje primjenu nekoliko različitih metoda za višekriterijsko odlučivanje (DEMATEL, AHP, SNAP). Stoga se od korisnika iziskuju interdisciplinarna znanja (rizici informacijske sigurnosti, kritični poslovni IT sustavi te metodologija višekriterijskoga odlučivanja) kako bi se novi model mogao koristiti u praksi kao potpora u donošenju adekvatnih (tj. informiranih) odluka.

Tako je prema FEDS okviru, a s obzirom na opisane heuristike te vrstu istraživačkog problema i definirane stroge zahtjeve za validacijom, odabrana strategija Ljudski rizik i učinkovitost (eng. *Human Risk & Effectiveness*) u svrhu vrednovanja.

3. Određivanje svojstava za evaluaciju

   Ovaj korak u formuliranju strategije odnosi se na ono što zapravo treba procijeniti. Tu se podrazumijeva odabir općeg skupa značajki, ciljeva i zahtjeva artefakta (dizajn i/ili instanca) koji će biti predmetom evaluacije. Detaljan odabir svojstava nužno je jedinstven za svaki artefakt, njegovu svrhu i njegovu situaciju tijekom procjene. S obzirom kako je u ovom znanstvenom istraživanju glavni cilj u DSR fazi vrednovanja pokazati valjanost (potvrđivanje hipoteze H1) i učinkovitost (potvrđivanje hipoteze H2) novog višekriterijskoga modela, tako je nužno odabrati i referentni model za usporedbu. Sustavnim pregledom literature [142] nije pronađen adekvatan višekriterijski model čije karakteristike bi se moglo uspoređivati s novim hibridnim višekriterijskim modelom s generičkim kriterijima za analizu i procjenu rizika u svrhu procjene kritičnih IT sustava. Također, međunarodni standard ISO/IEC 15408 s uobičajenim kriterijima za certifikaciju o računalnoj sigurnosti (eng. *Common Criteria for Information Technology Security Evaluation*, CC) kao subjekte procjene (eng. *Target of Evaluation*, TOE) razmatra samo strogo tehnološke i/ili sigurnosne

IT sustave (npr., mrežni vatrozidi, operacijski sustavi, sustavi za upravljanje bazama podataka, pametne kartice s certifikatom za omogućavanje kvalificiranog digitalnog potpisa, itd.), dok poslovni IT sustavi nisu u opsegu procjene. Ovo istraživanje kao problemsku domenu obuhvaća kritične poslovne IT sustave u financijskoj instituciji. Stoga je kao referentni model za vrednovanje (usporedbu rezultata) predložen model s kriterijima svojstvenima promatranom kritičnom poslovnom informacijskom sustavu zasnovan na istoj metodologiji (dizajnu) kao i model s generičkim ISRA kriterijima, a što uključuje primjenu više različitih i već spomenutih metoda za višekriterijsko odlučivanje.

Iako je sasvim logično korištenje takvog referentnog modela s inherentnim kriterijima promatranog sustava razvijenog na istim principima kao i ciljani model s generičkim ISRA kriterijima u svrhu validacije novog višekriterijskog modela, problematika koja se javlja jest što se za takav referentni model nije provelo testiranje odnosno evaluacija istoga. Stoga je potrebno napraviti određenu validaciju samog referentnog modela. Kako bi se to napravilo, potrebno je testirati općenita svojstva referentnog modela s inherentnim kriterijima prilagođavajući kriterije kao ciljeve dizajna (prema [153] na temelju međunarodnog standarda ISO/IEC 9126[18] za analizu kvalitete modela i mjera). Svojstva za evaluaciju referentnog modela s inherentnim kriterijima su preuzeta iz standarda ISO/IEC 25010 [158, 160] iz poglavlja vezano uz model kvalitete proizvoda (sustava ili softvera). Svojstva su sljedeća:

- Funkcionalna prikladnost (eng. *functional suitability*): Ova karakteristika predstavlja stupanj u kojemu predloženi višekriterijski model pruža funkcije koje udovoljavaju navedenim i impliciranim potrebama kada se koriste pod određenim uvjetima. Ova je karakteristika sastavljena od sljedećih podkarakteristika: funkcionalna cjelovitost, ispravnost i pogodnost.
- Performansna učinkovitost (eng. *performance efficiency*): Ova karakteristika predstavlja performanse višekriterijskoga modela u odnosu na količinu resursa korištenih pod navedenim uvjetima. Ova je karakteristika sastavljena od sljedećih podkarakteristika: korištenje vremena i resursa.
- Podesnost (eng. *compatibility*): Stupanj u kojem je višekriterijski model s inherentnim kriterijima spojiv sa postojećim procedurama i sustavima za procjenu kritičnih IT sustava i s njima povezanim sigurnosnim rizicima. Ova je

[18] ISO/IEC 9126 standard je zamijenjen novijim ISO/IEC 25010 standardom

karakteristika sastavljena od sljedećih podkarakteristika: koegzistencija i interoperabilnost.

- Upotrebljivost (eng. *usability*): Stupanj do kojega određeni korisnici mogu koristiti novi višekriterijski model za postizanje zadanih ciljeva na učinkovit i zadovoljavajući način u određenom kontekstu upotrebe. Ova je karakteristika sastavljena od sljedećih podkarakteristika: jednostavnost korištenja i zaštita korisnika od pogreške (npr. kod izračuna indeksa konzistentnosti pri davanju vlastitih procjena).
- Pouzdanost (eng. *reliability*): Stupanj do kojeg bi se donositelji odluka mogli osloniti na rezultate koje pruža model prilikom procjene kritičnih IT sustava. Ova je karakteristika sastavljena od sljedećih podkarakteristika: zrelost i razumljivost višekriterijskog modela za procjenu kritičnih IT sustava.
- Sigurnost (eng. *Security*): Stupanj u kojemu model sa svojstvenim kriterijima zadovoljava minimalne sigurnosne zahtjeve za adekvatnu procjenu kritičnih IT sustava. Ova je karakteristika sastavljena od sljedećih podkarakteristika: povjerljivost, cjelovitost, dostupnost, neporecivost, odgovornost i autentičnost.
- Održivost (eng. *Maintainability*): Ova karakteristika predstavlja stupanj učinkovitosti kojim se model sa svojstvenim kriterijima može izmijeniti kako bi ga se poboljšalo, ispravilo ili prilagodilo promjenama u okruženju i novim zahtjevima. Ova je karakteristika sastavljena od sljedećih podkarakteristika: modularnost, ponovna iskoristivost, promjenjivost i provjerljivost.
- Prenosivost (eng. *Portability*): Stupanj učinkovitosti predloženog referentnog modela kada se model potencijalno primjenjuje na različite IT sustave, ne samo na one kritične i povezane s glavnim bankarskim poslovnim operacijama. Npr., za procjenu operacijskih sustava, određenog sklopovlja, kriptografskih algoritama, rješenja u oblaku, itd. Ova je karakteristika sastavljena od sljedećih podkarakteristika: prilagodljivost i fleksibilnost modela s inherentnim kriterijima.

Za svako navedeno svojstvo referentnog modela s inherentnim kriterijima bilo je potrebno izmjeriti stav kako bi se dobilo uvid u relevantnost samog referentnog modela. Stručnjaci za informacijsku sigurnost su iskazali svoje stavove o opisanim svojstvima referentnog višekriterijskoga modela prema sljedećoj mjernoj skali [159]:

1 - Vrlo loše (eng. *Very bad*)

2 – Loše (eng. *Bad*)

3 – Dovoljno (eng. *Fair*)

4 – Dobro (eng. *Good*)

5 – Izvrsno (eng. *Excellent*).

Cijeli upitnik u izvornom obliku na engleskom jeziku odaslan stručnjacima za informacijsku sigurnost iz različitih financijskih institucija i povezanih FinTech tvrtki prikazan je u prilogu J.

Agregirani rezultati o karakteristikama referentnog višekriterijskoga modela s inherentnim kriterijima procijenjenim od strane stručnjaka za informacijsku sigurnost prikazani su sljedećom tablicom:

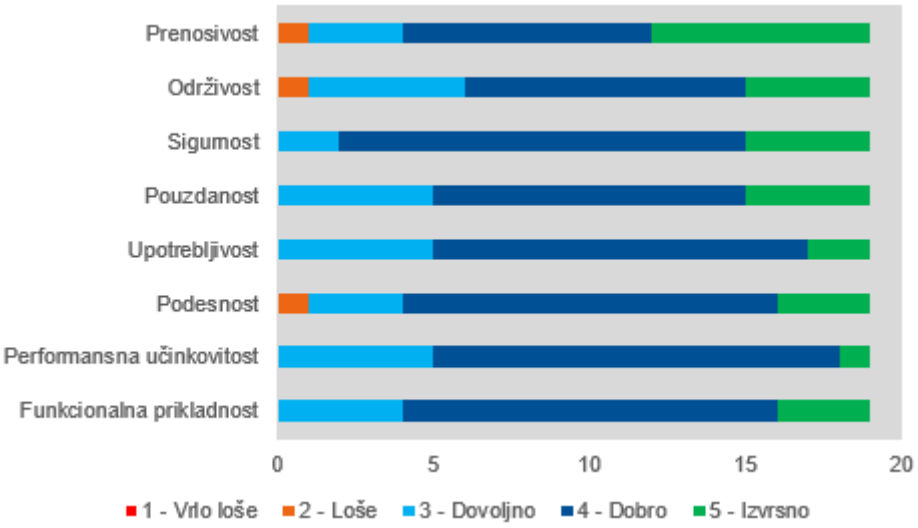
Tablica 6.8: Procijenjene vrijednosti karakteristika referentnog modela

Karakteristika referentnog modela	Mod		Aritmetička sredina ($\bar{x}$)	Standardna devijacija (SD)
	Vrijednost na skali	Pojavnost		
Funkcionalna prikladnost	4 - Dobro	12	3,9474	0,621266627
Performansna učinkovitost	4 - Dobro	13	3,7895	0,535303652
Podesnost	4 - Dobro	12	3,8947	0,737484463
Upotrebljivost	4 - Dobro	12	3,8421	0,602144316
Pouzdanost	4 - Dobro	10	3,9474	0,70504137
Sigurnost	4 - Dobro	13	4,1053	0,567151753
Održivost	4 - Dobro	9	3,8421	0,834212869
Prenosivost	4 - Dobro	8	4,1053	0,87527456

Tablica 6.8 prikazuje agregirane srednje vrijednosti svake pojedine karakteristike referentnog modela s inherentnim kriterijima dobivene od sigurnosnih IT stručnjaka. Također, iz tablice se vidi kako mod svake promatrane karakteristike ima vrijednost 4 – Dobro, te da je korigirana standardna devijacija (SD) značajno ispod 1,5 za svaku pojedinu karakteristiku. Tako se može zaključiti (prema referentnim vrijednostima za *Delphi* tehniku [115] i ISO 9126 analizu kvalitete modela i mjera [159]) da se predloženi višekriterijski model s inherentnim kriterijima za kritične bankovne transakcijske i interne platne sustave može smatrati validnim prema procjenama sigurnosnih stručnjaka te uzimati kao referentan za usporedbu s modelom s generičkim ISRA kriterijima.

Također, može se primijetiti kako kriterij performansna učinkovitost ima najmanju prosječnu (agregiranu) vrijednost. Takav stav ispitanika vjerojatno proizlazi iz činjenice kako je prilikom procjene kritičnih poslovnih IT sustava s inherentnim

kriterijima potrebno dosta vremena kako bi se dobilo željene rezultate (tj. omjere između alternativa), a što najprije uključuje računanje međusobnih zavisnosti i utjecaja između svojstvenih kriterija, klasteriranje kriterija te računanje dominacije između istih kako bi se dobilo težine kriterija s obzirom na cilj odlučivanja, te na kraju slijedi još i sama procjena kritičnih poslovnih IT sustava prema svim svojstvenim kriterijima (vidljivo u studijama slučaja), a čiji broj je svakako veći od generičkih ISRA kriterija.



Slika 6.8: Stavovi ispitanika o karakteristikama referentnog modela

Sa Slike 6.8 mogu se vidjeti i proporcije svih odgovora, tj. stavova ispitanika vezano uz karakteristike predloženog referentnog višekriterijskoga modela s inherentnim kriterijima. Ukupno 19 stručnjaka iz financijskih institucija je radilo procjenu referentnog modela s inherentnim kriterijima. Isti stručnjaci prethodno su radili i procjenu kritičnih poslovnih IT sustava na studijama slučaja.

Kod validacije referentnog modela s inherentnim kriterijima radilo se zapravo o *ex post* vrsti evaluacije s obzirom kako su eksperti najprije provodili rješavanje obje studije slučaja (Scenarij 1 i Scenarij 2). Tek kada su eksperti proveli studije slučaja te iskazali svoje procjene o utjecajima / zavisnostima između inherentnih kriterija, njihovoj važnosti u odnosu na cilj odlučivanja, kao i procjene kritičnih poslovnih IT sustava, nakon toga im je odaslan upitnik za mjerenje stavova o karakteristikama referentnog modela s inherentnim kriterijima. Razlog tomu je što se eksperte najprije htjelo upoznati sa svim karakteristikama oba modela (s inherentnim i generičkim evaluacijskim kriterijima) kako bi stručnjaci dobili uvid u sam model i njegovu

strukturu, složenost, način funkcioniranja, ciljeve te konačno i rezultate. Na taj način, primjenjujući *ex post* vrstu evaluacije, stručnjaci za informacijsku sigurnost mogli su svakako bolje procijeniti karakteristike referentnog modela s inherentnim kriterijima te tako i njihove procjene dobivaju na većoj relevantnosti.

4. Dizajn pojedinih evaluacijskih epizoda

   Odabirom strategije i određivanjem svojstava artefakta za evaluaciju, potrebno je dizajnirati i stvarno vrednovanje samog artefakta. U ovom koraku potrebno je razmotriti i određene heuristike za dizajniranje individualnih epizoda, npr. resursna ograničenja (dostupnost stručnjaka za istraživanje), definiranje plana o broju evaluacijskih epizoda te vremenu i načinu njihova provođenja. Takvim planom se zapravo definira tko radi evaluaciju novokreiranog artefakta, kako i kada (kojim redoslijedom). Tako je za potrebe provođenja studija slučaja definirano sljedećih 5 koraka odnosno evaluacijskih epizoda:

   1) Definiranje inherentnih kriterija za kritične informacijske sustave
   2) Računanje težina inherentnih kriterija za kritične informacijske sustave
   3) Evaluacija kritičnih informacijskih sustava pomoću inherentnih kriterija
   4) Evaluacija kritičnih informacijskih sustava pomoću generičkih ISRA kriterija
   5) Rangiranje i usporedba rezultata procjene kritičnih IT sustava dobivenih pomoću inherentnih kriterija u odnosu na rezultate dobivene procjenom pomoću ciljanog višekriterijskog modela s generičkim ISRA kriterijima.

   Detalji pojedinih aktivnosti unutar svake evaluacijske epizode predstavljeni su u studijama slučaja.

Tako će se u ovom poglavlju predstaviti validacija novog hibridnoga višekriterijskoga modela za procjenu, rangiranje i odabir kritičnih poslovnih IT sustava. Validacija višekriterijskoga modela provedena je za dva scenarija odnosno studije slučaja za procjenu, rangiranje i odabir sljedećih kritičnih poslovnih IT sustava:

- bankovni *online* (korisnički) transakcijski sustavi
- interni bankovni platni sustavi

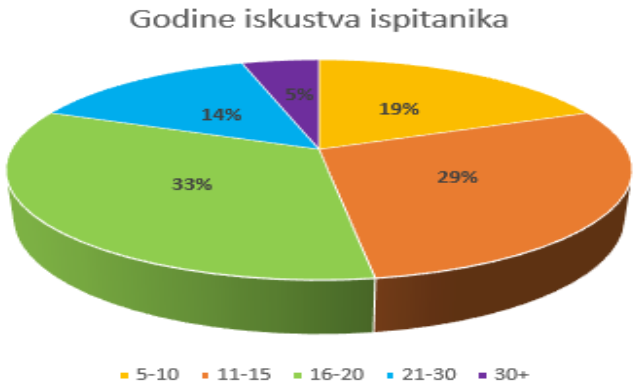
Za svaku navedenu studiju slučaja proces validacije je proveden u pet definiranih slijednih faza odnosno epizoda. Studija slučaja predstavlja oblik kvalitativnog istraživanja. Obje studije slučaja napravljene su vrlo intenzivno u kontekstu njihova trajanja i velike složenosti, te produbljeno i u realnom kontekstu na interaktivan i dinamičan način između istraživača i sudionika istraživanja. Ispitanici u studijama slučaja su ciljano izabrani sigurnosni

stručnjaci iz financijskih institucija i s njima povezanih FinTech tvrtki koji posjeduju relevantna znanja iz domene upravljanja rizicima informacijske sigurnosti i primijenjenih mjera zaštite za promatrane kritične IT sustave u svojim organizacijama. Svrha studije slučaja je ispitati primjenjivost i valjanost (**H1**) te učinkovitost (**H2**) novog višekriterijskoga modela na kritičnim poslovnim IT sustavima u financijskoj instituciji te tako ostvariti specifični istraživački cilj **C3**.

6.3.1. Ispitanici pri validaciji modela

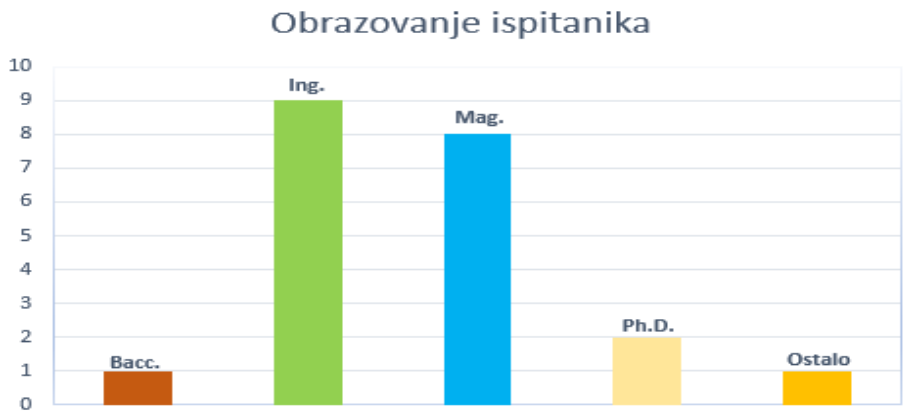
Uzorak ispitanika je izabran prema tzv. "uzorku prema prosudbi stručnjaka", a koji se preporuča ako se istraživanje provodi među stručnjacima iz neke uže specijalnosti [161]. Tijekom validacije višekriterijskoga modela na dvjema studijama slučaja, ukupno je sudjelovalo 21 ispitanika, tj. stručnjaka za informacijsku sigurnost iz različitih financijskih institucija u Europi. Od toga je u svakoj studiji slučaja sudjelovalo po 16 ispitanika, što znači kako je dio ispitanika sudjelovao samo u jednoj ili drugoj studiji slučaja, dok je veći dio sudjelovao u obje studije slučaja. Razlog tomu je što je za drugu studiju slučaja vezano uz procjenu kritičnih internih bankovnih platnih sustava zbog izrazite specifičnosti takvih sustava bilo potrebno pronaći dodatne stručnjake koji razumiju sigurnost platnog prometa u bankama.

Izgled anketnog upitnika koji sadrži pitanja vezano uz godine radnog iskustva, razinu edukacije, profesionalnu stručnost (certifikati) te obnaša li ispitanik trenutno rukovodeću poziciju u financijskoj instituciji, može se pronaći u Prilogu A.



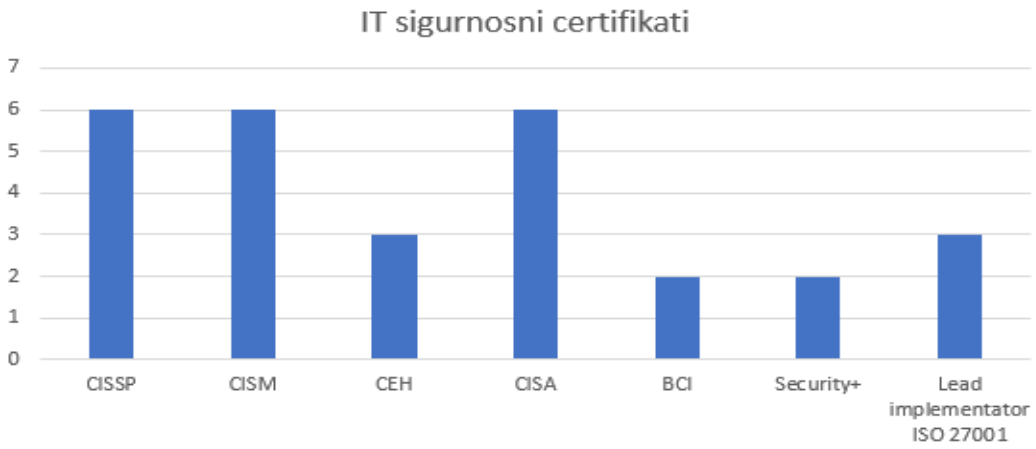
Slika 6.9: Iskustvo stručnjaka za IT sigurnost

Slika 6.9 prikazuje iskustvo stručnjaka za informacijsku sigurnost iz financijskih institucija. Sa slike je vidljivo kako velika većina ispitanika ima više od 10 godina radnog iskustva u financijskom sektoru u području IT i ICT sigurnosti. Pri tome je prosjek 16,1 godina relevantnog iskustva.



Slika 6.10: Obrazovanje stručnjaka za IT sigurnost

Slika 6.10 prikazuje razinu obrazovanja IT sigurnosnih stručnjaka. Vidljivo je kako kod velike većine ispitanika postignuta razina obrazovanja je magistar ili inženjer, a što je najčešće zapravo i ekvivalent jedno drugome (ovisno o pojedinoj nacionalnoj klasifikaciji za akademske i stručne nazive i stupnjeve).

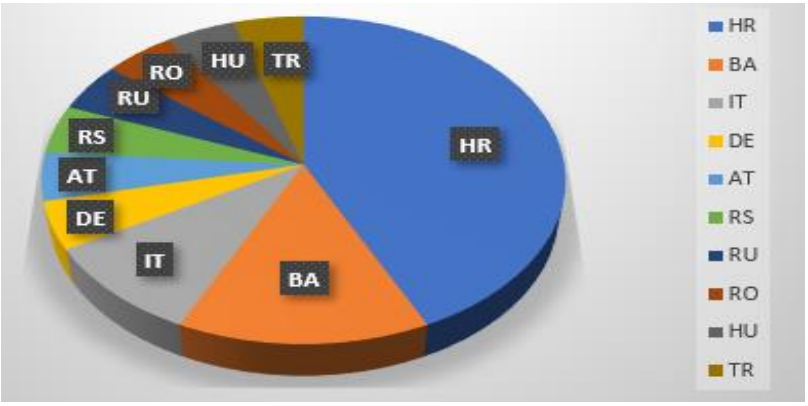


Slika 6.11: Zastupljenost IT sigurnosnih certifikata kod stručnjaka za IT sigurnost

Sa Slike 6.11 može se vidjeti zastupljenost odnosno broj industrijskih IT sigurnosnih certifikata kod ispitanih stručnjaka, pri čemu su CISSP, CISM i CISA certifikati najviše zastupljeni. Od ostalih stručnih certifikata koje posjeduju ispitanici, a koji nisu prikazani na grafu, treba izdvojiti CGEIT, SANS-ove certifikate GCIH i GCFA, LPIC-1, MCSA Security, Microsoft MTA Security Fundamentals te CRISC. Treba napomenuti da je svaki ispitanik morao posjedovati barem jedan industrijski certifikat iz domene informacijske sigurnosti kako bi se mogao kvalificirati kao relevantan ekspert za validaciju modela.

