UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

VPLIV RAZUMLJIVOSTI REZULTATOV UMETNE INTELIGENCE NA ZMOŽNOST OCENE TVEGANJ: VIDIK UPORABNIKOV

Ljubljana, oktober 2025 BENO KRAŠOVEC

IZJAVA O AVTORSTVU

Podpisani Beno Krašovec, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Vpliv razumljivosti rezultatov umetne inteligence na zmožnost ocene tveganj: vidik uporabnikov, pripravljenega v sodelovanju z red. prof. dr. Petrom Trkmanom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih del Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih del Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi;
11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 22. 09. 2025

Podpis študenta: Beno Krašovec

POVZETEK

Implementacija in uporaba sistemov umetne inteligence v malih in srednje velikih organizacijah pogosto temelji na zunanjem znanju in na pomanjkanju informacij za oceno s tem povezanih tveganj. Odločevalci v takšnih organizacijah pogosto preskočijo vprašanje, ali določen sistem umetne inteligence prinaša koristi, ki presegajo s tem povezana tveganja. Da bi ugotovil, katere informacije bi pomagale ublažiti to težavo, sem opravil intervjuje v različnih organizacijah v Sloveniji in v Švici. Preučeval sem predvsem percepcijo udeležencev v procesu odločanja o uvedbi umetne inteligence. Rezultati raziskave kažejo, kako bi se lahko povečalo sposobnost organizacij za ocenjevanje tveganj, povezanih z uvedbo in delovanjem sistemov umetne inteligence. Zaznane so nekatere razlike med organizacijami z različnimi ravnmi zmogljivosti ocenjevanja tveganj. Predlagani so ukrepi, ki lahko ublažijo negativne posledice pomanjkanja teh zmogljivosti.

KLJUČNE BESEDE: umetna inteligenca, implementacija UI, tveganja UI, dejavniki tveganja, sposobnost ocenitve tveganj, pomanjkanje lastnega znanja, vidik odločevalcev, ukrepi za obvladovanje tveganj.

CILJI TRAJNOSTNEGA RAZVOJA

ABSTRACT

An implementation and later operations of AI systems in small and medium organizations are often based on external knowledge and on a lack of information to asses related risks. Decision-makers in those organizations often skip over the question of whether a given AI system provides benefits which surpass related risks. To determine which information would help mitigate this problem, interviews with different types of stakeholders in organizations in Slovenia and in Switzerland were conducted. They examined the perspective of different participants in the decision-making process of an AI implementation. Research shows how the organizations' capacity to assess risks related to the implementation and operations of AI system could be increased. The research determined some distinctions in relation to different organizational levels of risk assessment capabilities and showed few suggestions how to mitigate the lack of them.

KEY WORDS: artificial inteligence, AI implementation, risk of AI, risk factors, risk assessment capability, lack of internal knowledge, decision-makers' perception, risk control measures.

SUSTAINABLE DEVELOPMENT GOALS

KAZALO

KAZALO SLIK

KAZALO TABEL

KAZALO PRILOG

KAZALO TABEL V PRILOGAH

SEZNAM KRATIC

angl. – angleško
A2A– (angl. Agent 2 Agent Protocol) – protokol povezovanja agentov umetne inteligence
AGI – (angl. Artificial General Intelligence) – splošna umetna inteligenca
AI TRiSM – (angl. Artificial Intelligence Trust, Risk, Security Management) – priporočilni okvir ravnanja s sistemi umetne inteligence
ANI – (angl. Artificial Narrow Intelligence) – ozka umetna inteligenca
API - (angl. Application Programming Interface) - aplikacijski programski vmesnik
ASI – (angl. Artificial Superintelligence) – umetna superinteligenca
CAPEX – (angl. Capital Expenditure) – kapitalski izdatki
CEO – (angl. Chief Executive Officer) – glavni izvršni direktor
CSS – (angl. Component Synergy Score) - kazalnik kvalitete med agentskega sodelovanja
GDPR – (angl. General Data Protection Regulation) – uredba o varstvu osebnih podatkov
GPT – (angl. Generative Pre-Trained Transformer) – prednaučen inteligentni sistem za ustvarjanje vsebin
IMRAD - (angl. Introduction, Method, Results, and Discussion) – struktura dokumenta: uvod, metoda, rezultati in diskusija
IT – informacijska tehnologija
LLM – (angl. Large Language Model) – veliki jezikovni model
NLP - (angl. Natural Language Processing) – obdelava naravnega jezika
OPEX – (angl. Operating Expenditure) – operativni izdatki
ROI - (angl. Return on Investment) – donosnost naložbe
SOTA - (angl. State of the Art) – najsodobnejša tehnologija
TUE - (angl. Tool Utilization Efficacy) – kazalnik učinkovitosti rabe orodij
UI – umetna inteligenca
XAI – (angl. Explainable Artificial Intelligence) – razložljiva umetna inteligenca

1 UVOD

Raziskava mednarodne svetovalne organizacije McKinsey & Company (McKinsey Survey, 2025) je na globalni ravni pokazala, da je 78 % anketiranih podjetij že uvedlo umetno inteligenco (v nadaljevanju tudi UI) v vsaj eni svoji poslovni funkciji. Po drugi strani pa po podatkih mednarodne organizacije ISACA® (nekoč angl. Information Systems Audit and Control Association®) 40 % organizacij sploh ne ponuja usposabljanja za umetno inteligenco, le 15 % organizacij pa ima formalno, celovito politiko, ki ureja uporabo tehnologije umetne inteligence (ISACA, 2024). Iz tega bi se dalo sklepati, da nekatera podjetja uvajajo in uporabljajo umetno inteligenco brez trdne strategije za obravnavo tveganj, povezanih z njeno uvedbo.

Med mnenji javno izpostavljenih strokovnjakov obstajajo velike razlike glede tega, katera tveganja je potrebno obravnavati pri uvajanju umetne inteligence. Kljub temu se vsi strinjajo, kakor pritrjujejo tudi poročila priznanih institucij, kot je Stanford University, da se nezaustavljive spremembe že dogajajo zaradi uvajanja umetne inteligence v številnih družbenih segmentih (Maslej in drugi, 2025), da vsa s tem povezana tveganja niso obravnavana in jih tudi ni mogoče ustrezno obravnavati. Opozarjajo, da uporabniki umetne inteligence ne bodo razmišljali o tem, kako agenti umetne inteligence (v nadaljevanju tudi agenti UI) delujejo, podobno kot ljudje ne razmišljajo o tem, kako električni sistem zagotavlja elektriko ali kako deluje Googlov iskalnik. Namesto tega bodo o umetni inteligenci razmišljali z vidika, kakšne rezultate je mogoče z njo doseči. V ta namen bodo uporabniki umetne inteligence potrebovali uporabniške vmesnike, ki bodo ponudili boljše upravljanje z njenimi rezultati. Da bi posameznik lahko to dobro izvajal, bo potreboval dobro splošno znanje in razgledanost, prilagodljivost in odzivnost na pojav nepredvidljivih ovir in priložnosti, ki jih lahko generirajo kompleksni sistemi, kakršni so sistemi interoperabilnih agentov umetne inteligence. Ozko specializiran ali zgolj tehnično podkovan uporabnik »ne bo dovolj«. Zmožnost realistične uporabe domišljije in razumevanja mogočih izidov bo največja individualna konkurenčna prednost (Diary Of A CEO, 2025).

1.1 Opis problema

Podjetja brez ustreznega zavedanja in znanja o umetni inteligenci torej že začenjajo z uporabo umetne inteligence. Uporaba slabo razumljenih algoritmov umetne inteligence (v nadaljevanju tudi algoritmi UI) v organizaciji predstavlja več pomembnih tveganj (Von Eschenbach, 2021): varnostne ranljivosti, tveganja glede skladnosti s predpisi in pravna tveganja (Stein, 2022), operativne pomanjkljivosti in netočne napovedi (Virvou, 2023), etične pomisleke (Guan in drugi, 2022), pristranske in diskriminatorne rezultate (Lebovits, 2019), kršitve zasebnosti in nejasno odgovornost, kar lahko spodkoplje zaupanje in ovira človeško sprejetje umetne inteligence (White House, 2023).

Po drugi strani pa lahko uporaba algoritmov umetne inteligence v organizaciji ponudi številne prednosti, ki izboljšujejo različne vidike poslovanja: večjo učinkovitost in produktivnost, izboljšano odločanje, nižje stroške, izboljšano uporabniško izkušnjo, večjo inovativnost, konkurenčno prednost, večjo varnost in zadovoljstvo zaposlenih (Wamba-Taguimdje in drugi, 2020).

Sprejemanje umetne inteligence oziroma percepcija njene uporabnosti in ustreznosti je lahko ključna za uspešnost njene uvedbe v organizaciji (Rane in drugi, 2024). Ker organizacije pogosto nimajo dovolj strokovnega znanja o umetni inteligenci, odločevalci v zvezi z uvajanjem umetne inteligence ne morejo ocenjevati tveganj brez zanašanja na zunanje strokovno znanje, ki pa je lahko pristransko zaradi navzkrižja interesov, kadar osebe s tem znanjem sodelujejo tudi pri promociji in prodaji sistemov umetne inteligence (v nadaljevanju tudi sistemi UI). Posledično nekateri odločevalci uvedbo umetne inteligence odlagajo v prihodnost. Povečevanje razumljivosti delovanja algoritmov UI in njihovih odločitev je v znanstveni literaturi pogosto obravnavano, redkeje pa problematika razumevanja dejanskih zmogljivosti, sposobnosti, dometa in posledic delovanja umetne inteligence z vidika njenih končnih uporabnikov (Rane in drugi, 2024).

Vse bolj se uveljavlja tudi razlaga umetne inteligence, ki jasno ločuje med procesno / algoritmično transparentnostjo umetne inteligence in nedeterminirano potencialno kreativnostjo njenih rezultatov (Chollet, 2025), kar nakazuje le delno uporabnost pristopa dosedanjih metod zagotavljanja razumljivosti umetne inteligence. Izpostavljajo se meje zmožnosti determiniranja sistemov umetne inteligence na podlagi baze prednaučenega znanja in začetnega stanja algoritmov sistema UI, saj se bo sistem znal sam prilagajati v danem trenutku, razmišljati v novih situacijah, abstrahirati problematiko, spoznavati do tedaj nezaznavne probleme in izumljati nove rešitve. Chollet (2025) pravi, da stopnjo splošne inteligence označuje učinkovitost razmerja med preteklimi izkušnjami kot njeno bazo znanja in obsegom njenih potencialnih rezultatov oz. obsegom njenih vzorcev obnašanja. Že v tem trenutku se vse več vodilnih modelov umetne inteligence spopada s tem – iz človeškega vidika nedeterminiranim in težko opredeljivim aspektom umetne inteligence, ki se deloma usmerja proti splošni umetni inteligenci (angl. Artificial General Intelligence, v nadaljevanju tudi AGI). Gre za kompromis dveh konceptov – prototipnega/intuitivnega in algoritemskega/kalkulativnega pristopa, ki se trenutno srečujeta v procesu programske sinteze sistemov UI. V tem procesu sistem umetne inteligence sam sproti izdeluje nove / spremenjene algoritme za reševanje problemov.

Kot kaže zasedanje francoskega senata v juliju 2025, se področje upravljanja s tveganji zaradi realnega geopolitičnega stanja dodatno zamegljuje zaradi teženj in intervencij izven evropskih institucij. Ponudniki digitalnih storitev so namreč dolžni spoštovati regulativo različnih držav, ki med seboj ni v zadostni meri usklajena, tako da npr. prihaja do predajanja privatnih podatkov uporabnikov teh storitev izven evropskim institucijam, ne da bi bili lastniki podatkov o tem obveščeni (le Sénat français, 2025).

Tudi zaradi opisanih trendov magistrsko delo preučuje dilemo, kako izboljšati sposobnost organizacije za opredeljevanje tveganj sistema umetne inteligence z osredotočanjem na ustrezne ukrepe že v začetni fazi uvajanja sistema. Moj prvotni vzgib za to temo je problematizacija vprašanja, ki sem ga zaznal pri interakciji z različnimi deležniki med promocijo sistemov umetne inteligence: "Kako iskati kompromis med tveganji sistema umetne inteligence zaradi nejasnih zmogljivosti, sposobnosti, dometa in posledičnih možnih vplivov sistema ter slabo razumljenih možnosti njegovih omejitev, v primerjavi s koristmi povečevanja produktivnosti, učinkovitosti in kakovosti - vse v situaciji, ko je težko oceniti pomembnost in verjetnost pojava teh tveganj?" Ker so argumentacije, ki obravnavajo to vprašanje, raznovrstne, sem se osredotočil predvsem na ukrepe v fazi uvajanja sistema umetne inteligence, ki lahko pomagajo odločevalcem v organizaciji, ki nimajo ustreznega dostopa do strokovnega znanja na področju umetne inteligence, da bi znali bolje oceniti tveganja njene uvedbe.

1.2 Namen in cilji magistrskega dela

Namen magistrskega dela je bil izboljšati razumevanje vpliva zmožnosti doumevanja sistema umetne inteligence s strani različnih skupin uporabnikov na njihovo sposobnost ocenjevanja tveganj, povezanih z njegovo uvedbo.

Cilj magistrskega dela je bil raziskati percepcijo odločevalcev v fazi sprejemanja odločitve o uvedbi umetne inteligence v podjetju – percepcijo o pomembnosti nekaterih potencialnih ukrepov, ki lahko pozitivno vplivajo na sposobnost sprejetja informirane odločitve o njeni uvedbi.

Osredotočil sem se na:

- preučitev trditve, da na sposobnost ocenjevanja tveganj vpliva stopnja razumevanja zmogljivosti sistemov umetne inteligence in stopnja razumevanja, kaj lahko počnejo,
- opredelitev nekaterih ukrepov omejevanja sistemov umetne inteligence kot ukrepov za povečanje razumevanja in zmanjšanje neopredeljivosti tveganj pri uvajanju sistema,
- opredelitev meril in metod za ocenjevanje tveganj, ki jih lahko zaznajo in ustrezno vrednotijo tudi deležniki, ki niso strokovnjaki za umetno inteligenco,
- predlog nekaterih ukrepov za izboljšanje sposobnosti ocenjevanja tveganj za deležnike, ki niso strokovnjaki za umetno inteligenco, kot so:
    - orodja za razložljivost,
    - tehnike vizualizacije,
    - sistemi spremljanja in usmerjanja delovanja UI.

Poskušal sem odgovoriti na raziskovalno vprašanje: »Kako lahko nekateri ukrepi v fazi odločanja o uvedbi sistema umetne inteligence pomagajo odločevalcem bolje ocenjevati tveganja, povezana z uvedbo?«.

1.3 Struktura magistrskega dela

Struktura magistrskega dela sledi IMRAD shemi poročanja o rezultatih raziskav (angl. Introduction, Method, Results, and Discussion).

V poglavjih Uvod in Literatura je opisan problem in so opredeljena vprašanja, ki so bila predmet raziskave. Predstavljeno je, kaj je že zapisano v literaturi in virih.

Nato je opredeljena uporabljena raziskovalna metoda kvalitativne analize - na kakšen način sem soočil, razvrstil in obdelal različna mnenja o problemu, ki ga raziskujem. Natančno je definirana izvedba analize.

Sledi analiza zbranih podatkov, oblikovanje sklepov in oblikovanje odgovorov na zastavljena vprašanja.

Na koncu so predstavljene zaključne ugotovitve in spoznanja tega raziskovalnega dela z opredelitvijo prispevka k znanju in uveljavljeni praksi obravnavanega področja. Opisani so predlogi za nadaljevanje raziskav izbranega problema.

2 PREGLED LITERATURE

Po Rane in drugi (2024) obstajajo ključni dejavniki (našteti so v poglavju 2.2.2), ki vplivajo na sprejemanje umetne inteligence v organizacijah in nasploh. Nekateri od njih se močno zanašajo na razumevanje umetne inteligence. Organizacije pogosto nimajo dovolj strokovnega znanja o umetni inteligenci, da bi obravnavale vse te dejavnike (Wei in Pardo, 2022). Njihovi odločevalci pri odločanju o uvedbi umetne inteligence tehtajo pozitivne in negativne učinke, pri čemer imajo zelo nejasno sliko tveganj zaradi slabo razumljenih zmožnosti umetne inteligence (Ranjan in drugi, 2021). Pogosto se morajo pri tem ocenjevanju zanašati na zunanje strokovno znanje (Wei in Pardo, 2022).

Vprašanje, kako izboljšati razumevanje odločanja in funkcionalnosti algoritmov umetne inteligence z vidika strokovnjakov za umetno inteligenco (Mohseni in drugi, 2021) – npr.: razložljiva umetna inteligenca (angl. Explainable Artificial Intelligence, v nadaljevanju XAI), izobraževanje in usposabljanje uporabnikov ter njihova vključenost v fazo uvajanja, spremljanje in revizija, okviri odgovornosti in človeški nadzor, je bilo v znanstveni literaturi pogosto obravnavano. Messeri in Crockett (2024) po drugi strani opozarjata na tendenco razlagalcev orodij umetne inteligence, da so prekomerno prepričani o pravilnosti, enoznačnosti in nevtralnosti algoritmov in baze znanja umetne inteligence, kar je po njunem mnenju pravzaprav utvara. Premalo pozornosti pa je namenjeno razumevanju dejanskih zmogljivosti, sposobnosti, dometa in posledic delovanja umetne inteligence z vidika njenih končnih uporabnikov (Rane in drugi, 2024).

2.1 Sistemi umetne inteligence

Kurzweil je v letu 1990 opredelil sistem umetne inteligence kot tehnološki sistem, zasnovan za izvajanje nalog, ki za izvajanje običajno zahtevajo človeško inteligenco. Te naloge lahko vključujejo učenje, sklepanje, reševanje problemov, zaznavanje in sprejemanje odločitev (Russell in Norvig, 1995).

Predvsem Minsky (McCarthy in drugi, 2006) je UI definiral kot znanost, ki "stroje" dela sposobne izvajati naloge, ki zahtevajo inteligenco, če jih izvajajo ljudje. McCarthy (2004) je po drugi strani UI definiral kot znanstveno disciplino, ki raziskuje "sposobnost strojev", da izvajajo naloge, s katerimi še niso bili seznanjeni in zanje niso bili posebej usposobljeni. Nahajamo se v obdobju, ko se po mnenju nekaterih težišče novega razvoja UI nagiba na McCarthyjevo stran (Chollet, 2025).

Sistemi umetne inteligence temeljijo na algoritmih strojnega učenja, globokega učenja in algoritmih obdelave naravnega človeškega jezika (angl. Natural Language Processing - NLP). Ti algoritmi obdelujejo podatke za učenje in odločanje, pri čemer potrebujejo ogromno procesorske moči. V tem delu se ne ukvarjam s specifikami posameznih vrst sistemov umetne inteligence, temveč s problematiko ocenjevanja sistemov, ki so prisotni na tržišču in so dostopni podjetjem. Komercialno dostopni modeli po letu 2022 prevladujoče temeljijo na velikih jezikovnih modelih (angl. Large Language Models, v nadaljevanju LLM), ki temeljijo na transformerski arhitekturi (Vaswani in drugi, 2017).

Karpathy (2025) pravi, da LLM postaja nov koncept računalnika - pojasnjuje LLM v vlogi centralne procesorske enote. Izpostavlja, da uporabniki komunicirajo z LLM pretežno preko dialoga, pri čemer pa opaža pomanjkanje učinkovitejšega uporabniškega vmesnika, ki bi človeku omogočal lažje obvladovati delovanje agentskega sistema UI.

Aprila 2025 je Google (Google, 2025) objavil nov protokol povezovanja agentov UI (angl. Agent2Agent Protocol – A2A), kar sedaj nenadoma omogoča sodelovanje agentov UI na povsem novi ravni in v ogromnem obsegu, kar dodatno aktualizira tudi avtonomne sisteme agentov umetne inteligence pri uvajanju UI v podjetjih. Da bi znali bolje pristopati k ocenjevanju tveganj pri uvajanju agentskih sistemov umetne inteligence, se je dobro zavedati njihovih ključnih značilnosti (Sapkota in drugi, 2025):

- avtonomije - sposobnosti samostojnega opravljanja nalog in upravljanju večstopenjskih nalog reševanja problemov brez stalnega človeškega nadzora;
- ciljno usmerjenega vedenja - prilagajanja svojih dejanj ob sledenju dolgoročnih ciljev, glede na kontekst in podatke, s katerimi se srečujejo;
- prilagodljivosti - sposobnosti učenja iz svojega okolja in ustreznega modificiranja svojega vedenja;

- proaktivnosti - proaktivnega iskanja informacij, sprejemanja odločitev in ukrepanja za doseganje svojih ciljev, za razliko od tradicionalnih modelov umetne inteligence, ki se odzivajo zgolj na vnose / zahteve.

Pri uvajanju UI se lahko srečujemo z različnimi stopnjami zmogljivosti sistemov umetne inteligence – od sistemov ozke umetne inteligence (angl. Artificial Narrow Intelligence, v nadaljevanju ANI) (Krieger in drugi, 2024), kot sta sistema osebnih asistentov Siri ali Alexa in priporočilni sistem Netflix, do sistemov, ki se bližajo splošni umetni inteligenci (AGI) (McLean in drugi, 2023), ki že znajo aplicirati znanje preko nejasno definiranih področij ukrepanja in odločanja. Za ocenjevanje tveganj je koristno vedeti, na kateri stopnji med obema tipoma se sistem, ki ga ocenjujemo, nahaja, kot tudi stopnjo njegove sposobnosti prilagajanja odzivov glede na zgodovino dialoga z uporabnikom. Na tem mestu le omenjam umetno superinteligenco (angl. Artificial Superintelligence - ASI), ki je v tem trenutku le hipotetična, a jo nekateri napovedujejo in bo v vseh pogledih presegala človeško inteligenco, vključno z ustvarjalnostjo, reševanjem problemov in čustveno inteligenco (Kim in drugi, 2024). V strokovni javnosti je zaznati tudi nasprotovanje temu pričakovanju. Nasprotniki pravijo (Findlay in drugi, 2024), da proporcionalna povezava med stopnjo inteligence in stopnjo zavesti (angl. consciousness) pri bioloških organizmih ne velja nujno tudi pri človeško ustvarjenih sistemih UI. Zato nasprotniki pravijo, da sistemi UI morda nikoli ne bodo sposobni zavestnega mišljenja. Opozarjajo, da sama sposobnost sistema UI, da oponaša delovanje človeške zavesti, še ne pomeni, da zavest dejansko poseduje.

2.1.1 Proces uvajanja umetne inteligence

Umetna inteligenca je vse bolj prisotna na področjih zdravstva pri diagnosticiranju, individualiziranih protokolih zdravljenja in razvoju novih zdravil, na področju financ pri odkrivanju zlorab, avtomatiziranega trgovanja in individualiziranja finančnih načrtov, na področju transporta pri zagotavljanju avtonomnega prevoza, upravljanju celovitih sistemov signalizacije in urejanja prometa ter na področjih podpore uporabnikom in usmerjanja v zabavno/informativne vsebine v realnem času. Vendar se tudi druge panoge soočajo z dilemo, kako v poslovanje vključiti pozitivne aspekte umetne inteligence, pri tem pa v čim večji meri izključiti njene negativne učinke (Nazar, 2021; Virvou, 2023).

Ti sistemi so lahko sestavljeni iz več posameznih agentov umetne inteligence, ki med seboj bolj ali manj sodelujejo in odražajo večjo ali manjšo mero avtonomnosti. Vpričo standardizacije med agentskega sodelovanja se avtonomni sistemi umetne inteligence več medsebojno sodelujočih agentov, ki ne potrebujejo človeškega posredovanja pri odločanju v realnem času, vse bolj približujejo komercialni uporabi na področjih podpore uporabnikom, odkrivanju internetnih groženj in postopkih avtonomnega sprejemanja odločitev v raznovrstnih poslovnih sistemih (Sapkota in drugi, 2025)

Že nameščeni sistemi umetne inteligence pogosto ne delujejo pravilno (Raji in drugi, 2022). Lahko delujejo naključno, so nameščeni ali integrirani neustrezno, ali pa so promovirani

zavajajoče. Avtorji opozarjajo, da se pri uvajanju sistemov UI namenja premalo pozornosti funkcionalnosti sistemov in spremljanju njihovih koristi, preveč pa zgolj tehničnemu in uredbeno - organizacijskemu vidiku uvedbe ter osredotočenju na etične vidike človeških vrednot.

Bankins in drugi (2024) opozarjajo na vse večjo integracijo UI v organizacijske prakse in procese, zaradi česar je razumevanje njenega vpliva na delavce in zasnovo delovnih mest ključnega pomena.

Po Bengio in drugi (2024) je trenutno obvladovanje tveganj pri uvajanju UI v podjetjih zelo oteženo. Praktična neizvedljivost obvladovanja tveganj je posledica trenutno nezadostno implementirane institucionalne zaščite uporabnikov UI in posledica nezagotavljanja odgovornosti velikih ponudnikov storitev UI za škodo, nastalo z uvedbo in uporabo njihovih storitev UI, z nejasno opredeljenimi tveganji.

Praktičen pristop k uvedbi UI je ponudila mednarodna razvojno svetovalna organizacija Gartner (Litan, 2024) v okviru njihovega modela AI TRiSM za upravljanje zaupanja, tveganj in varnosti UI (angl. Artificial Intelligence Trust, Risk, Security Management, v nadaljevanju tudi TRiSM). Napoveduje standardizacijo tovrstnega pristopa, njegovo prilagoditev podjetjem ter izboljšanje dostopnosti za podjetja, ki nimajo zadostnih lastnih virov za implementacijo predlaganega modela.

2.1.2 Tveganja umetne inteligence

Skupna značilnost raziskav tveganj v povezavi z umetno inteligenco je zbiranje in obdelovanje do nekaj let starih podatkov, kar vpričo izredno hitrega razvoja UI ne odraža nujno realnega stanja, s katerim se soočajo podjetja pri uvedbi in uporabi UI. Pogosto je možno in smiselno razbrati trenutno aktualne usmeritve iz strokovne literature.

Krieger in drugi (2024) npr. preučujejo tveganja, povezana z ANI in se fokusirajo na tri ključne dejavnike, ki vplivajo na percepcijo tveganja v zvezi z UI: občutek obvladovanja uporabniške izkušnje, zaupanje v UI in vzdrževanje zasebnosti. Ugotavljajo, da se rezultati zelo razlikujejo glede na spol in politično prepričanje preučevanih oseb ter da ni dovolj raziskano, kako ta percepcija nastaja in kaj nanjo vpliva.

McLean in drugi (2023) preučujejo tveganja, povezana z AGI in poudarjajo nezadostno obravnavo le teh v znanstveni in strokovni literaturi. Kot primere tveganj omenjajo predvsem neustrezno upravljanje AGI, neizključljivost možnosti, da se AGI sama umakne izpod nadzora človeških lastnikov/upravljavcev ter obstoj AGI z nevarnimi cilji ali z neustreznimi etičnimi merili in vrednotami.

Widinger in drugi (2021) kategorizirajo tveganja, povezana s sistemi UI, ki uporabljajo LLM, na: diskriminacijo, izključevanje in toksičnost, informacijske nevarnosti, škodo zaradi

dezinformacij, zlonamerno uporabo, škodo zaradi interakcije med človekom in računalnikom, vezano na specifičnost LLM in negativne posledice avtomatizacije delovnih mest in povzročene okoljske škode.

Razi in drugi (2025) pregledujejo zaupanje, tveganje in varnostni management več-agentskih sistemov umetne inteligence, temelječih na LLM modelih. Predlagajo specifično taksonomijo tveganj in dva nova kazalnika tveganosti: kazalnik kvalitete medagentskega sodelovanja (angl. Component Synergy Score - CSS) in kazalnik učinkovitosti rabe orodij v domeni sistemov samih (angl. Tool Utilization Efficacy – TUE). Preučujejo strategije, kako izboljšati razumljivost takšnih sistemov ter kako povečevati njihovo varnost skozi enkripcijske metode, odpornost na napade in skozi skladnost z zahtevami regulatornih organov in zakonodaje.

Wang in drugi (2023) opozarjajo na mnoga tveganja modelov GPT-4 in GPT-3.5, ki tako rekoč izključujejo njihovo uporabnost na področjih, ki predstavljajo velika tveganja za varnost ljudi, kot na primer zdravstvo, sodni postopki in finance. Opozarjajo na nevarne, škodljive in pristranske odgovore ter nevarnost iztekanja osebnih in privatnih informacij. Izpostavljajo, da novejša orodja v standardnih razmerah delujejo zanesljivejše, vendar so ranljivejša v primeru zlonamernih napadov.

Klyman (2024) je katalogiziral sprejemljive politike uporabe sistemov UI vodilnih desetih razvijalcev modelov UI. Ugotavlja pomembne razlike v pristopih k omejitvam vsebin povezanih npr. s politiko, prehranjevalnimi težavami, spolnimi navadami in usmeritvami, zdravniškimi nasveti, kakor tudi z omejitvami glede na namen uporabe, npr. za izdelavo ali uporabo orožja ter za nadzor nad ljudmi. Navaja tudi druge mehanizme, ki lahko omejujejo modele v smislu preprečevanja njihove škodljive uporabe: kaj model lahko dela in česa ne, kakšna je namenska uporaba modela, kakšne so omejitve uporabe modela ob uporabi API vmesnika (angl. Application Programming Interface) ter opredelitve odgovornosti tretjih oseb, kot so ponudniki storitev v oblaku, ponudniki podatkovnih baz in raznih internetnih platform. Vse te informacije so lahko koristen pripomoček pri ocenjevanju tveganj pri uvajanju posameznih modelov.

Poglobljena štiri-nivojska klasifikacija kategorij tveganj »The AIR Taxonomy« je bila izvedena na Kitajskem (Zeng in drugi, 2024). Z analizo osmih javnih politik oz. regulatornih dokumentov (med njimi iz Evropske unije, Združenih držav Amerike in Kitajske) in šestnajstih politik največjih ponudnikov storitev umetne inteligence iz privatnega sektorja so avtorji identificirali 314 kategorij tveganja. Izhajali so iz opredelitve tveganj v obstoječih dokumentih in regulativah, nastalih in določenih kot standard v javnem in privatnem sektorju po vsem svetu.

2.1.3 Dejavniki vpliva na tveganja

Na tveganja sistema umetne inteligence vpliva širok nabor dejavnikov, ki vključujejo tehnične značilnosti sistema, človeško interakcijo z njim, etične vidike ter širši družbeni in regulativni kontekst. Razumevanje teh dejavnikov je ključnega pomena za odgovorno načrtovanje, uvajanje in upravljanje sistemov UI (Bengio in drugi, 2024).

Med tehničnimi in sistemskimi dejavniki najdemo stopnjo razumljivosti delovanja algoritmov sistema UI, ki deluje kot črna škatla, in stopnjo razložljivosti njegovih posameznih odločitev (Mohseni in drugi, 2021). Med njimi se nahaja tudi stopnja kompleksnosti sistema UI, ki upošteva kompleksnost algoritmov posameznih UI agentov v sistemu, kakor tudi njihovo število in način njihove medsebojne povezanosti (Virvou, 2023). Med te dejavnike spada tudi velikost in ažurnost baze prednaučenega znanja (Virvou, 2023), stopnja odvisnosti delovanja sistema UI od baze prednaučenega znanja (Bengio in drugi, 2024), stopnja avtonomnosti sistema UI ter stopnja pomembnosti njegovih odločitev (Bengio in drugi, 2024). Pomembna je tudi stopnja povezanosti sistema UI z drugimi tehnološkimi in informacijskimi sistemi in stopnja posledičnega vpliva nanje.

Virvou (2023) opisuje dejavnike, povezane s podatki: zanesljivost in kvaliteto baze prednaučenega znanja, stopnjo elementov pristranskosti v prednaučenem znanju in njene transparentnosti, transparentnost delovanja sistema UI v situacijah brez ustreznega predznanja ter stopnjo varnosti pred kibernetskimi napadi na bazo predznanja. Al-Ansari in drugi (2024) dodajajo pomembnost stopnje varnosti osebnih in privatnih podatkov (ali se integrirajo v bazo prednaučenega znanja in, ali se shranjujejo, obdelujejo ali posredujejo brez vednosti lastnika).

Med človeškimi in organizacijskimi dejavniki se omenjajo: stopnja prekomernega zaupanja v odločitve sistema UI in stopnja resnosti potencialnih posledic (Ribera in Lapedriza, 2019), stopnja razložljivosti posameznih odločitev sistema UI z vidika uporabnika (Westphal in drugi, 2023), stopnja zadostnosti uporabniškega nadzora nad delovanjem sistema UI, stopnja ohranjanja lastništva nad akcijami in stopnja ohranjanja odgovornosti za posledicami teh akcij (Virvou, 2023), stopnja zmožnosti sodelovanja med sistemom UI in uporabnikom, stopnja prilagodljivosti razložljivosti odločitev sistema UI posameznemu tipu uporabnika, glede na njegove kognitivne sposobnosti in etične vrednote ter stopnja zrelosti organizacije, ki UI uvaja – v smislu digitalne pismenosti, v organizacijskem, strateškem in strokovnem smislu (Chowdhury in drugi, 2023).

Literatura našteva nekatere etične, zakonske in sociološko-kulturne faktorje, med drugimi stopnjo diskriminatornosti zaradi vgrajenih elementov pristranskosti (Virvou, 2023), stopnjo odgovornosti ponudnikov / razvijalcev sistemov UI za škodo, nastalo zaradi napačnih / nepravilnih / neustreznih / nezakonitih odločitev in akcij sistema (Bengio in drugi, 2024), stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in izven nje, ki bodo neposredno ali posredno čutili posledice delovanja sistema UI (Chowdhury in drugi,

2023), verjetnost uporabe sistema UI za nevarna dejanja, kot npr. njegova izraba za sisteme oboroževanja, množične manipulacije mnenj, nadzora nad ljudmi in kibernetskih napadov (Anderljung in drugi, 2024), stopnjo vpliva UI sistema na pravice in dolžnosti deležnikov (Bengio in drugi, 2024; Zeng in drugi, 2024) ter stopnjo zrelosti regulatornega okolja, kjer se sistem UI uvaja in uporablja (Zeng in drugi, 2024).

2.1.4 Razumljivost umetne inteligence

Na nekatere izmed naštetih dejavnikov vpliva na tveganja, ki jih navaja Rane in drugi (2024), še posebej vpliva razumevanje umetne inteligence. XAI se je uveljavila kot ključen ukrep za zagotavljanje razumljivosti delovanja algoritmov UI in kako algoritmi sprejemajo odločitve. S tem se povečuje zaupanje v UI. Pomembna je razumljivost celovitega delovanja UI sistema, kako je vpeto v poslovne procese podjetja ter kako in katere podatke uporablja. Pomemben je vidik poenostavitve postopka uporabe za ne-eksperte UI, kar pomeni, da uporaba UI sistema ne sme zahtevati nobenega tehničnega znanja. Odprta komunikacija v zvezi z omejitvami uporabe UI in potencialnimi pristranskostmi sistema UI ter izobraževanje uporabnikov sta ključni za njegovo pravilno in smotrno uporabo ter odpravljanje etičnih dilem.

2.1.5 Ukrepi v procesu uvajanja, ki vplivajo na tveganja

Med uvedbo sistema umetne inteligence lahko različni ukrepi pomembno vplivajo na nekatera tveganja, zlasti tista, ki izhajajo iz slabo razumljene UI. Ti ukrepi so usmerjeni k izboljšanju preglednosti, zagotavljanju odgovornosti in zmožnosti uravnavanja dejanskega delovanja UI ter interakcije z uporabniki.

Čeprav verjetnost dogodkov, povezanih z večino tveganj, nastopi šele v pouvedbeni fazi, se jih z vidika podjetij, ki UI uvajajo, lahko ocenjuje že v uvedbeni fazi (Slattery in drugi, 2024).

Sherman in Eisenberg (2024) sta predlagala standardizirano preduvedbeno razkritje tveganj, kar bi odločevalcem omogočalo lažjo primerjavo različnih ponudnikov in izvedbo analize tveganj in koristi. Predlagala sta opredelitev tveganj glede na: skladnost, robustnost uporabe, zaupnost, poštenost in nepristranskost, razumljivost in transparentnost, varnost, okoljske in družbene vplive, dolgoročna eksistencialna tveganja ter zlonamerno in nenamensko uporabo sistema.

Kot že pojasnjeno (Bengio in drugi, 2024), je trenutno obvladovanje tveganj pri uvajanju UI v podjetjih zelo oteženo. Uporabniki UI so zaradi tega na neki način prepuščeni širše družbenim institucionalnim ukrepom sistematičnega vlaganja v raziskave varnosti umetne inteligence in strategij blaženja njenih negativnih učinkov. Dodatno si podjetja lahko pomagajo le z morebitnimi nestandardiziranimi orodji oz. storitvami ponudnikov UI:

- za izboljšanje razumevanja in zaupanja uporabnikov ter omogočanje nadzora uporabe UI s pomočjo razložljive umetne inteligence,
- za izboljšanje nadzora odločanja za uporabnike pri spreminjanju priporočil UI,
- za osredotočenost uporabniškega vmesnika UI na človeka, s tem, da se zna prilagajati osebnim potrebam, vrednotam in dobremu počutju posameznika,
- za upravljanje izmenjave podatkov med uporabniki in UI ter zmanjšanje pristranskosti,
- za implementacijo strogih metodologij za oceno tveganj in upravljanje varnostnih incidentov,
- za vzpostavitev sistemov odgovorne umetne inteligence, ki zagotavljajo preglednost, odgovornost in spremljanje etičnih vidikov v celotnem življenjskem ciklu umetne inteligence,
- za upoštevanje konteksta uporabe in ciljne publike pri načrtovanju in vrednotenju sistemov umetne inteligence ter njihovih razlag v domeni uporabnikov in ne zgolj v domeni ponudnikov storitev UI.

Odgovor na zahtevo po obravnavi tveganj v povezavi z uvedbo in uporabo UI je npr. ponudila mednarodna organizacija Gartner (Litan, 2024) v okviru njenega modela AI TRiSM za upravljanje zaupanja, tveganj in varnosti UI. Zaveda se, da so organizacije pogosto slabo pripravljene za uvajanje UI in da se lahko zdi celovito upravljanje UI za organizacije preobremenjujoče. Predlaga primerjavo teh obremenitev s tveganji potencialnega neuspeha projektov uvajanja UI in povezanimi varnostnimi, finančnimi in reputacijskimi škodami. Opozarja na pomanjkljivo obravnavo tveganj ob uvajanju UI in težavno naknadno vključevanje ustreznih ukrepov v že uvedene delovne tokove umetne inteligence. Njen model glede na raziskavo Habbal in drugi (2024) zagotavlja zmanjšanje tveganja, izboljšane ukrepe za spremljanje modelov odločanja UI, zaščitne ukrepe pred tveganji zaradi vključenosti tretjih oseb v razvoj, uvajanje in vzdrževanje UI, zaščitne ukrepe pred zlonamernimi napadi, nevarnimi, netočnimi, ali neželenimi rezultati UI ter zaščitne ukrepe pred nepooblaščenimi dostopi do funkcionalnosti in dostopi do vhodno / izhodnih podatkov sistema UI.

Gartner napoveduje širitev na tri ključna področja:

- agentski nadzor umetne inteligence na avtonomni ravni,
- uveljavitev TRiSM z umetno inteligenco kot storitev na tržišču - pojavile se bodo storitve TRiSM za podporo malim in srednje velikim podjetjem, ki nimajo zadostnih lastnih virov,
- konsolidacijo trga in inovacije - zagotavljanje, da bo uvajanje in nadgrajevanje umetne inteligence postalo standardizirano in varno, zaupanja vredno in skladno s predpisi.

V letu 2025 je Gartner dodal priporočila naslednjih opredelitev sistema UI v praksi, ki zagotavljajo skladnost s cilji organizacije in regulatornimi predpisi ter zagotavljajo varnost in zanesljivost sistemov UI:

- katalog UI - popis vseh entitet umetne inteligence (modelov, agentov in aplikacij),
- mapiranje podatkov UI - podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI,
- neprestani monitoring nemotenega delovanja sistema, njegove zanesljivosti in varnosti,
- nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v realnem času.

2.2 Deležniki v sistemih umetne inteligence

Literatura obravnava različne vrste deležnikov v sistemih umetne inteligence, pri čemer prepoznava njihove raznolike vloge in pričakovanja ter različne ranljivosti, s katerimi se soočajo v povezavi z umetno inteligenco. Razumevanje teh različnih skupin deležnikov je ključnega pomena za spodbujanje sprejemanja in zagotavljanje odgovornega razvoja in uvajanja umetne inteligence (Ribera in Lapedriza, 2019).

Razčlenjevanje deležnikov sistemov UI na skupine v znanstveni literaturi je raznovrstno. Vsem delitvam pa je skupno uskupinjenje glede na skupinsko percepcijo uporabnosti UI, enostavnosti uporabe UI in stopnje zaupanja vanjo. Glavne skrbi vseh skupin so razumljivost in transparentnost odločitev UI, zaupnost izmenjevanja informacij s sistemom, njegova zanesljivost in uporabnost ter njegov vpliv na širšo skupnost (Reis in drugi, 2025).

Znotraj skupine končnih uporabnikov literatura posebej obravnava eksperte aplikativnih, strokovnih in poslovnih področij (v nadaljevanju domenski specialisti), ki značilno pomagajo oblikovati bazo znanja sistema UI in bolj pogosto sodelujejo pri revidiranju stopnje vplivnosti in področij odločanja sistema UI ter pri usmerjanju delovanja samega sistema (Al-Ansari in drugi, 2024; Reis in drugi, 2025; Ribera in Lapedriza, 2019).

Posebna skupina deležnikov sistema UI so eksperti UI, ki lahko s svojim znanjem pomagajo pri uvajanju UI oz. pomagajo ostalim deležnikom z razlago tehničnih možnosti in omejitev delovanja sistema UI (Al-Ansari in drugi, 2024; Reis in drugi, 2025; Ribera in Lapedriza, 2019).

Skupina deležnikov, ki niso direktni uporabniki sistema UI, so pa deležni učinkov njegovega delovanja, bodisi preko ekonomskih učinkov sistema na organizacijo, v kateri delajo, ali pa preko reorganizacije delovanja organizacije, ukinjanja delovnih mest itd., pogosto gledajo na sistem UI iz drugačne perspektive kot uporabniki UI. Tudi pogled te skupine je pomemben pri razumevanju in ocenjevanju tveganj sistema UI in njegovega vpliva na širše okolje (Butler in drugi, 2021).

Pri uvajanju nekega sistema UI seveda igrajo eno ključnih vlog tudi zakonodajalci in skrbniki regulatornih mehanizmov. Čeprav niso neposredni uporabniki sistema UI, pa so vsi ostali deležniki deležni usmeritev, omejitev in tveganj v povezavi z njihovim neupoštevanjem oz. neobravnavanjem na regulativni ravni (Krook in drugi, 2025).

V tem delu se omejujem le na tiste skupine deležnikov, ki pri odločanju o uvedbi nekega sistema UI v podjetju lahko neposredno sodelujejo. To so splošni uporabniki sistema UI ali deležniki, ki bodo posredno ali neposredno zgolj čutili posledice delovanja UI, domenski specialisti, eksperti informacijske tehnologije in eksperti UI. Te skupine so neodvisne od dejavnosti, s katero se podjetje ukvarja.

2.2.1 Sprejemanje umetne inteligence

Nagnjenost k sprejemanju umetne inteligence se nanaša na pozitiven odnos in pripravljenost uporabnikov, da sprejmejo, komunicirajo in integrirajo sisteme umetne inteligence v svoje vsakdanje življenje in delo. Pomeni prepričanje uporabnikov o uporabnosti, verodostojnosti in enostavnost uporabe umetne inteligence, kar vodi do njihovega namernega sprejetja in celo nakupa orodij in storitev, ki jih poganja umetna inteligenca. Nagnjenost uporabnikov k sprejemanju UI temelji na njihovi percepciji, da UI znatno izboljša njihovo učinkovitost in produktivnost, da prispeva h kolektivnemu napredku ter da je enostavna in intuitivna za uporabo. Z drugimi besedami, uspešno sprejemanje UI lahko pomeni uravnoteženost inovacij z družbeno blaginjo (Rane in drugi, 2024).

2.2.2 Dejavniki, ki vplivajo na sprejemanje umetne inteligence

Po Rane in drugi (2024) obstajajo ključni dejavniki, ki vplivajo na sprejemanje umetne inteligence v organizacijah. Stopnja njihovega vpliva / uveljavitve / realizacije v organizaciji hkrati odraža sprejemljivost UI:

- Tehnična infrastruktura predstavlja osnovo za učinkovito rabo UI – zagotavlja ustrezno hitrost in zmogljivost sistema UI.
- Dostopnost in kvaliteta podatkov določa zmogljivost učenja in odločanja.
- Izredna hitrost razvoja algoritmov UI terja odprtost sistema UI za posodabljanje.
- Podpora vodstva in odločevalcev v podjetju je ključna za pravočasno in pravilno uporabo UI ter pozitiven odnos do nje.
- Prilagodljivost organizacije poslovanja in sposobnost izrabe ter vključevanja novih tehnoloških rešitev v vsakodnevne dejavnosti sta pomembni, saj uporaba UI terja neprestano prilagajanje obstoječih in utečenih postopkov. Pomembna je stopnja integrabilnosti UI z obstoječimi sistemi. Zraven tega spada tudi ustrezna komunikacija med deležniki in njihovo usposabljanje za uporabo UI.
- Usklajenost iniciativ UI s strategijo in cilji podjetja zagotavlja optimizacijo razpoložljivih virov pri doseganju zastavljenih ciljev.
- Izdelava analize tveganj in koristi pri uvajanju umetne inteligence je nujna zaradi potencialno velikega CAPEX-a (angl. Capital Expenditure) in OPEX-a (angl. Operating Expenditure) in pri zagotavljanju pričakovane stopnje donosa (angl. Return on Investment, v nadaljevanju ROI).

- Afiniteta organizacij v branži za uporabo UI je lahko ključni motivacijski vzgib za uvedbo UI pri vseh konkurentih v branži.
- Pozitivna percepcija uporabnosti UI in zaupanje vanjo iz strani deležnikov zmanjša tveganje za neuspešno uvedbo in njeno operativno rabo.
- Tudi kultura sprejemanja tehnoloških novosti je pomembna pri uspešnosti uvedbe UI.
- Skladnost z zakonsko regulativnimi zahtevami in sledenje uveljavljenim in standardiziranim postopkom uvedbe UI zmanjšuje tveganja njene uvedbe.
- Nepristranskost in poštenost UI sta ključni za zagotavljanje etično sprejemljivih rezultatov sistema UI in nediskriminatorno delovanje UI.
- Standardizacija uporabe UI lahko poveča njeno sprejemljivost.
- Transparentnost in razložljivost algoritmov UI ter transparentnost rezultatov / izhodov / akcij sistema UI povečujeta opredeljivost stopnje zanesljivosti, točnosti in predvidljivosti UI.
- Določljivost odgovornosti in vlog posameznikov v zvezi s posledicami delovanja UI je bistvena v postopku preprečevanja škode in pri odpravljanju posledic škode zaradi učinkov sistema UI.
- Gradnja veščin in sistem neprestanega učenja uporabnikov utrjujeta uporabnost UI.
- Uporabniška izkušnja oz. enostavnost uporabe lahko vpliva na sprejetje UI.

2.2.3 Metode in orodja, ki vplivajo na sprejemanje umetne inteligence

Na sprejemanje in uporabo sistemov umetne inteligence vpliva večplasten nabor ukrepov, osredotočenih predvsem na izboljšanje zaupanja uporabnikov, razumevanja in splošne izkušnje. Uspešna integracija UI v vsakdanje življenje in v organizacijske delovne procese zahteva osredotočenost na več ključnih področij.

Prisotnost sistemov XAI pri delovanju sistema UI omogoča, da so procesi odločanja in logika UI razumljivi končnim uporabnikom. Ta pojasnila uporabnikom omogočajo razumevanje obdelave podatkov in opozarjajo na morebitne pristranskosti ali sistemske napake (Mohseni in drugi, 2021). To omogoča znatno krepitev zaupanja v sistem UI (Krook in drugi, 2025).

Učinkovitost pojasnil je lahko odvisna od tega, ali so ustrezno zasnovana za določenega uporabnika, saj lahko slabo zasnovana pojasnila povečajo zaznano kompleksnost naloge in potencialno škodujejo uporabnikovim rezultatom. Pojasniti ali utemeljiti morajo priporočila in prepričati uporabnike, da jih upoštevajo, zato morajo biti prilagojena posamezni skupini uporabnikov. Možnost prilagajanja ali spreminjanja priporočil sistema umetne inteligence na podlagi uporabniških mnenj pozitivno vpliva na uporabnikovo zaznavanje zaupanja in razumevanja sistema UI, zato je priporočljiva vključenost človeške / uporabniške vloge pri uravnavanju sistema UI (Westphal in drugi, 2023).

Al-Ansari in drugi (2024) poudarjajo pomembnost uporabniško usmerjenega pristopa pri zagotavljanju uporabnosti in sprejemljivosti sistema UI, kar vključuje fokusiranje na enostavne in intuitivne uporabniške vmesnike, prilagojene vsakemu tipu uporabnika.

Zmanjšanje pristranskosti in zagotavljanje pravičnosti v sistemih UI sta ključna za vzpostavitev zaupanja v njihove rezultate. Pristranskost lahko izvira iz algoritmov, vhodnih podatkov ali celo inherentnih vrednot razvijalcev (Virvou, 2023).

Obstoj preventivnih ukrepov in deklaracija skladnosti z veljavno regulativo iz strani razvijalcev sistemov UI, je običajno zagotovilo za preprečevanje diskriminacije in za skladnost z etičnimi merili. Zagotavljanje učinkovitosti, pravilnosti in velike zmogljivosti sistema UI povečuje zaupanje v sistem (Virvou, 2023).

Organizacije morajo poleg tehničnega znanja krepiti razvoj človeških veščin in kompetenc, vodenja, koordinacije ekip in strategije upravljanja v luči priložnosti, ki jih UI prinaša in nasploh preveriti stanje zrelosti organizacije za uporabo UI (Butler in drugi, 2021).

Zelo pomembna je jasna komunikacija strategije uvajanja UI v organizaciji, tako da vsi deležniki lahko razumejo potencialne posledice njene uvedbe, kar je še posebej pomembno, če UI prinaša reorganizacijo del ali potrebo po dodatnem usposabljanju zaposlenih v kombinaciji z ukinjanjem določenih delovnih mest. Ob tem je potrebno poudarjati dobrobiti, ki jih prinaša sistem UI (Virvou, 2023).

Da bi v organizacijah znali bolje ocenjevati razmerje med koristmi UI za povečanje učinkovitosti in produktivnosti na eni strani in zaskrbljenostjo glede morebitne škode za delavce in druge deležnike na drugi strani, se predlaga razdelitev tega postopka na obravnavo več skupin individualnih, skupinskih in organizacijskih dejavnikov, ki determinirajo odnose med človeško delovno silo in UI (Bankins in drugi, 2024): (1) sodelovanje med človekom in UI; (2) dojemanje algoritmičnih in človeških zmogljivosti; (3) odnos delavcev do UI; (4) UI kot nadzorni mehanizem pri algoritmičnem upravljanju dela na informacijskih platformah; in (5) posledice uporabe UI za trg dela. Avtorji opisujejo pet smeri prihodnjih raziskav v zvezi s tem:

- raziskovanje izrabe UI za zagotavljanje zadovoljstva in blaginje za delavce,
- raziskovanje dizajniranja učinkovitega sodelovanja med ljudmi in UI,
- raziskovanje vodstvenih pristopov pri uvajanju, ki bi maksimirali dobrobiti in minimizirali slabosti uvedbe UI,
- raziskovanje izrabe UI za promocijo poštenosti v delovnih procesih in poštenosti udeležbe v pozitivnih rezultatih uporabe UI,
- raziskovanje celovitega vpliva UI na organizacije.

Bankins in drugi (2024) ponujajo praktična priporočila za organizacije, ki uvajajo tehnologije UI, na:

- individualni ravni: pozitivna sporočilnost vodstva, nudenje pomoči pri uporabi UI,
- skupinski ravni: ugotavljanje in prioritiziranje delovnih postopkov, ki so najprimernejši za uporabo UI, ugotavljanje skupin in posameznikov, ki bodo priložnosti UI najbolje izkoristili,
- organizacijski ravni: iskanje komplementarnih priložnosti za UI, oz. izogibanje konkurenčnim priložnostim UI z vidika delavcev; omogočanje razširjanja zmogljivosti in znanja delavcev s pomočjo UI.

Na sprejemanje UI torej vpliva množica dejavnikov, ocena tega sprejemanja pa lahko temelji na različnih merilih in metodah ocenjevanja, ki merijo tako neposredno percepcijo sprejemanja UI iz strani deležnikov in navade obnašanja deležnikov, kot tudi temeljne lastnosti sistema samega. Ta merila so ključna za razumevanje, ali so sistemi UI ne le učinkoviti, ampak tudi zaupanja vredni in sprejeti s strani uporabnikov. Za ocenjevanje teh meril (v nadaljevanju tega poglavja so označeni med narekovaji) se lahko uporabljajo ankete, vprašalniki, intervjuji in meritve sprememb uspešnosti in učinkovitosti delovnih postopkov, na katere UI vpliva. V fazi uvajanja UI pa se lahko uporabljajo tudi prototipne rešitve in meritve uporabnosti. Nekatere izmed teh metod se lahko uporabijo tudi za statistično obdelavo vzorcev uporabe funkcionalnosti informacijskega sistema v povezavi z uporabo UI.

Westphal in drugi (2023) raziskujejo, kako »stopnja uporabniškega vpliva na delovanje sistema UI in na njegove izhode« povečuje »željo po sodelovanju in uporabi UI«. Povzemajo pomembnost sočasnega kultiviranja »percepcije zaupanja v UI« (ne nezaupljivosti, a hkrati ne prevelike zaupljivosti), »percepcije razumljivosti odločitev UI«, kakor tudi »percepcije, kako sam sistem razložljivosti UI deluje« (npr. ponazoritev delovanja z nevronskimi mrežami). Opozarjajo, da je pomembno spremljanje in uravnavanje »stopnje uporabniške kritičnosti do posameznih rezultatov« oz. priporočil UI. »Percepcija enostavnosti uporabe UI« in »percepcija uporabnosti UI« se lahko posredno določata preko merila »stopnje povečane zahtevnosti vsakodnevnih nalog zaradi vključitve UI« v kombinaciji s »stopnjo povečane produktivnosti posameznih nalog in delovnih mest zaradi vključitve UI«.

Virvou (2023) opozarja na možni razkorak med percepcijo uporabniške izkušnje (ki jo lahko opredeljujejo našteta merila) in dejansko stopnjo zanesljivosti, uporabnosti in nepristranskosti sistema UI.

Wongso in drugi (2025) so raziskovali uporabniško usmerjen pristop pri razvijanju sistemov UI, ki po uvedbi sistema zagotavlja večjo »stopnjo skladnosti delovanja posameznih uporabnikov s sprejetimi dogovori« ter večjo »odpornost na zavračanje sodelovanja«, večjo »stopnjo vključenosti UI v vsakodnevne naloge uporabnikov« in »tendenco rasti znanja uporabe UI med uporabniki UI«.

Objektivnejši merili sta lahko »stopnja povečane produktivnosti posameznih nalog in delovnih mest zaradi vključitve UI« in »stopnja donosa zaradi uporabe UI« (Mikalef in

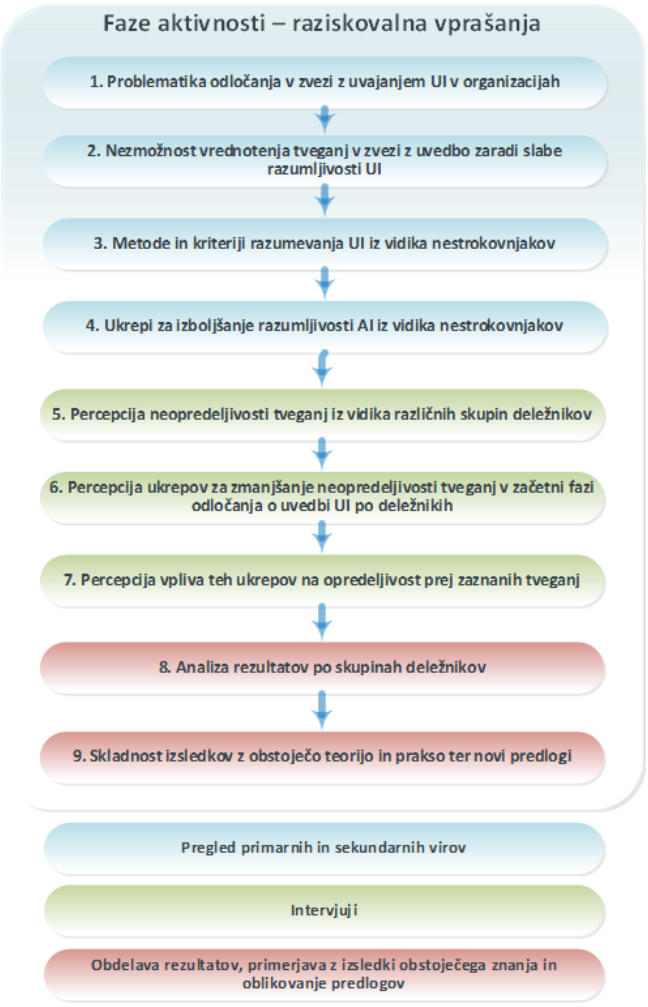
Gupta, 2021).