Slika 6.12: Razine odgovornosti ispitanika

Slika 6.12 prikazuje broj odnosno zastupljenost ispitanika koji imaju rukovodeći položaj (npr. CSO[19] ili CISO[20]) u odnosu na specijaliste u financijskim institucijama. Vidljivo je kako malo veći broj ispitanika ima rukovodeći položaj, tj. u poziciji su donošenja odluke o stanju sigurnosti informacijskog sustava (na temelju strukturirane procjene rizika) u financijskoj instituciji, a što je vrlo bitno u kontekstu ovog istraživanja i validacije višekriterijskoga modela na kritičnim poslovnim informacijskim sustavima.



Slika 6.13: Ispitanici prema zemljama u kojima rade

Na Slici 6.13 vidljivo je kako ispitanici (sigurnosni IT stručnjaci) koji su sudjelovali u procesu validacije modela na studijama slučajeva dolaze iz 10 različitih Europskih zemalja, iz čega proizlazi kako provedeno istraživanje ima i određenu međunarodnu dimenziju.

Iz svega navedenog može se zaključiti kako su stručnjaci odabrani za validaciju višekriterijskoga modela zaista kompetentni davati procjene u području IT sigurnosti.

[19] *Chief Security Officer (CSO) – Direktor sigurnosti, to je najviši izvršni direktor u organizaciji odgovoran za razvoj i nadzor politika i programa namijenjenih za smanjenje neusklađenosti te operativnih, strateških, financijskih i reputacijskih rizika koji se odnose na zaštitu ljudi, intelektualne i materijalne imovine.*

[20] *Chief Information Security Officer (CISO) – Direktor informacijske sigurnosti, to je izvršni direktor u organizaciji odgovoran za uspostavljanje i održavanje vizije, misije i strategije organizacije kako bi se osiguralo da su informacijska imovina i tehnologije adekvatno zaštićeni. CISO upravlja osobljem za identifikaciju, razvoj implementaciju i održavanje procesa u cijeloj organizaciji kako bi se smanjili IT sigurnosni rizici.*

6.3.2. Scenarij 1: Procjena kritičnih bankovnih *online* transakcijskih sustava

Ova studija slučaja odnosi se na procjenu najznačajnijih *online* bankovnih korisničkih transakcijskih sustava iz perspektive stručnjaka za informacijsku sigurnost. Pod *online* sustavima podrazumijevaju se oni sustavi dostupni krajnjim korisnicima preko internetske javne mreže za obavljanje transakcija, ugovaranje određenih usluga, pregled stanja po kartičnom poslovanju, itd. Najznačajniji transakcijski sustavi identificirani prema broju aktivnih korisnika te dostupni krajnjim korisnicima putem interneta su sljedeći:

- Elektroničko bankarstvo (eng. *e-banking*)
- Mobilno bankarstvo (eng. *m-banking*)
- Elektronička trgovina (eng. *e-commerce*).

S obzirom kako su ranijim istraživanjem već definirane težine generičkih ISRA kriterija (poglavlje 6.1.4), tako je bilo nužno provesti proces vrednovanja novog višekriterijskoga modela kroz pet koraka odnosno evaluacijskih epizoda za studiju slučaja sa kritičnim korisničkim bankovnim transakcijskim sustavima. Validacija je provedena na sljedeći način:

1) **Definiranje inherentnih kriterija za kritične bankovne transakcijske sustave**
   Kao osnova za definiranje inherentnih (svojstvenih) kriterija za kritične bankovne transakcijske sustave korišteno je istraživanje [139] pri čemu su analizirani i definirani sigurnosni ciljevi i mehanizmi informacijske sigurnosti. Sigurnosni mehanizam se definira kao uspostavljeni proces pomoću kojeg se ostvaruju određeni sigurnosni ciljevi. Tako su definirani inherentni kriteriji za studiju slučaja kritičnih bankovnih transakcijskih sustava sljedeći:
   - Autentikacija (eng. *Authentication*): Proces utvrđivanja identiteta nekog subjekta prilikom prijave na *online* bankovni transakcijski informacijski sustav putem interneta.
   - Autorizacija (eng. *Authorization*): Naziva se još i ovlaštenje, to je funkcija prava ili kontrole pristupa (privilegija) na resurse informacijskog sustava u kontekstu računalne sigurnosti za bankovne transakcijske sustave.
   - Kriptiranje (eng. *Encryption*): Proces kodiranja informacija kako bi se iste zaštitilo od neovlaštenog pristupa čime se ostvaruje sigurnosni cilj povjerljivosti informacija.
   - Digitalno potpisivanje (eng. *Digital Signing*): Proces potpisivanja bankovne transakcije kako bi se ostvarilo sigurnosni cilj neporecivost (eng. *Non-*

repudiation) – implicira kako strana koja je potpisala transakciju kao i strana primatelj transakcije ne mogu zanijekati izvršenu radnju.

- Dostupnost (eng. *Availability*): Računa se kao funkcija pouzdanosti (eng. *Reliability*) bankovnog transakcijskog informacijskog sustava pri čemu je isti dostupan korisnicima u traženom trenutku.
- Vođenje dnevnika (eng. *Logging*): Zapisivanje relevantnih sigurnosnih događaja (eng. *Audit trails*) koji se odvijaju na informacijskom sustavu, npr. pokušaji prijave i autorizacije (uspješni i neuspješni) na informacijski sustav, zapisi o greškama, zapisi o provedenim transakcijama, zapisi o izmjenama platnih naloga ili transakcija, itd.
- Rezervna kopija (eng. *Backup*): Kopija računalnih podataka koja se izrađuje zbog osiguranja, a u slučaju oštećenja ili gubitka izvornih podataka (korisničkih i/ili sistemskih) kritičnog bankovnog transakcijskog sustava.

2) Računanje težina inherentnih kriterija za bankovne korisničke *online* transakcijske sustave

Kako bi se dobile težine inherentnih kriterija bilo je nužno provesti istraživanje među stručnjacima za informacijsku sigurnost koji su, dajući svoje mišljenje, procjenjivali međusobne odnose (prema utjecajima/zavisnostima i dominaciji) između definiranih kriterija. Kao i u slučaju određivanja težina generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti, ovom prilikom također se koristila SNAP metoda. Kako bi se moglo izračunati težine inherentnih kriterija kritičnih bankovnih *online* transakcijskih sustava metodom SNAP11, potrebne su dvije ulazne komponente: utjecaji (zavisnosti) između elemenata i težine kriterija u odnosu na cilj odlučivanja. Prikupljanje podataka odrađeno je ispitivanjem stručnjaka za informacijsku sigurnost (*FinTech* zaposlenici) slanjem upitnika za ispunjavanje putem elektroničke pošte. Upitnik (Excel dokument) je sadržavao sljedeće radne stranice (eng. *sheets*) odnosno podfaze:

1. Podfaza (Trx_sys_influences stranica): Stručnjaci su davali ocjene na DEMATEL skali (0-4) o utjecajima (zavisnostima) između svojstvenih atributa za korisničke *online* bankovne transakcijske sustave popunjavajući Tablicu 6.9.

Tablica 6.9: Definiranje utjecaja (zavisnosti) između svojstvenih kriterija za *online* bankovne transakcijske sustave

Utjecaji između svojstvenih kriterija za bankovne online transakcijske sustave	Ath	Atz	E	DS	Av	L	B
Autentikacija (Ath)	0						
Autorizacija (Atz)		0					
Kriptiranje (E)			0				
Digitalno potpisivanje (DS)				0			
Dostupnost (Av)					0		
Logiranje (L)						0	
Rezervna kopija (B)							0

Izvorni oblik Tablice 6.9 koja je odaslana stručnjacima za informacijsku sigurnost s pripadajućim uputama o ispunjavanju nalazi se u Prilogu E.

Na temelju dobivenih podataka (što je bio inicijalni ulaz u SNAP metodu) od stručnjaka za informacijsku sigurnost iz financijskih institucija i FinTech tvrtki (prikupljeno ukupno 16 relevantnih odgovora) te provodeći cjelokupni postupak računanja utjecaja (zavisnosti) između inherentnih kriterija za bankovne transakcijske sustave pomoću SNAP metode (predstavljeno u poglavlju *6.1.3. SNAP metoda*), dobivene su sljedeće vrijednosti:

Tablica 6.10: Težine inherentnih kriterija s obzirom na utjecaje (zavisnosti) između elemenata za kritične bankovne transakcijske sustave

Svojstveni kriteriji	Težine svojstvenih kriterija (SNAP12)
Autentikacija	0,135265454
Autorizacija	0,105908484
Kriptiranje	0,173263665
Digitalno potpisivanje	0,117567661
Dostupnost	0,241961344
Logiranje	0,099104201
Sigurnosna kopija	0,126929191

Dobivene težine inherentnih (svojstvenih) kriterija za bankovne transakcijske sustave iz Tablice 6.10 zapravo odgovaraju izračunima za SNAP12 metodu. No, s obzirom na uočenu i definiranu problematiku istraživanja potrebno je dobiti i vrijednosti inherentnih kriterija u odnosu na cilj odlučivanja kako bi se pravilno mogle izračunati konačne težine inherentnih kriterija koristeći ciljanu SNAP11 metodu.

2. Podfaza (AHP_importance stranica): Stručnjaci su davali ocjene o važnosti svojstvenih kriterija u odnosu na cilj odlučivanja primjenom AHP metode. Identificirani svojstveni kriteriji za kritične bankovne *online* transakcijske sustave podijeljeni su u 4 klastera. Podjela klastera napravljena je prema logičkom principu koji je najprikladniji za definirane transakcijske sustave i problematiku istraživanja u dogovoru sa stručnjacima za informacijsku sigurnost. Tom prilikom koristila se standardna Saatyjeva skala [109] za usporedbu u parovima odnosno definiranje važnosti između svojstvenih kriterija. Tablice za popunjavanje s detaljnim uputama dostavljene stručnjacima za informacijsku sigurnost prikazane su u Prilogu F. Klasteri s pripadajućim elementima prikazani u tablicama koje slijede:

Tablica 6.11: Usporedbe kriterija unutar klastera CT1 (Identitet) za trx sustave

CT1 (Identitet)	Autentikacija	Autorizacija
Autentikacija	1	
Autorizacija		1

Tablica **CT1** ima za cilj usporediti važnost (dominaciju) između kriterija *autentikacija* i *autorizacija* unutar klastera **Identitet** (eng. *Identity*).

Tablica 6.12: Usporedbe kriterija unutar klastera CT2 (C-I-A) za trx sustave

CT2 (C-I-A)	Kriptiranje	Digitalno potpisivanje	Dostupnost
Kriptiranje	1		
Digitalo potpisivanje		1	
Dostupnost			1

Tablica **CT2** ima za cilj usporediti važnost između kriterija *kriptiranje, digitalno potpisivanje* i *dostupnost* unutar klastera **C-I-A**. Za svaku usporedbu u paru opet je potrebno postaviti i odgovarajuću recipročnu vrijednost. Također, tom prilikom obavezno se moralo slijediti i pravilo tranzitivnosti kako bi se nužno ispoštovalo omjer konzistentnosti **CR < 0,1**.

Tablica 6.13: Usporedbe kriterija unutar klastera CT3 (Forenzika) za trx sustave

CT3 (Forenzika)	Logiranje	Rezervna kopija
Logiranje	1	
Rezervna kopija		1

U tablici **CT3** rade se jednostavne usporedbe između elemenata *logiranje* i *rezervna kopija* unutar klastera **Forenzika** (eng. *Forensics*). S obzirom kako se međusobno uspoređuju samo dva elementa, tako nema mogućnosti ni potrebe za računanjem CR indeksa.

Tablica 6.14: Usporedbe klastera (CT4) za inherentne kriterije transakcijskih sustava

CT4 (klasteri)	Identitet	C-I-A	Forenzika
Identitet	1		
C-I-A		1	
Forenzika			1

Tablica **CT4** ima za cilj usporediti važnost (dominaciju) između definiranih klastera **Identitet**, **C-I-A** i **Forenzika**, tj. definirati koji kriterij odnosno klaster je važniji (kritičniji) u zaštiti korisničkih *online* bankovnih transakcijskih sustava. U svakoj tablici na glavnoj dijagonali vrijednosti su postavljene na 1 prema Saatyjevoj skali jer se međusobno uspoređuju isti elementi.

Težine svojstvenih kriterija za korisničke *online* bankovne transakcijske sustave s obzirom na cilj odlučivanja (međukorak za izračun SNAP11 kriterija) primjenom AHP metode prikazane su sljedećom tablicom:

Tablica 6.15: Težine svojstvenih kriterija za trx sustave s obzirom na cilj odlučivanja

Svojstveni kriteriji	Težine svojstvenih kriterija (AHP)
Autentikacija	0,205736222
Autorizacija	0,164580753
Kriptiranje	0,203349261
Digitalno potpisivanje	0,153751556
Dostupnost	0,074480352
Logiranje	0,110567964
Rezervna kopija	0,087533891

Konačne težine svojstvenih kriterija za kritične korisničke bankovne *online* transakcijske sustave dobivene primjenom aritmetičke sredine na vrijednosti iz Tablica 6.10 i Tablica 6.15 kao završnim korakom SNAP11 metode su sljedeće:

Tablica 6.16: Težine svojstvenih kriterija za trx sustave dobivene SNAP11 metodom

Svojstveni kriteriji	Težine svojstvenih kriterija (SNAP11)
Autentikacija	0,170500838
Autorizacija	0,135244618

Kriptiranje	0,188306463
Digitalno potpisivanje	0,135659609
Dostupnost	0,158220848
Logiranje	0,104836083
Rezervna kopija	0,107231541

Iz Tablice 6.16 može se primijetiti kako nema velikog odstupanja između vrijednosti težina svojstvenih kriterija za transakcijske sustave te kako se zapravo radi o normalnoj distribuciji pri čemu najveću težinu ima kriterij *kriptiranje* (eng. **Encryption**).

Postupak računanja težina svojstvenih kriterija SNAP11 metodom za transakcijske sustave prikazan je u Prilogu G.

3) Evaluacija kritičnih transakcijskih sustava pomoću inherentnih kriterija

Stručnjaci za informacijsku sigurnost imali su zadatak evaluirati transakcijske sustave pomoću inherentnih kriterija AHP metodom koristeći Saatyjevu standardnu skalu i postavljajući pritom općenito pitanje: *koji transakcijski sustav je kvalitetniji (i koliko) u odnosu na promatrani kriterij*? Pritom je za svaki korisnički transakcijski sustav trebalo uzimati u obzir implementirane sigurnosne kontrole u odnosu na promatrani kriterij prilikom davanja prosudbi.

Tablica 6.17: Tablica za usporedbu trx sustava prema kriteriju autentikacija

Autentikacija	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

Tablica 6.17 predstavlja primjer matrice koju su stručnjaci za informacijsku sigurnost trebali ispunjavati procjenjujući korisničke bankovne transakcijske sustave prema definiranim svojstvenim kriterijima, u ovom slučaju prema svojstvenom kriteriju *autentikacija*. Prilikom procjene kritičnih transakcijskih sustava prema kriteriju *autentikacija*, stručnjaci za informacijsku sigurnost trebali su uzimati u obzir autentikacijske faktore implementirane na informacijskom sustavu kao i načine njihove implementacije, npr. korisničko ime i lozinka, biometrija, dvo-faktorska autentikacija, itd. Prilikom procjene kritičnih transakcijskih sustava prema kriteriju *enkripcija*, stručnjaci za informacijsku sigurnost trebali su uzimati u obzir faktore

kao što su enkripcija i pohrana kredencijala, enkripcija povjerljivih podataka, enkripcija komunikacijskih kanala (TLS), itd.

Kako prema kriterijima *autentikacija* i *enkripcija*, tako su stručnjaci procjenjivali transakcijske sustave i prema svim ostalim definiranim svojstvenim kriterijima. Sve tablice za usporedbu u parovima s detaljnim objašnjenjima svojstvenih kriterija za bankovne transakcijske sustave dostavljene stručnjacima za informacijsku sigurnost prikazane su u Prilogu H. Na kraju je napravljena agregacija prosudbi (primjenom geometrijske sredine) za svaki promatrani svojstveni kriterij te su izračunati svojstveni vektori za te kriterije, a što je prikazano Tablicom 6.18.

Tablica 6.18: Vrijednosti vektora svojstvenih kriterija za trx sustave

Alternative \ Kriteriji	Autentikacija	Autorizacija	Kriptiranje	Digitalno potpisivanje	Dostupnost	Logiranje	Rezervna kopija
e-banking	0,372191993	0,386198686	0,359962141	0,442262711	0,405931898	0,393551596	0,371068639
m-banking	0,426442961	0,388951499	0,410070356	0,388810918	0,378993865	0,388203063	0,38427372
e-commerce	0,201365046	0,224849816	0,229967503	0,168926371	0,215074237	0,218245341	0,244657641

4) Evaluacija kritičnih transakcijskih sustava pomoću generičkih ISRA kriterija

Stručnjaci za informacijsku sigurnost imali su zadatak evaluirati transakcijske sustave pomoću generičkih kriterija za analizu i procjenu rizika AHP metodom koristeći Saatyjevu standardnu skalu i postavljajući pritom općenito pitanje: *koji transakcijski sustav ima veću izloženost sigurnosnom riziku u odnosu na promatrani kriterij rizika*? Za svaki promatrani ISRA kriterij trebalo je uzimati u obzir i faktore koji dodatno mogu utjecati na rizičnost transakcijskog sustava u odnosu na taj promatrani kriterij. Npr., za kriterij *vjerojatnost* (P), faktori koje je svakako trebalo uzeti u obzir (prema OWASP Risk Rating metodologiji [120]) su faktori agenta prijetnje (vještina napadača, motiv, metoda, mogućnosti, učestalost napada) i faktori ranjivosti (jednostavnost pronalaska ranjivosti, jednostavnost iskorištavanja, otkrivanje vektora upada).

Tablica 6.19: Tablica za usporedbu trx sustava prema kriteriju prijetnja

Prijetnja (T)	e-banking	m-banking	e-commerce
e-banking	**1**		
m-banking		**1**	
e-commerce			**1**

Tablica 6.19 predstavlja primjer matrice (3x3) koju su stručnjaci za informacijsku sigurnost trebali ispunjavati procjenjujući korisničke bankovne transakcijske sustave prema ISRA kriterijima, u ovom slučaju prema kriteriju *prijetnja* (**Threat**). Prilikom davanja vlastitih procjena/omjera između kritičnih transakcijskih sustava u odnosu na promatrani generički ISRA kriterij *prijetnja*, potrebno je promotriti koji sustav je više izložen različitim kibernetičkim prijetnjama, npr. zlonamjerni softver (virusi, crvi, kripto-blokeri), prisluškivanje, otmice, lažno predstavljanje, neovlašteni pristup, krađa identiteta, DDoS napadi, sve učestaliji RDoS napadi iznude (eng. *Ransom Denial of Service Attacks*), itd.

Na isti način kao za generički kriterij *prijetnja*, stručnjaci za informacijsku sigurnost morali su procjenjivati transakcijske sustave i prema svim ostalim definiranim generičkim ISRA kriterijima. Sve tablice za usporedbu u parovima s detaljnim objašnjenjima generičkih kriterija za bankovne transakcijske sustave i kako zapravo provesti usporedbe koje su dostavljene stručnjacima za informacijsku sigurnost prikazane su u Prilogu I. Na kraju je napravljena agregacija prosudbi (primjenom geometrijske sredine) za svaki promatrani generički ISRA kriterij te su izračunati svojstveni vektori generičkih kriterija za transakcijske sustave, a što je prikazano Tablicom 6.20.

Tablica 6.20: Svojstveni vektori generičkih ISRA kriterija za trx sustave

Alternative \ Kriteriji	**Prijetnja**	**Ranjivost**	**Vjerojatnost**	**Posljedica**	**Otpornost**
e-banking	0,300439318	0,346069687	0,392030313	0,4715484	0,307823618
m-banking	0,312925954	0,25058345	0,244493668	0,319128828	0,312331238
e-commerce	0,386634729	0,403346863	0,36347602	0,209322771	0,379845144

5) Rangiranje i usporedba rezultata procjene transakcijskih IT sustava dobivenih pomoću inherentnih kriterija u odnosu na rezultate dobivene višekriterijskim modelom s generičkim ISRA kriterijima

Kako bi se u procesu validacije potvrdila postavljena hipoteza **H1**, potrebno je napraviti rang i usporedbu rezultata dobivenih primjenom hibridnog modela s inherentnim i generičkim ISRA kriterijima za bankovne transakcijske sustave.

Tako su prilikom procjene transakcijskih sustava prema svojstvenim i generičkim ISRA kriterijima dobiveni sljedeći rezultati odnosno rang alternativa (rezultat umnoška vlastitih svojstvenih vektora i SNAP11 težina kriterija):

Tablica 6.21: Rang trx sustava prema svojstvenim kriterijima

Transakcijski sustavi (svojstveni kriteriji)	**Rang**
e-banking	0,388746283
m-banking	**0,397145997**
e-commerce	**0,21410772**

Iz Tablice 6.21 vidi se kako najveći ponder ima mobilno bankarstvo, što bi značilo kako je prema ocjenama stručnjaka za informacijsku sigurnost to bankovni transakcijski sustav koji ima ugrađene najbolje sigurnosne mehanizme i kontrole u odnosu na druge promatrane sustave. Zatim slijede elektroničko bankarstvo (eng. *e-banking*) te na kraju elektronička trgovina (eng. *e-commerce*) s najmanjim ponderom.

Tablica 6.22: Rang trx sustava prema generičkim ISRA kriterijima

Transakcijski sustavi (generički ISRA kriteriji)	**Rang**
e-banking	0,350640726
m-banking	**0,291067527**
e-commerce	**0,358291747**

Iz Tablice 6.22 vidi se kako najveći ponder ima *e-commerce* transakcijski sustav, zatim slijedi *e-banking* i na kraju *m-banking* s najmanjim ponderom. No, važno je napomenuti kako je prilikom procjene kritičnih korisničkih transakcijskih sustava prema ISRA kriterijima bilo potrebno primijeniti obrnutu logiku u odnosu na evaluaciju istih sustava pomoću inherentnih kriterija gdje se gledalo koji transakcijski sustav ima kvalitetnije implementiran promatrani sigurnosni mehanizam ili kontrolu, dok se pri procjeni transakcijskih sustava prema generičkim ISRA kriterijima gledalo koji je sustav zapravo rizičniji u odnosu na promatrani kriterij (u skladu s tim je definirano i pitanje koje se postavljalo prilikom procjene transakcijskih sustava). Tako se i rezultati za evaluaciju prema ISRA kriterijima čitaju na način koji transakcijski sustav je rizičniji (na isti način kako su se davale i procjene/omjeri). Stoga se rang alternativa odnosno kritičnih korisničkih bankovnih transakcijskih sustava prema generičkim ISRA kriterijima iščitava na način da se transakcijski sustav koji ima najmanji ponder smatra najmanje rizičnim u trenutku evaluacije i time zapravo zauzima prvo mjesto u rangu. Kad se takva obrnuta logika primijeni na rezultate dobivene procjenom sustava pomoću generičkih ISRA kriterija, tada imamo da je najmanje rizičan sustav *m-banking* pa zatim slijedi *e-*

banking dok se najrizičnijim korisničkim sustavom smatra *e-commerce*. Prema tome, rang dobiven procjenom transakcijskih sustava koristeći inherentne kriterije odgovara rangu dobivenom procjenjujući iste sustave pomoću generičkih kriterija za analizu i procjenu rizika. Iz toga proizlazi kako je potvrđena hipoteza **H1** u studiji slučaja za kritične korisničke bankovne transakcijske sustave.