»Detekcija ali odprava obstoječih ter prijava novih pristranskosti in diskriminacij« lahko prispeva k sprejemljivosti sistema UI, kakor tudi »stopnja ohranjanja uporabniškega lastništva nad nalogami«, kjer si uporabniki pomagajo z UI, ter hkrati »stopnja ohranjanja uporabniške odgovornosti za rezultate svojih nalog« (Mohseni in drugi, 2021). Pomembni merili sta »ali je sistem UI v celoti skladen z regulativo v določeni jurisdikciji« (Zeng in drugi 2024), npr. z GDPR in, »ali so tveganja in postopki njihove mitigacije ter odprave posledic škode obravnavani in zasledovani« (Mohseni in drugi, 2021).

3 METODOLOGIJA

Magistrsko delo temelji na pregledu strokovne in znanstvene literature iz področja obravnavane teme, na izvedbi strukturiranih intervjujev ter analizi njihovih rezultatov. Vrstni red raziskovalnih dejavnosti je prikazan na sliki 1.

Slika 1: Diagram poteka raziskovalnih aktivnosti



Vir: lastno delo.

Opis raziskovalnih faz:

Prvi sklop (točke od 1 do 4 na sliki 1): z opisno metodo sem pristopil k teoretičnemu ozadju magistrskega dela, pri čemer sem preučeval predvsem primarne vire s področij:

- tveganj, povezanih s sistemi umetne inteligence,
- vidikov različnih deležnikov v sistemih umetne inteligence,
- dejavnikov, ki vplivajo na tveganja, povezana s sistemi umetne inteligence,
- dejavnikov, ki vplivajo na preglednost in razumljivost sistemov umetne inteligence,
- dejavnikov, ki vplivajo na povečevanje zmožnosti vrednotenja tveganj v zvezi z uvedbo zaradi slabe razumljivosti UI,
- interakcije med človekom in umetno inteligenco,
- možnosti predstavitve rezultatov/zmožnosti umetne inteligence,
- uvajanja sistemov umetne inteligence,
- ukrepov v procesu uvajanja sistemov umetne inteligence, ki vplivajo na njeno razumljivost in zmanjšanje tveganj, oz. na zmožnost ocenitve tveganj.

Drugi sklop (točke 5, 6 in 7 na sliki 1): na podlagi ugotovitev iz 1. sklopa sem izvedel začetne intervjuje med različnimi vrstami deležnikov:

- strokovnjaki za umetno inteligenco,
- strokovnjaki za informacijske tehnologije z malo znanja o umetni inteligenci in
- strokovnjaki za poslovna področja.

Vse štiri vrste deležnikov so razdeljene v dve skupini (odločevalci in ne-odločevalci – ne-odločevalci so tisti, ki se odločajo le v okviru svojih aktivnosti in nalog v poslovnih procesih) in ne morejo neposredno vplivati na uporabo umetne inteligence v drugih aktivnostih podjetja ali na organizacijske odločitve/naložbe v zvezi z uporabo umetne inteligence.

Število in nabor intervjujev je sledilo zahtevam za dosego saturacije, ki naj bi bila dosežena v prvih dvanajstih intervjujih (Guest in drugi, 2006).

Med intervjuji sem zastavljal vprašanja (podrobno so navedena v prilogi 1) in veliko pozornost posvečal njihovi razumljivosti pri intervjuvancih. Odgovore sem shranjeval v strukturirano obliko. Nekateri intervjuvanci so odgovore zapisovali sami v smislu izpolnjevanja ankete. Način podajanja odgovorov so si izbrali sami. Nove ideje, ki so se pojavile v času izvajanja začetnih intervjujev, sem sproti vključeval v intervjuje in naknadno začetne intervjuvance prosil, da so se opredelili tudi do njih.

Tretji sklop (točki 8 in 9 iz slike 1): z metodo primerjave in združevanja sem oblikoval ugotovitve in zaključke raziskave, preveril skladnost izsledkov z obstoječo teorijo in prakso ter oblikoval nove predloge.

3.1 Metodološki pristop

Iz obstoječe literature sem povzel pogosto obravnavane vrste tveganj v zvezi z uvedbo sistema umetne inteligence, v zvezi z informacijami in dejavniki, ki lahko pomagajo pri analizi teh tveganj in v zvezi z metodami in postopki, ki lahko pomagajo organizaciji povečevati obvladovanje sistema umetne inteligence, in s tem tudi povečevati obvladovanje tveganj samih.

Na podlagi tega sem pripravil strukturo intervjujev (prikazano v prilogi 1), ki sem jo v postopku intervjujev nato neposredno predstavil intervjuvancem in jim jo predložil v izpolnjevanje (ali sem beležil njihove odgovore sam), ob izpolnjevanju ali odgovarjanju pa jim je bilo na voljo tolmačenje pomena vprašanj, tako da sem zagotovil veliko stopnjo skladnosti razumevanja problematike med vsemi intervjuvanci. Na to strukturo vprašanj sem sam beležil dodatna pojasnila in komentarje intervjuvancev. Nekatera vprašanja v anketnem delu intervjujev so bila na podlagi nekaj že izvedenih intervjujev dodana, zato sem s temi vprašanji naknadno soočil tiste intervjuvance, ki jih med intervjujem še niso obravnavali.

Med intervjuji sem beležil tudi odzive intervjuvancev, ki niso bili neposredno vezani na strukturiran / »anketni del« intervjujev. Ker so bila oblikovana šele med intervjuji samimi, nanje niso odgovarjali vsi intervjuvanci sproti, mi je pa uspelo naknadno pridobiti odgovore nanje od večine intervjuvancev.

V poglavju 3.2 je opisana struktura intervjujev, ki je predstavljala tudi osnovo za uporabo primerjalne metode preučevanja rezultatov intervjujev. Iz rezultatov intervjujev sem oblikoval povzetke in jih povezal s karakteristikami intervjuvancev ter oblikoval zaključke.

3.1.1 Omejitve

Zaradi ravnanja z občutljivimi podatki podjetij v tem raziskovalnem delu obstajajo določene omejitve, ki sem jih moral vnaprej sprejeti: nimam pravic za razkritje imen organizacij ali oseb, povezanih s to raziskavo. Le tako sem lahko pridobil dovoljenja za intervjuje in pridobil dovolj podatkov za izvedbo raziskave.

3.2 Kvalitativna raziskava - intervjuji

Skupno 28 intervjujev je potekalo z različnimi vrstami deležnikov v 13 organizacijah v Sloveniji in v Švici. Pri tem je posamezni intervjuvanec bil lahko hkrati potencialni uporabnik umetne inteligence v različnih vlogah – npr. kot strokovnjak umetne inteligence (oznaka A), kot strokovnjak informacijske tehnologije (v nadaljevanju IT) (oznaka a), kot domenski strokovnjak (oznaka B) in kot laični uporabnik (oznaka C). Ker me je zanimala razlika med intervjuvanci brez poglobljenega znanja o informacijski tehnologiji ali umetni inteligenci in ostalimi, sem prve označil z vrsto deležnika »B«, ostale pa z oznako »A«, če

so strokovnjaki za UI, oz. z oznako »a«, če niso. Ob upoštevanju tega je bila struktura intervjuvancev naslednja:

- 4 intervjuji / od tega z 2 neposrednima odločevalcema: s strokovnjaki za umetno inteligenco (A),
- 8 intervjujev / od tega s 4 neposrednimi odločevalci: s strokovnjaki za informacijske tehnologije z malo znanja o umetni inteligenci (a),
- 16 intervjujev / od tega s 7 neposrednimi odločevalci: s strokovnjaki za poslovna področja – z domenskimi specialisti (B).

Če pa se upoštevajo vse oznake posameznega deležnika (hkrati je lahko npr. strokovnjak za UI in domenski specialist itd.), potem je struktura vrste intervjuvancev naslednja:

- 4 strokovnjaki za umetno inteligenco,
- 12 strokovnjakov za informacijske tehnologije,
- 23 strokovnjakov za poslovna področja,
- 28 laičnih uporabnikov umetne inteligence.

Intervjuji so potekali v različnih vrstah organizacij. Število deležnikov in vrste deležnikov (najvišja hierarhična oznaka posameznega intervjuvanca) so podani v oklepajih. Informacije so podane v parih, ločenih z vejico – prva oznaka v paru opredeljuje vrsto deležnika, druga oznaka - za poševnico, pa število intervjuvancev:

- Organizacija - razvijalec in promotor umetne inteligence (A/2, B/2)
- Ponudnik storitev umetne inteligence (A/1, a/1)
- Razvijalec programske opreme in ponudnik storitev informacijskih tehnologij z malo znanja o umetni inteligenci (a/2, B/3)
- Mednarodno združenje kot uporabnik umetne inteligence z nekaj strokovnega znanja o umetni inteligenci (A/1, B/2)
- Vodilni nacionalni ponudnik v komercialnem, nepremičninskem in urbanem razvoju v vlogi uporabnika umetne inteligence z nekaj strokovnega znanja o umetni inteligenci (a/1, B/2)
- Nacionalni kulturni center kot uporabnik umetne inteligence z malo strokovnega znanja o umetni inteligenci (B/1)
- Proizvajalec v živilski industriji, močno vpleten v vertikalno globalno prehransko verigo kot uporabnik umetne inteligence z malo strokovnega znanja o umetni inteligenci (a/1, B/1)
- Nacionalno logistično podjetje, integrirano v globalni logistični konglomerat kot uporabnik umetne inteligence z nekaj strokovnega znanja o umetni inteligenci (a/1, B/1)
- Pomemben nacionalni proizvajalec in distributer električne energije v vlogi uporabnika umetne inteligence z nekaj strokovnega znanja o umetni inteligenci (B/1)
- Mala podjetja kot uporabniki umetne inteligence brez strokovnega znanja o umetni inteligenci (a/2, B/3)

Intervjuji so obravnavali dva hipotetična primera uvedbe sistema umetne inteligence, ki zajemata dva različna pristopa organizacij:

- uvedbo komercialno dostopnih sistemov UI velikih svetovnih ponudnikov. V ta namen je bila uporabljena hipotetična implementacija MS Copilota, ki lahko pomaga pri delu posameznikom / delu organizacije / ali celotne organizacije,
- uvedbo sistemov agentske UI, pri kateri lahko sodelujejo tudi manjši ponudniki UI storitev. V ta namen je bila uporabljena hipotetična implementacija sistema UI, ki bo vsako jutro za vsakega uporabnika pripravljal seznam potrebnih opravil, urejenih po pomembnosti.

Vprašanja (priloga 1) so se osredotočala na vidik malih in srednjih podjetij, ki običajno ne premorejo strokovnjakov za umetno inteligenco, se pa odločajo, ali bodo uvedli funkcionalnost umetne inteligence ali ne. Vprašanja so bila povezana s sposobnostjo organizacije intervjuvanca za ocenjevanje tveganj, kar bi ji omogočalo opravljanje analize tveganj in koristi ter omogočalo odločanje, ali nadaljevati z uvedbo ene ali druge predlagane funkcionalnosti umetne inteligence.

Začetni del vsakega intervjuja s štirimi vprašanji (priloga 1) je bil splošne narave in je služil karakterizaciji intervjuvanca. Intervjuvanec je bil seznanjen s postopkom. Izbral je, ali bo vprašalnik izpolnjeval sam ali le podajal ustne odgovore. Sledil je intervju iz petih delov (priloga 1): prvi trije deli s po dvema vprašanjema so obravnavali tveganja in s tem povezane sposobnosti ocenjevanja, četrti del z dvema vprašanjema se je dotikal dodatnih dejavnikov, orodij in informacij, ki bi lahko organizaciji pomagali pri ocenjevanju tveganj, peti del s štirimi vprašanji pa je obravnaval potencialne ukrepe, ki lahko pomagajo nestrokovnjakom pridobiti relevantne informacije ali zagotavljajo vpliv na dejavnike tveganja, ter je obravnaval percepcijo intervjuvanca, v kolikšni meri bi lahko obravnavani posamezni ukrepi pomagali pri sposobnosti ocenjevanja tveganj.

Nekateri deli intervjuja so bili sestavljeni iz dveh delov – iz prvega dela brez sugestij in predlogov in iz drugega dela, kjer je intervjuvanec bil zaprošen za opredelitev do podanih predlogov, vprašanj in sugestij.

Zadnji dve vprašanji petega dela intervjuja sta bili zastavljeni tako, da sta obravnavali dve virtualni situaciji:

- ko lahko organizacija pri uvedbi UI popolnoma zaupa razpoložljivemu strokovnemu znanju o umetni inteligenci,
- ko pri uvedbi UI organizacija ne more povsem zaupati razpoložljivemu strokovnemu znanju o umetni inteligenci.

Poleg zbiranja odgovorov na opisano strukturo intervjujev sem v analizo vključil tudi nekatera druga vprašanja, na katera sem pridobil odgovore od več kot polovice intervjuvancev (našteta so na koncu priloge 1).

4 REZULTATI

Rezultati intervjujev so podani v tabelah v nadaljevanju, vsi podrobni rezultati intervjujev pa se nahajajo v prilogi 2. Rezultati vseh intervjujev so opremljeni z deskriptivnimi oznakami intervjuvancev, ki služijo za nadaljnjo analizo po skupinah intervjuvancev.

- Vrsta intervjuvanca:
  - UI strokovnjak – oznaka A,
  - IT strokovnjak – oznaka a,
  - Domenski strokovnjak – oznaka B,
  - Laični uporabnik UI – oznaka C.
- Odločevalec (oznaka 1), soodločevalec – udeleženec odločanja (oznaka 2) ali neodločevalec (oznaka 3) o uvedbi / implementaciji UI.
- Ali intervjuvanec je (oznaka 1), ali še ni (oznaka 2) implementiral UI funkcionalnosti v privatnem ali profesionalnem življenju?
- Stopnja seznanjenosti z analizo tveganja pri uvajanju, razvoju ali implementaciji sistemov:
  - Redna uporaba analize (oznaka 1),
  - Občasna uporaba analize (oznaka 2),
  - Ne izvajam analize, a sodelujem pri njej (oznaka 3),
  - Sem seznanjen s postopkom, a ga ne izvajam in ne sodelujem (oznaka 4),
  - Nisem seznanjen s postopkom analize (oznaka 5).

Zbrani rezultati po skupinah so prikazani v poglavju 4.2 (Navzkrižna primerjava rezultatov).

4.1 Analiza odgovorov intervjuvancev

Rezultate anketnega dela intervjujev, ki so urejeni po opisanih sklopih vprašanj v prilogi 1, prikazujejo tabele v tem poglavju. Vprašanja so zapisana med narekovaji.

1. del: Identifikacija tveganj

Vprašanje A1: »Katera tveganja (poleg samega tveganja uvajanja) morate upoštevati pri razmišljanju o uvajanju funkcionalnosti umetne inteligence (eden od dveh opisanih primerov)?«.

Namen tega vprašanja je bil zaznati morebiten vidik tveganj, ki jih v intervjuje še nisem vključil, preveriti seznanjenost intervjuvanca s temo tveganj in preveriti njegovo percepcijo pomembnosti ocenjevanja tveganj. Odgovori intervjuvancev so zajemali konkretna tveganja, kot so varnost sistema UI iz različnih vidikov, nevarnost haluciniranja in pristranskih odgovorov sistema, nezavedno deljenje zaupnih informacij s sistemom, nevarnost škodljivih posledic zaradi nevključenosti ljudi »v postopek avtonomnega odločanja sistema«, netransparentnost prednaučene baze znanja, nejasnost obdelovanja posredovanih podatkov

v sistem, kje se ti podatki obdelujejo, ali se ti podatki shranjujejo in kje se shranjujejo, ali sistem lahko zagotavlja skladnost z veljavno regulativo in politikami organizacije, ali so/bodo uporabniki sistema ustrezno izobraženi, kakšen je namen sistema, kako se lahko uporablja in kako se ne sme uporabljati, itd. Prav vsi odgovori so opisovali tveganja, ki tvorijo eno izmed vrst tveganj, obravnavanih pod naslednjim vprašanjem.

Vprašanje A2: »Seznam kategorij tveganj, specifičnih za umetno inteligenco – označite, če razumete kategorijo tveganja ali/in podajte nov predlog.«.

Zadnja dva stolpca v tabeli 1 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki vrsto tveganja razumejo (oznaka 1 v celici tabele 1) in odstotek razumljivosti med vsemi intervjuvanci. Oznake intervjuvancev so obrazložene v poglavju 4.

Tabela 1: Poznavanje posamezne vrste tveganj iz strani intervjuvancev

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1			
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2			
	Seznanjenost s tveganjem																														**Število**	**%**
1	Pristranskost in pravičnost	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1		**27**	**96**
2	Zasebnost in kibernetska varnost	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		**26**	**93**
3	Transparentnost in odgovornost	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1	1	1		**22**	**79**
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	1	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	0	0	0	0			**18**	**64**
5	Etični vidiki	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		**28**	**100**
6	Zanesljivost, integriteta in varnost uporabe	1	1	1	0	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1		**23**	**82**
7	Upravljanje in regulacija	1	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1		**22**	**79**

Vir: lastno delo.

Opomba: tabela 1 prikazuje odgovore vseh intervjuvancev, vključno s karakterizacijo intervjuvancev (tudi v tabeli 37, v prilogi 2). Tudi odgovori na vsa ostala vprašanja so zbrana v ekvivalentnih podrobnih tabelah, vendar se nahajajo le v prilogi 2. V nadaljevanju tega poglavja 4.1 so rezultati odgovorov na vprašanja prikazani zbirno, podobno kot odgovori na prvo vprašanje v tabeli 2.

Tabela 2: Izražena seznanjenost z vrsto tveganja iz strani intervjuvancev

	Izražena seznanjenost z vrsto tveganja	Število pritrdilnih odgovorov	Odstotek pritrdilnih odgovorov
1	Pristranskost in pravičnost	27	96
2	Zasebnost in kibernetska varnost	26	93
3	Transparentnost in odgovornost	22	79
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	18	64
5	Etični vidiki	28	100
6	Zanesljivost, integriteta in varnost uporabe	23	82
7	Upravljanje in regulacija	22	79

Vir: lastno delo.

2. del: Ocenjevanje tveganj

Vprašanje B1: »V nekaj stavkih opišite postopek ocenjevanja tveganja.«.

Intervjuvanci brez moje pomoči v veliki večini niso znali našteti vseh faz ocenjevanja tveganj, vendar je naslednje vprašanje (B2) razjasnilo njihovo poznavanje problematike.

Vprašanje B2: »Ali poznate naslednje faze ocenjevanja tveganja?«.

V tabeli 3 je razvidno število pritrdilnih odgovorov/št. intervjuvancev, ki posamezno fazo ocenjevanja tveganja razumejo, in odstotek razumljivosti med vsemi intervjuvanci, ki je prikazan tudi grafično. Podrobni rezultati so zbrani v tabeli 38, v prilogi 2.

Tabela 3: Izražena seznanjenost s fazami ocenjevanja tveganj iz strani intervjuvancev

	Izražena seznanjenost s postopkom ocenjevanja tveganj	Število pritrdilnih odgovorov	Odstotek pritrdilnih odgovorov	0 100
1	Identifikacija tveganja	**28**	**100**	
2	Ranljivosti in predpogoji za nastanek	**20**	**71**	
3	Verjetnost nastanka	**22**	**79**	
4	Resnost vpliva	**27**	**96**	
5	Izračun ocene	**18**	**64**	
6	Blaženje, preprečevanje	**27**	**96**	
7	Upravljanje incidentov	**16**	**57**	

Vir: lastno delo.

3. del: Sposobnost organizacije za ocenjevanje tveganj

Vprašanje C1: »Bi organizacija znala oceniti vsako vrsto tveganja (pomislite na dva primera umetne inteligence)? Če je odgovor pritrdilen, označite tveganje z oznako 1.«.

Tabela 4: Izražena sposobnost ocenjevanja posamezne vrste tveganj z vidika organizacije ob implementaciji UI

	Izražena sposobnost organizacije za ocenjevanja tveganj	Število pritrdilnih odgovorov	Odstotek pritrdilnih odgovorov	0 100
1	Pristranskost in pravičnost	**12**	**43**	
2	Zasebnost in kibernetska varnost	**19**	**68**	
3	Transparentnost in odgovornost	**12**	**43**	
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	**7**	**25**	
5	Etični vidiki	**12**	**43**	
6	Zanesljivost, integriteta in varnost uporabe	**17**	**61**	
7	Upravljanje in regulacija	**11**	**39**	

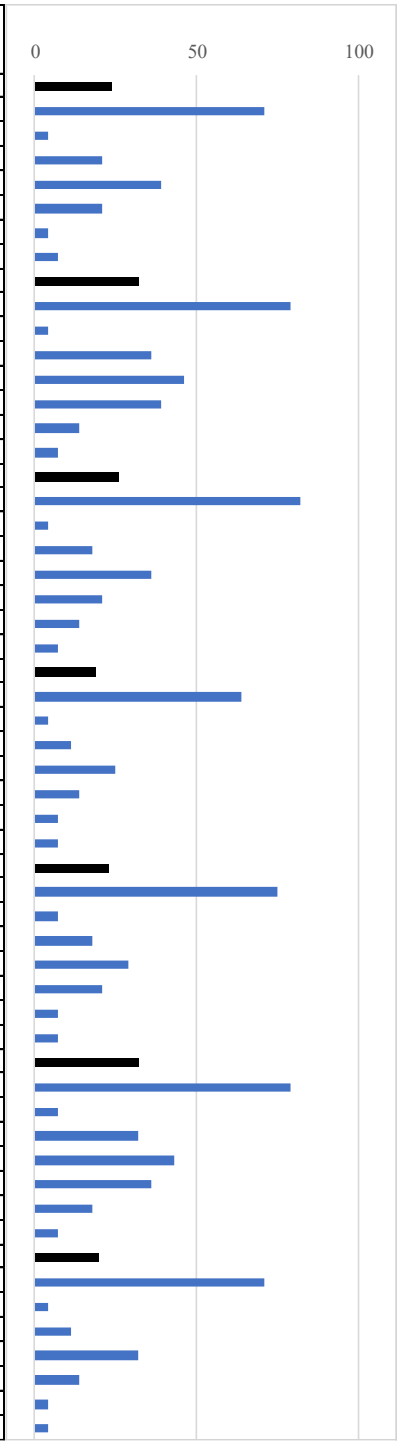
Vir: lastno delo.

Tabela 4 prikazuje število pritrdilnih odgovorov, da bi organizacija tveganja posamezne vrste tveganj znala oceniti in kolikšen odstotek med vsemi intervjuvanci to predstavlja. Odstotek je prikazan tudi grafično. Podrobni rezultati so zbrani v tabeli 39, v prilogi 2.

Vprašanje C2: »Bi bila organizacija sposobna ustrezno izvesti vsako fazo ocene tveganja pri vsaki vrsti tveganja?«.

Tabela 5: Sposobnost ocenjevanja posamezne vrste tveganj ob upoštevanju sposobnosti organizacije, da izvede vse faze ocenitve tveganj

		Izražena sposobnost organizacije, da oceni	Število pritrdilnih odgovorov	Odstotek pritrdilnih odgovorov
1	**Pristranskost in pravičnost**			**24**
		Identifikacija tveganja	20	71
		Ranljivosti in predpogoji za nastanek	1	4
		Verjetnost nastanka	6	21
		Resnost vpliva	11	39
		Izračun ocene	6	21
		Blaženje, preprečevanje	1	4
		Upravljanje incidentov	2	7
2	**Zasebnost in varnost**			**32**
		Identifikacija tveganja	22	79
		Ranljivosti in predpogoji za nastanek	1	4
		Verjetnost nastanka	10	36
		Resnost vpliva	13	46
		Izračun ocene	11	39
		Blaženje, preprečevanje	4	14
		Upravljanje incidentov	2	7
3	**Transparentnost in odgovornost**			**26**
		Identifikacija tveganja	23	82
		Ranljivosti in predpogoji za nastanek	1	4
		Verjetnost nastanka	5	18
		Resnost vpliva	10	36
		Izračun ocene	6	21
		Blaženje, preprečevanje	4	14
		Upravljanje incidentov	2	7
4	**Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov**			**19**
		Identifikacija tveganja	18	64
		Ranljivosti in predpogoji za nastanek	1	4
		Verjetnost nastanka	3	11
		Resnost vpliva	7	25
		Izračun ocene	4	14
		Blaženje, preprečevanje	2	7
		Upravljanje incidentov	2	7
5	**Etični vidiki**			**23**
		Identifikacija tveganja	21	75
		Ranljivosti in predpogoji za nastanek	2	7
		Verjetnost nastanka	5	18
		Resnost vpliva	8	29
		Izračun ocene	6	21
		Blaženje, preprečevanje	2	7
		Upravljanje incidentov	2	7
6	**Zanesljivost, integriteta in varnost**			**32**
		Identifikacija tveganja	22	79
		Ranljivosti in predpogoji za nastanek	2	7
		Verjetnost nastanka	9	32
		Resnost vpliva	12	43
		Izračun ocene	10	36
		Blaženje, preprečevanje	5	18
		Upravljanje incidentov	2	7
7	**Upravljanje in regulacija**			**20**
		Identifikacija tveganja	20	71
		Ranljivosti in predpogoji za nastanek	1	4
		Verjetnost nastanka	3	11
		Resnost vpliva	9	32
		Izračun ocene	4	14
		Blaženje, preprečevanje	1	4
		Upravljanje incidentov	1	4



Vir: lastno delo.

To vprašanje je podobno prejšnjemu, terja pa podrobnejši razmislek, ali bi bila organizacija res sposobna izvesti vse potrebne postopke za ocenitev tveganj. V tabeli 5 je razvidno število

pritrdilnih odgovorov/št. intervjuvancev, ki označujejo posamezno fazo ocenjevanja tveganj kot izvedljivo, in odstotek pritrdilnih odgovorov med vsemi intervjuvanci. V vrsticah, kjer so z odebeljeno pisavo opisane vrste tveganj, je v stolpcu »Odstotek pritrdilnih odgovorov« vidna povprečna ocenjena sposobnost organizacije za izvedbo vseh potrebnih postopkov za ocenitev tveganj dotične vrste. Odstotki so prikazani tudi grafično. Podrobni rezultati so zbrani v tabeli 40, v prilogi 2.

4. del: Koristne informacije in dejavniki pri uvajanju UI

Vprašanje D1: »Kateri so razlogi za slabšo zmožnost ocenjevanja tveganj? Katere dodatne informacije bi vaši organizaciji pomagale pri postopku ocenjevanja tveganj, oz. bi vam pomagale pri odločitvi, ali je vsako od tveganj "sprejemljivo" za uvedbo funkcionalnosti umetne inteligence?«.

Kot razloge za slabšo zmožnost ocenjevanja tveganj so intervjuvanci omenjali predvsem nezmožnost pridobivanja relevantnih informacij iz strani ponudnikov sistemov umetne inteligence, na podlagi katerih bi lahko ocenjevali tveganja.

> Primer izjave: »Glavni razlog je ta, da lokalni ponudniki sistemov umetne inteligence ne znajo povedati kaj bistveno drugega, kot je napisano že na spletnih straneh dejanskih »globalnih ponudnikov«. Vse te zadeve pa so po tistem, kar sem prebral, bolj splošne narave. Ali ne pomagajo kaj dosti, ali pa tem informacijam pač moraš verjeti, ne da bi se jih dalo dejansko preveriti. Kar od njih dobiš, so ponudbe za izobraževanje.«
>
> Primer izjave: »Zakaj vi (moja opomba: vprašanje je naslovljeno na ponudnika UI) in nepriznani ponudniki UI storitev? V tej luči predočite primerjavo OPEX in CAPEX? Kako lahko zagovarjate višje tveganje zaradi prekinitve poslovanja in izgube ugleda zaradi svoje majhnosti in malega števila referenc? Ali primerjalno ponujate dodatne funkcionalnosti, ki zmanjšujejo tveganja? Ali ponujate višjo stopnjo avtonomije pri regulaciji UI sistema?«

Na tem mestu omenjam še zanimive komentarje, kot npr. nezmožnost ocenitve kvalitete baze prednaučenega znanja, nezmožnost ocenitve varovanja podatkov, s katerimi se naslavlja sistem UI, …

> Primer izjave: »Neznana baza prednaučenega znanja, nejasna kvaliteta te baze, vprašanja glede zagotavljanja zaupnosti in varovanja vhodnih podatkov ter neuporabe teh podatkov za učenje modela samega.«
>
> Primer izjave: »Razumevanje osnovne baze znanja, na osnovi katere UI sistem deluje in politike integriranja novega znanja so ključne za ocenjevanje tveganj.«

… nezmožnost ocenitve kvalitete sodelovanja v sistem povezanih agentov UI …

> Primer izjave: »Mi razmišljamo npr., kako si pomagati z UI pri pripravljanju projektov. Ko gledamo rešitve, s katerimi se hvalijo po svetu, se nam zdi, da so to vse sistemi, v katere so ogromno vlagali – da so jih »prav naučili«. Kako zagotoviti, da je UI pravilno pred naučen zate? Zaenkrat se nam zdi, da bi nekako znali ocenjevali tveganja pri uporabi enostavne UI, ki izvaja vnaprej le zelo predvidene reči (moja opomba: »ozke UI« - angl. »Narrow AI«), če pa bo šlo vse skupaj res v smer samodejnega povezovanja in delovanja več agentov UI med seboj, pa nimamo pojma, kako bi to ocenjevali. Zdi se nam, da bi morali dobiti implementatorja UI, ki bi nas znal peljati čez vse to.«

… in težavo pri postavljanju metrike, ki bi spremljala učinkovitost delovnih procesov, ki bi jim sistem umetne inteligence na neki način asistiral.

> Primer izjave: »Ni mi jasno, kako meriti vpliv UI na učinkovitost ali uspešnost. Če bi mi to ponudnik UI znal pojasniti, bi lažje naredil »risk/benefit« analizo. Poleg tega mi ni jasno, kako oceniti varnost naših podatkov. Ali ni tako, da vsak uporabnik lahko da v sistem UI tisto, do česar ima sicer dostop? Ali lahko ponudnik garantira, da naši podatki ne bodo šli neznano kam?«

Tabela 6: Sposobnost organizacije odgovoriti na vprašanja v tabeli – sposobnost, ki povečuje zmožnost organizacije ocenjevati tveganja

N	Izražena sposobnost odgovarjanja na vprašanja ter preverjanja, oz. pridobivanja koristnih informacij	Št.	%	0 100
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	27	96	
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno inteligenco?	25	89	
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne inteligence?	23	82	
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in uporabnosti?	21	75	
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	20	71	
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali pritisk uporabnikov/javn…	18	64	
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	17	61	
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje in učinkovito sodel…	16	57	
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?	10	56	
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?	10	56	
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za upravljanje poslovn…	15	54	
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah aplikacij?	14	50	
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?	9	50	
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	13	46	
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev podatkov?	12	43	
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in multidisciplinarne ekipe z zaht…	12	43	
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	11	39	
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	11	39	
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do podatkov?	10	36	
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	10	36	
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni vmesniki, vizualne …	9	32	
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence ustvari napačne, pristr…	8	29	
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?	5	28	
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in izven nje?	5	28	
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	6	21	
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	6	21	
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti podatkov?	5	18	
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven organizacije)	3	17	
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove zanesljivosti in varnosti?	3	17	
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	3	17	

se nadaljuje

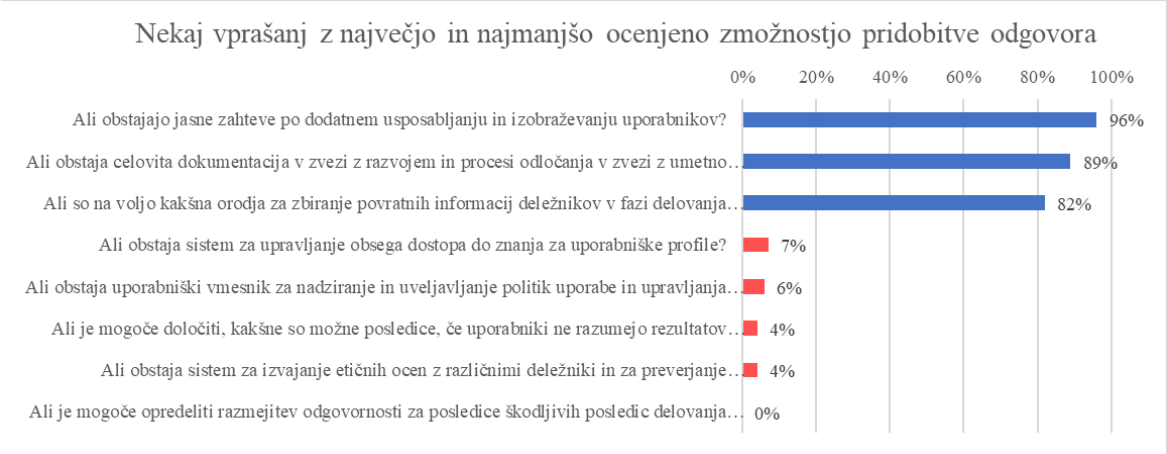
Tabela 6: Sposobnost organizacije odgovoriti na vprašanja v tabeli – sposobnost, ki povečuje zmožnost organizacije ocenjevati tveganja (nad.)

N	Izražena sposobnost odgovarjanja na vprašanja ter preverjanja, oz. pridobivanja koristnih informacij	Št.	%
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti podatkov?	4	14
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne inteligence?	4	14
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	4	14
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki dialoga, kot so dok…	4	14
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	4	14
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?	4	14
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen izid?	4	14
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	4	14
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne inteligence?	4	14
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali posamezne primere?	4	14
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	4	14
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov umetne inteligence?	3	11
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju umetne inteligence, t…	3	11
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	3	11
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega znanja?	2	11
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI?	2	11
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	2	7
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v real…	1	6
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne inteligence?	1	4
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z uveljavljenimi etičnimi …	1	4
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema UI med ponudnik…	0	0

Vir: lastno delo.

Vprašanje D2: »Odgovori na seznam vprašanj v tabeli 6 lahko organizaciji olajšajo ocenitev tveganj. Ocenite, ali imate oziroma bi imeli na voljo vire za pridobitev odgovorov na vsako od njih v procesu odločanja.«.

Tabela 7: Najbolje in najslabše "ocenjena" vprašanja



Vir: lastno delo.

V celoti in po številčnem vrstnem redu so vprašanja navedena v tabeli 36, v prilogi 1. Tabela 6 prikazuje število pritrdilnih odgovorov pri posameznem vprašanju – število intervjuvancev, ki menijo, da bi njihova organizacija znala pridobiti odgovor na zastavljeno vprašanje. Prikazan je tudi odstotek (v številčni in grafični obliki) takih intervjuvancev med vsemi intervjuvanci. V tabeli 7 so prikazana vprašanja, za katera intervjuvanci menijo z več kot 80-odstotno verjetnostjo, da bi njihove organizacije nanje znale odgovoriti, in vprašanja, za katera intervjuvanci menijo z več kot 90-odstotno verjetnostjo, da njihove organizacije

nanje ne bi znale pridobiti odgovora. Podrobni odgovori na vprašanje D2 so prikazani v tabeli 41, v prilogi 2.

5. del: Ukrepi pri uvajanju za ohranjanje nadzora nad sistemom UI v rokah nestrokovnjakov za UI

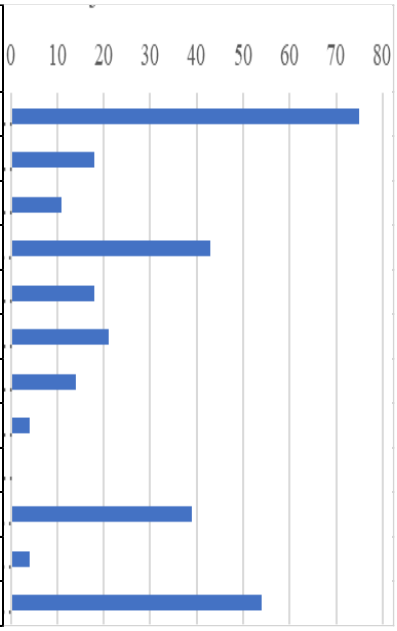
Vprašanje E1: »Si predstavljate kakršne koli ukrepe, ki bi lahko pomagali organizaciji, oz. osebam, ki niso strokovnjaki za umetno inteligenco, da bi lažje ocenili tveganja? Gre za ukrepe za lažje pridobivanje potrebnih informacij ali za povečevanje obvladovanja dejavnikov tveganja.«.

Večina intervjuvancev ni podalo novih predlogov. Največ predlogov, ki so jih podali, se je nanašalo na splošen ukrep – to je seznam predpripravljenih vprašanj, na katera bi poskušali pridobiti odgovore, npr. o podatkih glede baze prednaučenega znanja, o politikah varovanja podatkov, o pravni razmejitvi odgovornosti v zvezi s potencialno škodo, nastalo zaradi posledic delovanja sistema UI. Drugi sklop podanih predlogov je možno opisati kot pristop k ocenjevanju referenc ponudnika in ocenjevanju stopnje zanesljivosti delovanja podobnih, že izvedenih implementacij sistema UI.

Vprašanje E2: »Tukaj je nekaj predlogov za ukrepe. Izberite med njimi tri, ki bi vaši organizaciji bili najbolj v pomoč, ali pa podajte nov predlog.«.

Tabela 8: Uvrščanje ukrepov med tri najpomembnejše za povečevanje sposobnosti organizacije, da ocenjuje tveganja ob implementaciji UI

	Število uvrstitev posameznega ukrepa med tri najpomembnejše	Kolikokrat je bil ukrep izbran med tremi	Odstotek pojavitve ukrepa med prvimi tremi
1	Omejitev obsega delovanja UI in omejitev uporabnikov	21	75
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva	5	18
3	Zmanjševanje nedoločljivosti AI-user interakcij	3	11
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	12	43
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco	5	18
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI	6	21
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti	4	14
8	Sistem za razlago logike in sklepanja algoritmov sistema UI	1	4
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI	0	0
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	11	39
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI	1	4
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA	15	54



Vir: lastno delo.

Tabela 8 prikazuje število uvrstitev posameznega ukrepa med tri najpomembnejše z vidika povečevanja sposobnosti organizacije, da ocenjuje tveganja pri implementaciji UI. Tabela 8

prikazuje tudi odstotek pojavitve posameznega ukrepa med prvimi tremi. Podrobni rezultati so zbrani v tabeli 42, v prilogi 2.

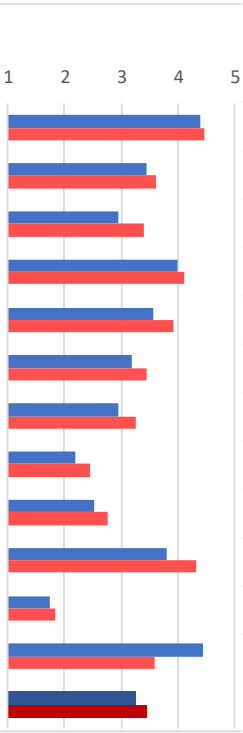
Vprašanje E3: »Vsak ukrep iz točke E2 ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, v kateri lahko organizacija popolnoma zaupa dostopnemu strokovnemu znanju o umetni inteligenci.«.

Tabela 9 združuje rezultate vprašanja E3 in E4. Tabela 9 prikazuje povprečno oceno pomembnosti posameznega ukrepa z vidika povečevanja sposobnosti organizacije, da ocenjuje tveganja pri implementaciji UI. Modre številke in palični grafični prikazi kažejo ocene pomembnosti ob predpostavki zaupanja strokovnosti implementatorjev in vzdrževalcev sistema UI, rdeče številke in grafični prikazi pa ocene ob predpostavki nezaupanja. Predpostavka zaupanja strokovnosti je, da organizacija lahko popolnoma zaupa ekspertnemu mnenju implementatorjev, za katerega organizacija prosi, je potrebno, ali ga od njih zahteva.

Vprašanje E4: »Vsak ukrep ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, ko organizacija ne more popolnoma zaupati dostopnemu strokovnemu znanju o umetni inteligenci.«.

Tabela 9: Ocene pomembnosti ukrepov ob implementaciji UI

	Ocenjevanje pozitivnosti ukrepov	Ocena ob popolnem zaupanju v razpoložljivo strokovno znanje UI	Ocena ob nezaupanju v razpoložljivo strokovno znanje UI
1	Omejitev obsega delovanja UI in omejitev uporabnikov	4,39	4,46
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva	3,46	3,61
3	Zmanjševanje nedoločljivosti AI-user interakcij	2,96	3,41
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	4	4,11
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco	3,58	3,92
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI	3,19	3,46
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti	2,96	3,25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI	2,19	2,46
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI	2,52	2,77
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	3,81	4,33
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI	1,74	1,85
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA	4,44	3,59
	Povprečje ocene	**3,27**	**3,44**

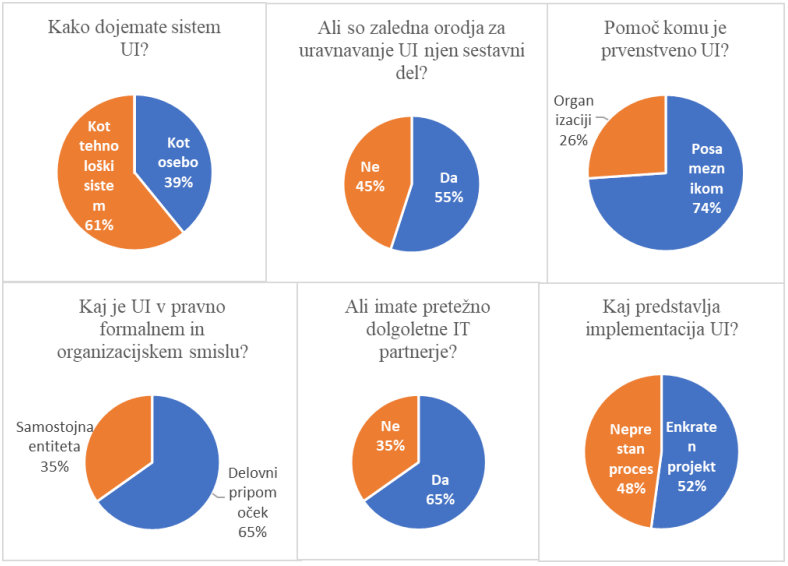


Vir: lastno delo.

Odgovori na vprašanje E4 so tudi prikazani v tabeli 9. Predpostavka nezaupanja strokovnemu znanju pomeni, da organizacija ne more popolnoma zaupati ekspertnemu mnenju implementatorjev, za katerega organizacija prosi, je potrebno, ali ga od njih zahteva. Podrobni rezultati odgovorov na vprašanji E3 in E4 so zbrani v tabelah 43 in 44, v prilogi 2.

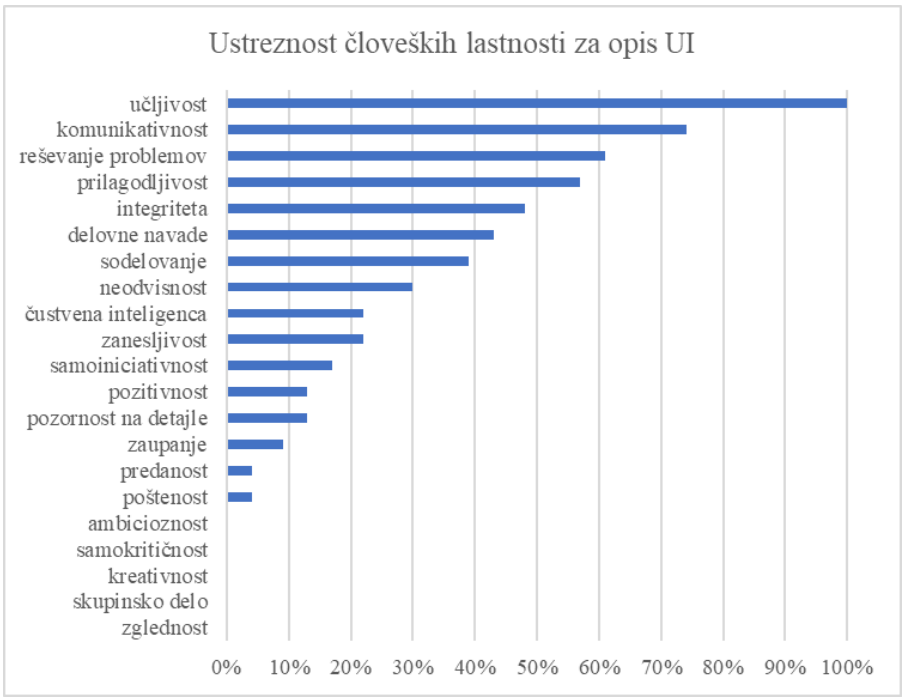
Izsledki nestrukturiranega dela intervjujev

Tabela 10: Grafični prikaz dodatnih informacij, ki so bile zbrane med intervjuji



Vir: lastno delo.

Tabela 11: Človeške lastnosti, ki najbolje opisujejo sistem UI



Vir: lastno delo.

V tabeli 45, v prilogi 2 podajam podrobne informacije, ki sem jih zbral na podlagi nestrukturiranega pogovora z intervjuvanci. Pogostost debatiranja o določenih temah sem zaznal med začetnimi intervjuji in jih nato sistematično začel vpeljevati v preostale intervjuje. Ker sem se z nekaterimi intervjuvanci dogovoril za naknadno srečanje v zvezi z nekaterimi dodatnimi vprašanji iz tabele 6, mi je pri nekaterih od njih uspelo pridobiti tudi stališča v zvezi z dodatnimi temami, ki so ponazorjene v grafih v tabeli 10 in v tabeli 11. Obe tabeli prikazujeta odgovore intervjuvancev na tista vprašanja, ki jih je odgovarjala večina intervjuvancev – v vseh navedenih primerih v obeh tabelah so zbrani odgovori 23 intervjuvancev.

4.2 Navzkrižna primerjava intervjujev

V poglavju 4.2 in v prilogi 3 se nahajajo tabele, ki prikazujejo rezultate intervjujev, zbrane in urejene po skupinah intervjuvancev. Na njihovi podlagi so v naslednjih poglavjih oblikovani sklepi s tabelaričnimi in grafičnimi ponazoritvami, ki bodo bralcu olajšale razumevanje napisanega. Zaradi vnaprej pripravljene strukture intervjujev je bila analiza rezultatov in primerjava odgovorov lažje izvedljiva. Za vsak sklop vprašanj (vprašanja so označena enako kot v prilogi 1 in v poglavju 4.1) so v prilogi 3 podane tabele zbranih odgovorov za vse različne zaznane skupine intervjuvancev. Podane so tudi tabele rezultatov, ki odgovore prikazujejo zbrane po združenih skupinah intervjuvancev na naslednji način:

- ker se raziskava osredotoča na razlike med percepcijo specialistov poslovnih področij, ki nimajo računalniško – tehničnega ozadja in ekspertov informacijske tehnologije, sem analiziral tudi združene rezultate skupin UI-ekspertov in IT-ekspertov (v nadaljevanju tudi UI&IT strokovnjaki),
- ker se raziskava osredotoča tudi na vidik zmožnosti ocenjevanja tveganj, sem analiziral tudi združene rezultate vseh skupin uporabnikov, ki področje ocenjevanja tveganj poznajo.

V pričujočem poglavju (poglavje 4.2) so prikazane le tabele z rezultati nekaterih skupin, tabele z rezultati vseh skupin pa so, kot rečeno, prikazane v prilogi 3. Na koncu poglavja 4.2 so po skupinah segmentirani tudi povzetki dodatnih informacij, zbranih med intervjuji, ki niso bile zajete v anketnem delu intervjujev.

Za vse tabele v poglavju 4.2 velja enaka razlaga prvih treh vrstic:

- v prvi vrstici se nahajajo oznake skupin intervjuvancev, katerih podatki se nahajajo v določenem stolpcu (gre za oznake, ki so razložene v poglavju 4);
- v drugi vrstici se nahaja opis skupine ali skupin intervjuvancev, ki predstavljajo podatke posameznega stolpca;
- v tretji vrstici se nahaja podatek o številu intervjuvancev, katerih odgovori so zajeti v posameznem stolpcu.

Pri vsaki tabeli se nahaja tudi vsebinska razlaga podatkov v številčnem delu tabele.

Rezultati odgovorov na vprašanje A2)

Tabela 12: Seznanjenost z vrstami tveganj po nekaterih zbirnih skupinah intervjuvancev

		Oznaka	A, a	B
		Opis	UI ali IT strokovnjak	Domenski specialist
	Vrsta tveganja	**Št. intervjujev**	12	16
1	Pristranskost in pravičnost		100	94
2	Zasebnost in kibernetska varnost		100	88
3	Transparentnost in odgovornost		100	63
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		92	44
5	Etični vidiki		100	100
6	Zanesljivost, integriteta in varnost uporabe		100	69
7	Upravljanje in regulacija		100	63
	Povprečje		**99**	**74**

Vir: lastno delo.

Številka v celici tabele 12 predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki je seznanjen s posamezno vrsto tveganj. Podatki za vse skupine intervjuvancev so vidni v tabelah 46 in 47 (priloga 3).

Rezultati odgovorov na vprašanje B2)

Tabela 13: Seznanjenost s fazami ocenjevanja tveganj po nekaterih zbirnih skupinah intervjuvancev

		Oznaka	A, a	B
		Opis	UI ali IT strokovnjak	Domenski specialist
	Faza ocenjevanja tveganj	**Št. intervjujev**	12	16
1	Identifikacija tveganja		100	100
2	Ranljivosti in predpogoji za nastanek		92	56
3	Verjetnost nastanka		100	63
4	Resnost vpliva		100	94
5	Izračun ocene		84	50
6	Blaženje, preprečevanje		100	94
7	Upravljanje incidentov		100	31
	Povprečje		**97**	**70**

Vir: lastno delo.

Številka v celici tabele 13 predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki menijo, da so seznanjeni s posamezno fazo ocenjevanja tveganj. Podatki za vse skupine intervjuvancev so vidni v tabelah 48 in 49 (priloga 3).

Rezultati odgovorov na vprašanje C1)

Številka v celici tabele 14 predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna ocenjevati posamezno vrsto tveganj pri implementaciji sistema UI. Podatki za vse skupine intervjuvancev so vidni v tabelah 50 in 51 (priloga 3).

Tabela 14: Percepcija sposobnosti ocenjevanja tveganj ob implementaciji UI po nekaterih zbirnih skupinah intervjuvancev

		Oznaka	A, a	B
		Opis	UI ali IT strokovnjak	Domenski specialist
	Vrsta tveganja	**Št. intervjujev**	12	16
1	Pristranskost in pravičnost		67	25
2	Zasebnost in kibernetska varnost		83	56
3	Transparentnost in odgovornost		75	19
4	Razumevanje možnosti in omejitev vhodnih podatkov in		34	19
5	Etični vidiki		59	31
6	Zanesljivost, integriteta in varnost uporabe		83	44
7	Upravljanje in regulacija		58	25
	Povprečje		**66**	**31**

Vir: lastno delo.

Rezultati odgovorov na vprašanje C2)

Tabela 15: Percepcija sposobnosti izvedbe vseh faz ocenjevanja tveganj ob implementaciji UI po nekaterih zbirnih skupinah intervjuvancev

		Oznaka	A, a	B
		Opis	UI ali IT strokovnjak	Domenski specialist
	Vrsta tveganja	**Št. intervjujev**	12	16
1	Pristranskost in pravičnost		33	17
2	Zasebnost in varnost		46	22
3	Transparentnost in odgovornost		40	16
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		29	12
5	Etični vidiki		36	14
6	Zanesljivost, integriteta in varnost		48	20
7	Upravljanje in regulacija		24	17
		Povprečje	**37**	**17**

Vir: lastno delo.

Številka v celici tabele 15 predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna izvesti vse faze ocenjevanja tveganj pri implementaciji sistema UI. Prikazani so le sumarni podatki sposobnosti ocenjevanja za vsako posamezno vrsto tveganj, podrobnosti za vsako fazo ocenjevanja tveganj pa so prikazane v tabelah 52 in 53 (priloga 3).

Rezultati odgovorov na vprašanje D2)

V tabeli 16 je v vrstici »Št. int.« prikazano število intervjuvancev, ki sestavljajo posamezno skupino v stolpcu tabele. Številka v celici spodnje vrstice v tabeli 16 predstavlja povprečni odstotek intervjuvancev določene skupine v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna z uporabo njej dostopnega znanja pridobiti odgovor na vprašanja iz tabele 6. Podrobni rezultati za vsako vprašanje so razvidni v tabelah 54 in 55 (priloga 3).

Tabela 16: Odstotkovno izražena percepcija intervjuvancev po nekaterih zbirnih skupinah intervjuvancev, da je organizacija sposobna pridobiti odgovore na vprašanja iz tabele 6

Oznaka		A, a	B
Opis		UI ali IT strokov-njak	Domenski specialist
Št. int.		12	16
Povprečno ocenjena zmožnost organizacije (zmožnost po skupinah je izražena v %), da odgovari na vprašanja, da preveri prisotnosti koristnih orodij ali da pridobi koristne informacije.		**42**	**24**

Vir: lastno delo.

Rezultati odgovorov na vprašanje E2)

Tabela 17: Percepcija pomembnosti ukrepov in orodij za povečevanje sposobnosti organizacije, da ocenjuje tveganja

		Oznaka	A, a	B
		Opis	UI ali IT strokovnjak	Domenski specialist
	Metode in ukrepi	**Št. intervjujev**	4	16
1	Omejitev obsega delovanja UI in omejitev uporabnikov		92	63
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		25	13
3	Zmanjševanje nedoločljivosti AI-user interakcij		9	13
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		42	44
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		9	25
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		17	25
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		9	19
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		9	0
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		0	0
10	Zaledni sistem nemenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		17	56
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		9	0
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		67	44

Vir: lastno delo.

Številka v celici tabele 17 predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki so izbrali metodo ali ukrep v vrstici tabele kot enega izmed treh najpomembnejših za povečevanje sposobnosti njihove organizacije, da izvede analizo tveganj pri implementaciji sistema UI. Podatki za vse skupine intervjuvancev so vidni v tabelah 59 in 60 (priloga 3).

Rezultati odgovorov na vprašanji E3) in E4)

Številka v celici tabele 18 predstavlja povprečno oceno koristnosti posameznega ukrepa v vrstici tabele (ocene od 1 do 5) z vidika intervjuvancev določene skupine v stolpcu tabele. Ocenjevali so koristnost ukrepa za povečevanje sposobnosti njihove organizacije, da izvede analizo tveganj pri implementaciji sistema UI. Za vsako skupino intervjuvancev in vsak ukrep sta v tabeli navedeni dve oceni. Z modro barvo je navedena ocena za situacijo, ko bi njihova organizacija pri implementaciji sistema UI lahko zaupala UI ekspertizi, ki bi jo imela na voljo. Z rdečo barvo je navedena ocena, če ekspertizi organizacija ne bi mogla zaupati. Podatki za vse skupine intervjuvancev so vidni v tabelah 61 in 62 (priloga 3).

Tabela 18: Ocena pomembnosti metod, ki povečujejo zmožnost ocenjevanja tveganj (po nekaterih zbirnih skupinah intervjuvancev)

		Oznaka	A, a		B	
		Opis	UI ali IT strokovnjak		Domenski specialist	
		Št. inter.	12		16	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,58	4,75	4,25	4,25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,34	3,58	3,56	3,63
3	Zmanjševanje nedoločljivosti AI-user interakcij		2,84	3,58	3,07	3,27
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4	4,25	4	4
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,17	3,67	3,93	4,14
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,17	3,58	3,21	3,36
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		2,84	3,25	3,06	3,25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,42	2,84	2	2,14
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		2,75	3	2,33	2,57
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,5	4,17	4,07	4,47
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		2,25	2,34	1,33	1,47
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,5	3,42	4,4	3,73

Vir: lastno delo.

Dodatne zabeležbe intervjujev

V celicah tabele 19, kjer so podatki navedeni kot npr. 

, je potrebno pomen posamezne številke pred dvopičjem razbrati iz opisa v vrstici, ki se nahaja v prvem stolpcu tabele. Za dvopičjem se za vsako številko nahaja število intervjuvancev v skupini, ki so izbrali opcijo, ki jo številka pred dvopičjem predstavlja. V celicah, kjer se nahaja številka med 0 in 100, številka predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki je izbral

posamezno človeško lastnost kot pričakovano lastnost sistema UI. Podatki za vse skupine intervjuvancev so vidni v tabeli 64 (priloga 3).

Tabela 19: Druga zbrana mnenja po nekaterih zbirnih skupinah intervjuvancev

Oznaka	A, a	B
Opis	UI ali IT strokovnjak	Domenski specialist
Št. interv.	9	14
Ali smatrate/obravnavate sistem UI kot tehnološki sistem (1), kot osebo (3) ali kot oboje (2) ?	**1: n=4 2: n=0 3: n=5**	**1: n=10 2: n=0 3: n=4**
Ali smatrate metode in orodja, obravnavana pod točkami od E1 do E4 v večini primerov kot del sistema UI (1), ali ne (2) ?	**1: n=9 2: n=0**	**1: n=14 2: n=0**
Ali bo služil sistem UI bolj kot pomoč posameznikom (1) ali kot pomoč organizaciji (2) ?	**1: n=7 2: n=2**	**1: n=10 2: n=4**
Ali bo sistem UI v pravno formalnem in organizacijskem smislu delovni pripomoček (1) ali samostojna entiteta (2) ?	**1: n=4 2: n=5**	**1: n=11 2: n=3**
Oznaka	A, a	B
Opis	UI ali IT strokovnjak	Domenski specialist
Št. interv.	9	14
S katerimi (človeškimi) lastnosti bi sistem UI najbolj poistovetili?		
integriteta	50	43
zanesljivost	21	21
zglednost	0	0
skupinsko delo	0	0
komunikativnost	75	64
zaupanje	8	7
poštenost	0	7
prilagodljivost	75	36
pozornost na detajle	29	0
kreativnost	0	0
samokritičnost	0	0
sodelovanje	42	36
pozitivnost	0	21
reševanje problemov	46	64
čustvena inteligenca	0	36
predanost	8	0
samoiniciativnost	13	21
učljivost	83	100
ambicioznost	0	0
neodvisnost	17	36
delovne navade	42	43
Ali imate pretežno dolgoletne IT partnerje: da (1) / ne (2) ?	**1: n=6 2: n=3**	**1: n=9 2: n=5**
Ali je implementacija sistema UI enkraten projekt (1), ali je pričakovati neprestano nadgrajevanje sistema UI (2) ?	**1: n=2 2: n=7**	**1: n=10 2: n=4**

Vir: lastno delo.