Za provjeru hipoteze **H2** koristila se jednostavna metrika o ekvivalentu radnog vremena (FTE) pri čemu su ispitanici bilježili koliko im je vremena potrebno za ispunjavanje definiranih tablica prilikom procjene korisničkih transakcijskih sustava s generičkim ISRA kriterijima u odnosu na procjenu, tj. validaciju modela s inherentnim kriterijima. Mjerenje je pokazalo kako je ispitanicima u prosjeku trebalo 5,67 sati za pravilno ispunjavanje tablica za procjenu transakcijskih sustava s inherentnim kriterijima, dok je istim ispitanicima bilo potrebno u prosjeku 3,95 sati za pravilno ispunjavanje svih tablica kod procjene transakcijskih sustava s generičkim kriterijima. Pri mjerenju je uključeno i vrijeme potrošeno na dodatne (naknadne) procjene koje su bile potrebne zbog grešaka nastalih u inicijalnim procjenama od strane pojedinih ispitanika, npr. zbog praznina u tabličnim poljima za popunu, neadekvatno postavljenih reciprociteta ili neodgovarajućeg izračuna indeksa konzistentnosti. S obzirom kako su ispitanici trebali značajnije manje vremena za procjenu transakcijskih sustava koristeći generičke kriterije u odnosu na procjenu istih sustava inherentnim kriterijima, hipoteza **H2** vezano uz učinkovitost višekriterijskog modela s generičkim kriterijima za analizu i procjenu rizika je potvrđena.

6.3.3. Scenarij 2: Procjena kritičnih bankovnih internih platnih sustava

Ova studija slučaja odnosi se na evaluaciju najznačajnijih internih bankovnih platnih sustava iz perspektive stručnjaka za informacijsku sigurnost i sigurnost bankovnih platnih sustava. Pod internim platnim sustavima podrazumijevaju se oni kritični bankovni informacijski sustavi koji nisu dostupni krajnjim korisnicima već isključivo određenim djelatnicima financijske institucije ovlaštenima za rad s platnim transakcijskim sustavima (npr. zadavanje, autorizacija, promjena i/ili provjera platnih naloga). Najznačajniji interni platni sustavi i sheme identificirani prema kritičnosti i broju platnih naloga su sljedeći:

- SWIFT[21] mreža (eng. *Society for Worldwide Interbank Financial Telecommunication*) – međubankarska komunikacijska mreža
- Sustav za podršku platnih usluga klijentima (eng. *Front Office Payment System*, FOS[22])
- SEPA[23] plaćanja (eng. *Single Euro Payments Area*).

Ovdje se zapravo međusobno uspoređuju kanali inicijacije plaćanja (FOS), komunikcijska infrastruktura za plaćanje (SWIFT) i platna shema (SEPA). Korisnost rezultata ove studije slučaja očituje se u tome da donositelji odluka saznaju koji od kritičnih platnih sustava je više izložen sigurnosnom riziku te prema tome ulože novčana sredstva u dodatne kontrole kako bi se nivelirale razlike, smanjili sami rizici te posljedično spriječili mogući financijski gubici koji kod takvih kritičnih sustava mogu biti izrazito veliki. Primjer velikog financijskog gubitka uzrokovanog kibernetičkim napadom je napad na centralnu banku Bangladeša [155].

S obzirom kako su ranijim istraživanjem već definirane težine generičkih ISRA kriterija (poglavlje 6.1.4), tako je bilo nužno provesti proces vrednovanja novog višekriterijskoga modela kroz pet koraka odnosno evaluacijskih epizoda za studiju slučaja sa kritičnim bankovnim internim platnim sustavima. Validacija je provedena na sljedeći način:

1) **Definiranje svojstvenih kriterija za kritične interne bankovne platne sustave**

   Kao i kod studije slučaja sa *online* korisničkim transakcijskim sustavima, i u ovoj studiji slučaja s kritičnim internim platnim sustavima kao osnova za definiranje inherentnih (svojstvenih) kriterija korišteno je istraživanje [139], pri čemu su analizirani i definirani sigurnosni ciljevi i mehanizmi informacijske sigurnosti. S obzirom kako interni bankovni platni sustavi potpadaju također pod vrstu transakcijskih sustava, tako su definirani svojstveni kriteriji sljedeći:

   autentikacija, *autorizacija*, *kriptiranje*, *cjelovitost poruke* (eng. *Message integrity*), *dostupnost*, *logiranje* i *rezervna kopija*. Razlika u odnosu na javno dostupne korisničke online transakcijske sustave je u tome što se za interne platne sustave

[21] SWIFT – Udruženje za svjetske međubankarske financijske telekomunikacije, to je sigurna komunikacijska mreža za prijenos transakcijskih poruka između banaka i drugih financijskih institucija. Izvor: https://www.swift.com/

[22] FOS – Šalterska aplikacija za podršku klijentima koja se spaja na pozadinski glavni bankarski sustav (eng. *backend core banking system*) u svrhu dohvaćanja, obrade, distribucije i pohrane podataka, npr. za identifikaciju klijenta, otvaranje/zatvaranje računa, obavljanje transakcija (klijent fizičkom prisutnošću zadaje platni nalog), itd.

[23] SEPA – Jedinstveno područje plaćanja u eurima na kojemu potrošači, poslovni subjekti i tijela javne vlasti mogu uplaćivati i primati plaćanja u eurima pod jednakim osnovnim uvjetima, pravima i obvezama, neovisno o njihovoj lokaciji. Cilj inicijative SEPA-e je uspostava jedinstvenog sustava platnog prometa. Izvor: http://www.sepa.hr/

umjesto atributa *digitalno potpisivanje* koristi atribut *cjelovitost poruke*. Razlog je što u kontekstu internih bankovnih platnih sustava ta vrsta atributa kvalitetnije opisuje potrebu za C-I-A svojstvom u internim platnim sustavima, gdje službenici provjeravaju te imaju mogućnost izmjene platnih naloga unutar određene aplikacije, npr. za poruke/platne naloge pristigle u sustav za red poruka (eng. *message queue*). Integritet poruke osigurava da pristigla poruka (platni nalog) u informacijskom sustavu financijske institucije nije promijenjena na neautorizirani način, čime se sprječavaju potencijalni financijski gubici i brojni rizici koji proizlaze takvim gubicima te se također posljedično omogućava i veće povjerenje u određenu financijsku instituciju.

2) Računanje težina svojstvenih kriterija za kritične bankovne interne platne sustave

Kako bi se dobilo težine svojstvenih kriterija za kritične interne bankovne platne sustave nužno je bilo provesti istraživanje među stručnjacima za informacijsku sigurnost koji su, dajući svoje mišljenje, procjenjivali međusobne odnose (prema dominaciji, tj. važnosti) između definiranih kriterija. Ovom prilikom također se koristila SNAP metoda. Za izračunavanje težina svojstvenih kriterija za bankovne interne platne sustave metodom SNAP11, nužne su dvije ulazne komponente: utjecaji (zavisnosti) između elemenata i težine kriterija u odnosu na cilj odlučivanja. Prikupljanje podataka odrađeno je ispitivanjem stručnjaka za informacijsku sigurnost (FinTech zaposlenici) slanjem upitnika putem elektroničke pošte. Upitnik (Excel dokument) je sadržavao sljedeće radne stranice odnosno podfaze:

1. Podfaza: Stručnjaci su davali ocjene na DEMATEL skali (0-4) o utjecajima (zavisnostima) između svojstvenih kriterija za interne bankovne platne sustave popunjavajući sljedeću tablicu:

   Tablica 6.23: Definiranje utjecaja (zavisnosti) između svojstvenih kriterija za interne bankovne platne sustave

Utjecaji između svojstvenih kriterija za interne bankovne platne sustave	Ath	Atz	E	Mi	Av	L	B
Autentikacija (Ath)	0						
Autorizacija (Atz)		0					
Kriptiranje (E)			0				
Cjelovitost poruke (Mi)				0			

Dostupnost (Av)					0		
Logiranje (L)						0	
Rezervna kopija (B)							0

Izvorni oblik Tablice 6.23 koja je odaslana stručnjacima za informacijsku sigurnost s pripadajućim uputama o pravilnom ispunjavanju korespondira tablici iz Priloga E za studiju slučaja s korisničkim transakcijskim sustavima s razlikom kako je za ovu studiju slučaja s internim platnim susatvima umjesto kriterija *digitalno potpisivanje* korišten svojstveni kriterij *cjelovitost poruke*.

Na temelju prikupljenih podataka (što je bio inicijalni ulaz u SNAP metodu) od stručnjaka za informacijsku sigurnost iz financijskih institucija i povezanih FinTech tvrtki (prikupljeno ukupno 16 relevantnih odgovora) te provodeći cjelokupni postupak računanja utjecaja (zavisnosti) između svojstvenih kriterija za kritične interne bankovne platne sustave pomoću SNAP metode (predstavljeno u poglavlju *6.1.3. SNAP metoda*), dobivene su sljedeće vrijednosti:

Tablica 6.24: Težine svojstvenih kriterija s obzirom na utjecaje (zavisnosti) između elemenata za kritične interne bankovne platne sustave

Svojstveni kriteriji	Težine svojstvenih kriterija (SNAP12)
Autentikacija	0,175783143
Autorizacija	0,128942398
Kriptiranje	0,182825089
Cjelovitost poruke	0,12039715
Dostupnost	0,200857167
Logiranje	0,058000024
Sigurnosna kopija	0,133195029

Dobivene težine svojstvenih kriterija za interne bankovne platne sustave iz Tablice 6.24 zapravo odgovaraju izračunima za SNAP12 metodu pa je stoga bio potreban prelazak na drugu podfazu.

2. Podfaza: Stručnjaci su davali ocjene o važnosti svojstvenih kriterija u odnosu na cilj odlučivanja primjenom AHP metode.

   Identificirani svojstveni kriteriji za kritične interne bankovne platne sustave podijeljeni su u 4 klastera na isti način kao i u prvoj studiji slučaja vezano uz korisničke *online* transakcijske sustave. Tako su težine svojstvenih kriterija za

interne bankovne platne sustave s obzirom na cilj odlučivanja (međukorak za izračun SNAP11 kriterija) primjenom AHP metode prikazane sljedećom tablicom:

Tablica 6.25: Težine svojstvenih kriterija za bankovne interne platne sustave s obzirom na cilj odlučivanja

Svojstveni kriteriji	Težine svojstvenih kriterija (AHP)
Autentikacija	0,175836419
Autorizacija	0,142163711
Kriptiranje	0,194465766
Cjelovitost poruke	0,183312304
Dostupnost	0,092484221
Logiranje	0,111188969
Rezervna kopija	0,100548611

Konačne težine svojstvenih kriterija za kritične interne bankovne platne sustave dobivene primjenom aritmetičke sredine na vrijednosti iz Tablica 6.24 i Tablica 6.25 kao završnim korakom SNAP11 metode su sljedeće:

Tablica 6.26: Težine svojstvenih kriterija za interne platne sustave dobivene SNAP11 metodom

Svojstveni kriteriji	Težine svojstvenih kriterija (SNAP11)
Autentikacija	0,175809781
Autorizacija	0,135553055
Kriptiranje	0,188645427
Cjelovitost poruke	0,151854727
Dostupnost	0,146670694
Logiranje	0,084594496
Rezervna kopija	0,11687182

Iz Tablice 6.26 vidljivo je kako najveću težinu (prema procjenama stručnjaka) ima svojstveni kriterij *kriptiranje*.

Postupak računanja težina svojstvenih kriterija SNAP11 metodom za kritične interne bankovne platne sustave u potpunosti odgovara postupku za korisničke *online* transakcijske sustave kako je prikazano u Prilogu G.

3) Evaluacija internih bankovnih platnih sustava pomoću svojstvenih kriterija

Stručnjaci za informacijsku sigurnost su evaluirali kritične interne bankovne platne sustave pomoću svojstvenih (inherentnih) kriterija AHP metodom koristeći Saatyjevu standardnu skalu i postavljajući pritom sljedeće pitanje: *koji interni*

bankovni platni sustav je kvalitetniji (i koliko) u odnosu na promatrani kriterij? Pritom je za svaki interni platni sustav trebalo uzimati u obzir implementirane sigurnosne kontrole u odnosu na promatrani kriterij prilikom davanja prosudbi. Metodologija procjene kritičnih platnih sustava prema svojstvenim kriterijima identična je kao i u prvoj studiji slučaja za korisničke *online* transakcijske sustave. Tako su izračunati svojstveni vektori promatranih inherentnih kriterija sljedeći:

Tablica 6.27: Svojstveni vektori inherentnih kriterija za interne bankovne platne sustave

Alternative \ Kriteriji	Autentikacija	Autorizacija	Kriptiranje	Cjelovitost poruke	Dostupnost	Logiranje	Rezervna kopija
SWIFT	0,45150615	0,410490621	0,415902753	0,417630536	0,389059766	0,387217056	0,3783431
FOS	0,245392263	0,281160829	0,261274685	0,247927305	0,243535227	0,315551304	0,307230963
SEPA	0,303101587	0,30834855	0,322822562	0,334442159	0,367405007	0,29723164	0,314425937

4) Evaluacija kritičnih bankovnih internih platnih sustava pomoću generičkih ISRA kriterija

Stručnjaci za informacijsku sigurnost su evaluirali kritične interne bankovne platne sustave pomoću generičkih kriterija za analizu i procjenu rizika AHP metodom koristeći Saatyjevu standardnu skalu i postavljajući pritom sljedeće pitanje: *koji interni bankovni platni sustav ima veću izloženost riziku u odnosu na promatrani kriterij rizika*? Za svaki promatrani ISRA kriterij trebalo je uzimati u obzir i faktore koji dodatno mogu utjecati na rizičnost internog platnog sustava u odnosu na sam promatrani kriterij, a prema OWASP Risk Rating metodologiji [120]. Metodologija procjene kritičnih bankovnih internih platnih sustava prema generičkim ISRA kriterijima identična je kao i u prvoj studiji slučaja za korisničke *online* transakcijske sustave. Vrijednosti svojstvenih vektora generičkih ISRA kriterija su sljedeće:

Tablica 6.28: Svojstveni vektori ISRA kriterija za interne bankovne platne sustave

Alternative \ Kriteriji	Prijetnja	Ranjivost	Vjerojatnost	Posljedica	Otpornost
SWIFT	0,282848481	0,214032868	0,272583551	0,422104981	0,280985523
FOS	0,452141074	0,52667717	0,410496705	0,234212284	0,318864272
SEPA	0,265010445	0,259289962	0,316919745	0,343682735	0,400150205

5) **Rangiranje i usporedba rezultata procjene bankovnih internih platnih IT sustava dobivenih pomoću inherentnih kriterija u odnosu na rezultate dobivene višekriterijskim modelom s generičkim ISRA kriterijima**

Kako bi se u procesu validacije potvrdilo postavljenu hipotezu **H1**, potrebno je napraviti rang i usporedbu rezultata dobivenih primjenom višekriterijskog modela sa svojstvenim i generičkim ISRA kriterijima za bankovne interne platne sustave.

Tako su prilikom procjene bankovnih internih platnih sustava prema svojstvenim i generičkim ISRA kriterijima dobiveni sljedeći rezultati odnosno rang alternativa (rezultat umnoška vlastitih svojstvenih vektora i SNAP11 težina kriterija):

Tablica 6.29: Rang internih bankovnih platnih sustava prema svojstvenim kriterijima

Interni bankovni platni sustavi (svojstveni kriteriji)	**Rang**
SWIFT mreža	**0,410937523**
Front Office sustav	**0,266511803**
SEPA plaćanja	0,322550674

Iz Tablice 6.29 vidi se kako najveći ponder ima SWIFT mreža, što bi značilo kako je prema procjenama stručnjaka za informacijsku sigurnost upravo to onaj bankovni interni platni sustav koji ima ugrađene najbolje sigurnosne mehanizme i kontrole u odnosu na druge promatrane sustave. Zatim slijedi SEPA platni sustav/shema te na kraju FOS sustav s najmanjim ponderom.

Tablica 6.30: Rang internih bankovnih platnih sustava prema generičkim ISRA kriterijima

Interni bankovni platni sustavi (generički ISRA kriteriji)	**Rang**
SWIFT mreža	**0,285744166**
Front Office sustav	**0,387518499**
SEPA plaćanja	0,326737335

Iz Tablice 6.30 vidi se kako najveći ponder ima FOS sustav, zatim slijedi SEPA sustav i na kraju SWIFT mreža s najmanjim ponderom.

U ovom slučaju procjene kritičnih bankovnih internih platnih sustava također je trebalo primijeniti obrnutu logiku u odnosu na procjenu istih sustava pomoću svojstvenih kriterija tako što se ponovno gledalo koji sustav je najrizičniji prema promatranim generičkim ISRA kriterijima. Tako se dobije da je najmanje rizičan sustav SWIFT mreža, zatim slijedi SEPA sustav, dok se najrizičnijim platnim sustavom smatra FOS sustav. Prema tome, rang alternativa dobiven procjenom internih platnih sustava koristeći svojstvene kriterije odgovara rangu dobivenom

procjenjujući iste platne sustave pomoću generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti. Iz toga proizlazi kako je potvrđena hipoteza **H1** u studiji slučaja za kritične bankovne interne platne sustave.

Za provjeru hipoteze **H2** ponovno se koristila jednostavna metrika o ekvivalentu radnog vremena (FTE) pri čemu su ispitanici bilježili koliko im je vremena potrebno za ispunjavanje definiranih tablica prilikom procjene internih platnih sustava s generičkim ISRA kriterijima u odnosu na procjenu, tj. validaciju modela s inherentnim kriterijima. Mjerenje je pokazalo kako je ispitanicima u prosjeku trebalo 6,65 sati za pravilno ispunjavanje tablica za procjenu internih platnih sustava s inherentnim kriterijima, dok je istim ispitanicima bilo potrebno u prosjeku 5,87 sati za pravilno ispunjavanje svih tablica kod procjene istih internih platnih sustava s generičkim ISRA kriterijima. Pri mjerenju je uključeno i vrijeme potrošeno na dodatne (naknadne) procjene koje su bile potrebne zbog grešaka nastalih u inicijalnim procjenama od strane pojedinih ispitanika, npr. zbog praznina u tabličnim poljima za popunu, neadekvatno postavljenih reciprociteta ili neodgovarajućeg izračuna indeksa konzistentnosti. S obzirom kako su ispitanici trebali manje vremena za procjenu internih platnih sustava koristeći generičke ISRA kriterije u odnosu na procjenu istih sustava pomoću inherentnih kriterija, hipoteza **H2** vezano uz učinkovitost višekriterijskog modela s generičkim kriterijima za analizu i procjenu rizika je potvrđena.

6.4. Kalibracija modela

Istraživačka metdodologija znanstveni dizajn podrazumijeva kako je to zapravo iterativni proces pri čemu je moguće vratiti se npr. iz faze *Vrednovanja* ponovno u fazu *Dizajn i razvoj* kako bi se pokušalo usavršiti novi artefakt, u ovom slučaju model za procjenu kritičnih informacijskih sustava. Tako je u ovom radu napravljena kalibracija modela na istim studijama slučaja na kojima je bila provedena i validacija modela, ali s reduciranim brojem generičkih atributa za analizu i procjenu rizika informacijske sigurnosti. Razlog za kalibraciju odnosno smanjenje broja generičkih kriterija leži u samoj definicija problema gdje se na učinkovitiji način želi procijeniti kritične informacijske sustave s generičkim kriterijima za analizu i procjenu rizika. S manjim brojem kriterija, logično, postiže se dodatna učinkovitost u procjeni kritičnih informacijskih sustava, ali pod uvjetom da se potvrdi hipoteza **H1** u kalibriranom modelu s takvim manjim brojem generičkih ISRA kriterija. Dakle, rang kritičnih IT rješenja

primjenjujući kalibrirani model s generičkim ISRA kriterijima mora se ponovno podudarati sa rangom dobivenim pri evaluaciji istih IT rješenja koristeći inherentne kriterije modela.

Atribut (kriterij) kojim je hibridni model s generičkim ISRA kriterijima reduciran, tj. koji je uklonjen u procesu kalibracije je **Otpornost** (eng. *Resiliency*). Razlog je taj što je atribut **Otpornost** imao najmanji indeks slaganja (potvrde) među ispitanicima prilikom prikupljanja podataka *Delphi* metodom vezano uz identifikaciju ključnih elemenata za analizu i procjenu rizika informacijske sigurnosti. Također, to je jedini atribut koji je od strane manjeg broja stručnjaka za informacijsku sigurnost označen suvišnim za novi hibridni višekriterijski model na način da su pojedini ispitanici dodjeljivali vrijednost 2-Ne slažem se tom atributu. Dodatno, preostala četiri atributa za analizu i procjenu rizika informacijske sigurnosti (*prijetnja, ranjivost, vjerojatnost* i *posljedica*) u novom višekriterijskom modelu u potpunosti odgovaraju funkciji rizika prema međunarodnom standardu ISO/IEC 27005, a u kojemu element **Otpornost** nije eksplicitno definiran.

Prilikom kalibracije modela i ponovnog računanja težina generičkih ISRA kriterija, korišteni su identični podaci kao i u poglavlju 6.1.4. prikupljeni od sigurnosnih stručnjaka prema DEMATEL skali, ali bez vrijednosti za kriterij **Otpornost**. Ponovno se prolazilo kroz isti postupak računanja težina generičkih ISRA kriterija SNAP11 metodom (opisano u poglavlju 6.1.3.) na sljedeći način:

1. Korištenje vrijednosti sa DEMATEL skale kao ulaznih parametara prikupljenih od sigurnosnih stručnjaka prethodnim istraživanjem
2. Računanje težina generičkih ISRA kriterija s obzirom na utjecaje (zavisnosti) između elemenata (SNAP12)
3. Računanje težina generičkih ISRA kriterija s obzirom na cilj odlučivanja (AHP)
   Treba napomenuti kako se u ovom koraku zapravo radilo samo o preuzimanju već izračunatih težina za kriterije *prijetnja* (**T**), *ranjivost* (**V**), *vjerojatnost* (**P**) i *posljedica* (**C**) koji su bili dio klastera **Rizik**, te dodatna računanja nisu bila potrebna jer usporedba između prethodno definiranih klastera **Rizik** i **Otpornost** nema nikakav utjecaj niti je primjenjiva na slučaj kalibracije modela bez atributa **Otpornost**.
4. Primjena aritmetičke sredine na vrijednosti dobivene iz prethodnih koraka kako bi se dobilo tražene težine SNAP11 metodom.

Tako su težine generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti bez elementa **Otpornost** za potrebe kalibracije novog višekriterijskog modela prikazane sljedećom tablicom:

Tablica 6.31: Težine generičkih ISRA kriterija bez elementa Otpornost

Generički ISRA kriteriji	Kalibrirane težine ISRA kriterija (SNAP11)
Prijetnja (T)	**0,228648927**
Ranjivost (V)	**0,374850372**
Vjerojatnost (P)	**0,137844055**
Posljedica (C)	**0,258656646**

Iz Tablice 6.31 vidljivo je kako u kalibriranom modelu najveću težinu ima generički kriterij *ranjivost*, dok u izvornom višekriterijskom modelu najveću težinu (Tablica 6.7) ima kriterij *otpornost* koji je uklonjen u kalibriranom modelu.

6.4.1. Kalibracija modela za studiju slučaja s korisničkim transakcijskim sustavima

Kalibracija modela za studiju slučaja vezano uz procjenu kritičnih bankovnih *online* transakcijskih sustava provedena je na sljedeći način:

1. Uklanjanje svih izračuna i vrijednosti za svojstveni vektor **Otpornost** dobivenih od sigurnosnih stručnjaka vezano uz transakcijske sustave te množenje novih vrijednosti ISRA svojstvenih vektora za transakcijske sustave sa novim kalibriranim SNAP11 težinama ISRA kriterija (Tablica 6.31) kako bi se dobilo rang korisničkih transakcijskih sustava.

   Tablica 6.32: Svojstveni vektori ISRA kriterija i SNAP11 težine bez kriterija Otpornost za kritične trx sustave

Alternative \ Kriteriji	Prijetnja	Ranjivost	Vjerojatnost	Posljedica	Kalibr. SNAP11 težine kriterija
e-banking	0,300439318	0,346069687	0,39203031	0,4715484	**0,228648927**
m-banking	0,312925954	0,25058345	0,24449367	0,319128828	**0,374850372**
e-commerce	0,386634729	0,403346863	0,36347602	0,209322771	**0,137844055**
					0,258656646

   Nakon množenja novih vrijednosti svojstvenih vektora generičkih ISRA elemenata za kritične korisničke transakcijske sustave sa kalibiranim težinama generičkih ISRA kriterija, dobije se Tablica 6.33.

   Tablica 6.33: Rang kritičnih trx sustava bez kriterija Otpornost

Transakcijski sustavi (generički ISRA kriteriji)	**Rang**
e-banking	0,374427654

m-banking	**0,281728274**
e-commerce	0,343844072

Tablica 6.33 prikazuje rang kritičnih bankovnih transakcijskih sustava procijenjenih novim hibridnim višekriterijskim modelom nakon procesa kalibracije (bez generičkog kriterija **Otpornost**).

2. Usporedba ranga za rezultate dobivene svojstvenim kriterijima u odnosu na rang dobiven generičkim ISRA kriterijima primjenom kalibriranog modela za kritične transakcijske sustave.

   Iz Tablice 6.33 proizlazi kako je *m-banking* sustav najmanje rizičan, zatim slijedi *e-commerce* sustav te na kraju *e-banking* kao najrizičniji bankovni korisnički transakcijski sustav. Uspoređujući rang rezultata dobivenih inicijalnim modelom sa svim ISRA kriterijima (Tablica 6.22) u odnosu na rang bez kriterija **Otpornost** (Tablica 6.33), vidi se blago odstupanje u rangu između rješenja na drugom i trećem mjestu, dok je u oba slučaja kao najbolje (najmanje rizično) rješenje *m-banking* s najmanjim ponderom rizika. Kada se novi rang za transakcijske sustave prema procjenama s ISRA kriterijima usporedi s rangom rješenja dobivenim procjenama i korištenjem svojstvenih kriterija, tada hipoteza **H1** nije u potpunosti zadovoljena, što znači kako je kalibrirani model (bez kriterija **Otpornost**) pri procjeni transakcijskih sustava valjan samo u slučaju kada se traži najbolje rješenje, ali ne i čitav rang preostalih kritičnih bankovnih *online* transakcijskih sustava.

6.4.2. Kalibracija modela za studiju slučaja s internim platnim sustavima

Kalibracija modela za studiju slučaja vezano uz procjenu kritičnih bankovnih internih platnih sustava provedena je na sljedeći način:

1. Uklanjanje svih izračuna i vrijednosti za svojstveni vektor **Otpornost** dobivenih agregacijom prosudbi vezano uz kritične interne bankovne platne sustave te množenje novih ISRA vrijednosti preostalih svojstvenih vektora za interne platne sustave sa novim SNAP11 težinama ISRA kriterija (Tablica 6.31) kako bi se dobilo rang alternativa.

Tablica 6.34: Svojstveni vektori ISRA kriterija i SNAP11 težine bez kriterija Otpornost za kritične interne platne sustave

Alternative \ Kriteriji	Prijetnja	Ranjivost	Vjerojatnost	Posljedica	Kalibr. SNAP11 težine kriterija
SWIFT	0,28284848	0,214032868	0,27258355	0,422104981	**0,228648927**
FOS	0,45214107	0,52667717	0,4104967	0,234212284	**0,374850372**
SEPA	0,26501045	0,259289962	0,31691974	0,343682735	**0,137844055**
					0,258656639

Nakon množenja novih vrijednosti svojstvenih vektora generičkih ISRA elemenata za kritične interne platne sustave sa kalibiranim težinama generičkih ISRA kriterija, dobije se Tablica 6.35.

Tablica 6.35: Rang kritičnih internih platnih sustava bez kriterija Otpornost

Interni platni sustavi (generički ISRA kriteriji)	**Rang**
SWIFT	**0,291657594**
FOS	**0,417971789**
SEPA	**0,290370617**

Tablica 6.35 prikazuje rang kritičnih bankovnih internih platnih sustava procijenjenih novim hibridnim višekriterijskim modelom nakon procesa kalibracije (bez generičkog kriterija **Otpornost**).

2. Usporedba ranga za rezultate dobivene svojstvenim kriterijima u odnosu na rang dobiven generičkim ISRA kriterijima primjenom kalibriranog modela za kritične interne platne sustave.

   Iz Tablice 6.35 proizlazi kako je *FOS* najrizičniji interni platni sustav s uvjerljivo najvećim (negativnim) ponderom, a što odgovara dobivenom rezultatu iz Tablice 6.30. Ipak, u ovom slučaju s kalibiranim modelom, rang nije identičan kao kod predloženog izvornog modela s uključenim kriterijem **Otpornost**, jer SWIFT ima negativniji relativni ponder u odnosu na SEPA sustav. No, razlike između dva promatrana sustava su izrazito male (tek vrijednost treće decimale), a što dovodi do spoznaje o velikoj osjetljivosti višekriterijskog modela u slučaju korištenja manjeg (reduciranog) broja kriterija. Tako se dolazi do zaključka o velikoj važnosti kriterija **Otpornost** te kako nema potrebe za daljnjim smanjivanjem broja generičkih kriterija predloženog višekriterijskoga modela u svrhu postizanja veće učinkovitosti jer to može prouzročiti pogrešne rezultate, a samim time i donošenje neadekvatne odluke,

što na koncu može dovesti do sigurnosnog, regulatornog, financijskog i reputacijskog rizika po organizaciju (financijsku instituciju).

6.5. Rasprava i zaključak

Završnim poglavljem ovoga rada predstavlja se sumarni pregled istraživačkog procesa po fazama, ostvarenje postavljenih ciljeva i hipoteza, ograničenja tijekom istraživačkog procesa, mogućnosti za buduća istraživanja, objava rezultata istraživanja te konačne zaključke.

Znanstveno istraživanje i izrada doktorskog rada vođeno je prema metodologiji znanstvenog dizajna (DSRM) primjenjujući odgovarajuće istraživačke metode u svakoj od istraživačkih faza. Istraživanje u svrhu izrade ovog doktorskog rada napravljeno je prema sljedećim fazama:

1. Sustavni pregled literature (SLR) vezano uz primjenu metoda višekriterijskoga odlučivanja u domeni rizika informacijske sigurnosti (izrada baze znanja)
2. Identifikacija ključnih elemenata za analizu i procjenu rizika pomoću *Delphi* tehnike ispitivanjem stručnjaka za informacijsku sigurnost iz financijskih institucija
3. Razvoj modela te odabir odgovarajuće metode za višekriterijsko odlučivanje u svrhu definiranja težina generičkih ISRA kriterija
4. Računanje težina generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti (SNAP11 metoda)
5. Odabir prikladne MCDM metode za evaluaciju alternativa, tj. kritičnih poslovnih IT sustava (AHP metoda)
6. Validacija predloženog višekriterijskoga modela na studijama slučaja
7. Kalibracija višekriterijskog modela (reduciranje kriterija *otpornost*)
8. Validacija referentnog modela s inherentnim kriterijima.

Svaka od navedenih istraživačkih faza bila je ključna za postizanje određenih ciljeva te davanje neophodnih odgovora i ulaza u sljedeću istraživačku fazu.

6.5.1. Pregled ostvarenih ciljeva i hipoteza

S obzirom na postavljeni glavni cilj istraživanja vezano uz donošenje informirane odluke o stanju sigurnosti kritičnih poslovnih IT sustava i povećanje učinkovitosti procesa

procjene i odabira istih, kao i rezultate dobivene kroz razne istraživačke faze, tako se može rezimirati ostvarenje specifičnih ciljeva:

- **C1**: Cilj je uspješno ostvaren provedbom sustavnog pregleda literature (SLR) te objavom rezultata u znanstvenom časopisu.
- **C2**: Cilj je uspješno ostvaren razvojem i demonstracijom novog višekriterijskoga modela s generičkim elementima za analizu i procjenu rizika informacijske sigurnosti strogom primjenom metodologije znanstvenog dizajna i odgovarajućih metoda, kao što su *Delphi* anketa, statističke metode te metoda dizajna.
- **C3**: Validacija novog višekriterijskoga modela za procjenu kritičnih poslovnih IT sustava napravljena je na različitim studijama slučaja pri čemu su potvrđene obje znanstvene hipoteze pa je tako ostvaren i specifični istraživački cilj **C3**.

Postavljene znanstvene hipoteze **H1** i **H2** potvrđene su u obje studije slučaja vezano uz procjenu kritičnih bankovnih korisničkih (*online*) transakcijskih sustava i procjenu kritičnih bankovnih internih platnih sustava.

Dodatno, procesom kalibracije i primjenom metoda eksperimenta i komparacije pokušalo se utvrditi da li novi višekriterijski model može biti još učinkovitiji reduciranjem generičkog elementa **Otpornost** iz samog modela. Prema prvoj studiji slučaja pokazalo se kako kalibrirani višekriterijski model može biti još učinkovitiji, ali da vrijedi samo ako se kao cilj traži najbolje (top) rješenje, ali ne vrijedi ako se želi dobiti čitav rang alternativa takvim reduciranim modelom. Prema drugoj studiji slučaja pokazalo se kako kalibrirani višekriterijski model ne daje adekvatne rezultate.

6.5.2. Kvalitativna analiza modela i istraživački doprinos

Nakon završene faze vrednovanja i kalibracije modela, slijedi analiza predstavljenog višekriterijskoga modela te analiza rezultata dobivenih sa obje studije slučaja.

Postoji nekoliko značajnih karakteristika novog predloženog višekriterijskoga modela za procjenu kritičnih poslovnih IT sustava, a koje zapravo predstavljaju i vrlo važan istraživački doprinos. Prvenstveno radi se o definiranim generičkim kriterijima za analizu i procjenu rizika informacijske sigurnosti te njihovim pripadajućim težinama, a što bi trebalo olakšati i unaprijediti proces procjene kritičnih poslovnih IT sustava. Pri tome je predviđen manji utrošak resursa (u vidu vremena i broja IT stručnjaka), jer nema potrebe za ponovnom identifikacijom inherentnih (svojstvenih) kriterija i računanjem njihovih težina svaki put iznova za procjenu

nekih kritičnih poslovnih IT sustava. Druga izrazito važna karakteristika modela su definirani utjecaji i zavisnosti (tj. povratna veza, eng. *feedback*) između generičkih ISRA kriterija za evaluaciju alternativa. Kao što je otkriveno sustavnim pregledom literature [142], povratna veza između evaluacijskih elemenata je u pravilu zanemarena u mnogim postojećim modelima te stoga definiranje takvih odnosa predstavlja najznačajniju kvalitativnu snagu te znanstveni doprinos novog višekriterijskog modela. To je posebno bitno jer iz definicije rizika informacijske sigurnosti je jasno kako između elemenata sigurnosnih rizika postoje brojne međusobne zavisnosti i utjecaji te da pojedini elementi zapravo ne mogu egzistirati samostalno bez međuovisnosti o drugim elementima iz skupa. Također, dodatna prednost modela je nezavisnost evaluacijskih (ISRA) kriterija i alternativa. To svakako podrazumijeva univerzalnost modela koji bi trebao podržavati procjenu različitih informacijskih sustava, a ne samo specifičnih kao što bi to bio slučaj za neke IT sustave pri korištenju kriterija svojstvenih promatranom sustavu.

U studijama slučaja pokazano je kako je proces procjene kritičnih poslovnih IT sustava značajno skraćen i pojednostavljen prilikom korištenja već definiranih generičkih ISRA kriterija u odnosu na procjenu istih IT sustava korištenjem kriterija inherentnih promatranim poslovnim IT sustavima. Znači, predloženi model s generičkim ISRA kriterijima je učinkovitiji u odnosu na model s inherentnim kriterijima. To pokazuju i konkretne brojke dobivene tijekom procesa validacije, a vezano uz testiranje hipoteze **H2** u obje studije slučaja, čime se zapravo daje odgovor na istraživačko pitanje P1 i ostvaruje općeniti (glavni) cilj istraživanja vezano uz povećanje učinkovitosti procesa procjene kritičnih IT sustava.

Korištenje generičkih kriterija za analizu i procjenu rizika može se smatrati određenom manjkavosti odnosno ograničenjem modela s obzirom kako će inherentni atributi određenog IT sustava uvijek bolje odgovarati takvim sustavima u usporedbi s generičkim kriterijima, što je sasvim razumljivo i logično. No, glavna zamisao modela s generičkim ISRA kriterijima je ionako bila na većoj učinkovitosti u vidu manjeg utroška resursa u procesu procjene kritičnih IT sustava, ali s ciljem da procjene budu adekvatne, tj. točne uspoređujući ih s modelom s inherentnim kriterijima.

U prvoj studiji slučaja vezano uz procjenu kritičnih bankovnih korisničkih transakcijskih sustava pokazano je kako model s generičkim ISRA kriterijima daje identične rezultate (rang alternativa) kad se za evaluaciju koriste kriteriji svojstveni samim bankovnim *online* transakcijskim sustavima. Razlog za odabir iste metodologije za generičke ISRA kriterije i za svojstvene kriterije za potrebe definiranja, grupiranja, izračunavanja i procjene alternativa je kako neki drugi adekvatni (referentni) model nije pronađen sustavnim pregledom

literature (a što je detaljno objašnjeno u poglavlju *6.3. Vrednovanje višekriterijskoga modela* prilikom evaluacije samog referentnog modela s inherentnim kriterijima). Također, ovakav pristup može se smatrati najpreciznijim u svrhu validacije predloženog višekriterijskoga modela za procjenu i rangiranje kritičnih poslovnih IT sustava.

Razlozi zbog kojih su IT sigurnosni stručnjaci ocijenili kako je *m-banking* sustav najsigurniji (prema svojstvenim kriterijima/kontrolama) odnosno najmanje rizičan (prema generičkim ISRA kriterijima), su sljedeći (sumirano prema dobivenim komentarima):

- Današnje moderne aplikacije za mobilno bankarstvo su izvorne (eng. *native*), što znači kako su prilagođene određenom operacijskom sustavu (iOS ili Android), pri čemu se moraju provesti rigorozni testovi i validacija prije nego što aplikacija postane dostupna za preuzimanje u trgovini (to posebno vrijedi za Apple Store).
- S obzirom kako su aplikacije za *m-bankarstvo* izvorne, to znači da takve aplikacije obično nisu ranjive na najčešće napade prema OWASP Top 10 sigurnosnim rizicima web aplikacija [108], kao što su unakrsno skriptiranje (eng. *Cross-site scripting*, XSS) ili SQL ubacivanje (eng. *SQL injection*, SQLi), jer u takve mobilne aplikacije nisu uključene uobičajene web komponente, za razliku od standardnog internetskog bankarstva i posebno *e-trgovine*.
- Aplikacije *m-bankarstva* u pravilu koriste snažnu (dvofaktorsku) autentifikaciju, pri čemu je jedan faktor autentifikacije sam mobilni uređaj (nešto što korisnik ima), a drugi je PIN (nešto što korisnik zna) ili biometrijski element (prepoznavanje otiska prsta ili lica – nešto što korisnik jest). S druge strane, brojne web stranice za *e-trgovinu* još uvijek ne zahtijevaju jaku provjeru autentičnosti ili dodatne elemente za autorizaciju platnih transakcija pa su tako i metom brojnih kibernetičkih napada i posljedično prijevara. Osim toga, prilikom autentikacije na aplikaciju *m-bankarstva*, većina banaka u svojim poslužiteljskim pozadinskim (eng. *back-end*) sustavima ima ugrađene kontrole za zaštitu od prijevara (eng. *antifraud controls*) primjenom tehnika skeniranja karakteristika uređaja i softvera (eng. *device fingerprint*), na što su banke u Europskoj Uniji prisiljene i regulativom [143], a što svakako značajno doprinosi povjerenju u sigurnosne aspekte mobilnog baknarstva.
- Stručnjaci za informacijsku sigurnost koji rade u bankarskom sektoru vodili su se i odredbama tehničkog standarda za snažnu autentikaciju klijenata te zajednički i sigurni otvoreni standard komunikacije, a koji predviđa i određene iznimke ([143], *Chapter III*) od snažne autentikacije kako bi se omogućilo jednostavniji i brži pristup

internetskim web platnim sustavima. Takav oblik mogućeg smanjena restrikcija i kontrola u pristupu *e-banking* web aplikacijama svakako pridonosi nešto kritičnijem razmišljanju prema *e-banking* web orijentiranim sustavima i mogućim vektorima napada kroz ranjivosti koje se otvaraju potencijalnim smanjenjem sigurnosnih kontrola.

- Unatoč velikoj popularnosti mobilnih aplikacija, glavni kibernetički napadi danas se i dalje odnose na web aplikacije jer ipak znatno manje napora i znanja je potrebno za napad na neku web aplikaciju gdje postoje već gotovi i testirani alati sa skupom naredbi i iskoristivosti (eng. *exploits*), u usporedbi s mobilnom aplikacijom pri čemu je za napad potrebno utrošiti znatno više resursa (vremena, opreme, softvera, naprednih tehničkih vještina i financijskih sredstava). Ali, predviđanje je kako bi se trend svakako mogao promijeniti u budućnosti (npr. zbog pojave specijaliziranih i besplatnih hakerskih modula za *m-banking* aplikacije), pa je stoga prijedlog definitivno ponoviti procjenu bankarskih internetskih transakcijskih sustava u dogledno vrijeme na nešto većoj populaciji ispitanika (sigurnosnih IT stručnjaka iz financijske industrije).

Kalibriranim modelom u prvoj studiji slučaja za kritične korisničke transakcijske sustave nije se potvrdila hipoteza H1, tj. rang alternativa pri usporedbi rezultata za generičke i svojstvene kriterije nije isti. Takav kalibrirani model je za najmanje rizičan korisnički transakcijski sustav kao rezultat dao *m-banking*, što je identično kao i kod predloženog višekriterijskog modela koji uključuje element **Otpornost**, a koji je ciljano izostavljen u kalibriranom modelu. Dakle, ako bi se kao cilj evaluacije postavilo da se traži isključivo najbolje rješenje, a ne cjelokupni rang kritičnih korisničkih transakcijskih sustava što predstavlja dosta rigorozno ograničenje za validaciju modela i dokazivanje hipoteze H1 (prema definiranoj metrici M1), u tom slučaju bi i takav kalibrirani višekriterijski model zaista bio zadovoljavajući. To svakako ukazuje i na važnost generičkog kriterija **Otpornost**, ali moguće i osjetljivost predloženog modela na promjene njegove inicijalne strukture, kao i na važnost i konzistentnost u procjenama sigurnosnih IT stručnjaka.

U drugoj studiji slučaja vezano uz procjenu kritičnih bankovnih internih platnih sustava pokazano je kako model s generičkim ISRA kriterijima daje identične rezultate (rang alternativa) kada se za evaluaciju koriste kriteriji svojstveni samim bankovnim internim platnim sustavima, što znači potvrđena je hipoteza **H1**. Razlozi zbog kojih su IT sigurnosni stručnjaci

ocijenili kako je SWIFT platni sustav najsigurniji (prema svojstvenim kriterijima/kontrolama) odnosno najmanje rizičan (prema generičkim ISRA kriterijima), su sljedeći:

- Međunarodna SWIFT organizacija je objavila vlastiti program sigurnosti klijenata (eng. *Customer Security Programme*, CSP) koji je uspostavljen sa svrhom aktivne podrške klijentima u borbi protiv kibernetičkih napada. Tako je u sklopu tog programa objavljen i okvir za korisničke sigurnosne kontrole (eng. *Customer Security Controls Framework*, CSCF) koji se sastoji od obveznih i preporučenih sigurnosnih kontrola za sve SWIFT korisnike [157]. To je sve napravljeno sa svrhom jačanja sigurnosti globalnog bankarskog sustava.
- FOS korisnički sustav pokrenut je na Windows računalima u financijskoj instituciji, pri čemu je ta vrsta operacijskog sustava (OS) izložena stalnim naprednim vrstama prijetnji (eng. *Advanced Persistent Threats*, APT) od strane napadača. Npr., *phishing* elektornička pošta koja sadržava poveznicu za preuzimanje malicioznog koda ili sam maliciozni kod u privitku elektroničke poruke (danas najčešće sa svrhom zaključavanja datoteka na disku i traženja otkupnine, tzv. *ransomware*). Probojem u Windows OS omogućava se ujedno i proboj u FOS sustav, a najčešće zbog korištenja iste autentikacije preuzimanjem Kerberos ticketa ili otiska (eng. *hash*) lozinke, tzv. *Pass-the-Ticket* (PtT), *Pass-the-Hash* (PtH), *Overpass-the-Hash* i *Golden Ticket* napadi na Kerberos autentikaciju Active Directory infrastrukture.
- Brojnost prijetnji, ranjivosti i iskoristivosti svakako je značajnija po Windows sustave u odnosu na sve druge operacijske sustave, a što se može potvrditi pregledom NIST baze ranjivosti [145] i dostupne baze iskoristivosti [146]. Stoga je i logično kako je FOS sustav identificiran kao najrizičniji u odnosu na ostale promatrane interne bankovne platne sustave.
- SEPA platna shema je strogo standardizirana pri čemu se platne transakcije obavljaju u skladu sa ISO 20022 XML formatom platnih poruka pa stoga pružaju i veću razinu sigurnosti za sve entitete u platnom procesu (inicijator plaćanja, banka platitelja i banka primatelja novčane doznake).
- Treba istaknuti kako je ispitanicima u drugoj studiji slučaja trebalo značajnije više vremena za procjenu internih platnih IT sustava koristeći i inherentne i generičke kriterije u odnosu na prvu studiju slučaja, iako su obje studije slučaja imale identičan broj inherentnih i generičkih kriterija po kojima se kritične IT sustave procjenjivalo.