4.3 Oblikovanje sklepov

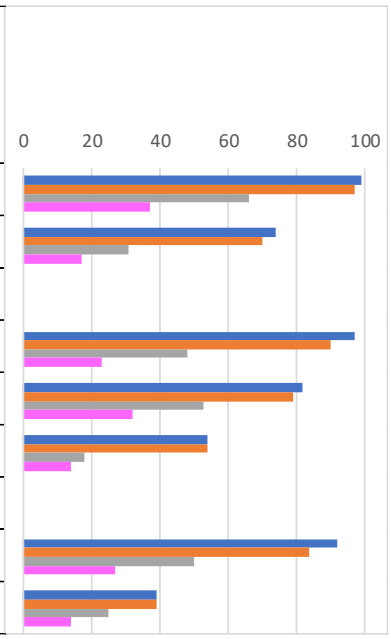
V nadaljevanju so analizirani rezultati iz prejšnjega poglavja 4.2.

Pri poznavanju vrste tveganj (v tabeli 20 so podatki v zvezi s tem obarvani modro) je opazna razlika med skupino UI&IT strokovnjakov (strokovnjaki umetne inteligence in informacijske tehnologije), kjer je njihova izražena stopnja poznavanja vrste tveganj 99 %

in skupino domenskih specialistov, kjer je njihova izražena stopnja poznavanja 74 %. Izražene stopnje udeleženosti v procesu ocenjevanja tveganj so proporcionalno povezane z izraženimi stopnjami poznavanja vrste tveganj iz strani intervjuvancev (podrobni rezultati so prikazani v tabelah 37, 38, 39 in 40, v prilogi 2). Izraženo poznavanje vrste tveganj pada tudi s padanjem stopnje udeleženosti v postopkih odločanja v zvezi z implementacijo IT sistemov: od 97 % za odločevalce, preko 82 % za tiste, ki v postopku odločanja sodelujejo, do 54 % za tiste, ki pri njih ne sodelujejo.

Tabela 20: Izražene sposobnosti ocenjevanja tveganj po različnih skupinah intervjuvancev

Oznaka	Opis skupine intervjuvancev	Št. inter-vjujev	Poznava-nje vrste tveganj	Poznava-nje postopka ocenjeva-nja tveganj	Pavšalna ocena sposobnosti ocenitve tveganj ob implementaciji UI	Ocena na podlagi izvedljivosti vseh potrebnih postopkov
A, a	UI ali IT strokovnjak	12	99	97	66	37
B	Domenski specialist	16	74	70	31	17
1	Odločevalec	13	97	90	48	23
2	Udeleženec odločanja	11	82	79	53	32
3	Ni vključen v odločanja	4	54	54	18	14
1-4	Seznanjen sem z ocenjev. tveganj	24	92	84	50	27
5	Nisem seznanjen	4	39	39	25	14



Vir: lastno delo.

Tudi pri poznavanju ocenjevanja postopka tveganj (v tabeli 20 so podatki v zvezi s tem obarvani oranžno) je opaziti razliko med skupino UI&IT strokovnjakov, kjer je izražena stopnja poznavanja teh postopkov 97 % in domenskimi specialisti, kjer je stopnja 70 %. Poznavanje teh postopkov pada tako s stopnjo udeleženosti v postopkih odločanja (za odločevalce: 90 %, za udeležence pri odločanju: 79 %, za preostale: 54 %), kot tudi s stopnjo vključenosti v postopek obravnavanja tveganj (pada od 94 % do 39 %, kar je podrobneje razvidno iz rezultatov v tabeli 40).

Zanimivi so tudi rezultati, prikazani v tabeli 20 s sivo in z rožnato barvo, ki obravnavajo organizacijsko sposobnost ocenitve tveganj v zvezi z uvedbo sistema UI. Na tem mestu združujem ugotovitve rezultatov sklopov intervjujev C1 in C2. Na vprašanje o intervjuvančevi percepciji sposobnosti njegove organizacije, da oceni tveganja z razpoložljivimi resursi v postopku odločanja o implementaciji UI (podatki v sivi barvi), je bilo opaziti bistveno bolj optimistične odgovore v primerjavi z istim vprašanjem za vsako fazo ocenjevanja tveganj posebej (podatki rožnate barve). Izkazalo se je, da so ob podrobnejšem premisleku o sposobnosti ocenjevanja tveganj (na podlagi preverjanja, ali bi

bili sposobni izvesti vsako izmed potrebnih faz pri ocenjevanju tveganj), intervjuvanci zmanjšali ocenitev sposobnosti o uspešni ocenitvi tveganj. UI&IT strokovnjaki so jo znižali iz prvotnih 66 % na 37 %, domenskimi specialisti pa iz prvotnih 31 % na 17 %. Opazno je bilo tudi znatno zmanjšanje tozadevne percepcije pri odločevalcih (iz 48 % na 23 %) in pri vseh, ki so seznanjeni s postopkov ocenjevanja tveganj (iz 50 % na 27 %).

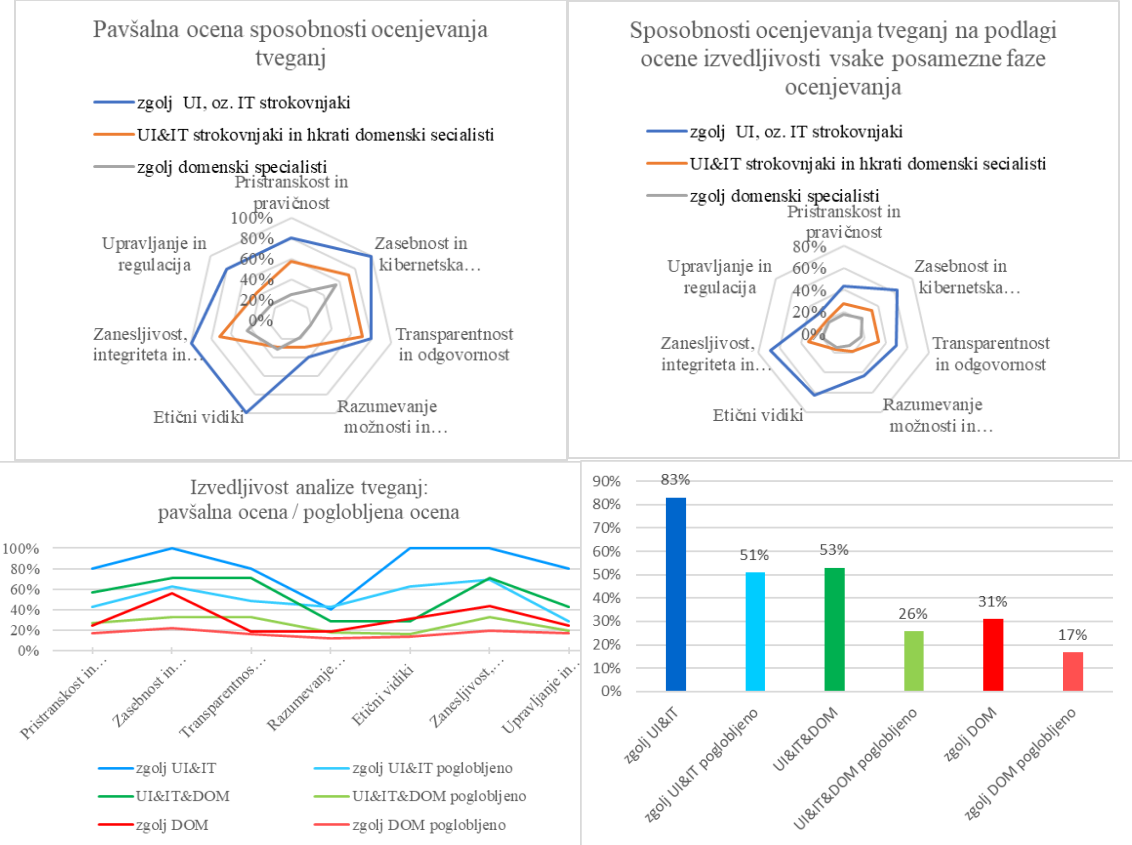
Analiziral sem tudi razlike glede na to, ali domenski specialisti posedujejo / ne posedujejo strokovna znanja iz področja IT in UI (podatki so prikazani v tabeli 21 - razpredelnice, polarni diagrami in črtni ter stolpčni grafi). Opazno je precejšnje zmanjšanje povprečne percepcije UI&IT strokovnjakov, ki so v svoji karieri postali tudi domenski specialisti, da je organizacija sposobna ocenjevanja tveganj (pri pavšalni ocenitvi sposobnosti (vprašanje C1) je le ta padla iz 83 % na 53 %, pri poglobljenem razmisleku na podlagi sposobnosti izvedbe vseh faz ocenjevanja tveganja (vprašanje C2) pa je padla iz 51 % na 26 %. V črtnih in stolpčnih grafih tabele 21 kratica »zgolj UI&IT« predstavlja združeno skupino UI in IT strokovnjakov, ki hkrati niso domenski specialisti, kratica »UI&IT&DOM« predstavlja združeno skupino UI in IT strokovnjakov, ki so hkrati domenski specialisti, kratica »zgolj DOM« pa predstavlja skupino domenskih specialistov, ki niso hkrati tudi UI ali IT strokovnjaki. Opisane kratice s pripisom »poglobljeno« predstavljajo odgovore opisanih skupin na vprašanje C2, kratice brez pripisa pa na vprašanje C1.

Tabela 21: Percepcija različnih skupin intervjuvancev o sposobnosti organizacije, da ocenjuje tveganja (zgoraj: vprašanje C1, spodaj: vprašanje C2)

	Zmožnost ocenjevanja tveganj (vprašanje C1)	**zgolj UI, oz. IT strokovnjaki**	**UI&IT strokovnjaki in hkrati domenski secialisti**	**zgolj domenski specialisti**
1	Pristranskost in pravičnost	80%	57%	25%
2	Zasebnost in kibernetska varnost	100%	71%	56%
3	Transparentnost in odgovornost	80%	71%	19%
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	40%	29%	19%
5	Etični vidiki	100%	29%	31%
6	Zanesljivost, integriteta in varnost uporabe	100%	71%	44%
7	Upravljanje in regulacija	80%	43%	25%
	Povprečje	**83%**	**53%**	**31%**
	Zmožnost ocenjevanja tveganj (vprašanje C2)	**zgolj UI, oz. IT strokovnjaki**	**UI&IT strokovnjaki in hkrati domenski secialisti**	**zgolj domenski specialisti**
1	Pristranskost in pravičnost	43%	27%	17%
2	Zasebnost in kibernetska varnost	63%	33%	22%
3	Transparentnost in odgovornost	49%	33%	16%
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	43%	18%	12%
5	Etični vidiki	63%	16%	14%
6	Zanesljivost, integriteta in varnost uporabe	69%	33%	20%
7	Upravljanje in regulacija	29%	20%	17%
	Povprečje	**51%**	**26%**	**17%**

se nadaljuje

Tabela 21: Percepcija različnih skupin intervjuvancev o sposobnosti organizacije, da ocenjuje tveganja (zgoraj: vprašanje C1, spodaj: vprašanje C2) (nad.)

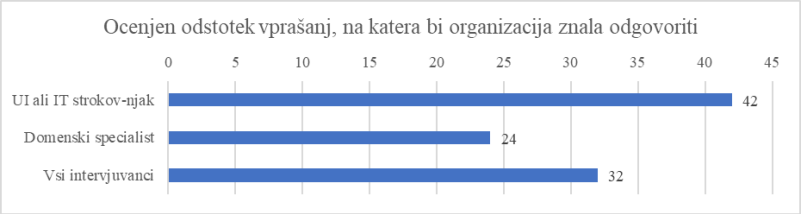


Vir: lastno delo.

Pri rezultatih ocenjevanja organizacijske sposobnosti pridobitve odgovorov na vprašanja, ki lahko pomagajo pri povečevanju njene sposobnosti ocenjevanja tveganj v zvezi z implementacijo sistema UI, sem opazil bistveno razliko med deležem vprašanj, na katera naj bi organizacije znale najti odgovor, in deležem vprašanj, na katera naj ne bi znale odgovoriti. Za vizualni oris te razlike sem v tabeli 22 prikazal sumarne podatke in v tabeli 56 (priloga 3) z zeleno barvo označil vprašanja, na katera bi posamezna skupina intervjuvancev znala pridobiti odgovor z vsaj 80-odstotno verjetnostjo ter z rdečo barvo vprašanja, kjer je izražena verjetnost manjša od 20 %. Kombinacij rešljivih vprašanj in skupin intervjuvancev je cca 8 %, drugih (nerešljivih kombinacij) pa cca 42 %. Tabela 57 (priloga 3) na ekvivalenten način prikazuje kombinacije z vsaj 90-odstotno oz. z največ 10-odstotno verjetnostjo pridobitve odgovorov na ponujena vprašanja. Kombinacij rešljivih vprašanj in skupin intervjuvancev je v tem primeru cca 3 %, slabo rešljivih pa cca 31 %. Povprečna percepcija vseh intervjuvancev, da bi njihova organizacija bila sposobna pridobiti odgovore na vprašanja, je 32 % (UI&IT strokovnjaki: 42 %, domenski specialisti: 24 %).

Tabela 22: Percepcija skupin intervjuvancev, da bi organizacija znala odgovarjati na zastavljena vprašanja iz tabele 6

	Oznaka	A, a	B		1	2	3		1-4	5
	Opis	UI ali IT strokov-njak	Domenski specialist		Odločeva-lec	Udeleže-nec odločanja	Ni vključen v odločanja		Seznanjen z ocenjev. tveganj	Nisem seznanjen
	Št. int.	12	16		13	11	4		24	4
Število vprašanj, kjer so intervjuvanci izrazili več kot 90% prepričanje, da bi njihova organizacija znala poiskati odgovor		1	2		1	3	2		1	4
Število vprašanj, kjer so intervjuvanci izrazili več kot 80% prepričanje, da bi njihova organizacija znala poiskati odgovor		6	3		4	4	2		2	4
Število vprašanj, kjer so intervjuvanci izrazili več kot 20% in manj kot 80% prepričanje, da bi njihova organizacija znala poiskati odgovor		36	17		27	18	28		27	10
Število vprašanj, kjer so intervjuvanci izrazili manj kot 20% prepričanje, da bi njihova organizacija znala poiskati odgovor		9	31		20	29	21		22	37
Število vprašanj, kjer so intervjuvanci izrazili manj kot 10% prepričanje, da bi njihova organizacija znala poiskati odgovor		5	24		5	19	21		7	37
Povprečje izraženega prepričanja intervjuvancev, da bi njihova organizacija znala poiskati odgovore na vprašanja		**42**	**24**		**36**	**29**	**21**		**33**	**16**



Vir: lastno delo.

Pri ugotavljanju sposobnosti organizacij za pridobivanje relevantnih informacij, ki bi jim pomagale ocenjevati tveganja, rezultati kažejo, da bi organizacije po mnenju intervjuvancev s precejšnjo verjetnostjo znale odgovoriti predvsem na tri vprašanja iz tabele 6:

- Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?
- Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno inteligenco?
- Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne inteligence?

Vprašanj, na katera organizacije ne bi znale najti odgovora, je zares veliko. To kaže na to, da je zanje praktično zelo težko izvajati ocenjevanje tveganj. Med njimi še posebej izstopajo vprašanja z izraženo manj kot 10-odstotno verjetnostjo pridobitve odgovorov, med katerimi na prvo vprašanje nihče ne bi znal poiskati odgovora:

- Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema UI med ponudnikom sistema, implementatorjem sistema UI ter organizacijo-uporabnikom sistema?
- Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne inteligence?
- Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z uveljavljenimi etičnimi smernicami in standardi?

- Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega znanja?
- Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI?
- Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v realnem času?
- Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov umetne inteligence?
- Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?

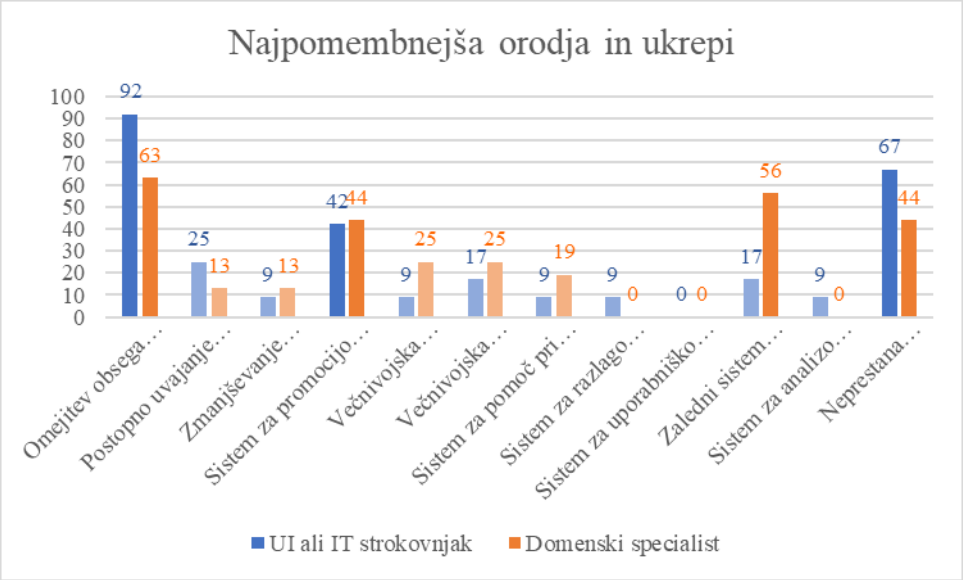
Pri analizi treh najprimernejših metod ali ukrepov (iz stališča vsake skupine intervjuvancev), ki bi pomagale izboljševati sposobnost organizacijskega ocenjevanja tveganj sistema UI, so v razpredelnici tabele 23 z zeleno barvo označeni najpogosteje izbrani pozitivni ukrepi in z rdečo najmanj pogosto izbrani ukrepi. Na stolpičnem grafu tabele 23 je dobro vidno, da med vsemi prednjači pozitivnost ukrepa: »Omejitev obsega delovanja UI in omejitev uporabnikov«. Izstopa tudi velika razlika med percepcijo UI&IT strokovnjakov in domenskih specialistov za pozitivnost ukrepa: »Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence«. UI&IT strokovnjaki ga ne uvrščajo med tri najpozitivnejše (zgolj 17 % ga označuje kot takega), za domenske specialiste pa je drugi najpomembnejši (56 %).

Tabela 23: Percepcija pomembnosti ukrepov in orodij, ki povečujejo zmožnost organizacije, da ocenjuje tveganja (odstotkovno izražena pogostost uvrstitve ukrepa med tri najpomembnejše)

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Metode in ukrepi	**Št. intervjujev**	12	16		13	11	4		24	4
1	Omejitev obsega delovanja UI in omejitev uporabnikov		92	63		92	73	25		79	90
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		25	13		15	18	25		17	10
3	Zmanjševanje nedoločljivosti AI-user interakcij		9	13		0	27	0		8	10
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		42	44		54	36	25		46	50
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		9	25		23	0	50		17	10
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		17	25		23	9	50		21	10
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		9	19		8	18	25		12	10
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		9	0		0	9	0		4	0
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		0	0		0	0	0		0	0
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		17	56		23	45	75		33	60
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		9	0		8	0	0		4	0
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		67	44		54	64	25		58	50

se nadaljuje

Tabela 23: Percepcija pomembnosti ukrepov in orodij, ki povečujejo zmožnost organizacije, da ocenjuje tveganja (odstotkovno izražena pogostost uvrstitve ukrepa med tri najpomembnejše) (nad.)



Vir: lastno delo.

Dva ukrepa izstopata pri ocenjevanju pomembnosti dvanajstih ukrepov in metod v dveh različnih situacijah glede stopnje zaupanja v UI strokovnost, do katere ima organizacija dostop (tabela 24):

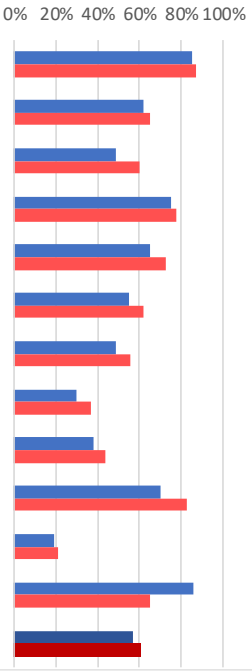
- v prvi situaciji, ko pri izbiranju ukrepov in metod za izboljšanje ocenjevanja tveganj organizacije lahko zaupajo UI-strokovnjakom, ki so vključeni v implementacijo (podatki so prikazani modro),
- in v drugi situaciji, ko jim ne morejo zaupati (podatki so prikazani rdeče).

Pri dveh spodaj navedenih ukrepih je torej razlika v izraženi percepciji intervjuvancev med obema situacijama največja – pri prvem ukrepu v eno smer, pri drugem ukrepu v drugo smer:

- ukrep »Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence« izkazuje največje povečanje vpliva na sposobnost ocenjevanja tveganj, če UI-strokovnjakom ne gre zaupati, v primerjavi s situacijo, da jim organizacije lahko zaupajo (ocena pozitivnega vpliva ukrepa se poveča za 13 %),
- ukrep »Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi najsodobnejše tehnologije (angl. State of the Art, v nadaljevanju SOTA)« pa izkazuje največje zmanjšanje vpliva na sposobnost ocenjevanja tveganj, če UI-strokovnjakom pri implementaciji ne gre zaupati, v primerjavi s situacijo, ko se jim lahko zaupa (ocena pozitivnega vpliva ukrepa se zmanjša za 21 %).

Tabela 24: Odstotkovno izražena pozitivnost ukrepa ali orodja

	Odstotek doseganja maksimalne ocene pozitivnosti ukrepov	Ocena ob popolnem zaupanju v razpoložljivo strokovno znanje UI	Ocena ob nezaupanju v razpoložljivo strokovno znanje UI
1	Omejitev obsega delovanja UI in omejitev uporabnikov	85%	87%
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva	62%	65%
3	Zmanjševanje nedoločljivosti AI-user interakcij	49%	60%
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	75%	78%
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco	65%	73%
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI	55%	62%
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti	49%	56%
8	Sistem za razlago logike in sklepanja algoritmov sistema UI	30%	37%
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI	38%	44%
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	70%	83%
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI	19%	21%
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA	86%	65%
	Povprečje doseganja maksimalne ocene	**57%**	**61%**



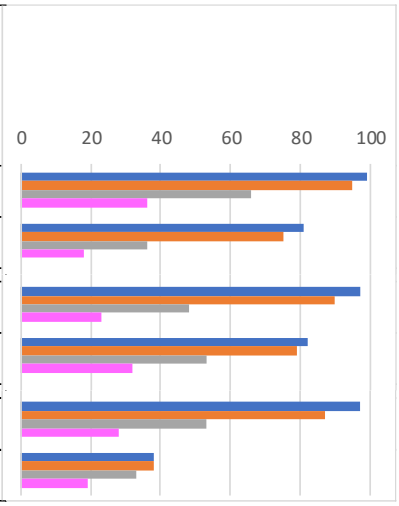
Vir: lastno delo.

4.4 Preverjanje raziskovalnih vprašanj

Tezi raziskovalnega dela, da podjetja brez razpoložljivega oz. dosegljivega strokovnega znanja o umetni inteligenci in informacijski tehnologiji težko ocenjujejo tveganja pri implementaciji sistema UI, pritrjujejo rezultati intervjujev. Z namenom natančnejše preverbe pravilnost teze, sem iz obravnavanih rezultatov izločil intervjuvance, ki niso del »odločevalskega postopka o implementaciji UI« (tabela 25). Podobno zaključkom iz tabele 20, je tudi iz tabele 25 razvidno, da je percepcija odločevalcev o organizacijski sposobnosti ocenjevanja tveganj precej nižja brez tega strokovnega znanja (pade iz 66 % na 36 %, oz. iz 36 % na 18 %) in da percepcija pade tudi v podjetjih, kjer je sicer znanje prisotno, a so izkušnje UI&IT strokovnjakov prepletene tudi z izkušnjami, znanjem, zahtevami in potrebami domenskih področij (tabela 26). UI&IT strokovnjaki, ki so tudi domenski specialisti, namreč izražajo poglobljeno zavedanje problematike pri ocenjevanju tveganj. Njihova izražena sposobnost ocenitve tveganj (26 %) je bližje percepcije domenskih specialistov (18 %) kot svojih UI&IT kolegov (51 %) (tabela 27).

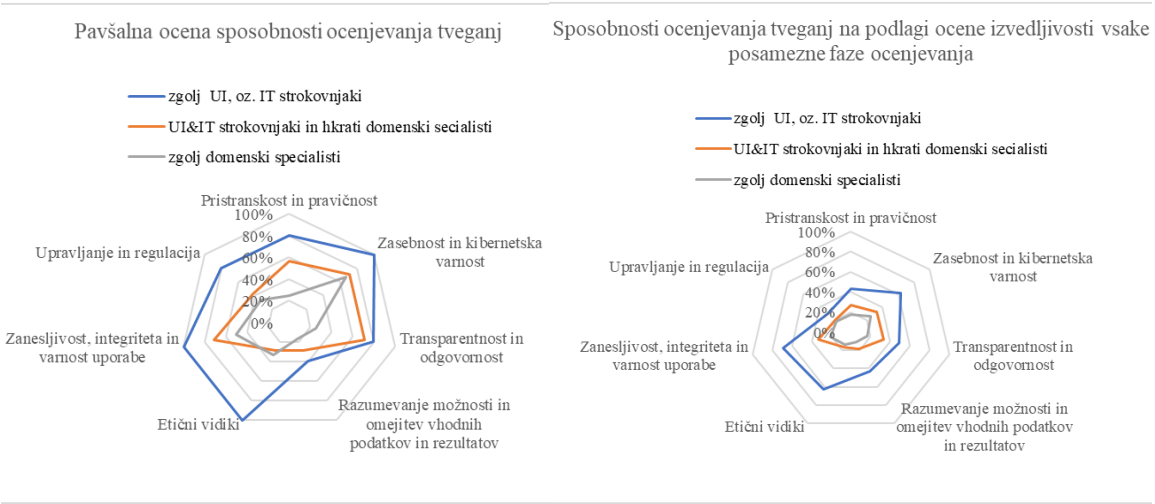
Tabela 25: Izražene sposobnosti ocenjevanja tveganj po različnih skupinah odločevalcev

Oznaka	Opis skupine odločevalcev	Št. inter-vjujev	Poznava-nje vrste tveganj	Poznava-nje postopka ocenjeva-nja tveganj	Pavšalna ocena sposobnosti ocenitve tveganj ob implementaci ji UI	Ocena na podlagi izvedljivosti vseh potrebnih postopkov
A, a	UI ali IT strokovnjak	12	99	95	66	36
B	Domenski specialist	12	81	75	36	18
1	Odločevalec	13	97	90	48	23
2	Udeleženec odločanja	11	82	79	53	32
1-3	Seznanjen sem z ocenjev. tveganj	21	97	87	53	28
5	Nisem seznanjen	3	38	38	33	19



Vir: lastno delo.

Tabela 26: Percepcija sposobnosti organizacije, da oceni posamezne vrste tveganj – levi diagram kaže percepcije brez podrobnejšega premisleka o zmožnosti izvajanja posameznih faz ocenjevanja tveganj, desni diagram pa kaže percepcijo ob upoštevanju podrobnosti



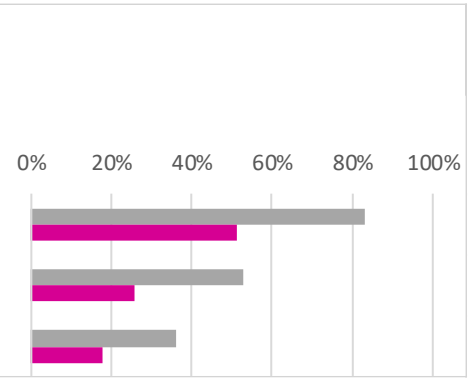
Vir: lastno delo.

Razlika v povprečni percepciji odločevalcev (v nadaljevanju odstavka: »povprečje skupine«), da bi bila organizacija sposobna pridobiti odgovore na vprašanja iz tabele 6, ki povečujejo njeno sposobnost ocenjevanja tveganj, se razlikuje med različnimi skupinami odločevalcev (tabela 28 in podrobnejša tabela 58 v prilogi 3). Povprečje skupine domenskih specialistov, da bi njihova organizacija znala odgovoriti na vprašanja, znaša 23 % in je za 19 odstotnih točk manjše od skupine UI&IT strokovnjakov, torej je skoraj polovico manjše. Zanimivi so bili komentarji UI&IT strokovnjakov, ki so dobro razumeli pomen vprašanj iz tabele 6, a hkrati komentirali, da v večini primerov pri implementaciji in uporabi UI ne bi imeli na voljo ukrepa ali orodja, ki ga posamezno vprašanje naslavlja. Z vidika sposobnosti

ocenitve tveganj so skoraj za polovico bolj optimistični od domenskih specialistov, vendar se sama višina tveganja iz njihovega vidika ne bi bistveno razlikovala od višine ocene domenskih specialistov, ki pa sploh ne bi znali odgovoriti na večino vprašanj in bi torej predpostavljali neobstoj pozitivnih orodij ali ukrepov. Posledično oboji izražajo veliko verjetnost visoko ocenjenih tveganj, prvi zaradi večinoma negativnih odgovorov na podana vprašanja, drugi pa zaradi nezmožnosti pridobitve odgovorov nanje.