Razlog tomu leži u velikoj složenosti i izrazitoj specifičnosti bankovnih internih platnih sustava.

Kalibriranim modelom u drugoj studiji slučaja za kritične bankovne interne platne sustave nije se potvrdila hipoteza H1, tj. rang alternativa pri usporedbi rezultata za generičke i svojstvene kriterije nije isti. Zbog izrazito male razlike u ponderima između SWIFT i SEPA promatranih platnih sustava, vidljivo je kako se radi o velikoj osjetljivosti i zapravo neadekvatnosti višekriterijskoga modela s generičkim ISRA kriterijima u slučaju smanjenja broja evaluacijskih kriterija (tj. bez kriterija **Otpornost**). Stoga se svakako ne preporuča korištenje takve vrste kalibriranog modela u svrhu dobivanja potencijalno veće učinkovitosti jer može dovesti do pogrešnih rezultata, zaključaka i (ne)informiranih odluka koje pak dovode do ostvarenja određenih rizika.

S obzirom na dobivene rezultate sa obje studije slučaja, predstavljeni višekriterijski model s ukupno pet generičkih kriterija za analizu i procjenu rizika informacijske sigurnosti može se svakako koristiti pri evaluaciji, rangiranju i odabiru kritičnih poslovnih IT sustava.

6.5.3. Ograničenja istraživanja

Tijekom provođenja znanstvenog istraživanja uočena su i određena ograničenja, a što je moguće u određenoj manjoj mjeri utjecalo i na dobivene rezultate istraživanja. Npr.:

- Nepoznavanje AHP metodologije od strane manjeg broja stručnjaka za informacijsku sigurnost pri čemu su bila nužna dodatna objašnjenja kako bi stručnjaci mogli ispravno popuniti tablice usporedbi u parovima, a što je rezultiralo dužim trajanjem istraživanja.
- Pronalazak odgovarajućeg broja stručnjaka koji razumiju bankarsku poslovnu domenu, razinu zaštite kritičnih informacijskih sustava koji su se procjenjivali te sigurnosne rizike po iste sustave. To se posebno odnosi na drugu studiju slučaja vezano uz interne platne sustave pri čemu su se tražila vrlo specifična znanja o platnim sustavima te razinama zaštite istih kao i izloženosti rizicima takvih kritičnih bankovnih sustava.
- Veliki broj tablica za usporedbu u parovima za ispitanike kod validacije modela, pri čemu se moglo primijetiti pad koncentracije ispitanika što je rezultiralo pogreškama kod procjena (npr. praznine u tabličnim poljima za popunu, neadekvatno postavljeni reciprociteti ili neodgovarajući CR). Stoga su bile potrebne

naknadne iteracije za određeni broj ispitanika, a što je opet dodatno produžilo tijek istraživanja pri procesu validacije višekriterijskoga modela s generičkim ISRA kriterijima.

- Ekstremni omjeri (npr., 7:1 ili 9:1) između pojedinih elemenata/alternativa, koji se inače u praksi relativno rijetko koriste za AHP metodu (iako sama Saatyjeva skala to omogućava), dobiveni od strane čak i jako malog broja ispitanika mogu prouzročiti značajnije promjene u težinama kriterija pa tako i u konačnom rangu alternativa u slučaju manjeg broja ispitanih stručnjaka. Stoga je bilo nužno naglasiti ispitanicima prilikom slanja upitnika o važnosti davanja konzistentnih procjena i suzdržavanja korištenja ekstremnih omjera te svakako imati veći broj ispitanika od minimalno potrebnog broja 5 kako bi se dobilo vjerodostojne rezultate. Iz tog razloga je bilo nemoguće pronaći veći broj stručnjaka za informacijsku sigurnost (npr. 15 ispitanika) koji bi mogli procijeniti određeni kritični informacijski sustav unutar jedne organizacije, već je svaki stručnjak procjenjivao sustav u financijskoj instituciji u kojoj je zadužen za zaštitu informacijskog sustava te se nakon toga radilo agregaciju takvih procjena.
- Stroga definicija metrike M1 kako se traži potpuni rang kritičnih poslovnih IT sustava svakako predstavlja značajno ograničenje u vidu dokazivanja hipoteze H1 (što je primijećeno tijekom kalibracije modela za studiju slučaja vezano uz transakcijske sustave), u odnosu kada bi se tražilo odstupanje samo od najboljeg rješenja.
- Nemotiviranost sudionika za sudjelovanje u istraživanju zbog složenosti i zahtjevnosti samog istraživanja
- Relativno malen, ali ipak dovoljan broj eksperata koji su sudjelovali u istraživanju.

6.5.4. Mogućnosti za buduća istraživanja

S obzirom na širinu domene sigurnosti informacijskih sustava, svakako postoje brojne mogućnosti za buduća istraživanja vezano uz primjenu novog višekriterijskoga modela s generičkim ISRA kriterijima. Prijedlozi i smjernice su sljedeći:

- Ponoviti istraživanje vezano uz kritične bankovne korisničke transakcijske sustave na način da se postojećim inherentnim kriterijima pridodaju kriteriji *antimalware* i zaštita od prijevara (eng. *antifraud*) te napraviti usporedbu rezultata sa dosadašnjom

provedenom studijom. Razlog uvođenju ovih dvaju elemenata proizlazi iz recentne europske direktive o sigurnosti platnih sustava [143], gdje se nalaže svim pružateljima usluga platnih transakcija uvođenje dodatnih sigurnosnih standarda, mehanizama i alata u svrhu zaštite kritičnog informacijskog sustava.

- Napraviti studiju slučaja gdje se kao alternativa uz postojeće korisničke bankovne transakcijske sustave uspoređuje i određeni transakcijski kriptosustav, npr. Bitcoin. Razlog je sve veća zastupljenost transakcijskih kriptosustava u platnom prometu.
- Generičke kriterije za analizu i procjenu rizika iz klastera **Rizik** podijeliti na dodatne klastere i ponovno zatražiti od sigurnosnih stručnjaka povratnu informaciju (tj. stav o utjecajima i zavisnostima između kriterija) kako bi se vidjelo postoji li značajna razlika u težinama kriterija koristeći takav dodatno klasterirani pristup za ISRA kriterije. Npr., elemente *prijetnja* i *ranjivost* staviti u jedan klaster, a elemente *vjerojatnost* i *posljedica* u drugi klaster (što bi odgovaralo osnovnoj formuli za procjenu rizika, Rizik = vjerojatnost x posljedica). Moguće kako bi se tako dobilo težine ISRA kriterija koje bi još više korelirale s težinama inherentnih kriterija, a samim time bi i rezultati procjene kritičnih IT sustava provedeni višekriterijskim modelom s generičkim ISRA kriterijima bili precizniji i vjerodostojniji.
- Ponoviti istraživanje za studije slučaja sa istim ekspertima, ali uz promjenu pozicija (redoslijeda) alternativa u matricama za usporedbu kako bi se uvidjelo da li postoji pristranost odnosno određeni psihološki efekt prilikom uspoređivanja u parovima.
- Napraviti istraživanje na dodatnim studijama slučaja. Npr., s obzirom na današnju sveprisutnost usluga u oblaku (eng. *cloud services*), napraviti validaciju modela na nekom od takvih servisa s naglaskom na SaaS (*Software as a Service*) vrstu servisa zbog daleko veće zastupljenosti u odnosu na PaaS (*Platform as a Service*) ili IaaS (*Infrastructure as a Service*) vrste servisa u oblaku, iako bi se i takve vrste servisa također moglo procjenjivati. Pritom bi se moguće kao referentni model za usporedbu moglo koristiti Cloud Control Matrix okvir definiran od strane CSA (*Cloud Security Alliance*) za potrebe STAR provjere (eng. *CSA STAR attestation*) ukoliko je takva provjera već napravljena za određeni servis u oblaku.
- Napraviti istraživanje (studiju slučaja) s primjenom modela za tehnološko-sigurnosne sustave (npr. za kritične poslužiteljske operacijske sustave ili za napredni mrežni vatrozid) na način da se ponovno računaju težine generičkih ISRA kriterija za zadani kontekst, ali i da se iskoriste već postojeće izračunate težine za kritične

poslovne IT sustave te tako napravi usporedba rezultata. Moguće kako bi tom prilikom bila nužna dodatna kalibracija modela u vidu proširenja postojećih generičkih ISRA kriterija s novim elementima (podkriterijima) odnosno faktorima rizika kako bi se dobili precizniji rezultati, npr. faktori agenta prijetnje, faktori ranjivosti, faktori tehničkog utjecaja, faktori poslovnog utjecaja te njihovi pripadajući podkriteriji. Kao post-analiza za studiju slučaja sa sigurnosno-tehnološkim sustavima svakako istražiti da li i u kojoj mjeri inherentni kriteriji koreliraju sa prijetnjama, ranjivostima i iskoristivostima takvih sustava.

- Prilikom evaluacije kritičnih IT rješenja pokušati koristiti neku od metoda eliminacije odnosno nadmašivanja (eng. *outranking*) umjesto AHP metode te usporediti rezultate dobivene AHP-om. Dodatno, u pojedinim slučajevima odabira IT rješenja korištenje metode eliminacije možda dodatno ubrza proces evaluacije eliminacijom neadekvatnog IT sustava.
- Fazifikacija ulaznih vrijednosti za generičke kriterije u svrhu izračuna SNAP11 težina kriterija kako bi se eventualno smanjilo utjecaje ekstremnih omjera (npr., 7:1 ili 9:1) između kriterija te moguće dobilo preciznije rezultate prilikom procjene kritičnih IT sustava. Činjenica kako se fazifikacijom i defazifikacijom proces izračuna težinskih vrijednosti odužuje u određenoj mjeri, no to se ipak može kompenzirati tako što se automatiziraju izračuni korištenjem softverskih alata. Osim toga, tim procesom se smanjuje neizvjesnost vezano uz subjektivnost korisničkih procjena, čime se postiže veća preciznost i vjerodostojnost. Samim time primjenom dodatne MCDM metode (neizraziti AHP) koja se sve više koristi u znanstvenim istraživanjima, novi hibridni višekriterijski model s generičkim ISRA kriterijima bi tako dobio i veći značaj na svojoj znanstvenoj vrijednosti.

6.5.5. Komunikacija

Završna procesna faza u metodologiji znanstvenog dizajna je predstavljanje novog artefakta i zaključaka. Prezentacija rješenja, tj. javna objava u obliku publikacije znanstvenog rada u časopisu i doktorske disertacije. Znanstveni radovi proizašli procesom istraživanja tijekom izrade ovog doktorskog rada su sljedeći:

- D. Maček, I. Magdalenić and N. Begičević Ređep, "A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information

Security Risk Assessment," *International Journal of Safety and Security Engineering*, vol. 10, no. 2, pp. 161-174, April 2020.
DOI: https://doi.org/10.18280/ijsse.100202

- D. Maček, I. Magdalenić and N. Begičević Ređep, "Towards a Hybrid Model for the Evaluation of Critical IT Systems," in *Quality of Software and Services: Central European Conference on Information and Intelligent Systems* (*CECIIS 2020*), Varaždin, Croatia, October 07-09, 2020, pp. 1-7.
https://ceciis.foi.hr/sites/default/files/ceciis2020/QSS/CECIIS-2020_paper_61.pdf
- D. Maček, I. Magdalenić and N. Begičević Ređep, "A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment," *Mathematics*, vol. 9, no. 9, p. 1045, May 2021. DOI: https://doi.org/10.3390/math9091045

6.5.6. Zaključak

Metode za višekriterijsko odlučivanje značajno se koriste u raznim istraživačkim poljima i disciplinama, a jedna od važnih primjena svakako je i domena informacijske sigurnosti. Dizajnom i razvojem novog višekriterijskoga modela s generičkim kriterijima za analizu i procjenu rizika te sustavnim pregledom literature (SLR) ostvaren je očekivani znanstveni doprinos. Odabirom novog višekriterijskoga modela s generičkim kriterijima, stručnjaci za informacijsku sigurnost i donosioci odluka ne moraju iznova trošiti resurse na istraživanje svojstvenih kriterija nužnih za evaluaciju sustava prilikom nabave nekog novog poslovnog IT rješenja ili sustava, već se mogu osloniti na novokreirani artefakt i iskoristiti definirane evaluacijske (generičke) kriterije za analizu i procjenu rizika te njihove pripadajuće (izračunate) težine. Također, primjenom novog višekriterijskoga modela smanjuje se i broj ponavljajućih zadataka (usporedbe u parovima prema određenim svojstvenim kriterijima) koje bi stručnjaci koji evaluiraju IT sustave trebali obavljati. Ponovna iskoristivost novokreiranog artefakta (u ovom slučaju višekriterijskoga modela) jedan je od glavnih kvalitativnih rezultata proizašlih iz istraživačkog procesa primjenom metodologije znanstvenog dizajna.

Novi hibridni višekriterijski model pokazao je kako je moguće izračunati težine generičkih kriterija te procijeniti i rangirati kritične poslovne IT sustave integrirajući pritom glavne elemente za analizu i procjenu rizika kao generičke evaluacijske kriterije u SNAP kao

sasvim novu metodu za višekriterijsko odlučivanje. Time je i sama SNAP metoda dobila na većoj relevantnosti u smislu adekvatne primjene iste.

Rezultati sa studije slučaja ukazuju na to kako je novi višekriterijski model podesan za kritične poslovne IT sustave u financijskom sektoru, dok bi za primjenu modela vezano uz sigurnosno-tehnološke sustave trebalo svakako provesti dodatna istraživanja.

Model je zamišljen tako da bude ujedno i modularan te po potrebi omogućava proširenje definiranih kriterija dodavanjem određenih faktora kao podkriterija kako bi se moguće dobili još precizniji rezultati o razini rizičnosti pojedinih IT sustava. Npr., kao što su faktori agenta prijetnje (razina vještine napadača, motiv, metoda, prilika), faktori ranjivosti (jednostavnost pronalaska, iskoristivost, otkrivanje upada) ili faktori utjecaja (gubitak povjerljivosti, cjelovitosti, dostupnosti, privatnosti, regulatorne usklađenosti, financija, reputacije). Stoga je planirano i daljnje unapređenje višekriterijskoga modela razvojem programske podrške u obliku web aplikacije kako bi modularnost bila transparentnija i jednostavnija za korištenje.

Literatura

[1] *2016 list of global systemically important banks (G-SIBs)*, Financial Stability Board, Nov 21, 2016. [Online]. Available: http://www.fsb.org/wp-content/uploads/2016-list-of-global-systemically-important-banks-G-SIBs.pdf/. [Accessed: 25-Feb-2017].

[2] *Other Systemically Important Institutions (O-SIIs)*, European Banking Authority, 2016. [Online]. Available: http://www.eba.europa.eu/risk-analysis-and-data/other-systemically-important-institutions-o-siis-/2016/. [Accessed: 25-Feb-2017].

[3] M. Adu-Gyamfi, "The Bankruptcy of Lehman Brothers: Causes, Effects and Lessons Learnt," *Journal of Insurance and Financial Management*, vol. 1, no. 4, pp. 132-149, 2016.

[4] A.R. Raghavan and L. Parthiban, "The effect of cybercrime on a Bank's finances," *International Journal of Current Research and Academic Review*, vol. 2, no. 2, pp. 173-178, Feb. 2014.

[5] R. Gandhi *et al*., "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28-38, March 2011. DOI: 10.1109/MTS.2011.940293

[6] C. Biancotti, "Cyber Attacks: Preliminary Evidence from the Bank of Italy's Business Surveys," *Bank of Italy Occasional Paper*, no. 373, Feb. 2017. [Online]. Available: https://www.bancaditalia.it/pubblicazioni/qef/2017-0373/index.html?com.dotmarketing.htmlpage.language=1. [Accessed: 23-Oct-2018].

[7] T. Maurer, A. Levite and G. Perkovich, "Toward a global norm against manipulating the integrity of financial data," *Economics, The Open-Access, Open-Assessment E-Journal*, no. 38, June 2017. [Online]. Available: http://www.economics-ejournal.org/economics/discussionpapers/2017-38/file/. [Accessed: 17-Jul-2017].

[8] J. Berr, "WannaCry ransomware attack losses could reach $4 billion," *CBS News*, May 16, 2017. [Online]. Available: http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/. [Accessed: 21-May-2017].

[9] O. Suess, "Next WannaCry Cyber Attack Could Cost Insurers $2.5 Billion," *Bloomberg*, July 7, 2017. [Online]. Available: https://www.bloomberg.com/news/articles/2017-07-06/the-next-wannacry-cyber-attack-could-cost-insurers-2-5-billion/. [Accessed: 10-Jul-2017].

[10] S. Kess *et al*., "The Equifax Data Breach," *The CPA Journal*, December 2017 issue. [Online]. Available: https://www.cpajournal.com/2017/12/15/equifax-data-breach/. [Accessed: 25-Feb-2018].

[11] *Meltdown and Spectre*, Vulnerabilities in modern computers leak passwords and sensitive data. [Online]. Available: https://meltdownattack.com/. [Accessed: 17-Apr-2019].

[12] H.F. Tipton and S. Hernandez, *Official (ISC)² Guide to the CISSP CBK*, Third Edition, (ISC)² Press, Auerbach Publications, New York, 2013.

[13] *Guide for Conducting Risk Assessments*, Information Security, NIST Special Publication 800-30, Revision 1, September 2012. [Online]. Available: https://www.nist.gov/privacy-framework/nist-sp-800-30.

[14] J.E. Mbowe *et al*., "A Conceptual Framework for Threat Assessment Based on Organization's Information Security Policy," *Journal of Information Security*, vol. 5, no. 4, pp. 166-177, Oct. 2014. DOI: 10.4236/jis.2014.54016

[15] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–78, 2007. https://doi.org/10.2753/MIS0742-1222240302

[16] V. Vaishnavi and B. Kuechler, "Design Science Research in Information Systems," *Design science research in information systems and technology*, Association for Information Systems, Atlanta, Georgia, USA. [Online]. Available: http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf/. [Accessed: 20-Feb-2017].

[17] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*, Elsevier Inc., Waltham, MA, USA, 2011.

[18] P. Sikavica *et al*., *Poslovno odlučivanje*, Školska knjiga, Zagreb, 2014.

[19] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *International Journal of Information Management*, vol. 28, no. 5, pp. 413-422, October 2008. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

[20] L.A. Gordon and M.P. Loeb, "Budgeting process for information security expenditures," *Communications of the ACM - Personal information management*, vol. 49, no. 1, pp. 121-125, January 2006. https://doi.org/10.1145/1107458.1107465

[21] S. Fenz *et al*., "Current challenges in information security risk management," *Information Management & Computer Security*, vol. 22, no. 5, pp. 410-430, 2014. https://doi.org/10.1108/IMCS-07-2013-0053

[22] K. Barker, "The gap between real and perceived security risks," *Computer Fraud & Security*, vol. 2014, no. 4, pp. 5-8, April 2014. https://doi.org/10.1016/S1361-3723(14)70478-6

[23] N. Pearson, "A larger problem: financial and reputational risks," *Computer Fraud & Security*, vol. 2014, no. 4, pp.11-13, April 2014. https://doi.org/10.1016/S1361-3723(14)70480-4

[24] P.I. Hoh *et al*., "A Security Risk Analysis Model for Information Systems," in *Proceedings of Lecture Notes in Computer Science*, New York, USA, Springer-Verlag Inc, pp. 505-513, 2005. https://doi.org/10.1016/j.ins.2013.02.036

[25] M.S. Merkow and J. Breithaupt, *Information Security: Principles and Practices*, 2nd Edition, Pearson IT Certification, June 2014.

[26] ISO/IEC 27001:2013, Information Technology, Security techniques, Information security management systems – requirements.

[27] P. Shamala, R. Ahmada and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45-52, Jul. 2013. https://doi.org/10.1016/j.jisa.2013.07.002

[28] ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management, 2018.

[29] IEC/FDIS 31010:2019, *Risk management – Risk assessment techniques*, 2019.

[30] Principles for the Sound Management of Operational Risk, Bank for International Settlements, June 2011.

[31] F. Fiordelisi, M.G. Soana and P. Schwizer, "Reputational losses and operational risk in banking," *The European Journal of Finance*, vol. 20, no. 2, pp. 105-124, 2014. https://doi.org/10.1080/1351847X.2012.684218

[32] Verizon's annual Data Breach Investigations Report (DBIR), "Verizon: Data Breach Investigations Report 2020," *Computer Fraud & Security*, vol. 2020, no. 6, page 4, June 2020. https://doi.org/10.1016/S1361-3723(20)30059-2

[33] Z. Krakar *et al*., *Korporativna informacijska sigurnost*, Zavod za informatičku djelatnost Hrvatske d.o.o., Zagreb, 2014.

[34] ISO Guide 73:2009, Risk management – Vocabulary, 2009.

[35] AS/NZS 4360:2004, *Risk Management*, Australian/New Zealand Standard.

[36] *Managing Information Security Risk*, Organization, Mission and Information System View, Information Security, NIST Special Publication 800-39, March 2011. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

[37] *Enterprise Risk Management – Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), September 2004.

[38] ISO 31000:2018, *Risk management – Guidelines*, Edition 2, Technical Committee: ISO/TC 262 Risk management, February 2018.

[39] *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2, October 2018. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[40] H. Simon, *The New Science of Management Decision*, New Jersey, USA, Prentice Hall, 1977.

[41] G.H. Tzeng and J.J. Huang, *Multiple Attribute Decision Making: Methods and Applications*, CRC Press: A Chapman & Hall Book, Boca Raton, FL, 2011.

[42] P. Bernstein, *Against the Gods: The Remarkable story of Risk*, John Wiley & Sons, New York, USA, 1996.

[43] D. Bernoulli, "Exposition of a New Theory on the Measurement of Risk," *Econometrica*, vol. 22, no. 1, pp. 23-36, January 1954. https://doi.org/10.2307/1909829

[44] J. von Neumann and O. Morgenstern, *Theory of games and economic behavior*, 2nd Edition, Princeton, New Jersey, Princeton University Press, 1947.

[45] D. Dubois and H. Prade, *Fuzzy Sets and Systems: Theory and Applications*, Mathematics in Science and Engineering, vol. 144, Academic Press, New York, November 1980.

[46] R. Farrell, "Securing the Cloud: Governance, Risk, and Compliance Issues Reign Supreme," *Information Security Journal: A Global Perspective*, vol. 19, no. 6, pp. 310-319, January 2010. https://doi.org/10.1080/19393555.2010.514655

[47] S. Drissi and H. Medromi, "A New Risk Assessment Approach for Cloud Consumer," *Journal of Communication and Computer*, vol. 11, pp. 52-58, January 2014. DOI:10.17265/1548-7709/2014.01 007

[48] N. Al-Safwani, Y. Fazea and H. Ibrahim, "ISCP: In-Depth Model for Selecting Critical Security Controls," *Computers & Security*, vol. 77, pp. 565-577, August 2018. https://doi.org/10.1016/j.cose.2018.05.009

[49] M.A. Mohyeddin and H. Gharaee, "FAHP-TOPSIS Risks Ranking Models in ISMS" in *7th International Symposium on Telecommunications* (IST), Tehran, Iran, September 09-11, 2014, pp. 879-881. DOI: 10.1109/ISTEL.2014.7000827

[50] C. Zopounidis and M. Doumpos, *Multiple Criteria Decision Making: Applications in Management and Engineering*, Springer International Publishing, Switzerland, 2017.

[51] D.J. Landoll, *The Security Risk Assessment Handbook*, A Complete Guide for Performing Security Risk Assessments, Boca Raton, FL, Auerbach Publications, 2006.

[52] S. Khandelwal, "How Did Hackers Who Stole $81 Million from Bangladesh Bank Go Undetected?," *The Hacker News*, April 25, 2016. [Online]. Available: https://thehackernews.com/2016/04/swift-bank-hack.html/. [Accessed: 23-May-2018].

[53] S. Harris, *CISSP All-in-One Exam Guide*, 6th Edition, McGraw-Hill Osborne Media, 2013.

[54] S. Payne, *A Guide to Security Metrics*, SANS Institute, Information Security Reading Room, June 2006.

[55] *Zakon o kritičnim infrastrukturama*, Narodne Novine, NN56/13, [Online]. Available: http://narodne-novine.nn.hr/clanci/sluzbeni/2013_05_56_1134.html. [Accessed: 14-Jan-2019].

[56] Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, Narodne Novine, NN 64/18, [Online]. Available: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_07_64_1305.html. [Accessed: 20-Sep-2018].

[57] S. Kurkovsky, *Software Engineering: Critical Systems*, Department of Computer Science, Central Connecticut State University, CS 530 classes, 2010.

[58] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired.com, 2018. [Online]. Available: https://www.wired.com/story/notpetyacyberattack-ukraine-russia-code-crashed-the-world/. [Accessed: 09-Oct-2020].

[59] S.T. March and G.F. Smith, "Design and natural science research on information technology," *Decision Support Systems*, vol. 15, no. 4, pp. 251-266, December 1995. https://doi.org/10.1016/0167-9236(94)00041-2

[60] A.R. Hevner *et al*., "Design Science in Information Systems Research," *MIS Quarterly*, Research Essay, vol. 28, no. 1, pp. 75-105, March 2004. DOI: 10.2307/25148625

[61] A.R. Hevner, "A Three Cycle View of Design Science Research," *Scandinavian Journal of Information Systems*, vol. 19, no. 2, pp. 87–92, 2007. https://aisel.aisnet.org/sjis/vol19/iss2/4

[62] R.L. Keeney and H. Raiffa, *Decision with multiple objectives: Preferences and value tradeoffs*, New York NY: John Wiley and Sons, 1976.

[63] *Inventory of risk assessment and risk management methods*, ENISA ad hoc working group on risk assessment and risk management, European Network and Information Security Agency (ENISA), March 2006. Available: https://www.enisa.europa.eu/publications/inventory-of-risk-assessment-and-risk-management-methods. [Accessed: 25-Jun-2018]

[64] *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, Technical Department of ENISA, Section Risk Management, European Network and Information Security Agency (ENISA), June 2006. Available: https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools. [Accessed: 24-Jun-2018].

[65] S. Fenz and A. Ekelhart, "Verification, Validation, and Evaluation in Information Security Risk Management," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 58-65, Mar-Apr 2011. DOI: 10.1109/MSP.2010.117

[66] R. Leszczyna and E. Egozcue, "ENISA Study: Challenges in Securing Industrial Control Systems," in *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection*, C. Laing, A. Badii and P. Vickers, Hershey PA: IGI Global, 2013, pp. 105-143.

[67] *Comparison of Risk Management Methods and Tools*, ENISA, European Union Agency for Cybersecurity. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/comparison/comparison.html/. [Accessed: 23-Jun-2018].

[68] A. Shameli-Sendi, R. Aghababaei-Barzegar and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14-30, March 2016. https://doi.org/10.1016/j.cose.2015.11.001

[69] L. Pan and A. Tomlinson, "A Systematic Review of Information Security Risk Assessment," *International Journal of Safety and Security Engineering*, vol. 6, no. 2, pp. 270-281, 2016. DOI: 10.2495/SAFE-V6-N2-270-281

[70] M. Alcántara and A. Melgar, "Risk Management in Information Security: A Systematic Review," *Journal of Advances in Information Technology*, vol. 7, no. 1, pp. 1-7, February 2016. DOI: 10.12720/jait.7.1.1-7

[71] J. Chai, J. N.K. Liu and E. W.T. Ngai, "Application of decision-making techniques in supplier selection: A systematic review of literature," *Expert Systems with Applications*, vol. 40, no. 10, pp. 3872-3885, August 2013. https://doi.org/10.1016/j.eswa.2012.12.040

[72] T. Hunjak, "Mathematical foundations of the methods for multicriterial decision making," *Mathematical Communications*, vol. 2, no. 2, pp. 161-169, December 1997. https://core.ac.uk/download/pdf/14376401.pdf

[73] B. Kitchenham and S. Charters, *Guidelines for performing Systematic Literature Reviews in Software Engineering*, Keele University and Durham University Joint Report, EBSE Technical Report, July 2007. Available: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

[74] A.K. Sangaiah *et al.*, "Towards an efficient risk assessment in software projects–Fuzzy reinforcement paradigm," *Computers & Electrical Engineering*, vol. 71, pp. 833-846, October 2018. https://doi.org/10.1016/j.compeleceng.2017.07.022

[75] A. Rodríguez, F. Ortega and R. Concepción, "An intuitionistic method for the selection of a risk management approach to information technology projects," *Information Sciences*, vol. 375, pp. 202-218, January 2017. https://doi.org/10.1016/j.ins.2016.09.053

[76] T.Yu. Chernysheva *et al.*, "Information Systems Project Risk Assessment: Expert Approach," *Applied Mechanics and Materials*, vol. 682, pp. 539-543, October 2014. https://doi.org/10.4028/www.scientific.net/AMM.682.539

[77] M.A. Mohyeddin and H. Gharaee, "FAHP-TOPSIS Risks Ranking Models in ISMS," in *7th International Symposium on Telecommunications, IST'2014*, Tehran, Iran, September 9-11, 2014, pp. 879-881. DOI: 10.1109/ISTEL.2014.7000827

[78] C-C. Lo and W-J. Chen, "A hybrid information security risk assessment procedure considering interdependences between controls," *Expert Systems with Applications*, vol. 39, no. 1, pp. 247-257, January 2012. https://doi.org/10.1016/j.eswa.2011.07.015

[79] K. Zhang and L. Shao, "Research on the Quantitative Methods of Classified Information System Security Risk Assessment," in *International Conference on Logistics, Informatics and Service Science* (*LISS*), Beijing, China, July 23-26, 2014, pp. 571-575. https://doi.org/10.1007/978-3-662-43871-8_82

[80] M.C. Lee, "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method," *International Journal of Computer Science & Information Technology* (*IJCSIT*), vol. 1, no. 1, pp. 29-45, February 2014. http://airccse.org/journal/jcsit/6114ijcsit03.pdf

[81] W. Tianshui and Z. Gang, "A New Security and Privacy Risk Assessment Model for Information System Considering Influence Relation of Risk Elements," in *International Conference on Broadband and Wireless Computing, Communication and Applications* (*BECCA*), Guangzhou, China, November 08-10, 2014, pp. 233-238. DOI: 10.1109/BWCCA.2014.76

[82] Q. Yu and Y.J. Shen, "Research of Information Security Risk Prediction based on Grey Theory and ANP," in *IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference* (*IMCEC*), Xian, China, October 03-05, 2016, pp. 107-113. DOI: 10.1109/IMCEC.2016.7867182

[83] N.B. Anuar *et al.*, "Incident prioritisation using analytic hierarchy process (AHP): Risk Index Model (RIM)," *Security and Communication Networks*, vol. 6, no. 9, pp. 1087-1116, September 2013. https://doi.org/10.1002/sec.673

[84] Hiete *et al.*, "Trapezoidal fuzzy DEMATEL method to analyze and correct for relations between variables in a composite indicator for disaster resilience," *OR Spectrum*, vol. 34, no. 4, pp. 971-995, October 2012. https://doi.org/10.1007/s00291-011-0269-9

[85] K-Y. Kim and K-S. Na, "Business information system recovery priority decision using TOPSIS on interval data," *Journal of Systems and Information Technology*, vol. 16, no. 2, pp. 103-112, May 2014. https://doi.org/10.1108/JSIT-12-2013-0068

[86] H.Y. Tsai and Y.L. Huang, "An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks," *IEEE Transactions on Reliability*, vol. 60, no. 4, pp. 801-816, December 2011. DOI: 10.1109/TR.2011.2170117

[87] Y.L. Huang and W.L. Sun, "An AHP-based Risk Assessment for an Industrial IoT Cloud," in *18th IEEE International Conference on Software Quality, Reliability and Security Companion* (*QRS-C*), Lisbon, Portugal, July 16-20, 2018, pp. 637-638. DOI: 10.1109/QRS-C.2018.00112

[88] H.J. Kim, "Online Social Media Networking and Assessing Its Security Risks," *International Journal of Security and Its Applications*, vol. 6, no. 3, pp. 11-18, July 2012.

[89] *Security and Privacy Controls for Information Systems and Organizations* (*Final Public Draft*), NIST Special Publication 800-53, Revision 5, Joint Task Force, National Institute of Standards and Technology, March 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5-draft

[90] N. Al-Safwani, S. Hassan and N. Katuk, "A Multiple Attribute Decision Making for Improving Information Security Control Assessment," *International Journal of Computer Applications*, vol. 89, no. 3, pp. 19-24, March 2014. DOI: 10.5120/15482-4222

[91] N. Al-Safwani, Y. Fazea and H. Ibrahim, "ISCP: In-Depth Model for Selecting Critical Security Controls," *Computers & Security*, vol. 77, pp. 565-577, August 2018. https://doi.org/10.1016/j.cose.2018.05.009

[92] Y.P. Yang, H.M. Shieh and G.H. Tzeng, "A VIKOR technique based on DEMATEL and ANP for information security risk control assessment," *Information Sciences*, vol. 232, pp.482-500, May 2013. https://doi.org/10.1016/j.ins.2011.09.012

[93] M. Meng, "The research and application of the risk evaluation and management of information security based on AHP method and PDCA method," in *International Conference on Information Management, Innovation Management and Industrial Engineering*, Xi'an, China, 23-24 November, 2013, pp. 379-383. DOI: 10.1109/ICIII.2013.6703597

[94] M. Moeti and B.M. Kalema, "Analytical Hierarchy Process Approach for the Metrics of Information Security Management Framework," in *International Conference on Computational Intelligence, Communication Systems and Networks*, Tetovo, Macedonia, 27-29 May, 2014, pp. 89-94. DOI: 10.1109/CICSyN.2014.31

[95] M. Li and M. Bardi, "A risk assessment method of cloud computing based on multi-level fuzzy comprehensive evaluation," in *International Conference on Cyberspace Technology* (*CCT 2014*), Beijing, China, 8-10 November, 2014, pp. 1-4. DOI: 10.1049/cp.2014.1377

[96] Z. Ruo-xin *et al.*, "Model for cloud computing security assessment based on AHP and FCE," in *9th International Conference on Computer Science & Education*, Vancouver, BC, Canada, 22-24 August, 2014, pp. 197-202. DOI: 10.1109/ICCSE.2014.6926454

[97] C.K. Fan and T.C. Chen, "The Risk Management Strategy of Applying Cloud Computing," *International Journal of Advanced Computer Science and Applications* (*IJACSA*), vol. 3, no. 9, pp. 18-27, 2012. DOI: 10.14569/IJACSA.2012.030903

[98] R. Alguliyev and F. Abdullayeva, "Development of risk factor management method for federation of clouds," in *International Conference on Connected Vehicles and Expo* (*ICCVE*), Vienna, Austria, 3-7 November, 2014, pp. 24-29. DOI: 10.1109/ICCVE.2014.7297548

[99] C. Su *et al.*, "Information Network Risk Assessment Based on AHP and Neural Network," in *10th International Conference on Communication Software and Networks* (*ICCSN*), Chengdu, China, 6-9 July, 2018, pp. 227-231. DOI: 10.1109/ICCSN.2018.8488314

[100] F. Farzan *et al.*, "Cyber-related risk assessment and critical asset identification in power grids," in *IEEE PES Innovative Smart Grid Technologies Conference* (*ISGT*), Washington, DC, USA, 19-22 February, 2014, pp. 1-5. DOI: 10.1109/ISGT.2014.6816371

[101] Y. Ru *et al.*, "Risk Assessment of Cyber Attacks in ECPS Based on Attack Tree and AHP," in *International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery* (*ICNC-FSKD*), Changsha, China, 13-15 August, 2016, pp. 465-470. DOI: 10.1109/FSKD.2016.7603218

[102] Z.F. Eren-Dogu and C.C. Celikoglu, "Information security risk assessment Bayesian prioritization for AHP group decision making," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 11, pp. 8019-8032, November 2012. http://www.ijicic.org/ijicic-ksi-12.pdf

[103] Z. Tan and P. Li, "Group Decision-Making Information Security Risk Assessment Based on AHP and Information Entropy," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 4, no. 15, pp. 2361-2366, August 2012. https://maxwellsci.com/print/rjaset/v4-2361-2366.pdf

[104] T. Wu and G. Zhao, "A Novel Risk Assessment Model for Privacy Security in Internet of Things," *Wuhan University Journal of Natural Sciences*, vol. 19, no. 5, pp. 398-404, October 2014. https://doi.org/10.1007/s11859-014-1031-3

[105] H. Grushka *et al.*, "CyberRank-Knowledge Elicitation for Risk Assessment of Database Security," in *Proceedings of the 25th ACM International Conference on Information and Knowledge Management* (*CIKM 2016*), Indianapolis, Indiana, USA, October 24-28, 2016, pp. 2009-2012. https://doi.org/10.1145/2983323.2983896

[106] D. Maček, I. Magdalenić and N. Ivković, "Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard," in *Information Systems Security: Central European Conference on Information and Intelligent Systems* (*CECIIS 2012*), Varaždin, Croatia, 19-21 September, 2012, pp. 305-311. Available: http://archive.ceciis.foi.hr/app/public/conferences/1/papers2012/iss2.pdf

[107] D. Maček and D. Alagić, "Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique," *Journal of Information and Organizational Sciences*, vol. 41, no. 1, pp. 69-87, June 2017. DOI: https://doi.org/10.31341/jios.41.1.5

[108] *OWASP Top 10 Web Application Security Risks*, 2017. [Online]. Available: https://owasp.org/www-project-top-ten/. [Accessed: 09-Nov-2020].

[109] T.L. Saaty, "Decision making with the analytic hierarchy process," *International Journal of Services Sciences*, vol. 1, no. 1, pp.83–98, 2008. DOI: 10.1504/IJSSCI.2008.017590

[110] T.L. Saaty, "Fundamentals of the Analytic Hierarchy Process," in *The Analytic Hierarchy Process in Natural Resource and Environmental Decision Making*, RWS Publications, Pittsburgh, PA, 2006, pp. 15-35.

[111] T.L. Saaty, "The Analytic Hierarchy and Analytic Network Measurement Processes: Applications to Decisions under Risk," *European Journal of Pure and Applied Mathematics*, vol. 1, no. 1, pp. 122-196, 2008. Available: https://www.ejpam.com/index.php/ejpam/article/view/6

[112] C.C. Hsu and B.A. Sandford, "The Delphi Technique: Making Sense of Consensus," *Practical Assessment, Research & Evaluation*, vol. 12, no. 10, pp. 1-8, August 2007. DOI: https://doi.org/10.7275/pdz9-th90

[113] T.L. Saaty, *Decision Making with Dependence and Feedback: The Analytic Network Process*, 2nd Edition. RWS Publications, Pittsburgh, PA, 2001.

[114] N. Menold and K. Bogner, *Design of Rating Scales in Questionnaires, GESIS Survey Guidelines*, Version 2.0, GESIS – Leibniz-Institut für Solzialwissenschaften, Mannheim, Germany, December 2016. DOI: 10.15465/gesis-sg_en_015

[115] L. Giannarou and E. Zervas, "Using Delphi technique to build consensus in practice," *International Journal of Business Science and Applied Management*, vol. 9, no. 2, pp. 65-82, 2014. https://business-and-management.org/library/2014/9_2--65-82-Giannarou,Zervas.pdf

[116] A. Gabus and E. Fontela, "World Problems, An Invitation to Further Thought within The Framework of DEMATEL," *Battelle Geneva Research Centre*, Geneva, Switzerland, 1972.

[117] S-L. Si *et al.*, "DEMATEL Technique: A Systematic Review of the State-of-the-Art Literature on Methodologies and Applications," *Mathematical Problems in Engineering*, vol. 2018, January 2018. https://doi.org/10.1155/2018/3696457

[118] J. Michnik, "Weighted Influence Non-linear Gauge System (WINGS) – An analysis method for the systems of interrelated components," *European Journal of Operational Research*, vol. 228, no. 3, pp. 536-544, August 2013. https://doi.org/10.1016/j.ejor.2013.02.007

[119] N. Kadoić, B. Divjak and N. Begičević Ređep, "Integrating the DEMATEL with the analytic network process for effective decision-making," *Central European Journal of Operations Research*, vol. 27, no. 3, pp. 653-678, September 2019. https://doi.org/10.1007/s10100-018-0601-4

[120] *OWASP Risk Rating Methodology*, Category: OWASP Testing Project, 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology. [Accessed: 19-Sep-2019].

[121] N. Kadoić, N. Begičević Ređep and B. Divjak, "A new method for strategic decision-making in higher education," *Central European Journal of Operations Research*, vol. 26, no. 3, pp. 611-628, September 2018. https://doi.org/10.1007/s10100-017-0497-4

[122] D. Horvat i D. Munđar, "Rangiranje web stranica," *Osječki matematički list*, vol. 17, no. 1, pp. 51-62, 2017, Available: https://hrcak.srce.hr/186508.

[123] N. Kadoić, "A new method for analysis of complex decision making problems based on the analytic network process and the social network analysis," Ph.D. dissertation, Faculty of Organization and Informatics Varaždin, University of Zagreb, 2018. Available: https://repozitorij.foi.unizg.hr/islandora/object/foi:3569

[124] *Threat modeling for drivers, Driver Security Guidance*, Microsoft Dev Center, Dec 5, 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers/. [Accessed: 02-Sep-2019].

[125] S. Brin and L. Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," in *7th International World-Wide Web Conference* (*WWW 1998*), Brisbane, Australia, 14-18 April, 1998. Available: http://infolab.stanford.edu/~backrub/google.html. [Accessed: 20-Sep-2019].

[126] E. Yazgan and A. Korkut Üstün, "Application of Analytic Network Process: Weighting of Selection Criteria for Civil Pilots," *Journal of Aeronautics and Space Technologies*, vol. 5, no. 2, pp. 1-12, July 2011. http://www.jast.hho.edu.tr/index.php/JAST/article/view/259

[127] T.L. Saaty, "Applications of Analytic Network Process in Entertainment," *Iranian Journal of Operations Research*, vol. 1, no. 2, pp. 41-55, 2009. http://iors.ir/journal/article-1-63-en.pdf

[128] B. Roy, *Multicriteria Methodology for Decision Aiding* (*Nonconvex Optimization and Its Applications*), Dordrecht, The Netherlands, Kluwer Academic Publishers, 1996.

[129] J. Wątróbski *et al.*, "Generalised framework for multi-criteria method selection," *Omega*, vol. 86, pp. 107-124, July 2019. https://doi.org/10.1016/j.omega.2018.07.004

[130] C. Salinesi and E. Kornyshova, "Choosing a Prioritization Method – Case of IS Security Improvement," in *The 18th Conference on Advanced Information Systems Engineering* (*CAiSE '06*), *Forum Proceedings, Theme: Trusted Information Systems*, Luxembourg, June 5-9, 2006.

[131] A. Ishizaka and Nemery, *Multi-criteria Decision Analysis: Methods and Software*, 1st edition, John Wiley & Sons Ltd, West Sussex, UK, 2013.

[132] E. Kornyshova and C. Salinesi, "MCDM Techniques Selection Approaches: State of the Art," in *Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Multicriteria Decision Making* (MCDM 2007), Honolulu, HI, USA, April 01-05, 2007, pp. 22-29. DOI: 10.1109/MCDM.2007.369412

[133] Y. Li and M.A., "A Multiple Criteria Decision Analysis (MCDA) software selection framework," in *Proceeding of the 47th Hawaii International Conference on System Sciences* (HICSS), Waikoloa, Hawaii, USA, January 06-09, 2014, pp. 1084–1094. DOI: 10.1109/HICSS.2014.141

[134] ISACA, *Certified in Risk and Information Systems Control*, CRISC, Review Manual, 6th Edition, Schaumburg, IL, US, 2015.

[135] C. Shao and W. Yang, "Fuzzy AHP Decision Making Method for Insert Grade Selection," in *Proceedings of the 2010 IEEE International Conference on Information and Automation* (ICIA), Harbin, China, June 20-23, 2010, pp. 2415-2418. DOI: 10.1109/ICINFA.2010.5512283

[136] M.S. Dwi Putra *et al.*, "Fuzzy Analytical Hierarchy Process Method to Determine the Quality of Gemstones," *Advances in Fuzzy Systems*, vol. 2018, Special Issue. DOI: https://doi.org/10.1155/2018/9094380

[137] L.A. Zadeh, "Fuzzy Sets," *Information Control*, vol. 8, no. 3, pp. 338–353, June 1965. DOI: https://doi.org/10.1016/S0019-9958(65)90241-X

[138] M.I. Tariq *et al.*, "Prioritization of Information Security Controls Through Fuzzy AHP for Cloud Computing Networks and Wireless Sensor Networks," *Sensors*, vol. 20, no. 5, pp. 1-39, February 2020. DOI: https://doi.org/10.3390/s20051310

[139] Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance: Discussion about the Meaning, Scope, and Goals," in *Organizational, Legal, and Technological Dimensions of Information System Administration* (Chapter 10), IGI Global, 2014. DOI: 10.4018/978-1-4666-4526-4.ch010

[140] W. Stallings, *Operating Systems: Internals and Design Principles*, 8th Edition, Pearson Education, Prentice Hall, New Jersey, US, 2014.

[141] Z. Stapić *et al.*, "Scrutinizing systematic literature review process in software engineering," *TEM Journal*, vol. 5, no. 1, pp. 104-116, February 2016. DOI: 10.18421/TEM51-16

[142] D. Maček, I. Magdalenić and N. Begičević Ređep, "A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment," *International Journal of Safety and Security Engineering*, vol. 10, no. 2, pp. 161-174, April 2020. DOI: https://doi.org/10.18280/ijsse.100202

[143] *Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication*, Official Journal of the European Union. [Online]. Available: https://eur-lex.europa.eu/eli/reg_del/2018/389/oj. [Accessed: 10-Sep-2020].