Tabela 27: Percepcija odločevalcev glede na njihova strokovna in specialistična znanja

Opis skupine odločevalcev	**Št. inter-vjujev**	**Pavšalna ocena sposobnosti ocenitve tveganj ob implementaci ji UI**	**Ocena na podlagi izvedljivosti vseh potrebnih postopkov**
zgolj UI, oz. IT strokovnjaki	5	83%	51%
UI&IT strokovnjaki in hkrati domenski secialisti	7	53%	26%
zgolj domenski specialisti	12	36%	18%



Vir: lastno delo.

Tabela 28: Ocenjena sposobnost organizacije, da pridobi odgovore na vprašanja pri dveh skupinah odločevalcev

Oznaka	A, a	B
Opis	UI ali IT strokovnjak	Domenski specialist
Št. intervjuvancev	12	12
Povprečna izražena sposobnost pridobitve odgovorov na vprašanja	**42%**	**23%**

Vir: lastno delo.

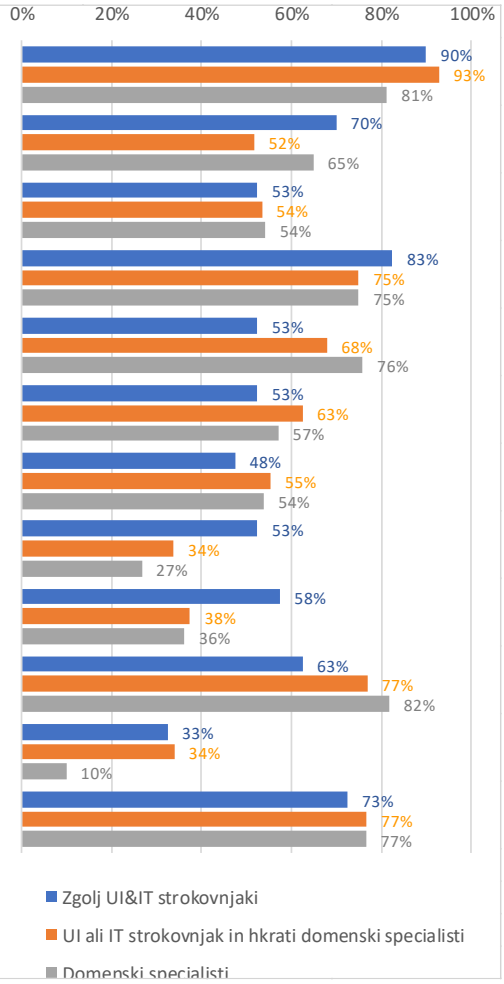
Povprečno odstopanje ocene pomembnosti ukrepov in orodij, ki povečujejo organizacijsko sposobnost ocenjevanja tveganj, med skupinami:

- domenskih specialistov,
- domenskih specialistov, ki posedujejo tudi UI&IT strokovna znanja in
- UI&IT strokovnjaki,

je izračunano iz podatkov tabele 63, v prilogi 3. Med skupinama domenskih specialistov in domenskih specialistov, ki posedujejo tudi UI&IT strokovna znanja, se povprečna ocena razlikuje za 6 odstotnih točk, medtem ko se med skupinama UI&IT strokovnjakov in domenskih specialistov, ki posedujejo tudi UI&IT strokovno znanje, razlikuje za 10 odstotnih točk (absolutne razlike prikazujeta dva stolpca »Abs. Razlika« v tabeli 63, priloga 3).

Tabela 29: Percepcija treh skupin odločevalcev o pozitivnosti vpliva ukrepov na sposobnost organizacije, da ocenjuje tveganja pri implementaciji UI

	Povprečno ocenjena pozitivnost ukrepa
1	Omejitev obsega delovanja UI in omejitev uporabnikov
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva
3	Zmanjševanje nedoločljivosti AI-user interakcij
4	Sistem za promocijo varovanih privatnih in osebnih podatkov
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti
8	Sistem za razlago logike in sklepanja algoritmov sistema UI
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA



Vir: lastno delo.

Dve orodji izstopata pri razliki v percepciji njune pomembnosti med domenskimi specialisti in UI&IT strokovnjaki, ki niso domenski specialisti (tabela 29):

- orodje »Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco« je za domenske specialiste pozitivnejše za 23 odstotnih točk,
- orodje »Zaledni sistem, namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence« pa je pozitivnejše za 19 odstotnih točk.

Prvo orodje lahko vpliva na tveganja, ki zadevajo razumljivost zmogljivosti sistema UI in razumljivost možnosti omejevanja vhodnih podatkov v sistem UI ter omejevanja izhodov iz sistema UI. Drugo orodje se nanaša na zmožnost zavestnega vpliva uporabnikov oz. organizacije na delovanje sistema UI in omogoča večjo odzivnost na potrebe, spremembe in priložnosti ter naslavljanje s tem povezanih tveganj. Po drugi strani je zanimivo, da vse tri

skupine odločevalcev izražajo najmanjšo sposobnost ocenjevanja tveganj prav v zvezi z »Razumljivostjo zmožnosti sistema UI in razumljivostjo omejitev vhodnih in izhodnih podatkov« (tabela 26). To potrjuje tezo, da lahko sistem umetne inteligence (brez kakršnih koli dodatnih orodij in ukrepov) uporabnikom in organizaciji ponuja nepredstavljivo in nenadzorovano širok nabor rezultatskih možnosti. Ne more tudi preprečiti ali nadzorovati analize in obdelave vseh informacij, do katerih ima posamezni uporabnik dostop (informacij, ki jih izmenjuje s sistemom UI), zaradi česar je izvedba ocene tveganj zelo težko izvedljiva.

Pomanjkanje razumevanja dejanskih zmogljivosti, sposobnosti in dometa sistema UI ter pomanjkanje razumevanja posledic njegovega delovanja z vidika nestrokovnjakov za umetno inteligenco, so predvsem domenski specialisti prepoznali kot kritično slabost v zvezi s sposobnostjo ocenjevanja tveganj, in preko preferiranih orodij in ukrepov izrazili interes iskanja rešitev za ta problem. V manjši meri so to prepoznali UI&IT strokovnjaki. Prav tako so domenski specialisti preko preferiranih orodij in ukrepov izrazili potrebo po sistemu, ki bi jim omogočil večji vpliv na opredeljevanje dosegljivih zmogljivosti, sposobnosti in dometa sistema UI ter vpliv na uravnavanje posledic delovanja sistema umetne inteligence.

Tabela 30: Odstotkovno izražena pomembnost ukrepov/orodij, ki povečujejo organizacijsko zmožnost ocenjevanja tveganj (po zbirnih skupinah intervjuvancev) - zeleno so označene pozitivnosti nad 75 % in rdeče pozitivnosti pod 40 %

		Oznaka	A, a		B		1		2		1-3	
		Opis	UI ali IT strokovnjak		Domenski specialist		Odločevalec		Udeleženec odločanja		Seznanjen z ocenjevanjem tveganj	
		Št. inter.	12		12		13		11		21	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		90%	94%	90%	90%	92%	96%	86%	86%	89%	92%
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		59%	65%	67%	67%	60%	66%	66%	66%	61%	64%
3	Zmanjševanje nedoločljivosti AI-user interakcij		46%	65%	57%	59%	56%	67%	45%	55%	51%	63%
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		75%	81%	80%	80%	79%	83%	75%	78%	79%	82%
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		54%	67%	73%	78%	67%	79%	58%	63%	62%	73%
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		54%	65%	58%	60%	67%	73%	43%	50%	59%	67%
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		46%	56%	50%	52%	54%	64%	41%	43%	48%	55%
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		36%	46%	23%	25%	31%	41%	28%	31%	30%	37%
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		44%	50%	36%	41%	44%	52%	35%	38%	39%	45%
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		63%	79%	75%	84%	67%	79%	70%	85%	67%	80%
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		31%	34%	5%	9%	19%	25%	18%	18%	20%	24%
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		88%	61%	91%	68%	94%	67%	83%	60%	89%	63%

Vir: lastno delo.

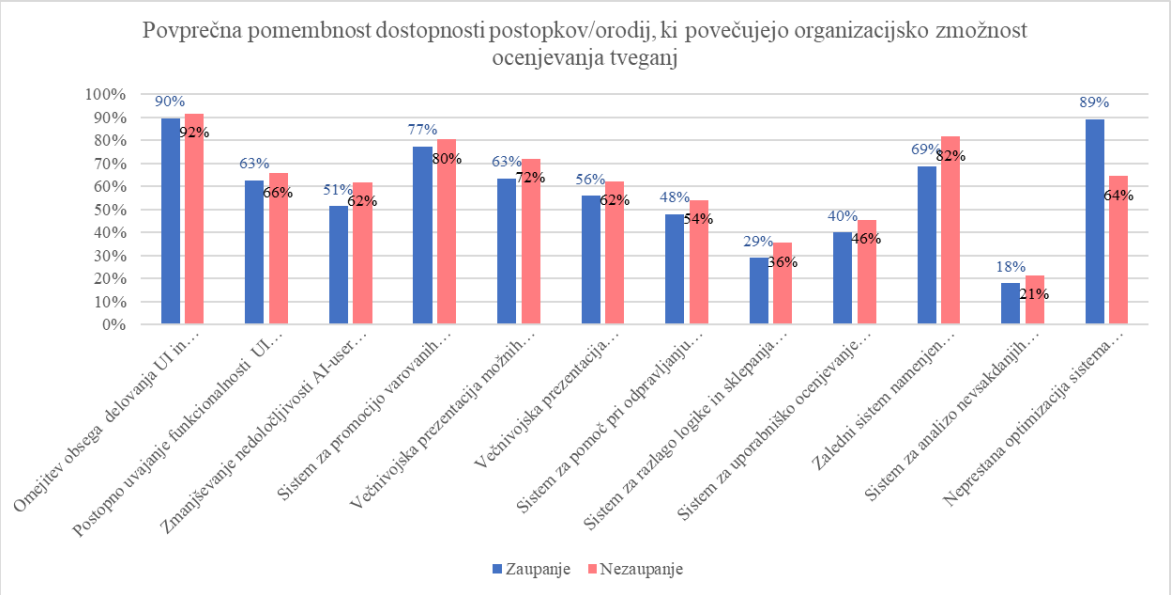
Za razjasnjevanje vprašanja »Kako lahko z nekaterimi ukrepi v fazi odločanja o uvedbi sistema umetne inteligence pomagajo odločevalcem pri njeni uvedbi bolje ocenjevati tveganja povezana z uvedbo?« sem se osredotočil zgolj na analizo skupin intervjuvancev, kot jih kaže tabela 30, saj te skupine predstavljajo tiste, ki hkrati sodelujejo v postopkih odločanja o implementaciji in so tudi vključeni v postopek ocenjevanja tveganj. V

nadaljevanju sem zaznane ocene posameznih ukrepov/orodij, če so uvedeni skupaj z uvedbo sistema umetne inteligence, preračunal v njihovo procentualno izraženo pozitivnost po enačbi (1). Komentar: ocena 1 predstavlja 0 %, ocena 5 pa 100 %.

$$Pozitivnost = ((Ocena - 1) \ / 4) * 100\ \% \qquad (1)$$

Pozitivnost nekaterih ukrepov se precej spreminja glede na pričakovano stopnjo zaupanja v strokovno znanje o umetni inteligenci. Razlika je še bolj opazna, kot je bilo predstavljeno na podlagi rezultatov vseh intervjuvancev in je ponazorjena na tabeli 31:

Tabela 31: Percepcija odločevalcev o pozitivnosti ukrepov in orodij, ki povečujejo sposobnost organizacije, da ocenjuje tveganja, ki so povezana z implementacijo UI



Vir: lastno delo.

- za orodje »Zaledni sistem, namenjen nestrokovnjakom za umetno inteligenco – za prilagajanje delovanja sistema umetne inteligence« je izraženo največje povečanje vpliva na organizacijsko sposobnost ocenjevanja tveganj, če strokovnjakom za umetno inteligenco ni mogoče zaupati, v primerjavi s situacijo, ko jim je mogoče zaupati (povprečna ocena pozitivnega vpliva orodja se poveča za 13 odstotnih točk),
- za postopek »Neprekinjena optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA« je izraženo največje zmanjšanje vpliva na sposobnost ocenjevanja tveganj, če strokovnjakom za umetno inteligenco pri uvedbi ni mogoče zaupati, v primerjavi s situacijo, ko jim je mogoče zaupati (ocena pozitivnega vpliva postopka se zmanjša za 25 odstotnih točk).

Nekateri drugi izsledki pri ocenjevanju pozitivnega vpliva ukrepov in orodij (tabela 30 in tabela 32):

- Vse kategorije intervjuvancev zelo pozitivno ocenjujejo ukrep: »Omejitev obsega delovanja umetne inteligence in omejitve uporabnikov«. Pozitivnost tega ukrepa se giblje med 81 % in 97 %.
- Vse skupine intervjuvancev ocenjujejo ukrep vzpostavitve »Sistema za spodbujanje zaščitenih zasebnih in osebnih podatkov« s pozitivnostjo med 72 % in 85 %.
- Vzpostavitev »Zalednega sistema, namenjenega nestrokovnjakom na področju umetne inteligence – za prilagoditev delovanja sistema umetne inteligence« domenski specialisti ocenjujejo kot zelo pozitivno (med 72 % in 87 %) ne glede na stopnjo zaupanja v »strokovno znanje na področju umetne inteligence«. Domenski specialisti ukrep ocenjujejo s pozitivnostjo med 72 % in 77 % tudi v situaciji, ko gre zaupati »strokovnemu znanju na področju umetne inteligence«, medtem ko njegova pozitivnost v tej situaciji pri UI&IT strokovnjakih, ki niso domenski specialisti pade na 50 %, kar je v skladu s prejšnjimi utemeljitvami.
- V primeru zaupanja v »strokovno znanje o umetni inteligenci« vse skupine kažejo med 80 % in 94 % pozitivnosti za ukrep »Nenehna optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA«. Pozitivnost razumljivo močno pade, če strokovnemu znanju o umetni inteligenci ni mogoče zaupati (60 % do 68 %).
- Preseganje 75-odstotne pozitivnosti za posamezen ukrep je zaznati le še pri vzpostavitvi orodja »Večstopenjska predstavitev možnih področij rezultatov sistema umetne inteligence, prilagojena razumljivosti za nestrokovnjake s področja umetne inteligence«, in sicer pri domenskih specialistih in odločevalcih, v situaciji, ko strokovnemu znanju o umetni inteligenci ni mogoče zaupati.

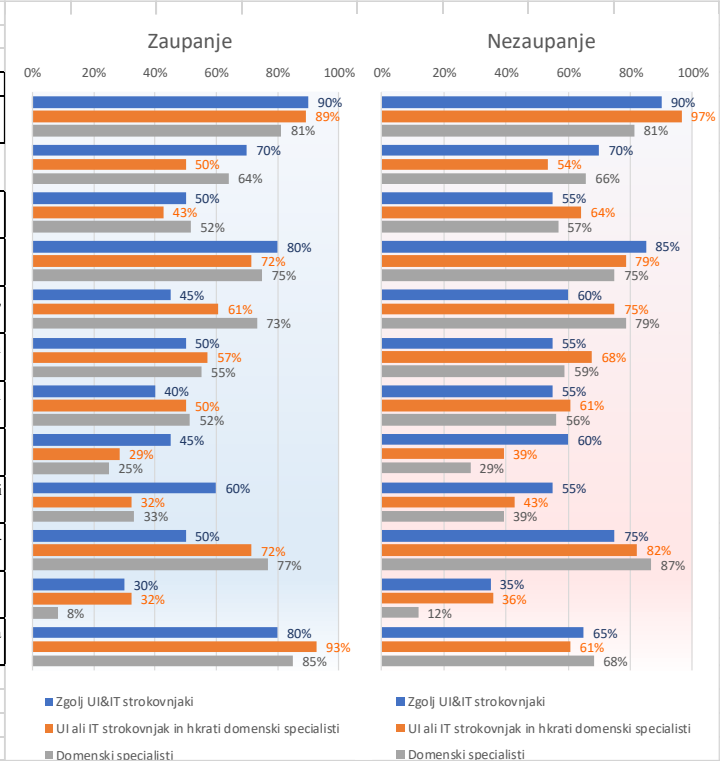
Najslabše so bili ocenjeni ukrepi:

- »Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI« - zgolj med 5 % in 36 % za različne skupine intervjuvancev.
- »Sistem za razlago logike in sklepanja algoritmov sistema UI« - med 23 % in 60 %.
- »Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI« - med 32 % in 60 %.

Pri prvih dveh »negativno ocenjenih ukrepih« obstaja velika razlika v dojemanju njihove pozitivnosti med UI&IT strokovnjaki in domenskimi specialisti. Rezultati kažejo, da domenski specialisti ne pripisujejo velikega pomena razumljivosti samih algoritmov in razumljivosti razlage, kako sistem umetne inteligence pride do posamezne odločitve (povprečna pozitivnost 24 %), še manj pa analizi nenavadnih uporab sistema umetne inteligence (povprečna pozitivnost 7 %). Z vidika razumljivosti sistema umetne inteligence jih bistveno bolj zanima predstavitvena zmogljivost samega sistema umetne inteligence – sposobnost ponazarjanja, kaj je z njim mogoče in dovoljeno doseči. Izražena povprečna pozitivnost za ta ukrep je pri njih 76 %.

Tabela 32: Pozitivnost ukrepov ob implementaciji UI z vidika treh skupin odločevalcev

	Ukrepi in orodja
1	Omejitev obsega delovanja UI in omejitev uporabnikov
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva
3	Zmanjševanje nedoločljivosti AI-user interakcij
4	Sistem za promocijo varovanih privatnih in osebnih podatkov
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti
8	Sistem za razlago logike in sklepanja algoritmov sistema UI
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA



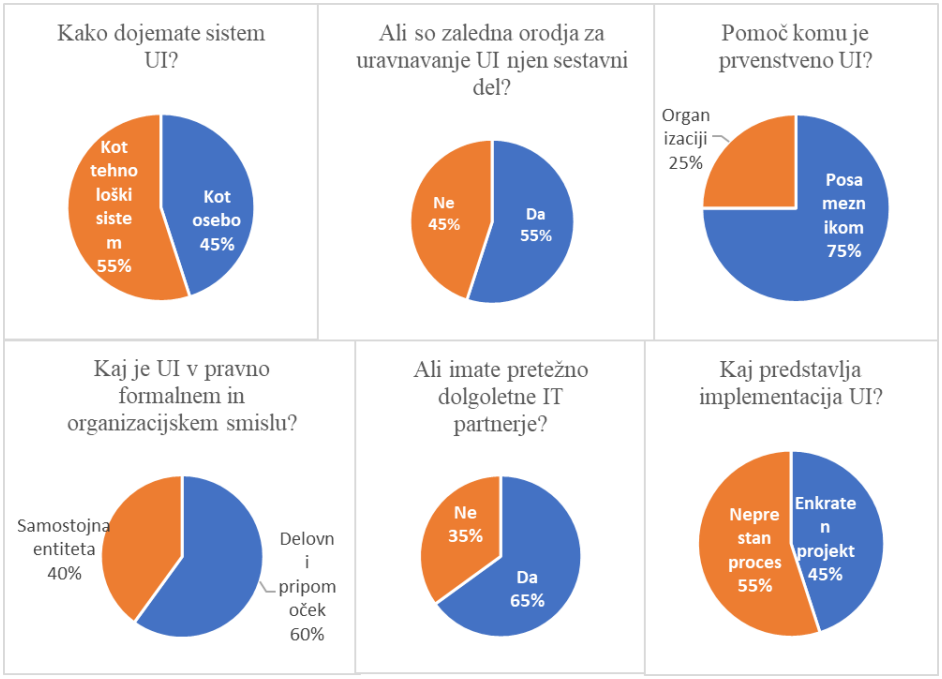
Vir: lastno delo.

Pri domenskih specialistih je opazno izraženo zavedanje povezave med percepcijo negotovosti pri ocenjevanju tveganj (tabela 20), povezanih s transparentnostjo in odgovornostjo (zgolj 16 % izražene sposobnosti) in pozitivnostjo ukrepa, ki povečuje splošno uporabniško razumljivost sistema UI. Prav tako domenski specialisti izražajo zelo nizko sposobnost ocenjevanja tveganj (tabela 20), povezanih z etičnimi vidiki uvedbe in uporabe sistema UI (povprečno zgolj 14 % izražene sposobnosti). Zanimivo je, da tako menijo tudi tisti domenski specialisti, ki so hkrati UI&IT strokovnjaki, kar je v nasprotju z mnenjem UI&IT strokovnjakov, ki niso hkrati domenski specialisti. Ti menijo, da je morebitni obstoj trditev ponudnikov sistemov UI, da njihovi sistemi UI upoštevajo etične norme, lahko zadosten razlog, da ni potrebno preverjati tveganj v zvezi s tem oz. da so tveganja v zvezi s tem relativno nizka.

Tudi nestrukturiran del pogovorov z intervjuvanci, ki so vključeni v odločevalski proces, je pokazal nekaj zanimivosti (tabela 33 in tabela 34). 45 % intervjuvancev meni, da bi sistem UI lahko obravnavali tako kot tehnološki sistem kot osebo. Ocenili so, da so po primernosti uporabe učljivost, komunikativnost, sposobnost reševanja problemov, prilagodljivost in integriteta tiste človeške lastnosti, ki najbolje opisujejo sistem UI. 75 % jih meni, da bo sistem UI bolj pomagal posameznikom pri njihovih vsakodnevnih delovnih opravilih, kot sami organizaciji. 40 % jih meni, da bi bilo treba sistem UI obravnavati kot neodvisno entiteto v pravnem, formalnem in organizacijskem smislu. 55 % jih meni, da je po uvedbi sistema UI pričakovati nenehno potrebo po njegovi optimizaciji, nadgradnji in prilagajanju

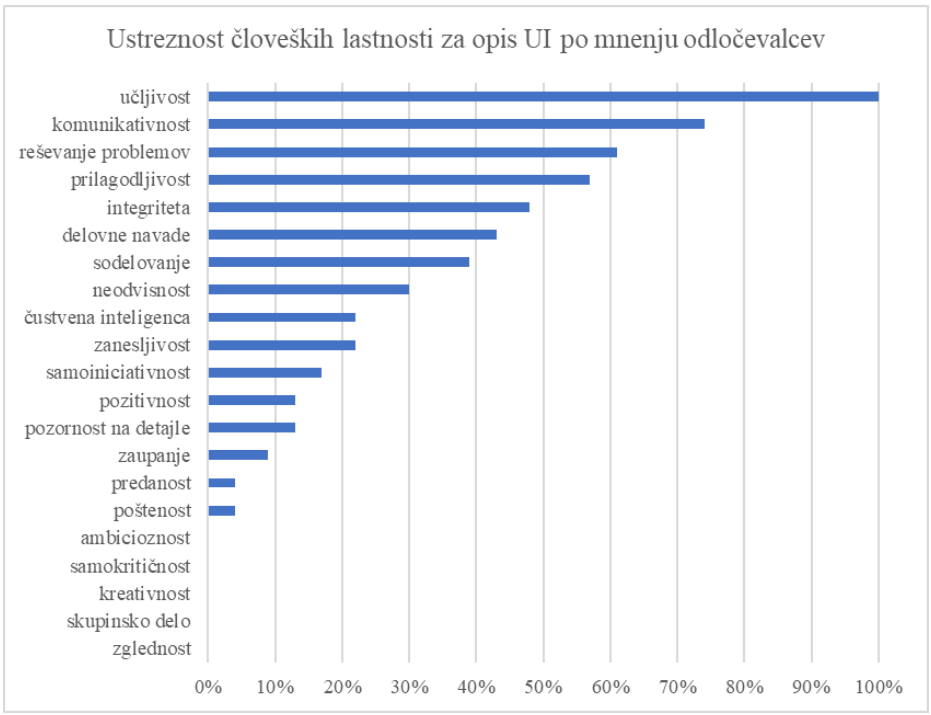
sprotnim potrebam organizacije, skladno s stanjem najsodobnejše tehnologije. 55 % jih tudi meni, da so zaledni sistemi, ki bi pomagali organizaciji pri samostojnejšem uravnavanju sistema UI, njegov sestavni del, ne glede na uporabljeno tehnologijo.

Tabela 33: Grafični prikaz dodatnih informacij, ki so bile zbrane med odločevalci



Vir: lastno delo.

Tabela 34: Človeške lastnosti, ki po mnenju odločevalcev najbolje opisujejo UI



Vir: lastno delo.

5 RAZPRAVA

Osredotočanje na mnenje domenskih specialistov, ki hkrati niso tudi UI ali IT strokovnjaki, je pokazalo potrebo po uporabi določenih ukrepov ali orodij, kar bi organizacijam brez poglobljenega strokovnega znanja o UI omogočalo lažje obvladovanje tveganj bodisi s povečevanjem razumljivosti oz. z obvladovanjem in omejevanjem področij, s katerimi naj se sistem UI sooča, bodisi z orodji, ki bi pomagali omejevati možne načine uporabe sistema UI glede na karakteristike in potrebe posameznih skupin uporabnikov.

Večji poudarek na sposobnost zagotavljanja zgolj želenih funkcionalnosti sistemov UI z vidika organizacije ter na spremljanje njihovih učinkov in koristi ter manjši poudarek na tehnično-organizacijsko-etični vidik uvedbe in uporabe sistema UI je skladen z navajanji Raji in drugi (2022).

Majhna sposobnost domenskih specialistov pri ocenjevanju tveganj, povezanih s transparentnostjo in odgovornostjo, ter njihova nizko izražena sposobnost ocenjevanja tveganj, povezanih z etičnimi vidiki uvedbe in uporabe sistema UI, pritrjuje ugotovitvam Bengio in drugi (2024). Avtorji pravijo, da je to posledica trenutno nezadostno implementirane institucionalne zaščite uporabnikov UI in posledica nezagotavljanja odgovornosti velikih ponudnikov storitev UI za škodo, nastalo z uvedbo in uporabo njihovih storitev UI z nejasno opredeljenimi tveganji.

Tako kot Krieger in drugi (2024) tudi raziskava kaže, da občutek organizacije, da lahko obvladuje in vpliva na uporabniško izkušnjo vseh skupin uporabnikov, pozitivno vpliva na percepcijo tveganja. Domenski specialisti to obvladovanje izražajo preko pomembnosti orodij in ukrepov, ki uporabniško izkušnjo izboljšujejo. Tako kot Krieger in drugi (2024), vse skupine intervjuvancev izražajo veliko naklonjenost metodam za obvladovanje privatnih in osebnih podatkov (obvladovanju zasebnosti).

Izsledki raziskave tudi pritrjujejo raziskavi Klyman (2024), ki z ciljem zmanjševanja tveganj priporoča omejevanje in determiniranje sistemov UI v smislu kaj sistem lahko dela in česa ne, kakšna je namenska uporaba sistema in kakšna je razmejitev odgovornosti za škodljive posledice delovanja sistema UI.

Izsledki kategorizacije vrst tveganj »The AIR Taxonomy« (Zeng in drugi, 2024) pojasnjujejo, zakaj nihče izmed intervjuvancev ne bi znal odgovoriti na vprašanje v zvezi z razmejitvijo odgovornosti za posledice škodljivih efektov delovanja sistema UI med različnimi deležniki. Zeng in drugi (2024) namreč pojasnjujejo, da je opredelitev tveganj pri največjih ponudnikih storitev UI celo podrobnejša od regulatornih zahtev posameznih jurisdikcij, vendar se med seboj opredelitve zelo razlikujejo in so večkrat oblikovane v obliki priporočil, smernic in teženj in ne v obliki deklarativnih zahtev in trditev.

Zanimiva je tudi primerjava človeških lastnosti: učljivosti, komunikativnosti, sposobnosti reševanja problemov, prilagodljivosti in integritete, ki bi po mnenju intervjuvancev najbolje

opisovale sistem UI, z navajanji Sapkota in drugi (2025). Avtorji poleg učljivosti, sposobnosti samostojnega reševanja problemov in prilagodljivosti omenjajo še proaktivnost sistema UI kot značilnost prihajajočih sistemov UI, ki se za razliko od tradicionalnih modelov umetne inteligence ne bodo odzivali zgolj na vnose oz. zahteve uporabnikov. Tudi percepcija skoraj polovice intervjuvancev se strinja z Bankins in drugi (2024), ki opozarjajo na vse večjo integracijo UI v organizacijske prakse in procese, zaradi česar je razumevanje njenega vpliva na organizacijo dela v podjetjih ključnega pomena.

5.1 Prispevek k stroki in omejitve raziskave

Nisem zaznal raziskovalnega dela, ki bi preučeval uvajanje umetne inteligence v organizacijah z malo dostopnega znanja o umetni inteligenci z vidika želj in dilem odločevalcev v teh organizacijah, v povezavi z njihovo zmožnostjo obravnavanja tveganj, povezanih z implementacijo ali uporabo sistema UI. V tem smislu raziskava preučuje vidike uvajanja sistemov umetne inteligence, ki so do sedaj malo raziskani, kar vpričo že zdaj izjemno pomembne in v prihodnje pričakovano še pomembnejše vloge UI v družbi ni zanemarljivo.

Izsledki te raziskave so že vključeni v prodajne strategije ponudnika sistemov in storitev UI, ki bo skušal njene izsledke uporabiti kot diferenciatorje njegove konkurenčnosti pri prodiranju na trg malih in srednjih podjetij.

Obstoječo raziskavo bi se dalo razširiti z analiziranjem razlik med pridobljenimi rezultati intervjuvancev glede na velikost njihove organizacije. V primeru nadaljevanja podobnih raziskav bi kredibilnost izsledkov povečala obdelava večjega števila intervjuvancev ali anketirancev, vendar se po drugi strani zavedam problematike zbiranja relevantnih in preverjeno razumljenih informacij. Pri tem je omembe vredna omejitev za takšno raziskavo tudi (ne)pripravljenost organizacij, da bi sodelovale pri raziskavi, saj vsak tovrsten intervju terja veliko poglabljanja in časa, predvsem pa intervjuvanci zahtevajo zaupnost in anonimizacijo deljenih informacij. Zanimivo bi bilo raziskovati tudi dejavnike, ki vplivajo na dostopnost strokovnega znanja o umetni inteligenci, in dejavnike, ki vplivajo na stopnjo zaupanja vanjo ter njihov vpliv na percepcijo uporabnosti različnih ukrepov in orodij, ki jih organizacije pogrešajo pri implementaciji in uporabi UI. Spreminjanje percepcije uporabnosti ukrepov in orodij bi bilo zanimivo preučevati tudi z vidika medsebojnih vplivov različnih skupin deležnikov znotraj iste organizacije. V ta namen bi bilo seveda potrebno identificirati vplivne dejavnike, ki učinkujejo na ta medsebojni vpliv.

Izbrana raziskovalna metoda, ki je vključevala izvajanje strukturiranih intervjujev, predstavlja kompromis med dobrimi in slabimi platmi intervjujev na eni strani in anket na drugi strani. Prvi, med drugim, omogočajo poglobljeno in potrebam prilagojeno seznanjanje intervjuvancev z raziskovalnimi vprašanji in posledično zagotavljanje, da so odgovori res pridobljeni na zadostno podobni osnovi razumevanja raziskovalne problematike pri vseh

intervjuvancih. Ankete na drugi strani omogočajo zbiranje večjega števila podatkov, predvsem pa njihovo strukturiranje in posledično lažjo in kvalitetnejšo analizo.

Uporabljena raziskovalna metoda zaradi intenzivnega interaktivnega odnosa med raziskovalcem in intervjuvanci po mojem mnenju ne zagotavlja nujno nepristranskosti dobljenih rezultatov. Del intervjuvancev namreč na začetku intervjujev ni imel jasno izoblikovanega mnenja glede raziskovalnih vprašanj. Stališča so v določeni meri oblikovali med intervjujem samim. Čeprav sem veliko pozornost polagal na nevtralnost pogovorov in svojih komentarjev ter nesugestivnost pri iskanju odgovorov na raziskovalna vprašanja, ne gre zanemariti možnosti, da sem z vidika raziskave pristransko vplival na intervjuvance.

6 SKLEP

Raziskava kaže, da se dojemanje odločevalcev, ki nimajo dostopa do zadostnega strokovnega znanja o umetni inteligenci, nekoliko razlikuje od dojemanja tistih, ki to znanje imajo na voljo ali menijo, da do njega lahko dostopajo. Opazna je razlika v razumevanju pomena orodij, ki bi organizaciji omogočala obvladovanje tveganj pri implementaciji sistemov umetne inteligence in pri njihovi uporabi. Tisti brez ustreznega znanja o umetni inteligenci izražajo:

- potrebo po orodju, ki uporabnikom omogoča njihovemu razumevanju prilagojeno predstavitev zmožnosti sistema umetne inteligence, omejitev in obvladovanje nekontrolirane izmenjave zaupnih podatkov s sistemom umetne inteligence ter izboljšano razumevanje mogočih uporab rezultatov sistema umetne inteligence,
- potrebo po zalednem sistemu, namenjenemu nestrokovnjakom na področju umetne inteligence, za prilagajanje in usmerjanje operativnega delovanja sistema umetne inteligence.

Opisano orodje in zaledni sistem opredeljujejo odločevalci kot sestavni del sistema umetne inteligence, neodvisno od uporabljene tehnologije.

Raziskava nakazuje, da podjetja z malo dostopnega znanja o umetni inteligenci, iščejo ponudnike sistemov umetne inteligence, ki bi jim omogočili večjo mero avtonomije vpliva na delovanje teh sistemov, ko so enkrat uvedeni, ne da bi za vsako intervencijo potrebovali zunanjo strokovno pomoč. Na umetno inteligenco gledajo tudi kot na novega zaposlenega in ne zgolj kot na neki tehnološki sistem. Nanjo želijo imeti vpliv v smislu njenega usmerjanja in njenega omejevanja, podobno kot pri delavcih.

SEZNAM KLJUČNE LITERATURE

1. Bankins, S., Ocampo, A. C., Marrone, M., Restubog, S. L. D. in Woo, S. E. (2024). A multilevel review of artificial intelligence in organizations: Implications for

organizational behavior research and practice. *Journal of organizational behavior*, *45*(2), 159-182. https://doi.org/10.1002/job.2735
2. Bengio, Y., Hinton, G., Yao, A., Song, D., Abbeel, P., Darrell, T., ... Mindermann, S. (2024). Managing extreme AI risks amid rapid progress. *Science*, *384*(6698), 842-845.. https://doi.org/10.1126/science.adn0117
3. Mohseni, S., Zarei, N. in Ragan, E.D. (2021). A Multidisciplinary Survey and Framework for Design and Evaluation of Explainable AI Systems. *ACM Transactions on Interactive Intelligent Systems (TiiS), 11(3-4), 1-45.* https://dl.acm.org/doi/10.1145/3387166
4. Raji, I. D., Kumar, I. E., Horowitz, A. in Selbst, A. D. (2022). The Fallacy of AI Functionality. *In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency,* 959-972. https://doi.org/10.1145/3531146.3533158
5. Rane, N.L., Choudhary, S.P. in Rane, J. (2024). Acceptance of artificial intelligence: key factors, challenges, and implementation strategies. *Journal of Applied Artificial Intelligence, 5*(2), 50-70. https://doi.org/10.48185/jaai.v5i2.1053
6. Ribera, M. in Lapedriza, A. (2019, 20. marec). Can we do better explanations? A proposal of user-centered explainable AI. *Joint Proceedings of the ACM IUI 2019Workshops*, Los Angeles, USA, March 20, 2019, dosegljivo na: http://hdl.handle.net/10609/99643
7. Virvou, M. (2023) Artificial Intelligence and User Experience in reciprocity: Contributions and state of the art. *Intelligent Decision Technologies,* 17 (2023) 73–125. https://journals.sagepub.com/doi/pdf/10.3233/IDT-230092

LITERATURA IN VIRI

1. Al-Ansari, N., Al-Thani, D. in Al-Mansoori, R.S. (2024). User-Centered Evaluation of Explainable Artificial Intelligence (XAI): A Systematic Literature Review. Wiley, Human Behavior and Emerging Technologies, 1(2024), 4628855, 1-28. https://doi.org/10.1155/2024/4628855
2. Anderljung, M., Hazell, J. in von Knebel, M. (2024). Protecting society from AI misuse: when are restrictions on capabilities warranted?. *AI & SOCIETY*, *40*(5), 3841-3857. https://doi.org/10.1007/s00146-024-02130-8
3. Butler, T., Espinoza-Limón, A. in Seppälä, S. (2021). Towards a capability assessment model for the comprehension and adoption of AI in organisations. *Journal of AI, Robotics & Workplace Automation*, 1(1), Autumn/Fall 2021, 18-33. https://www.ingentaconnect.com/content/hsp/airwa/2021/00000001/00000001/art00004
4. Chollet, F. (2025, 16. junij). *How We Get To AGI*. [Video: posneto na AI Startup School, San Francisco]. YouTube. Pridobljeno 24. junija 2025 s https://youtu.be/5QcCeSsNRks?si=xEU3R4aJu9BwSg0H
5. Chowdhury, S., Dey, P., Joel-Edgar, S., Bhattacharya, S., Rodriguez-Espindola, O., Abadie, A. in Truong, L. (2023). Unlocking the value of artificial intelligence in human

resource management through AI capability framework. *Human resource management review*, *33*(1), 100899. https://doi.org/10.1016/j.hrmr.2022.100899

6. Diary Of A CEO (2025, 12. maj). *AI Agents Emergency debate: These jobs won't exist in 24 months! We must prepare for what's coming!* [Video]. YouTube. Pridobljeno 2. junija 2025 s https://www.youtube.com/watch?app=desktop&v=JMYQmGfTltY
7. Findlay, G., Marshall, W., Albantakis, L., David, I., Mayner, W. G., Koch, C. in Tononi, G. (2024). Dissociating artificial intelligence from artificial consciousness. *arXiv preprint arXiv:2412.04571v2*. https://doi.org/10.48550/arXiv.2412.04571
8. Google (2025, 9. april). *A new era of Agent Interoperability*. [Blog: Google announcing the Agent2Agent Protocol (A2A)]. https://developers.googleblog.com/en/a2a-a-new-era-of-agent-interoperability/
9. Guan, H., Dong, L. in Zhao, A. (2022). Ethical Risk Factors and Mechanisms in Artificial Intelligence Decision Making. *Behav. Sci.*, 2022, 12, 343. https://doi.org/10.3390/bs12090343
10. Guest, G., Bunce, A. in Johnson, L. (2006). How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59-82. https://doi.org/10.1177/1525822X05279903
11. Habbal A., Khalif Ali M. in Ali Abuzaraida M. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. Expert Systems with Applications, 240, 2024, 122442, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2023.122442
12. ISACA AI Pulse Poll (2024). *The AI Reality: IT Pros Weigh in On Knowledge Gaps, Policies, Jobs Outlook and More*. ISACA. https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/infographics/2024-global-ai-infographic-524.pdf
13. Karpathy, A. (2025, 17. junij). *Software Is Changing (Again).* [Video: posneto na AI Startup School, San Francisco]. YouTube. Pridobljeno 24. junija 2025 s https://youtu.be/LCEmiRjPEtQ?si=9zcS9dAUuKyT6OzF
14. Keding, C. in Meissner, P. (2021). Managerial Overreliance on AI-Augmented Decision-Making Processes: How the Use of AI-Based Advisory Systems Shapes Choice Behavior in R&D Investment Decisions. *Technological Forecasting and Social Change*, 171: 120970. https://doi.org/10.1016/j.techfore.2021.120970
15. Kim, H., Yi, X., Yao, J., Lian, J., Huang, M., Duan, S., ... Xie, X. (2024). The road to artificial superintelligence: A comprehensive survey of superalignment. arXiv preprint arXiv:2412.16468. https://arxiv.org/abs/2412.16468
16. Klyman K. (2024). Acceptable Use Policies for Foundation Models. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 7(1), 752-767. https://doi.org/10.1609/aies.v7i1.31677
17. Krieger, J. B., Bouder, F., Wibral, M. in Almeida, R. J. (2024). A systematic literature review on risk perception of Artificial Narrow Intelligence, *Journal of Risk Research*, 1-19. https://doi.org/10.1080/13669877.2024.2350725

18. Krook, J., Winter, P., Downer, J. in Blockx, J. (2025). A systematic literature review of artificial intelligence (AI) transparency laws in the European Union (EU) and United Kingdom (UK): a socio-legal approach to AI transparency governance. *AI and Ethics*, 1-22. https://doi.org/10.1007/s43681-025-00674-z
19. Le Sénat français. (2025, 10. junij). *Audition de MM. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France.* Le Sénat français:Comptes rendus de la ce commande publique, Mardi 10 juin 2025. https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html?utm_source=chatgpt.com
20. Lebovits H. (2019) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, *Public Integrity, 21:4, 448-452*, https://doi.org/10.1080/10999922.2018.1511671
21. Litan, A. (2024). *Tackling Trust, Risk and Security in AI Models*. Gartner. Pridobljeno 2. junija 2025 s https://www.gartner.com/en/articles/ai-trust-and-ai-risk
22. Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., ... Oak, S. (2025). Artificial intelligence index report 2025. *arXiv preprint arXiv:2504.07139*. https://doi.org/10.48550/arXiv.2504.07139
23. McCarthy J. (2004). *What is Artificial Intelligence?* Stanford University. Computer Science Department. https://cse.unl.edu/~choueiry/S09-476-876/Documents/whatisai.pdf
24. McCarthy, J., Minsky, M. L., Rochester, N. in Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, *27*(4), 12-12. https://doi.org/10.1609/aimag.v27i4.1904
25. McKinsey Survey (2025). *The state of AI: How organizations are rewiring to capture value*. McKinsey. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/
26. McLean, S., Read, G. J. M., Thompson, J., Baber, C., Stanton, N. A. in Salmon, P. M. (2023). The risks associated with Artificial General Intelligence: A systematic review, *Journal of Experimental & Theoretical Artificial Intelligence*, 35:5, 649-663, https://doi.org/10.1080/0952813X.2021.1964003
27. Messeri, L. in Crockett, M. J. (2024). Artificial intelligence and illusions of understanding in scientific research. Nature 627, 49–58 (2024). https://doi.org/10.1038/s41586-024-07146-0
28. Mikalef, P. in Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. *Information & management*, *58*(3), 103434. https://doi.org/10.1016/j.im.2021.103434
29. Nazar, M., Alam, M. M., Yafi, E. in Su'ud, M. M. (2021). A systematic review of human–computer interaction and explainable artificial intelligence in healthcare with artificial intelligence techniques. *IEEE Access*, *9*, 153316-153348. doi: 10.1109/ACCESS.2021.3127881.

30. Ranjan, C., Chatterjee, S., Vrontis, D. in Thrassou, A. (2021). Adoption of Robust Business Analytics for Product Innovation and Organizational Performance: The Mediating Role of Organizational Data-Driven Culture. *Annals of Operations Research,* (2024) 339:1757–1791. https://doi.org/10.1007/s10479-021-04407-3
31. Reis, M.I. , Gonçalves, J.N.C., Cortez, P., Carvalho, M.S. in Fernandes, J.M. (2025). A context-aware decision support system for selecting explainable artificial intelligence methods in business organizations. *Computers in Industry,* 165 (2025) 104233. https://doi.org/10.1016/j.compind.2024.104233
32. Russell, S. J. in Norvig P. (1995). Artificial Intelligence A Modern Approach. *Artificial Intelligence. Prentice-Hall, Egnlewood Cliffs* 25.27 (1995): 79-80. ISBN 0-13-103805-2
33. Sapkota, R., Roumeliotis K. I. in Karkee M. (2025). AI Agents vs. Agentic AI: A Conceptual Taxonomy, Applications and Challenges. *arXiv preprint arXiv:2505.10468v4*. https://arxiv.org/pdf/2505.10468v4
34. Sherman, E. in Eisenberg, I. (2024). Ai risk profiles: A standards proposal for pre-deployment ai risk disclosures. In *Proceedings of the AAAI Conference on Artificial Intelligence.* 38 (21), 23047-23052). https://doi.org/10.1609/aaai.v38i21.30348
35. Slattery, P., Saeri, A. K., Grundy, E. A., Graham, J., Noetel, M., Uuk, R., ... in Thompson, N. (2024). The AI risk repository: A comprehensive meta-review, database, and taxonomy of risks from artificial intelligence. *arXiv preprint arXiv:2408.1262*. https://arxiv.org/pdf/2408.12622
36. Stein, A. L. (2022). Assuming the risks of artificial intelligence. *Boston University Law Review*, 102 (3), 979-1036. Preneseno iz HeinOnline: file:///C:/Users/beno/Downloads/ssrn-4076188.pdf
37. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser. Ł. in Polosukhin, I. (2017). Attention is all you need. *Advances in neural information processing systems*, *30*. ISBN: 9781510860964.
38. Von Eschenbach, W. J. (2021). Transparency and the black box problem: Why we do not trust AI. *Philosophy & Technology*, *34*(4), 1607-1622. https://doi.org/10.1007/s13347-021-00477-0
39. Wamba-Taguimdje, S. L., Wamba, S. F., Kamdjoug, J. R. K. in Wanko, C. E. T. (2020). Influence of artificial intelligence (AI) on firm performance: the business value of AI-based transformation projects. *Business process management journal*, *26*(7), 1893-1924. https://doi-org.ezproxy.lib.ukm.si/10.1108/BPMJ-10-2019-0411
40. Wang, B., Chen, W., Pei, H., Xie, C., Kang, M., Zhang, C., ... in Li, B. (2023). DecodingTrust: A Comprehensive Assessment of Trustworthiness in GPT Models. *arXiv preprint arXiv:2306.11698v1*. Dosegljivo na: https://blogs.qub.ac.uk/wp-content/uploads/sites/7/2024/01/A-comprehensive-Assessment-of-Trustworthiness-in-GPT-Models.pdf
41. Wei, R. in Pardo, C. (2022). Artificial Intelligence and SMEs: How can B2B SMEs Leverage AI Platforms to Integrate AI Technologies?. *Industrial Marketing*

Management, 107 (2022), 466-483,ISSN 0019-8501, https://doi.org/10.1016/j.indmarman.2022.10.008

42. Weidinger, L., Mellor, J., Rauh, M., Griffin, C., Uesato, J., Huang, P. S., ... in Gabriel, I. (2021). Ethical and social risks of harm from language models. *arXiv preprint arXiv:2112.04359*. https://arxiv.org/abs/2112.04359
43. Westphal, M., Vössing, M., Satzger, G., Yom-Tov, G. B. in Rafaeli, A. (2023). Decision control and explanations in human-AI collaboration: Improving user perceptions and compliance. *Computers in Human Behavior*, *144*, 107714. https://doi.org/10.1016/j.chb.2023.107714
44. White House. (2023). *President Biden Issues Executive Order on Safe, Secure and Trustworthy Artificial Intelligence in.: Imperative on tech companies to share information with the government.* The White House. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
45. Wongso, B., Lienaka, K. N., Firstian, V. in Magdalena, Y. (2024). User-centered design in AI applications: a systematic literature review. In *2024 International Conference on Information Management and Technology (ICIMTech).* 524-529. IEEE. DOI: 10.1109/ICIMTECH63123.2024.10780823
46. Zeng, Y., Klyman, K., Zhou, A., Yang, Y., Pan, M., Jia, R., ... Li, B. (2024). Ai risk categorization decoded (air 2024): From government regulations to corporate policies. *arXiv preprint arXiv:2406.17864*. https://arxiv.org/abs/2406.17864

PRILOGE

Priloga 1: Struktura intervjujev in vprašanja

Uvodni del: Začetna vprašanja (4 vprašanja)

Prosim, opišite se. Označite vsaj eno možnost.

- Strokovnjak za umetno inteligenco
- IT-strokovnjak
- Strokovnjak za določeno področje
- Laični uporabnik umetne inteligence

Ali je del vašega dela v vaši organizaciji tudi vplivanje na odločitve glede pridobitve, razvoja ali uvajanja novega izdelka, storitve, IT-izdelka ali IT-storitve?

- Da, sem odločevalec
- Da, sem "del" procesa odločanja
- Ne

Ste v zasebnem življenju že kdaj pridobili IT izdelke ali IT storitve?

- Da
- Ne

Ali poznate analizo tveganj in koristi pri odločanju o pridobitvi, razvoju ali uvedbi novega izdelka, storitve, IT-izdelka ali IT-storitve? Označite najboljši odgovor. Zasebni/poklicni vidik ni pomemben.

- Uporabljam ga ves čas
- Uporabljam ga včasih
- Sem vključen v ta proces
- Seznanjen sem z njim, vendar nisem vključen v
- Nisem seznanjen z njim

1. del intervjuja: Identifikacija tveganj (2 vprašanji)

A1) Katera tveganja (poleg samega tveganja uvajanja) morate upoštevati pri razmišljanju o uvajanju funkcionalnosti umetne inteligence (eden od dveh opisanih primerov)?

A2) Seznam kategorij tveganj, specifičnih za umetno inteligenco – označite, če razumete kategorijo tveganja ali/in podajte nov predlog.

- Seznanjen/a sem z vsemi.
- Pristranskost in pravičnost: Sistemi umetne inteligence lahko podedujejo pristranskosti iz svojih učnih podatkov, kar vodi do nepoštenih ali diskriminatornih rezultatov. Pristranski algoritmi lahko na primer vplivajo na postopke zaposlovanja ali odobritve posojil.

- Zasebnost in varnost: Sistemi umetne inteligence pogosto zahtevajo velike količine podatkov, ki lahko vključujejo občutljive osebne podatke. Nepooblaščen dostop ali kršitve podatkov lahko ogrozijo zasebnost in varnost.
- Preglednost in odgovornost: Postopki odločanja umetne inteligence so lahko nepregledni, zaradi česar je težko razumeti, kako se odločitve sprejemajo. To pomanjkanje preglednosti lahko ovira odgovornost in zaupanje.
- Razumljivost možnosti in omejitev vhodnih in izhodnih podatkov: Umetna inteligenca lahko ponudi nepredstavljivo širok spekter rezultatov in lahko analizira vse informacije, do katerih že imate pravico dostopa. Težko je oceniti tveganja, če sta ti dve »področji« tako široki.
- Etični vidiki: Uporaba umetne inteligence lahko sproži etična vprašanja, kot sta vpliv na zaposlovanje in možnost zlorabe pri nadzoru ali avtonomnem orožju.
- Zanesljivost, integriteta in varnost: Zagotavljanje zanesljivega in varnega delovanja sistemov umetne inteligence v vseh pogojih je ključnega pomena. Napake v kritičnih sistemih, kot so zdravstvo ali avtonomna vozila, imajo lahko resne posledice.
- Upravljanje in regulacija: Vzpostavitev učinkovitih okvirov upravljanja in predpisov za obvladovanje tveganj umetne inteligence je zapletena. Zahteva ravnovesje med inovacijami in zaščito pred morebitno škodo.
- Z nobenim od njih nisem seznanjen.
- Drugo:

2. del intervjuja: Ocenjevanje tveganj (2 vprašanji)

B1) V nekaj stavkih opišite postopek ocenjevanja tveganja.

B2) Ali poznate naslednje faze ocenjevanja tveganja?

- Poznane so mi vse
- Prepoznavanje tveganja
- Ranljivosti in predispozicijski pogoji
- Verjetnost pojava tveganja
- Velikost vpliva tveganja
- Določanje tveganja
- Zmanjševanje, sprejemanje, izogibanje tveganju in delitev stroškov
- Stroški obravnave tveganja
- Z nobeno od njih nisem seznanjen/a

3. del intervjuja: Sposobnost organizacije za ocenjevanje tveganj (2 vprašanji)

C1) Bi organizacija znala oceniti vsako vrsto tveganja (pomislite na dva primera umetne inteligence)? Če je odgovor pritrdilen, označite tveganje ali predlagajte novo.

- To bi lahko storil za vse.
- Pristranskost in pravičnost: Sistemi umetne inteligence lahko podedujejo pristranskosti iz svojih učnih podatkov, kar vodi do nepoštenih ali diskriminatornih rezultatov. Na

primer, pristranski algoritmi lahko vplivajo na postopke zaposlovanja ali odobritve posojil.

- Zasebnost in varnost: Sistemi umetne inteligence pogosto zahtevajo velike količine podatkov, ki lahko vključujejo občutljive osebne podatke. Nepooblaščen dostop ali kršitve podatkov lahko ogrozijo zasebnost in varnost.
- Preglednost in odgovornost: Postopki odločanja umetne inteligence so lahko nepregledni, zaradi česar je težko razumeti, kako se odločitve sprejemajo. To pomanjkanje preglednosti lahko ovira odgovornost in zaupanje.
- Razumljivost možnosti in omejitev vhodnih podatkov in rezultatov: Umetna inteligenca lahko ponudi nepredstavljivo širok spekter rezultatov in lahko analizira vse informacije, do katerih že imate pravice dostopa. Težko je oceniti tveganja, če sta ti dve »področji« tako široki.
- Etični vidiki: Uporaba umetne inteligence lahko sproži etična vprašanja, kot sta vpliv na zaposlovanje in možnost zlorabe pri nadzoru ali avtonomnem orožju.
- Zanesljivost, integriteta in varnost: Zagotavljanje zanesljivega in varnega delovanja sistemov umetne inteligence v vseh pogojih je ključnega pomena. Napake v kritičnih sistemih, kot so zdravstvo ali avtonomna vozila, imajo lahko resne posledice.
- Upravljanje in regulacija: Vzpostavitev učinkovitih okvirov upravljanja in predpisov za obvladovanje tveganj umetne inteligence je zapletena. Zahteva uravnoteženje inovacij z zaščito pred morebitno škodo.
- Za nobenega od njih tega ne bi mogel storiti.
- Drugo:

C2) Bi bila organizacija sposobna ustrezno izvesti vsako fazo ocene tveganja pri vsaki vrsti tveganja? Če je odgovor pritrdilen, označite posamezno polje v tabeli 35.

Tabela 35: Vrste tveganj in faze njihovega ocenjevanja

	Ne za vse faze	Identifikacija tveganja	Verjetnost nastanka	Resnost vpliva	Izračun ocene	Blaženje, preprečevanje	Upravljanje incidentov
Pristranskost in pravičnost							
Zasebnost in varnost							
Transparentnost in odgovornost							
Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov							
Etični vidiki							
Zanesljivost, integriteta in varnost							
Upravljanje in regulacija							

Vir: lastno delo.

4. del intervjuja: Koristne informacije in vplivni dejavniki pri uvajanju UI (2 vprašanji)

D1) Kateri so razlogi za slabšo zmožnost ocenjevanja tveganj? Katere dodatne informacije in ukrepi bi vaši organizaciji pomagali pri postopku ocenjevanja tveganj, oz. bi vam pomagali pri odločitvi, ali je vsako od tveganj "sprejemljivo" za uvedbo funkcionalnosti umetne inteligence?

D2) Pridobljeni odgovori na spodnji seznam vprašanj lahko organizaciji olajšajo ocenitev tveganj. Preverite, ali imate, oziroma bi imeli na voljo vire za pridobitev odgovorov na vsako izmed njih v procesu odločanja.

Ali ocenjujete, da vaša organizacija lahko pridobi odgovor na vprašanja v tabeli 36 pri uvajanju UI? Za vsako vprašanje odgovorite z »da« ali »ne«.

Tabela 36: Vprašanja v zvezi s koristnimi informacijami in vplivnimi dejavniki pri uvajanju UI

1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za upravljanje poslovnih sprememb?
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali pritisk uporabnikov/javnosti/kulture za začetek uporabe umetne inteligence?
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov umetne inteligence?
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti podatkov?
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti podatkov?
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev podatkov?
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?
13	Kakšna je raven interpretativnosti modela, ali so na voljo kakšna orodja za interpretativnost?
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno inteligenco?
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne inteligence?
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju umetne inteligence, tehničnega znanja in poznavanja področja deležnikov?
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne inteligence?
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?

se nadaljuje

Tabela 36: Vprašanja v zvezi s koristnimi informacijami in vplivnimi dejavniki pri uvajanju UI (nad.)

21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki dialoga, kot so dokumenti, e-pošta, fizična dejanja ...?
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne inteligence?
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen izid?
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne inteligence?
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah aplikacij?
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence ustvari napačne, pristranske ali slabo razumljene rezultate?
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, proti dejstva ali posamezne primere?
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni vmesniki, vizualne predstavitve, odločitvena drevesa, globoke nevronske mreže, zemljevidi pomembnosti)?
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in uporabnosti?
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in multidisciplinarne ekipe z zahtevanimi veščinami in znanjem?
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje in učinkovito sodelovanje s sistemi umetne inteligence?
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do podatkov?
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z uveljavljenimi etičnimi smernicami in standardi?
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven organizacije)

se nadaljuje

Tabela 36: Vprašanja v zvezi s koristnimi informacijami in vplivnimi dejavniki pri uvajanju UI (nad.)

43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega znanja?
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema UI med ponudnikom sistema, implementatorjem sistema UI ter organizacijo-uporabnikom sistema?
46	Ali je mogoče oceniti stopnjo vpliva UI sistema na dobrobiti skupnosti deležnikov v organizaciji in izven nje?
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI?
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove zanesljivosti in varnosti?
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v realnem času?
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije?

Vir: lastno delo.