[144] N. Begičević, "Multicriteria decision making models for stategic planning of e-learning implementation," Ph.D. disseration, Faculty of Organization and Informatics Varaždin, University of Zagreb, 2008. Available: https://repozitorij.foi.unizg.hr/islandora/object/foi:367

[145] NIST *National Vulnerability Database* (NVD), Information Technology Laboratory. [Online]. Available: https://nvd.nist.gov/vuln/full-listing. [Accessed: 20-Nov-2020].

[146] Exploit Database. [Online]. Available: https://www.exploit-db.com/. [Accessed: 20-Nov-2020].

[147] NetMarketShare, Market Share Statistics for Internet Technologies. [Online]. Available: https://netmarketshare.com/. [Accessed: 20-11-2020].

[148] C. Lagarde, "Estimating Cyber Risk for the Financial Sector," *IMFBlog, Insights & Analysis on Economics & Finance*, 2018. [Online]. Available: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector. [Accessed: 23-11-2020].

[149] H. Singh Lallie *et al*., "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *arXivLabs: experimental projects with community collaborators*, Cornell University, 2020. Available: https://arxiv.org/abs/2006.11929

[150] S. Hakak *et al.*, " Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," *IEEE Access*, *8*, 124134-124144, June 2020. DOI: 10.1109/ACCESS.2020.3006172

[151] N.F. Mahad *et al.*, "The application of fuzzy analytic hierarchy process (FAHP) approach to solve multi-criteria decision making (MCDM) problems," *Journal of Physics:Conference Series*, vol. 1358, *12th Seminar on Science and Technology*, 2–3 October, 2018, Kota Kinabalu, Sabah, Malaysia. https://iopscience.iop.org/article/10.1088/1742-6596/1358/1/012081/pdf

[152] A.J. Onwuegbuzie and R.B. Johnson, "The Validity Issue in Mixed Research," *Research in the Schools*, vol. 13, no. 1, pp. 48-63, Spring 2006.

[153] J. Venable, J. Pries-Heje and R. Baskerville, "FEDS: a Framework for Evaluation in Design Science Research," *European Journal of Information Systems*, vol. 25, no. 1, pp. 77-89, 2016. DOI: 10.1057/ejis.2014.36

[154] M.K. Sein *et al.*, "Action Design Research," *MIS Quarterly*, vol. 35, no. 1, pp. 37-56, March 2011. https://doi.org/10.2307/23043488

[155] News, "Bangladesh bank raiders manipulated Swift software," *Computer Fraud & Security*, vol. 2016, no. 5, page 3, May 2016. https://doi.org/10.1016/S1361-3723(16)30042-2

[156] Cyber-Security vs. Information Security. [Online]. Available: https://medium.com/thirty-degrees/cyber-security-vs-information-security-575ba3762f62. [Accessed: 28-Nov-2019].

[157] SWIFT Customer Security Controls Framework. [Online]. Available: https://www.swift.com/myswift/customer-security-programme-csp/security-controls#:~:text=The%20mandatory%20security%20controls%20establish,security%20gains%20and%20risk%20reduction. [Accessed: 16-Dec-2020].

[158] ISO/IEC 25010:2011, *Systems and software engineering* – Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models.

[159] A. Abran and R.E. Al-Qutaish, "ISO 9126: Analysis of Quality Models and Measures," *Software metrics and software metrology*, IEEE Computer Society, Wiley, 2010.

[160] ISO 25000 software and data quality, ISO 25000 Portal. [Online]. Available: https://iso25000.com/index.php/en/. [Accessed: 20-Apr-2020].

[161] M. Žugaj, K. Dumičić and V. Dušak, *Temelji znanstvenoistraživačkog rada: metodologija i metodika*, Fakultet organizacije i informatike, Varaždin, 2006.

[162] T.L. Saaty, *Multicriteria Decision Making: The Analytic Hierarchy Process*, RWS Publications, 4922 Ellsworth Avenue, Pittsburgh, PA 15213, 1980.

[163] N. Begičević Redep, "Multicriteria decision making models for stategic planning of e-learning implementation," Ph.D. dissertation, Faculty of Organization and Informatics Varaždin, University of Zagreb, 2008. Available: https://repozitorij.unizg.hr/islandora/object/foi:367

[164] T.L. Saaty and L.G. Varga, *Decision Making with the Analytic Network Process*, Economic, Political, Social and Technological Applications with Benefits, Opportunities, Costs and Risks, Springer US, 2006. Available: https://www.springer.com/gp/book/9781441941541

[165] T.L. Saaty, *Theory and Applications of the Analytic Network Process: Decision Making with Benefits, Opportunities, Costs, and Risks*, RWS Publications, Pittsburgh, 2005.

Prilog A: Upitnik za prvi krug Delphi metode

U nastavku se nalazi upitnik za prvi krug *Delphi* metode koji je u travnju 2019. poslan elektroničkom poštom stručnjacima za informacijsku sigurnost iz različitih financijskih institucija i FinTech tvrtki u više europskih zemalja. Upitnik (Excel dokument) je izaslan na engleskom jeziku pa se takav i prilaže u izvornom obliku.

No.	Research question	Answer (mandatory)	Your explanation of the answer (optional)	Moderator's explanations
1	Do you consider **Threat** (**T**) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Threat** represents the probability of an event in which an attacker will make some damage to a particular business system. The analysis of threats is the first step that needs to be done in the process of risk assessment. Some of the most important threats in financial institutions are unauthorized access, malicious programs like viruses and worms, channel interception, data disclosure, denial of services that must be available 24x7 (e.g. online and mobile banking, e-commerce), etc.
2	Do you consider **Vulnerability** (**V**) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Vulnerability** is a characteristic of an IT asset or business process to indicate its weakness to some kind of attack. Vulnerability is linked to a **threat** that exploits it.
3	Do you consider **Probability** (**P**) (or **Likelihood**) as a critical risk element necessary for evaluation of IT and IT security solutions?			According to **OWASP Risk Rating Methodology**, factors to assess the **Likelihood** are the following: 1. Threat agent factors: Skill level Participant Motive Method Opportunity Size Frequency of attack 2. Vulnerability factors: Ease of discovery Ease of exploit Awareness Intrusion detection
4	Do you consider **Consequence** (**C**) (or Impact) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Consequence** represents a loss of economic, symbolic or psychological value for organization (i.e. reputational risk for the bank in case of loss or theft of data, unavailability of certain parts of information systems, reduced levels of service quality, etc.). According to **OWASP Risk Rating Methodology**, factors to assess the level of **Impact** are the following: 1. For technical impact: Loss of confidentiality Loss of integrity Loss of availability Loss of accountability 2. For business impact: Financial damage Reputation damage Non-compliance Privacy violation
5	Do you consider **Resiliency** (**R**) as a critical risk element necessary for evaluation of IT and IT security solutions?			The element is considered to evaluate how much and whether the IT solution is resilient regarding the other risk elements (**T**, **V**, **P**, **C**) that make influence on **Resiliency**. **Resilience** or **elasticity** is the speed with which the organization can successfully recover, reorganize itself and prepare to resume operations after a significant violation or failover of prescribed security policies. For the purpose of this research, resiliency attirbute is considered to be used for the evaluation of IT solutions.
6	Do you consider any other critical risk element that should be included in the set of criteria for evaluation of IT and IT security solutions (**Yes**/**No**)?			If **Yes**, then the detailed rationale for additional risk element is **mandatory**. Feel free to write your suggestions.

Skala mogućih odgovora (eng. *Answers*) na postavljena pitanja:

1 - Strongly disagreed
2 - Disagreed
3 - Neutral
4 - Agreed
5 - Strongly agreed

Skup individualnih pitanja:

Set of individual questions: **With these questions, the intention is to get more valuable info that makes You fully competent for giving necessary judgements related to Risk management topic in the research.**		Answer (mandatory)	Your explanation of the answer (optional)	Moderator's explanations
1	Please indicate your education degree.	Bacc. Ing. Mag. PhD Other		In case Your answer is **Other**, feel free to write some comments.
2	Please indicate all professional **certificates** you hold related to **information security**.			E.g., CISSP, CISM, CEH, Security+, OSCP, GIAC, CRISC, etc. Feel free to write all.
3	Please indicate the **number** of years of Your **work experience** in the field of **IT** and **Information Security**.			The number of years of Your experience in **IT** and **IT Security area** is required, not your overall work experience in other non-IT areas.
4	Do You hold managerial position in your organization at the moment?			E.g., CSO, CISO, CIO, BCM, Head of antifraud, etc.

Prilog B: Upitnik za drugi krug Delphi metode

U nastavku se nalazi upitnik za drugi krug *Delphi* metode koji je u srpnju 2019. poslan elektroničkom poštom stručnjacima za informacijsku sigurnost iz različitih financijskih institucija i FinTech tvrtki u više europskih zemalja. Upitnik (Excel dokument) je izaslan na engleskom jeziku istim sudionicima koji su odgovorili na upitnik iz prvog kruga istraživanja *Delphi* metodom.

No.	Research question	Answer (mandatory)	Your explanation of the answer (optional, not necessary)	Moderator's explanations	Results of the first phase (just for Your orientation)			
					Mode		Arithmetic mean (average)	Standard deviation (SD)
					Value	Frequency		
1	Do you consider **Threat** (**T**) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Threat** represents the probability of an event in which an attacker will make some damage to a particular business system. The analysis of threats is the first step that needs to be done in the process of risk assessment. Some of the most important threats in financial institutions are unauthorized access, malicious programs like viruses and worms, channel interception, data disclosure, denial of services that must be available 24x7 (e.g. online and mobile banking, e-commerce), etc.	5 - Strongly agreed	24 (out of 38)	4,55	0,6857
2	Do you consider **Vulnerability** (**V**) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Vulnerability** is a characteristic of an IT asset or business process to indicate its weakness to some kind of attack. Vulnerability is linked to a **threat** that exploits it.	5 - Strongly agreed	23 (out of 38)	4,53	0,6872
3	Do you consider **Probability** (**P**) (or **Likelihood**) as a critical risk element necessary for evaluation of IT and IT security solutions?			According to **OWASP Risk Rating Methodology**, factors to assess the **Likelihood** are the following: 1. Threat agent factors: Skill level Participant Motive Method Opportunity Size Frequency of attack 2. Vulnerability factors: Ease of discovery Ease of exploitation Awareness Intrusion detection	5 - Strongly agreed	21 (out of 38)	4,34	0,8785
4	Do you consider **Consequence** (**C**) (or Impact) as a critical risk element necessary for evaluation of IT and IT security solutions?			**Consequence** represents a loss of economic, symbolic or psychological value for organization (i.e. reputational risk for the bank in case of loss or theft of data, unavailability of certain parts of information systems, reduced levels of service quality, etc.). According to **OWASP Risk Rating Methodology**, factors to assess the level of **Impact** are the following: 1. For technical impact: Loss of confidentiality Loss of integrity Loss of availability Loss of accountability 2. For business impact: Financial damage Reputation damage Non-compliance Privacy violation	5 - Strongly agreed	25 (out of 38)	4,63	0,5413
5	Do you consider **Resiliency** (**R**) as a critical risk element necessary for evaluation of IT and IT security solutions?			The element is considered to evaluate how much and whether the IT solution is resilient regarding the other risk elements (**T**, **V**, **P**, **C**) that make influence on **Resiliency**. **Resilience** or **elasticity** is the speed with which the organization can successfully recover, reorganize itself and prepare to resume operations after a significant violation or failover of prescribed security policies. For the purpose of this research, resiliency attirbute is considered to be used for the evaluation of IT solutions.	5 - Strongly agreed	16 (out of 38)	4,13	0,9056
6	Do you consider **Ease of Exploit** (**E**) as a critical risk element necessary for evaluation of IT and IT security solutions?			Ease of Exploit (**E**) or **Exploitability** is a parameter that describes the level of expertise, knowledge, advanced training, special tools and equipment and time needed by an attacker in order to successfully carry out an attack on an information system.	N/A	N/A	N/A	N/A

Skala mogućih odgovora (eng. *Answers*) na postavljena pitanja je ista kao i u prvom krugu Delphi metode (1-5).

Prilog C: Tablice za procjenu važnosti generičkih kriterija u odnosu na cilj odlučivanja primjenom AHP metode

CT1	Resiliency	Risk
Resiliency	1	
Risk		1

Resiliency	0,5
Risk	0,5

Saaty's scale		Reciprocal values
1	equal importance	1
3	weak dominance	1/3 (0,3333)
5	strong dominance	1/5 (0,2)
7	proven dominance	1/7 (0,1429)
9	absolute dominance	1/9 (0,1111)
all real numbers can be used between 1 and 9, including 2, 4, 6, 8		1/2, 1/4, 1/6, 1/8

In first Comparison Table **(CT1)** which criterion (cluster) is more important, Resiliency or Risk, in protecting the value of IT assets, and how much on the Saaty scale? Put value from the scale in the table in the row of stronger element. On other empty place put reciprocal value of the previous Saaty's value used. On diagonal, there are 1, because here, same elements are compared, and when something is the same (equal), we use 1 on Saaty scale.

Example: If **Risk** cluster is 2 times more important when compared to Resiliency, then CT1 would look like:

CT1 example	Resiliency	Risk
Resiliency	1	0,5
Risk	2	1

CT2	p	t	v	c
p	1			
t		1		
v			1	
c				1

CR*	-1,1235955

* should be less than 0.1

Please compare criteria **p**, **t**, **v** and **c** in pairs in **CT2** with respect to **Risk** cluster. Domination-relationships between any two criteria will appear twice in the table: put the Saaty value in the row of the criterion that dominates over another, and its reciprocal value on the other position. **Transitivity** rule must be satisfied: if **v** dominates over **t**, and **t** dominates over **p**, then **v** dominates over **p**. When transitivity concept is broken, **CR** (Consistency Ratio) value increases. When you finish comparison procedure, **CR** should be less than 0.1 to accept your input. If it is higher, please make some comparisons once again.
Hint: It's necessary to look how each element from the row is important when compared with risk element from the column, e.g. when compared v->t then the value could be 4, and the reciprocal t->v must be 0,25.

CT2 example	Probability	Threat	Vulnerability	Consequence
Probability	1	0,333333	0,2	0,166666667
Threat	3	1	0,25	0,2
Vulnerability	5	4	1	0,5
Consequence	6	5	2	1

Prilog D: SNAP11 postupak za generičke ISRA kriterije

U ovom prilogu daje se postupak za računanje težina generičkih ISRA kriterija, počevši od agregacije prikupljenih prosudbi vezano uz utjecaje i zavisnosti između elemenata.

Aggregation (Z matrix)	Threat (T)	Vulnerability (V)	Probability (P)	Consequence (C)	Resiliency (R)
Threat (T)	0	2,4348	2,4783	2,6522	1,6522
Vulnerability (V)	3,0000	0	3,0435	2,6087	2,3478
Probability (P)	2,3043	1,6957	0	1,7391	1,5652
Consequence (C)	2,0435	1,6957	1,6522	0	2,3913
Resiliency (R)	1,9565	1,9565	1,6522	2,9565	0
Calculation of column sums and identification of max column sum	9,3043	7,7826	8,8261	**9,9565**	7,9565
				0,0913	

max column sum

S matrix					
	0	0,2222	0,2262	0,2421	0,1508
	0,2738	0	0,2778	0,2381	0,2143
	0,2103	0,1548	0	0,1587	0,1429
	0,1865	0,1548	0,1508	0	0,2183
	0,1786	0,1786	0,1508	0,2698	0

E matrix (n=5)					
	0,2	0,2	0,2	0,2	0,2
	0,2	0,2	0,2	0,2	0,2
	0,2	0,2	0,2	0,2	0,2
	0,2	0,2	0,2	0,2	0,2
	0,2	0,2	0,2	0,2	0,2

G matrix					
	0,03	0,2189	0,2223	0,2358	0,1582
	0,2627	0,03	0,2661	0,232380952	0,2121
	0,2088	0,1615	0,03	0,1649	0,1514
	0,1885	0,161547619	0,158174603	0,03	0,2155
	0,1818	0,1818	0,158174603	0,2594	0,03

I-G					
	1	-0,2189	-0,2223	-0,2358	-0,1582
	-0,2627	1	-0,2661	-0,2324	-0,2121
	-0,2088	-0,1615	1	-0,1649	-0,1514
	-0,1885	-0,1615	-0,1582	1	-0,2155
	-0,1818	-0,1818	-0,1582	-0,2594	1

inverse (I-G)					
	1,7076	0,8042	0,8631	0,9321	0,7723
	1,0106	1,7086	0,9833	1,0291	0,8930
	0,7732	0,6708	1,5785	0,7723	0,6701
	0,7842	0,6938	0,7387	1,6601	0,7409
	0,8198	0,7429	0,7769	0,9092	1,6009

G * inverse	Threat (T)	Vulnerability (V)	Probability (P)	Consequence (C)	Resiliency (R)	r	c	r-c	N1	SNAP12	AHP	SNAP11
Threat (T)	0,7588	0,8283	0,8890	0,9601	0,7955	4,2317	4,2483	-0,0166	1,7235	0,198096379	0,105824012	0,151960196
Vulnerability (V)	1,0409	0,7599	1,0128	1,0600	0,9198	4,7934	3,7590	1,0344	2,7744	0,318888835	0,186796789	0,252842812
Probability (P)	0,7964	0,6910	0,6259	0,7955	0,6902	3,5989	4,0888	-0,4899	1,2502	0,143692265	0,057177557	0,100434911
Consequence (C)	0,8077	0,7147	0,7609	0,7099	0,7631	3,7562	4,4619	-0,7057	1,0344	0,118888835	0,196417034	0,157652935
Resiliency (R)	0,8444	0,7651	0,8002	0,9365	0,6489	3,9952	3,8175	0,1778	1,9179	0,220433685	0,453784608	0,337109146
	4,2483	3,7590	4,0888	4,4619	3,8175			1,7401	8,7004			1

Prilog E: Tablica za procjenu utjecaja (zavisnosti) između svojstvenih kriterija za korisničke transakcijske sustave

Criteria influences for critical online transaction systems in the bank (m-banking, e-banking, e-commerce)	Authentication	Authorization	Encryption	Digital signing	Availability	Logging	Backup
Authentication	0						
Authorization		0					
Encryption			0				
Digital signature				0			
Availability					0		
Logging						0	
Backup							0

0 (no influence)
1 (low influence)
2 (medium influence)
3 (high influence)
4 (very high influence)

Instructions: You need to estimate how each row (from the left) influences on the column.

Prilog F: Tablice za procjenu važnosti svojstvenih kriterija u odnosu na cilj odlučivanja primjenom AHP metode za korisničke transakcijske sustave

CT1 (Identity)	Authentication	Authorization
Authentication	1	
Authorization		1

Saaty's scale		Reciprocal values
1	equal importance	1
3	weak dominance	1/3 (0,3333)
5	strong dominance	1/5 (0,2)
7	proven dominance	1/7 (0,1429)
9	absolute dominance	1/9 (0,1111)
all real numbers can be used between 1 and 9, including 2, 4, 6, 8		1/2, 1/4, 1/6, 1/8

Instructions:

In the first Comparison Table (**CT1 Identity**) it's necessary to assess which criterion (i.e. **security mechanism**) for online transaction system is more important inside Identity cluster, **Authentication** or **Authorization**, in protecting the value of IT assets, and how much on the Saaty scale. Please put the value from the Saaty scale in the table in the row of stronger element. On other empty place put reciprocal value of the previous Saaty's value used. On diagonal, there are 1s, because here, the same elements are compared, and when something is the same (equal), we use 1 on Saaty scale. So, You look how **row** dominates (is more important) than the column.

Example: If **Authentication** criterion is 2 times more important when compared to **Authorization** for online trx system, then **CT1** would look like:

CT1 example1	Authentication	Authorization
Authentication	1	2
Authorization	0,5	1

Example: If **Authentication** and **Authorization** criteria should be equal according to Your expertise, then **CT1** would look like:

CT1 example2	Authentication	Authorization
Authentication	1	1
Authorization	1	1

CT2 (C-I-A)	Encryption	Digital signing	Availability
Encryption	1		
Digital signing		1	
Availability			1

CR*	-1,923077

* must be less than 0.1 and positiv

Instructions:

Please compare security mechanisms criteria of **Encryption**, **Digital signing** and **Availability** in pairs in **CT2** table with respect to **C-I-A (Confidentiality, Integrity, Availability)** cluster. Encryption satisfies Confidentiality goal, Digital signing of online transactions satisfies integrity and non-repudiation goals, while Availability/Reliability is self-explained security meschanism and security goal. Domination-relationships between any two criteria will appear twice in the table: put the Saaty value in the row of the criterion that dominates over another criteria from the column, and its reciprocal value on the appropriate position. **Transitivity** rule must be satisfied: e.g., if **Encryption** dominates over **Digital signing**, and **Digital signing** dominates over **Availability**, then **Encryption** dominates over **Availability**. When transitivity concept is broken, **CR** (Consistency Ratio) value increases.
It's necessary to look how each element from the row is important when compared with the element from the column, e.g. when compared Encryption -> Digital signing, then the value could be 4 and the reciprocal comparison Digital signing -> Encryption must be 0,25.

CT2 example1	Encryption	Digital signing	Availability
Encryption	1	3	4
Digital signing	0,3333	1	2
Availability	0,25	0,5	1

CT2 example2	Encryption	Digital signing	Availability
Encryption	1	1	2
Digital signing	1	1	3
Availability	0,5	0,3333	1

Important: When You finish with the comparisons procedure, **CR** value must be less than 0.1 (and positive) for **CT2** and **CT4** in order to accept your inputs. If it's higher, please make checks and do some comparisons once again in order to be within the defined boundaries. CR value is not calculated for CT1 and CT3 because only 2 elements are compared.

CT3 (Forensic)	Logging	Backup
Logging	1	
Backup		1

Instructions:

The same as for CT1 table, it's necessary to provide simple comparisons between 2 elements (i.e. **security mechanisms**) for **CT3 (Forensic)** cluster, in this case **Logging** and **Backup**.

Example: If You consider that **Logging** criterion is 3 times more important when compared to **Backup** criterion, then **CT3** table would look like:

CT3 example1	Logging	Backup
Logging	1	3
Backup	0,3333	1

Example: If You consider that **Backup** criterion is 2 times more important when compared to **Logging** criterion, then **CT3** table would look like:

CT3 example2	Logging	Backup
Logging	1	0,5
Backup	2	1

CT4 (clusters)	Identity	C-I-A	Forensic
Identity	1		
C-I-A		1	
Forensic			1

CR*	-1,9230769

* must be less than 0.1 and positive

Instructions:

For this **CT4** table, it's necessary to compare the clusters itself on the same way as You did previously for other comparisons in this sheet. E.g., whether and at what level the **Identity** cluster is more important than **C-I-A** cluster, etc. Again, You look on how row dominates (is more important) than the column, and also appropriate reciprocal values must be set.

CT4 example1	Identity	C-I-A	Forensic
Identity	1	0,5	3
C-I-A	2	1	4
Forensic	0,3333	0,25	1

CT4 example2	Identity	C-I-A	Forensic
Identity	1	1	2
C-I-A	1	1	3
Forensic	0,5	0,3333	1

Prilog G: SNAP11 postupak za izračun svojstvenih kriterija za korisničke bankovne transakcijske sustave

Aggregation (Z matrix)	Authentication	Authorization	Encryption	Digital signing	Availability	Logging	Backup
Authentication	0	3,3125	2,25	2,8125	1,75	2,125	1,125
Authorization	2,875	0	1,5625	1,9375	2	1,9375	1,125
Encryption	2,5	1,75	0	2,9375	1,9375	1,4375	1,5625
Digital signature	2,5625	2,25	2,8125	0	1,1875	1,5	1,25
Availability	2,6875	2,375	2,25	2	0	1,875	2
Logging	1,8125	1,5625	1,25	1,3125	1,8125	0	1,375
Backup	1,0625	1	1,25	1,125	2,25	1,25	0
Calculation of column sums and identification of max column sum	13,5	12,25	11,375	12,125	10,9375	10,125	8,4375

S matrix						
0	0,228448276	0,15517241	0,193965517	0,12068966	0,146552	0,0775862
0,198275862	0	0,10775862	0,13362069	0,13793103	0,133621	0,0775862
0,172413793	0,120689655	0	0,202586207	0,13362069	0,099138	0,1077586
0,176724138	0,155172414	0,19396552	0	0,08189655	0,103448	0,0862069
0,185344828	0,163793103	0,15517241	0,137931034	0	0,12931	0,137931
0,125	0,107758621	0,0862069	0,090517241	0,125	0	0,0948276
0,073275862	0,068965517	0,0862069	0,077586207	0,15517241	0,086207	0

E matrix (n=7)						
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286
0,14285714	0,14286	0,142857143	0,142857143	0,142857143	0,14286	0,14286

G matrix						
0,021428571	0,215609606	0,15332512	0,186299261	0,12401478	0,145998	0,0873768
0,189963054	0,021428571	0,1130234	0,135006158	0,13866995	0,135006	0,0873768
0,167980296	0,124014778	0,02142857	0,193626847	0,13500616	0,105696	0,1130234
0,171644089	0,153325123	0,18629926	0,021428571	0,09104064	0,10936	0,0947044
0,178971675	0,160652709	0,15332512	0,138669951	0,02142857	0,131342	0,13867
0,127678571	0,113023399	0,09470443	0,098368227	0,12767857	0,021429	0,102032
0,083713054	0,080049261	0,09470443	0,087376847	0,15332512	0,094704	0,0214286

I-G						
1	-0,21561	-0,153325123	-0,18629926	-0,12401478	-0,146	-0,08738
-0,18996305	1	-0,113023399	-0,13500616	-0,13866995	-0,13501	-0,08738
-0,1679803	-0,12401	1	-0,19362685	-0,13500616	-0,1057	-0,11302
-0,17164409	-0,15333	-0,186299261	1	-0,09104064	-0,10936	-0,0947
-0,17897167	-0,16065	-0,153325123	-0,13866995	1	-0,13134	-0,13867
-0,12767857	-0,11302	-0,094704433	-0,09836823	-0,12767857	1	-0,10203
-0,08371305	-0,08005	-0,094704433	-0,08737685	-0,15332512	-0,0947	1

inverse (I-G)						
1,603381857	0,743728467	0,66111431	0,714841547	0,60990875	0,609465	0,4942642
0,698417201	1,506180812	0,57438265	0,617143577	0,56870819	0,550925	0,4510705
0,703806835	0,63606428	1,49423817	0,683321882	0,58357881	0,544069	0,4871085
0,688465154	0,640518223	0,63404967	1,504129986	0,53502427	0,53221	0,4587269
0,743551237	0,69324271	0,6524626	0,670097631	1,4941732	0,590856	0,5302305
0,56237174	0,52336212	0,48180797	0,505780148	0,48918568	1,361508	0,403976
0,484205497	0,45488925	0,44390331	0,456025629	0,47402057	0,412684	1,2832536

G * inverse	Authentication	Authorization	Encryption	Digital signing	Availability	Logging	Backup
Authentication	0,63774004	0,759665506	0,67528104	0,73015958	0,62297823	0,622525	0,5048555
Authorization	0,713383284	0,538456115	0,58669085	0,630368082	0,58089479	0,562731	0,4607363
Encryption	0,71888841	0,649694229	0,52625756	0,697964494	0,59608407	0,555728	0,4975466
Digital signature	0,703217979	0,654243613	0,64763645	0,536361343	0,54648908	0,543615	0,4685568
Availability	0,759484478	0,708097911	0,66644394	0,684456866	0,52619119	0,603517	0,5415925
Logging	0,574422563	0,534577022	0,49213243	0,516618294	0,49966823	0,390683	0,4126326
Backup	0,49458133	0,464636877	0,45341552	0,465797606	0,48417816	0,421527	0,3107519
	4,601718083	4,309371273	4,0478578	4,261726266	3,85648374	3,700327	3,1966722

r	c	r-c	N1	SNAP12	AHP	SNAP11
4,55321	4,601718083	-0,0485128	0,86438	0,135265454	0,205736222	**0,170500838**
4,07326	4,309371273	-0,23611119	0,67678	0,105908484	0,164580753	**0,135244618**
4,24216	4,047857798	0,1943053	1,1072	0,173263665	0,203349261	**0,188306463**
4,10012	4,261726266	-0,16160613	0,75129	0,117567661	0,153751556	**0,135659609**
4,48978	3,856483744	0,63330068	1,54619	0,241961344	0,074480352	**0,158220848**
3,42073	3,700326694	-0,27959226	0,6333	0,099104201	0,110567964	**0,104836083**
3,09489	3,196672199	-0,1017836	0,81111	0,126929191	0,087533891	**0,107231541**
		0,91289294	6,39025	1	1	1

Prilog H: Tablice za procjenu kritičnih bankovnih korisničkih transakcijskih sustava prema svojstvenim kriterijima

When defining the ratios between alternatives (i.e. online transaction systems), the crucial question to ask is: which system is **better** in terms of observed security criterion/mechanism? E.g. which system has better authentication, better encryption features, etc.

Saaty's scale		Reciprocal values
1	equal importance	1
3	weak dominance	1/3 (0,3333)
5	strong dominance	1/5 (0,2)
7	proven dominance	1/7 (0,1429)
9	absolute dominance	1/9 (0,1111)
all real numbers can be used between 1 and 9, including 2, 4, 6, 8		1/2, 1/4, 1/6, 1/8

Authentication	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

1	1	1
1,0000	0,0000	0,0000
0,0000	1,0000	0,0000
0,0000	0,0000	1,0000

e-banking	0,3333
m-banking	0,3333
e-commerce	0,3333

0,3333	0,0000	0,0000
0,0000	0,3333	0,0000
0,0000	0,0000	0,3333
0,3333	0,3333	1,0000
0,3333	0,3333	1,0000
0,3333	0,3333	1,0000

lambda (λ)	1
CI	-1
CR*	-1,923076923

* must be less than 0.1 and positive

Instructions:

When giving Your judgments/evaluation between critical online trx systems, consider **authentication factors** implemented in Your environment, e.g. username/pwd, biometrics, 2FA, etc., and try to assess which system is better (can be also equal).

Example1: If You consider that e-banking system has 2 times better **Authentication** security mechanisms than m-banking and 4 times better than e-commerce, then the table would look like:

Auth_example1	e-banking	m-banking	e-commerce
e-banking	1	2	4
m-banking	0,5	1	3
e-commerce	0,25	0,33333333	1

Example2: If You consider that e-banking and m-banking systems are equal in terms of strengths of **Authentication** security mechanisms, but are better than e-commerce, then the table would look like:

Auth_example2	e-banking	m-banking	e-commerce
e-banking	1	1	2
m-banking	1	1	3
e-commerce	0,25	0,333333333	1

Note:

All the numbers and calculations You see on the left side are just to present the complexity of mathematical procedure and computations, but please do not change it, all You need to fill are the fields in tables filled in green.

Important: When You finish with the comparisons procedure, CR value must be less than 0.1 (and positive) to accept your input. If it's higher, please make checks and do some comparisons once again in order to be within the defined boundaries.

Authorization	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923

* must be less than 0.1 and positive

When giving Your evaluation between online trx systems, consider **access rights** implemented in Your environment for those systems, e.g. whether user is allowed to see only his/her profile details and account balance, implementation of authorization rules, potential path traversal, etc.

Encryption	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923
		* must be less than 0.1 and positive	

When giving Your evaluation between online trx systems, consider the following implementations of **encryption** in Your systems: encryption of credentials, encryption of confidential data, encryption of communication channels (TLS), etc.

Digital signing of transactions	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923
		* must be less than 0.1 and positive	

When giving Your evaluation between online trx systems, consider how transactions are **signed** for each of the solution in Your environment, e.g. by password, MAC (Message Authentication Code), OTP (One-Time Password), biometrics, etc., and rank it.

Availability	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923
		* must be less than 0.1 and positive	

When giving Your evaluation between online trx systems, consider whether and how **high availability** features are implemented in Your environment for those critical systems, e.g. for network components, web servers, application servers, DB servers, etc.

Logging	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923
		* must be less than 0.1 and positive	

When giving Your evaluation between online trx systems, consider to which extent (or granularity) **audit logs** are recorded for actions done by admins and users on the online transaction systems.

Backup	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1
		CR*	-1,923076923
		* must be less than 0.1 and positive	

When giving evaluation between online trx systems, consider whether and how **backup** is implemented (full, incremental, differential) in Your environment for those critical systems, e.g. for web server files, application servers, DB servers.

FTEs:	
How much time (approximately) You needed to give all inputs and correctly complete calculations in this sheet with evaluation of critical online trx solution by examining security mechanisms (in hours)? E.g.: 1, 1.5, 2, 3, 5 hours, etc.	Time

Prilog I: Tablice za procjenu kritičnih bankovnih korisničkih transakcijskih sustava prema generičkim ISRA kriterijima

When defining the ratios between online transaction systems, the crucial question to ask is: which system has the bigger **risk** exposure in terms of observed risk criterion?

Saaty's scale		Reciprocal values
1	equal importance	1
3	weak dominance	1/3 (0,3333)
5	strong dominance	1/5 (0,2)
7	proven dominance	1/7 (0,1429)
9	absolute dominance	1/9 (0,1111)
all real numbers can be used between 1 and 9, including 2, 4, 6, 8		1/2, 1/4, 1/6, 1/8

Threat	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

CR*	-1,9230769

* must be less than 0.1 and positive

Instructions:

Threat represents the probability of an event in which an attacker will make some damage to a particular system. When giving Your evaluation/ratios between critical online trx systems regarding **Threat** risk criterion, consider which system is more exposed to various ICT security threats, e.g. malware (viruses, worms, cryptolockers), eavesdropping, hijacking, impersonating, unauthorized access, phishing, DDoS attacks, etc.

Example1: If You consider that e-commerce system has 2 times **higher risk** in terms of **Threat** than e-banking and 4 times higher risk in terms of **Threat** than m-banking, then the table would look like:

Threat_example1	e-banking	m-banking	e-commerce
e-banking	1	3	0,5
m-banking	0,3333	1	0,25
e-commerce	2	4	1

Example2: If You consider that all presented critical online systems have the same **risk** level in terms of **Threat**, then the table would look like:

Threat_example2	e-banking	m-banking	e-commerce
e-banking	1	1	1
m-banking	1	1	1
e-commerce	1	1	1

Important Note:

When giving Your evaluation/ratios between critical online trx systems regarding **Threat**, **Vulnerability**, **Probability** and **Consequence**, the logic is opposite from the previous sheet where You needed to evaluate online banking systems according to positive/best implementation of security mechanism, but now You consider which online trx system is **more risky** according to the observed risk criteria.

Vulnerability	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

CR*	-1,9230769

* must be less than 0.1 and positive

Vulnerability is a characteristic of an IT asset to indicate its weakness to some kind of attack. Vulnerability is linked to a threat that exploits it. When giving Your evaluation/ratios between critical online trx systems regarding **Vulnerability** risk criterion, consider which system is usually more vulnerable to attacks, e.g. existence of exploit, non-existence or weak implementation of 2FA, missing of channel encryption, etc.

Example1: If You consider that e-commerce system is 5 times more vulnerable than m-banking and 3 more vulnerable than e-banking, then the table would look like:

Vuln_example1	e-banking	m-banking	e-commerce
e-banking	1	2	0,3333
m-banking	0,5	1	0,2
e-commerce	3	5	1

Probability	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

CR*	-1,9230769

* must be less than 0.1 and positive

When giving Your evaluation/ratios between critical online trx systems regarding **Probability** risk criterion, consider **Threat Agent factors** (Skill level, Participant, Motive, Method, Opportunity, Size, Frequency of attack) and **Vulnerabiltiy factors** (Ease of discovery, Ease of exploitation, Awareness, Intrusion detection) for each of the observed system.

Example1: If You consider that for e-commerce system there is a 5 times **higher Probability** of a successful attack than for e-banking and 4 times higher **Probability** than for m-banking, then the table would look like:

Threat_example1	e-banking	m-banking	e-commerce
e-banking	1	2	0,2
m-banking	0,5	1	0,25
e-commerce	5	4	1

Consequence	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

CR*	-1,9230769

* must be less than 0.1 and positive

Consequence (or **Impact**) represents a loss of economic, symbolic or psychological value for organization, i.e. reputational risk for the bank in case of loss or theft of data, unavailability of certain parts of information systems, reduced levels of service quality, etc.
When giving Your evaluation/ratios between critical online trx systems regarding **Consequence** risk criterion, consider which trx system would have been most impacted in case of a cyber attack.

Example1: If You consider that e-banking system has 5 times **higher risk** in terms of **Consequence** than e-commerce and 3 times **higher risk** in terms of **Consequence** than m-banking, then the table would look like:

Threat_example1	e-banking	m-banking	e-commerce
e-banking	1	3	5
m-banking	0,3333	1	2
e-commerce	0,2	0,5	1

Resiliency	e-banking	m-banking	e-commerce
e-banking	1		
m-banking		1	
e-commerce			1

Resiliency element is considered to evaluate how much and whether the IT solution is resilient regarding the other risk elements (Threat, Vulnerability, Probability and Consequence) that make influence on Resiliency element itself. **Resilience** or **elasticity** is the speed with which the organization can successfully recover after a significant violation or failover of prescribed security policies. For the purpose of this research and model validation, the resiliency attribute is considered to be used for the evaluation of critical IT solutions.
When giving Your evaluation between online trx systems, consider how resilient is each of these solutions in Your environment regarding cyber threats and vulnerabilities, e.g. whether adequate security controls exist like antimalware solution, anti-APT, **high availability** features, anti-fraud system, encryption of communications, application visibility on FWs, IPS, anti-DDoS, etc.

Example1: If You consider that e-commerce system is 3 times **more risky** than e-banking and m-banking systems in terms of **Resiliency**, and e-banking is 2 times less resilient (i.e. **more risky**) than m-banking, then the table would look like:

Threat_example1	e-banking	m-banking	e-commerce
e-banking	1	2	0,3333
m-banking	0,5	1	0,3333
e-commerce	3	3	1

CR*	-1,9230769

* must be less than 0.1 and positive

FTEs:	
How much time (approximately) You needed to give all inputs and correctly complete calculations in this sheet with evaluation of critical online trx solution by generic risk criteria (in hours)? E.g.: 1, 2, 3 hours, etc.	Time

Prilog J: Upitnik za validaciju referentnog modela s inherentnim kriterijima

No.	Research question for the reference multicriteria model with inherent criteria for critical business banking systems	Answer (mandatory)	Your explanation of the answer (optional, not necessary)	Moderator's explanations
1	How much do You consider the reference model as **functionally suitable**?			This characteristic represents the degree to which a proposed multicriteria model provides functions that meet stated and implied needs when used under specified conditions. This characteristic is composed of the following sub-characteristics that should be considered: • Completeness, correctness and appropriateness
2	How much do You consider the reference model as **performance efficient**?			This characteristic represents the performance of the multicriteria model relative to the amount of resources used under stated conditions. This characteristic is composed of the following sub-characteristics that should be considered: • Time and resource utilization
3	How much do You consider the reference model as **compatible**?			Degree to which a multicriteria model is compatible with the existing procedures and systems for evaluating of critical IT systems and related security risks. This characteristic is composed of the following sub-characteristics that should be considered: • Co-existence and interoperability
4	How much do You consider the reference model as **usable**?			Degree to which a new multicriteria model can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. This characteristic is composed of the following sub-characteristics that should be considered: • Ease of use and user error protection (e.g. for calculation of Consistency Ratio)
5	How much do You consider the reference model as **reliable**?			Degree to which decision makers could rely on the results provided by the model when critical IT systems are evaluated. The following sub-characteristics should be considered: • Maturity of the model and easiness to understand the multicriteria model for the evaluation of critical IT systems
6	How much do You consider the reference model as **secure**?			Degree to which a model with inherent criteria satifies the minimum security requirements to adequately evaluate critical business IT systems. This characteristic is composed of the following sub-characteristics that should be considered: • Confidentiality, integrity, availability, non-repudiation, accountability and authenticity
7	How much do You consider the reference model as **maintainable**?			This characteristic represents the degree of effectiveness and efficiency with which a model with inherent criteria can be modified to improve it, correct it or adapt it to changes in environment, and in requirements. This characteristic is composed of the following sub-characteristics that should be considered: • Modularity, reusability, changeability and testability
8	How much do You consider the reference model as **portable**?			Degree of effectiveness and efficiency of the proposed multicriteria model when the model is potentially applied on different IT systems, not just critical ones or related to banking business. E.g., for the evaluation of operating systems, specific hardware, cryptographic algorithms, cloud-based solutions, etc. The following sub-characteristics should be considered: • Adaptability and flexibility of the model with inherent criteria.

Skala mogućih odgovora:

1 - Very bad
2 - Bad
3 - Fair
4 - Good
5 - Excellent

Životopis autora

Davor Maček rođen je 16. lipnja 1982. godine u Zagrebu. Srednju školu Sesvete, opća gimnazija, završava 2000. godine i tada upisuje Fakultet organizacije i informatike (FOI) u Varaždinu Sveučilišta u Zagrebu, smjer Informacijski sustavi. Na FOI-ju diplomira u ožujku 2007. iz kolegija Programsko inženjerstvo na temu "Izrada financijskog sustava uporabom MS SQL Servera". Neposredno nakon toga zapošljava se u Zagrebačkoj banci u sektoru Informatike kao sistem inženjer za Microsoft platformu. U studenom 2008. godine upisuje specijalistički poslijediplomski studij "Upravljanje sigurnošću i revizija informacijskih sustava" na FOI-ju koji završava u ožujku 2011. s temom završnog rada "Zaštita unutarnje mreže banke od sigurnosnih prijetnji i usporedba mogućih rješenja". Svoje akademsko obrazovanje nastavlja krajem 2012. godine upisom na poslijediplomski doktorski studij na Fakultetu organizacije i informatike u Varaždinu.

Uz polaganje Microsoft certifikata, stručno usavršavanje nastavlja upisom Cisco CCNA Akademije koju završava 2013. godine. Iste godine prelazi u sigurnosni odjel Zagrebačke banke gdje radi na poslovima zaštite informacijskog sustava, a nakon toga u rujnu 2015. godine kao izaslani radnik banke odlazi u Beč na radno mjesto ICT Security koordinatora za CEE zemlje članice UniCredit grupe. Trenutno radi kao ICT sigurnosni stručnjak u tvrtki UniCredit Services GmbH Wien, članici UniCredit grupe.

Popis objavljenih znanstvenih radova

Znanstveni časopisi s međunarodnom recenzijom:

1. D. Maček, I. Magdalenić and N. Begičević Ređep, "A Model for the Evaluation of Critical IT Systems Using Multicriteria Decision-Making with Elements for Risk Assessment," *Mathematics*, vol. 9, no. 9, p. 1045, May 2021. DOI: https://doi.org/10.3390/math9091045
2. D. Maček, I. Magdalenić and N. Begičević Ređep, "A Systematic Literature Review on the Application of Multicriteria Decision Making Methods for Information Security Risk Assessment," *International Journal of Safety and Security Engineering*, vol. 10, no. 2, pp. 161-174, April 2020. DOI: https://doi.org/10.18280/ijsse.100202
3. D. Maček and D. Alagić, "Comparisons of Bitcoin Cryptosystem with Other Common Internet Transaction Systems by AHP Technique," *Journal of Information and Organizational Sciences*, vol. 41, no. 1, pp. 69-87, June 2017. DOI: https://doi.org/10.31341/jios.41.1.5

Znanstveni radovi objavljeni u zbornicima međunarodnih skupova:

1. D. Maček, I. Magdalenić and N. Begičević Ređep, "Towards a Hybrid Model for the Evaluation of Critical IT Systems," in *Quality of Software and Services: Central European Conference on Information and Intelligent Systems* (*CECIIS 2020*), Varaždin, Croatia, October 07-09, 2020, pp. 1-7. https://ceciis.foi.hr/sites/default/files/ceciis2020/QSS/CECIIS-2020_paper_61.pdf
2. D. Alagić and D. Maček, "Metamodeling as an approach for better computer resources allocation in web clusters," in *39th International Convention on Information and Communication Technology, Electronics and Microelectronics* (*MIPRO*), Opatija, Croatia, June 2016, pp. 214-219. DOI: 10.1109/MIPRO.2016.7522140
3. D. Maček, I. Magdalenić and N. Ivković, "Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard," in *Information Systems Security: Central European Conference on Information and Intelligent Systems* (*CECIIS 2012*), Varaždin, Croatia, September 19-21, 2012, pp. 305-311. http://archive.ceciis.foi.hr/app/index.php/ceciis/index/pages/view/ProceedingsArchive2012
4. D. Maček, I. Magdalenić and N. Ivković, "Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods," in *Information Systems Security: Central European Conference on Information and Intelligent Systems* (*CECIIS 2011*), Varaždin, Croatia, September 21-23, 2011, pp. 133-138. http://archive.ceciis.foi.hr/app/index.php/ceciis/2011/paper/view/478

Položeni certifikati

- **(ISC)²**:
  - *Certified Information Systems Security Professional* (CISSP), June 2015
  - *Certified Cloud Security Professional* (CCSP), July 2018
- **EC-Council**:
  - *Certified Ethical Hacker* (CEH), December 2016
- **Cisco**:
  - *Cisco Certified Network Associate* (CCNA), September 2013
- **Microsoft**:
  - (exam AZ-900) *Microsoft Azure Fundamentals*, February 2020
  - Microsoft Certified IT Professional (MCITP):
    - (exam 70-647) *Windows Server 2008, Enterprise Administrator*, February 2011
    - (exam 70-646) *Windows Server 2008, Server Administrator*, April 2010
  - Microsoft Certified Technology Specialist (MCTS)
    - (exam 70-662) *Microsoft Exchange Server 2010, Configuring*, September 2012
    - (exam 70-680) *Windows 7, Configuring*, November 2010
    - (exam 70-643) *Windows Server 2008 Applications Infrastructure, Configuring*, April 2010
    - (exam 70-642) *Windows Server 2008 Active Directory, Configuring*, October 2009
    - (exam 70-640) *Windows Server 2008 Network Infrastructure, Configuring*, February 2010
  - Microsoft Certified Professional
    - (exam 70-291) *Implementing, Managing and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*, November 2008
    - (exam 70-290) *Managing and Maintaining a Microsoft Windows Server 2003 Environment*, June 2008.