5. del intervjuja: Ukrepi pri uvajanju UI, ki povečujejo obvladovanje sistema UI z vidika nestrokovnjakov za UI (4 vprašanja)

E1) Si predstavljate kakršne koli ukrepe, ki bi lahko pomagali organizaciji, oz. osebam, ki niso strokovnjaki za umetno inteligenco, da bi lažje ocenili tveganja? Gre za ukrepe za lažje pridobivanje potrebnih informacij ali za povečevanje obvladovanja dejavnikov tveganja.

E2) Tukaj je nekaj predlogov za ukrepe. Izberite tri med njimi, ki bi vaši organizaciji bili najbolj v pomoč, ali pa podajte nov predlog:

1. Omejitev obsega delovanja sistema UI in omejitve uporabnikov: jasna opredelitev obsega uporabe umetne inteligence za različne vrste uporabnikov. Z zožitvijo fokusa na določene naloge ali domene lahko različni deležniki bolje razumejo in obvladujejo morebitna tveganja.

2. Postopno uvajanje funkcionalnosti UI in njenega vpliva: Sisteme umetne inteligence naj se uvajajo postopoma. Začne naj se z enostavnejšimi uvajanji. Širitev uvedbe naj sledi pridobitvi razumevanja in nadzora nad vedenjem sistema.

3. Zmanjševanje nedoločljivosti interakcij med UI in uporabniki: začne naj se s sistemom umetne inteligence, ki naj ima čim bolj determinirane komunikacijske kanale med uporabniki in sistemom umetne inteligence. Zmanjšuje naj se možnost izmenjave prepovedanih / zaupnih informacij.

4. Sistem za promocijo varovanih privatnih in osebnih podatkov: sistem zagotavlja, da občutljivi podatki opravijo postopek odobritve, preden se izmenjujejo z zunanjimi zmogljivostmi umetne inteligence; sistem zagotavlja spremljanje vseh takšnih dogodkov.

5. Večnivojska prezentacija možnih področij delovanja sistema UI, prilagojeno razumljivosti za nestrokovnjake za UI: uporabniški vmesnik za prezentacijo vseh poslovnih področij, procesov in aktivnosti, kjer je umetna inteligenca implementirana, in omogočanje vrtanja v globino za pridobitev več informacij.

6. Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI: uporabniški vmesnik za prezentacijo vseh uporabniških profilov s svojimi karakteristikami po poslovnih področjih, kjer je umetna inteligenca implementirana, in omogočanje vrtanja v globino za pridobitev več informacij.

7. Avtomatiziran sistem in interaktivni uporabniški vmesnik za odpravljanje težav in nerazumljivosti ter poročanje o pristranskosti.

8. Dostopnost razlag za uporabnike, da bolje razumejo osnovno logiko ali sklepanje algoritmičnega sistema UI (racionalna, pravična ali protidejstvena razlaga).

9. Uporabniško vrednotenje razumljivosti in uporabnosti UI: ocenjevanje in ponavljanje razlag s pomočjo anket, intervjujev in interaktivnega sistema zbiranja informacij uporabnikov.

10. Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema UI – uporabniški vmesnik za parametriziranje, za tokokroge odobritev in vključevanja uporabnikov v procese UI odločanja, za iskanje, za fokusiranje na določena področja, za oblikovanje rezultatov, za določanje komunikacijskih tokokrogov seznanjanja z rezultati...

11. Analiza scenarijev: sistem za izvajanje analize nevsakdanjih scenarijev in raziskovanje novih možnih rezultatov. To vključuje ustvarjanje hipotetičnih situacij, da se ugotovi, kako bi se umetna inteligenca lahko obnašala v različnih pogojih.

12. Neprestana optimizacija sistema umetne inteligence z vidika strokovnjakov za UI na podlagi SOTA: strokovnjaki za umetno inteligenco ponujajo smernice glede na namen funkcionalnosti UI, naravo vključenih podatkov, veljavne politike varstva podatkov, pravne omejitve in usmeritve, glede na sprejemljivosti tveganj za ugled organizacije in posameznikov itd.

Drugo:

E3) Vsak ukrep iz točke E2 ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, v kateri lahko organizacija popolnoma zaupa dostopnemu strokovnemu znanju o umetni inteligenci:

1 Omejitev obsega delovanja UI in omejitev uporabnikov
2 Postopno uvajanje funkcionalnosti UI in njenega vpliva

3 Zmanjševanje nedoločljivosti interakcij med UI in uporabniki
4 Sistem za promocijo varovanih privatnih in osebnih podatkov
5 Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco
6 Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI
7 Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti
8 Sistem za razlago logike in sklepanja algoritmov sistema UI
9 Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI
10 Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence
11 Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI
12 Optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA

E4) Vsak ukrep ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, ko organizacija ne more popolnoma zaupati dostopnemu strokovnemu znanju o umetni inteligenci (seznam ukrepov je bil identičen kot pri točki E2 in E3).

Drugi izsledki intervjujev

Poleg zbiranja odgovorov na opisano strukturo intervjujev sem zbiral tudi druge informacije (vprašanja in odgovore), med katerimi sem v analizo vključil tista vprašanja, na katera sem pridobil odgovore od 23 izmed 28 intervjuvancev (82 %):

- ali smatrate/obravnavate sistem UI kot tehnološki sistem, kot osebo ali kot oboje?
- ali smatrate metode in orodja, obravnavana pod točkami od E1 do E4, kot del sistema UI, ali ne?
- s katerimi (človeškimi) lastnosti bi sistem UI najbolj poistovetili?
- ali bo služil sistem UI bolj kot pomoč posameznikom ali kot pomoč organizaciji?
- ali bo sistem UI v pravno formalnem in organizacijskem smislu delovni pripomoček ali samostojna entiteta?
- ali imate pretežno dolgoletne IT partnerje
- ali je implementacija Sistema UI enkraten projekt ali je pričakovati neprestano nadgrajevanje sistema UI

Priloga 2: Podrobni rezultati intervjujev

Podrobni odgovori na vprašanje A2) »Seznam kategorij tveganj, specifičnih za umetno inteligenco – označite, če razumete kategorijo tveganja ali/in podajte nov predlog« so predstavljeni v tabeli 37.

Zadnja dva stolpca v tabeli 37 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki vrsto tveganja razumejo (oznaka 1 v celici tabele 37) in odstotek razumljivosti med vsemi intervjuvanci. Oznake intervjuvancev so obrazložene v poglavju 4.

Tabela 37: Rezultati - poznavanje posamezne vrste tveganj iz strani intervjuvancev

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
	Seznanjenost s tveganjem																													**Število**	**%**
1	Pristranskost in pravičnost	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	**27**	**96**
2	Zasebnost in kibernetska varnost	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**26**	**93**
3	Transparentnost in odgovornost	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1	1	1	**22**	**79**
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	0	0	0	0	**18**	**64**
5	Etični vidiki	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**28**	**100**
6	Zanesljivost, integriteta in varnost uporabe	1	1	1	0	1	1	1	1	1	0	0	1	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	**23**	**82**
7	Upravljanje in regulacija	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	1	0	1	1	1	1	1	**22**	**79**

Vir: lastno delo.

Podrobni odgovori na vprašanje B2) »Ali poznate naslednje faze ocenjevanja tveganja?«:

Tabela 38: Rezultati - poznavanje posameznih faz ocenjevanja tveganj iz strani intervjuvancev

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
	Seznanjenost s postopkom																													**Število**	**%**
1	Identifikacija tveganja	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**28**	**100**
2	Ranljivosti in predpogoji za nastanek	1	1	1	0	1	1	1	0	1	0	0	1	1	0	1	0	0	1	1	1	1	0	1	1	1	1	1	1	**20**	**71**
3	Verjetnost nastanka	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	0	1	1	1	1	1	1	**22**	**79**
4	Resnost vpliva	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**27**	**96**
5	Izračun ocene	1	0	1	0	1	1	1	1	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	1	1	1	1	1	**18**	**64**
6	Blaženje, preprečevanje	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	**27**	**96**
7	Upravljanje incidentov	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	1	0	1	0	0	**16**	**57**

Vir: lastno delo.

Zadnja dva stolpca v tabeli 38 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki fazo ocenjevanja tveganja razumejo, in odstotek razumljivosti med vsemi intervjuvanci. Oznake intervjuvancev so obrazložene v poglavju 4.

Podrobni odgovori na vprašanje C1) »Bi organizacija znala oceniti vsako vrsto tveganja (pomislite na dva primera umetne inteligence)? Če je odgovor pritrdilen, označite tveganje z oznako 1.«:

Tabela 39: Rezultati - sposobnost dejanskega ocenjevanja posamezne vrste tveganj z vidika organizacije

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
	Zmožnost ocenjevanja tveganj za:																													**Število**	**%**
1	Pristranskost in pravičnost	1	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	0	0	1	0	1	0	1	0	0	0	0	0	**12**	**43**
2	Zasebnost in kibernetska varnost	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	1	0	1	1	1	1	0	1	0	1	1	1	0	**19**	**68**
3	Transparentnost in odgovornost	1	1	0	0	1	0	1	0	0	0	0	0	1	1	1	1	0	0	1	0	1	0	0	0	0	0	1	1	0	**12**	**43**
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	**7**	**25**
5	Etični vidiki	1	1	1	0	0	1	1	0	0	0	0	1	1	1	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	**12**	**43**
6	Zanesljivost, integriteta in varnost uporabe	1	1	1	0	1	1	1	0	0	0	0	1	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1	0	**17**	**61**
7	Upravljanje in regulacija	1	1	0	0	0	0	1	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0	0	0	0	1	0	**11**	**39**

Vir: lastno delo.

Zadnja dva stolpca v tabeli 39 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki bi tveganja posamezne vrste tveganj znali oceniti, in odstotek intervjuvancev s pritrdilnim odgovorom med vsemi intervjuvanci. Oznake intervjuvancev so obrazložene v poglavju 4.

Podrobni odgovori na vprašanje C2) »Bi bila organizacija sposobna ustrezno izvesti vsako fazo ocene tveganja pri vsaki vrsti tveganja?«.

V primeru pritrdilnega odgovora v tabeli 40 je polje obarvano zeleno. Zadnja dva stolpca v tabeli 40 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki posamezno fazo ocenjevanja tveganj za posamezno vrsto tveganj smatrajo kot izvedljivo in odstotek intervjuvancev s pritrdilnim odgovorom med vsemi intervjuvanci. V vrsticah, kjer so z odebeljeno pisavo opisane vrste tveganj, je v stolpcu »Število« podano skupno število pritrdilnih odgovorov za posamezno fazo ocenjevanja znotraj dotične vrste tveganj in delež pritrdilnih odgovorov v stolpcu »%«. Oznake intervjuvancev so obrazložene v poglavju 4.

Tabela 40: Rezultati - sposobnost ocenjevanja posamezne vrste tveganj ob upoštevanju dejanske sposobnosti organizacije, da izvede vse faze ocenitve tveganj

		vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	a	B	a	B	B		
		odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
		implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
		stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
																															Število	**%**
1	**Pristranskost in pravičnost**																														**47**	**24**
		Identifikacija tveganja	1	1	1	1	1	1						1	1	1		1	1	1	1	1	1		1	1	1	1	1		**20**	**71**
		Ranljivosti in predpogoji za nastanek		1																											**1**	**4**
		Verjetnost nastanka		1			1	1						1			1								1							**6**	**21**
		Resnost vpliva	1	1			1	1						1		1	1								1	1	1	1			**11**	**39**
		Izračun ocene					1	1						1						1		1			1						**6**	**21**
		Blaženje, preprečevanje		1																											**1**	**4**
		Upravljanje incidentov	1	1																											**2**	**7**

se nadaljuje

Tabela 40: Rezultati - sposobnost ocenjevanja posamezne vrste tveganj ob upoštevanju dejanske sposobnosti organizacije, da izvede vse faze ocenitve tveganj (nad.)

		vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	a	B	a	B	B	
		odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1	
		implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
		stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
																														Število	**%**
2	**Zasebnost in varnost**																													**63**	**32**
		Identifikacija tveganja	1	1	1	1	1	1	1					1	1	1	1	1	1		1	1	1		1	1	1	1	1	1	**22**	**79**
		Ranljivosti in predpogoji za nastanek		1																											**1**	**4**
		Verjetnost nastanka	1	1			1	1	1					1								1			1		1	1			**10**	**36**
		Resnost vpliva	1	1			1	1	1					1		1						1			1	1	1	1	1		**13**	**46**
		Izračun ocene	1				1	1	1					1							1	1	1		1		1	1			**11**	**39**
		Blaženje, preprečevanje	1	1			1																					1			**4**	**14**
		Upravljanje incidentov	1	1																											**2**	**7**
3	**Transparentnost in odgovornost**																													**51**	**26**
		Identifikacija tveganja	1	1	1	1	1	1	1					1	1	1	1	1	1	1	1	1	1		1	1	1	1	1	1	**23**	**82**
		Ranljivosti in predpogoji za nastanek		1																											**1**	**4**
		Verjetnost nastanka		1			1		1					1														1			**5**	**18**
		Resnost vpliva	1	1			1		1					1		1									1	1	1	1			**10**	**36**
		Izračun ocene					1		1					1							1		1					1			**6**	**21**
		Blaženje, preprečevanje	1	1			1																					1			**4**	**14**
		Upravljanje incidentov	1	1																											**2**	**7**
4	**Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov**																													**37**	**19**
		Identifikacija tveganja	1	1	1	1	1	1						1	1	1	1	1	1		1		1		1	1	1	1			**18**	**64**
		Ranljivosti in predpogoji za nastanek		1																											**1**	**4**
		Verjetnost nastanka	1	1										1																	**3**	**11**
		Resnost vpliva	1	1										1		1									1	1	1				**7**	**25**
		Izračun ocene	1											1							1		1								**4**	**14**
		Blaženje, preprečevanje	1	1																											**2**	**7**
		Upravljanje incidentov	1	1																											**2**	**7**
5	**Etični vidiki**																													**46**	**23**
		Identifikacija tveganja	1	1	1	1	1	1	1					1	1	1		1	1	1	1	1	1		1	1	1	1	1		**21**	**75**
		Ranljivosti in predpogoji za nastanek		1				1																							**2**	**7**
		Verjetnost nastanka	1	1				1	1					1																	**5**	**18**
		Resnost vpliva	1	1					1					1		1									1	1	1				**8**	**29**
		Izračun ocene	1					1	1					1							1		1								**6**	**21**
		Blaženje, preprečevanje	1	1																											**2**	**7**
		Upravljanje incidentov	1	1																											**2**	**7**
6	**Zanesljivost, integriteta in varnost**																													**62**	**32**
		Identifikacija tveganja	1	1	1	1	1	1	1					1	1	1	1	1	1		1	1	1		1	1	1	1	1	1	**22**	**79**
		Ranljivosti in predpogoji za nastanek		1				1																							**2**	**7**
		Verjetnost nastanka	1	1			1	1	1					1								1					1	1			**9**	**32**
		Resnost vpliva	1	1			1	1	1					1		1						1			1	1	1	1			**12**	**43**
		Izračun ocene	1				1	1	1					1							1	1	1				1	1			**10**	**36**
		Blaženje, preprečevanje	1	1			1	1																				1			**5**	**18**
		Upravljanje incidentov	1	1																											**2**	**7**
7	**Upravljanje in regulacija**																													**39**	**20**
		Identifikacija tveganja		1	1	1	1	1	1					1	1	1	1	1	1		1	1	1		1	1	1	1	1		**20**	**71**
		Ranljivosti in predpogoji za nastanek		1																											**1**	**4**
		Verjetnost nastanka		1										1								1									**3**	**11**
		Resnost vpliva		1										1		1	1					1				1	1	1			**9**	**32**
		Izračun ocene												1							1	1	1								**4**	**14**
		Blaženje, preprečevanje		1																											**1**	**4**
		Upravljanje incidentov		1																											**1**	**4**

Vir: lastno delo.

Podrobni odgovori na vprašanje D2) »Odgovori na seznam vprašanj (tabela 36) lahko organizaciji olajšajo ocenitev tveganj. Preverite, ali imate, oziroma bi imeli na voljo vire za pridobitev odgovorov na vsako od njih v procesu odločanja.«.

Zadnja dva stolpca v tabeli 41 prikazujeta število pritrdilnih odgovorov/št. intervjuvancev, ki menijo, da bi njihova organizacija znala pridobiti odgovor na zastavljeno vprašanje in odstotek takih intervjuvancev med vsemi intervjuvanci. V tabeli 41 so z zeleno označeni pritrdilni odgovori. Celice z znakom »vprašaj« prikazujejo primere, kjer intervjuvanec ni razumel vprašanja, ali ni znal dati odgovora. Celice, ki so prazne, označujejo primere, ko z vprašanjem intervjuvanec sploh ni bil seznanjen.

Tabela 41: Rezultati - sposobnost organizacije odgovoriti na vprašanja v tabeli – sposobnost, ki povečuje zmožnost organizacije ocenjevati tveganja

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1	
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2	
	Vprašanja - zmožnost odgovarjanja nanje/ preverjanja / pridobivanja prisotnosti koristnih dejavnikov in informacij																												**Št.**	**%**
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	0	0	1	1	0	1	0	0	1	1	0	**20**	**71**
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za upravljanje poslovnih sprememb?	1	1	1	1	1	0	0	1	1	0	0	0	1	1	1	1	1	0	0	1	0	0	1	0	0	0	1	0	**15**	**54**
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali pritisk uporabnikov/javnosti/kulture za začetek uporabe umetne inteligence?	1	1	1	0	1	1	1	1	1	0	0	0	1	0	1	1	0	0	0	1	0	1	1	1	1	1	1	0	**18**	**64**
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	**27**	**96**
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**6**	**21**
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov umetne inteligence?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**3**	**11**
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	1	1	1	0	1	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	1	0	1	1	1	1	1	0	**17**	**61**
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti podatkov?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	**5**	**18**
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	1	1	1	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	1	1	1	1	0	**13**	**46**
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti podatkov?	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev podatkov?	1	1	1	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	0	1	1	1	1	0	**12**	**43**
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	1	1	1	0	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1	0	0	**11**	**39**
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	1	1	0	0	1	1	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	**11**	**39**
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno inteligenco?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	0	1	1	1	1	1	1	**25**	**89**
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne inteligence?	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1	1	1	0	**23**	**82**
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	1	?	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	**6**	**21**
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju umetne inteligence, tehničnega znanja in poznavanja področja deležnikov?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	?	**3**	**11**
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne inteligence?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	**4**	**14**
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	**3**	**11**
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**2**	**7**
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki dialoga, kot so dokumenti, e-pošta, fizična dejanja …?	1	1	0	?	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	1	1	0	?	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne inteligence?	1	?	0	0	0	0	0	0	0	0	0	0	0	0	0	?	0	0	0	0	0	0	0	0	0	0	0	0	**1**	**4**
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen izid?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	?	0	0	0	0	0	0	0	0	**4**	**14**
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne inteligence?	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	?	0	0	0	0	0	0	0	0	0	**4**	**14**
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah aplikacij?	1	1	1	0	1	1	0	1	1	0	0	0	1	0	1	1	0	0	0	1	1	0	1	0	0	1	0	0	**14**	**50**
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence ustvari napačne, pristranske ali slabo razumljene rezultate?	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	1	0	0	1	0	0	**8**	**29**
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali posamezne primere?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni vmesniki, vizualne predstavitve, odločitvena drevesa, globoke nevronske mreže, zemljevidi pomembnosti)?	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	1	0	0	0	0	0	1	1	0	0	0	0	0	**9**	**32**
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in uporabnosti?	1	1	1	1	1	1	0	0	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	0	0	**21**	**75**
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in multidisciplinarne ekipe z zahtevanimi veščinami in znanjem?	1	1	1	1	1	1	0	0	1	0	0	1	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	**12**	**43**
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje in učinkovito sodelovanje s sistemi umetne inteligence?	1	1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	0	0	0	1	1	1	1	0	0	0	0	0	**16**	**57**
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do podatkov?	1	1	1	0	0	0	0	1	1	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	**10**	**36**
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z uveljavljenimi etičnimi smernicami in standardi?	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**1**	**4**
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	**4**	**14**
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	1	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	1	1	0	**10**	**36**
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?				1	1	1		0	0	0	0	0	1	1	0	0	0			0	0	0		0		0				**5**	**28**
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?				1	1	1		0	0	0	0	0	1	1	0	1	1			0	0	1		1		0				**9**	**50**
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven organizacije)				1	1	0		0	0	0	0	0	0	0	0	1	0			0	0	0		0		0				**3**	**17**
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega znanja?				1	1	0		0	0	0	0	0	0	0	0	0	0			0	0	0		0		0				**2**	**11**
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?				1	1	0		0	0	0	0	0	1	1	0	0	1			1	1	1		1		1				**10**	**56**
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema UI med ponudnikom sistema, implementatorjem sistema UI ter organizacijo-uporabnikom sistema?				0	0	0		0	0	0	0	0	0	0	0	0	0			0	0	0		0		0				**0**	**0**
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in izven nje?				0	0	0		0	0	0	0	0	0	1	0	1	0			1	0	0		1		1				**5**	**28**
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?				1	1	0		0	0	0	0	0	1	1	0	1	0			1	1	1		1		1				**10**	**56**
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI?				1	1	0		0	0	0	0	0	0	0	0	0	0			0	0	0		0		0				**2**	**11**
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove zanesljivosti in varnosti?				0	0	0		0	0	0	0	0	1	0	1	0	0			0	0	1		0		0				**3**	**17**
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v realnem času?				0	0	0		0	0	0	0	0	0	0	1	0	0			0	0	0		0		0				**1**	**6**
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije				0	0	0		0	0	0	0	0	0	1	0	0	1			0	0	1		0		0				**3**	**17**

Vir: lastno delo.

Podrobni odgovori na vprašanje E2) »Tukaj je nekaj predlogov za ukrepe. Izberite tri med njimi, ki bi vaši organizaciji bili najbolj v pomoč, ali pa podajte nov predlog.«.

Zadnja dva stolpca v tabeli 42 prikazujeta število uvrstitev posameznega ukrepa med prve tri in odstotek izbire posameznega ukrepa med prve tri med vsemi intervjuvanci.

Tabela 42: Rezultati - trije najpomembnejši ukrepi za povečevanje zmožnosti ocenjevanja tveganj

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	a	B	B		
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2	
	Trije najpomembnejši ukrepi																												**Število**	**%**
1	Omejitev obsega delovanja UI in omejitev uporabnikov	1	1		1	1	1	1	1	1			1	1		1	1	1	1		1	1		1	1		1	1	**21**	**75**
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva			1					1							1		1					1						**5**	**18**
3	Zmanjševanje nedoločljivosti AI-user interakcij								1						1												1			**3**	**11**
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	1	1	1		1	1						1		1		1		1		1				1			1		**12**	**43**
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco									1	1	1	1								1									**5**	**18**
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI											1	1		1			1										1	1		**6**	**21**
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti																		1		1			1						1	**4**	**14**
8	Sistem za razlago logike in sklepanja algoritmov sistema UI																			1											**1**	**4**
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI																														**0**	**0**
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	1			1	1						1	1			1			1			1	1	1					1		**11**	**39**
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI																1														**1**	**4**
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA				1	1	1	1		1	1			1	1					1		1		1	1	1	1	1			**15**	**54**

Vir: lastno delo.

Podrobni odgovori na vprašanje E3) »Vsak ukrep iz točke E2 ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, v kateri lahko organizacija popolnoma zaupa dostopnemu strokovnemu znanju o umetni inteligenci.«.

Zadnji stolpec v tabeli 43 predstavlja povprečno oceno pomembnosti posameznega ukrepa ob predpostavki zaupanja ekspertizi implementatorjev in vzdrževalcev sistema UI. Predpostavka zaupanja ekspertizi je, da organizacija lahko popolnoma zaupa ekspertnemu mnenju implementatorjev, za katerega organizacija prosi, je potrebno, ali ga od njih zahteva.

Tabela 43: Rezultati - ocene pomembnosti ukrepov ob zaupanju v razpoložljivo strokovno znanje o umetni inteligenci

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	B	a	B	a	B	B	
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
	Popolno zaupanje v strokovnost UI																														**Povprečje**
1	Omejitev obsega delovanja UI in omejitev uporabnikov	5	5	3	5	5	5	5	5	5	2	3	5	4	4	4	5	5	5	3	5	4	3	5	5	3	5	5	5		**4,39**
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva	3	3	3	2	3	4	5	4	4	2	3	3	3	5	3	4	5	4	4	3	3	5	3	3	3	2	4	4		**3,46**
3	Zmanjševanje nedoločljivosti AI-user interakcij	1	4	3	1	3	3	5	4	4	2	3	3	3	5	3	4		3	2	3	3	2	3	1	4	2	3	3		**2,96**
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	5	4	4	3	4	5	4	4	4	3	2	5	3	4	4	5		5	3	4	3	4	4	5	4	4	5	4		**4**
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco	3	1	3	3	3	4	3	5	5	5	5	2	3	4	3	4		4	3	5	3	4	4	3	3	4		4		**3,58**
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI	2	4	3	2	3	3	3	4	4	4	5	2	4	2	3	5		3	3	3	3	1	3	1	5	5		3		**3,19**
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti	3	1	2	3	3	2	3	3	3	3	3	2	3	2	4	4	4	3	4	3	3	5	2	1	2	4	3	5		**2,96**
8	Sistem za razlago logike in sklepanja algoritmov sistema UI	3	3	2		2	2	1	3	3	3	3	2	2	2	4	2		2	5	2	1	1	2	1	2	2	1	1		**2,19**
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI	2	5	2	4	2	3	3	3	3	2	2	2	2	2	4	3		2	4	2	1	2	2	1	2	3	2	3		**2,52**
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	5	1	4	4	4	3	3	4	4	4	4	4	4	5	4	4		4	3	4	4	5	4	4	3	3	3	5		**3,81**
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI	2	5	1	1	2	2	1	1	1	1	1	4	2	1	4	1		1	1	1	1	1	2	4	2	2	1	1		**1,74**
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA	3	5	5	5	5	5	4	5	5	3	4	5	5	4	4	5		5	4	4	5	3	4	4	5	5	5	4		**4,44**

Vir: lastno delo.

Podrobni odgovori na vprašanje E4) »Vsak ukrep ocenite od 1 do 5 (1 – manj verjetno, 5 – najbolj verjetno), da bi za vašo organizacijo ukrep ustrezno zmanjšal dvoumnost ocene tveganja. Predpostavimo situacijo, ko organizacija ne more popolnoma zaupati dostopnemu strokovnemu znanju o umetni inteligenci.«.

Tabela 44: Rezultati - ocene pomembnosti ukrepov ob nezaupanju v razpoložljivo strokovno znanje o umetni inteligenci

	vrsta uporabnika	A	A	B	B	a	A	a	a	B	B	B	B	A	B	a	B	B	B	a	B	a	B	B	B	a	B	a	B	B	
	odločevalec da/sodelujem/ne	2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	2	1	1	1		
	implementacija UI da/ne	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo tveganj	2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2		
	Nepopolno zaupanje v strokovnost UI																														**Povprečje**
1	Omejitev obsega delovanja UI in omejitev uporabnikov	5	5	3	5	5	5	5	5	5	2	3	5	5	4	5	5	5	5	3	5	4	3	5	5	3	5	5	5		**4,46**
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva	3	5	3	2	3	4	5	4	4	2	3	4	3	5	4	4	5	4	4	3	3	5	3	3	3	2	4	4		**3,61**
3	Zmanjševanje nedoločljivosti AI-user interakcij	1	5	3	1	3	3	5	4	4	3	3	4	4	5	4	4		3	4	3	3	2	3	3	4	4	4	3		**3,41**
4	Sistem za promocijo varovanih privatnih in osebnih podatkov	5	5	4	3	4	5	4	4	4	3	2	5	4	4	4	5		5	3	4	4	4	4	5	4	4	5	4		**4,11**
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno	3	3	4	3	4	4	3	5	5	5	5	3	4	4	4	4		4	3	5	3	4	4	4	4	4		4		**3,92**
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI	2	4	4	2	3	4	4	4	4	4	5	3	5	2	4	5		3	3	3	3	1	3	2	5	5		3		**3,46**
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti	3	3	2	3	4	2	3	3	4	4	3	3	4	2	4	4	4	3	4	3	3	5	2	2	2	4	3	5		**3,25**
8	Sistem za razlago logike in sklepanja algoritmov sistema UI	3	5	2		2	2	1	3	3	3	3	3	3	2	4	2		2	5	2	1	1	2	2	2	3	1	2		**2,46**
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI	2	5	2	4	2	3	3	3	4	2	3		3	2	4	3		2	4	2	1	2	2	2	2	4	2	4		**2,77**
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence	5	4	5	5	4	4	4	4	4	5	5	4	4	5	4	4		5	3	4	5	5	5	5	3	4	3	5		**4,33**
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI	2	5	1	1	2	2	1	2	2	1	1	4	2	1	4	1		1	1	1	1	1	2	4	2	2	1	2		**1,85**
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA	3	5	4	5	3	3	2	3	3	3	4	5	3	3	4	4		3	4	3	3	3	3	3	5	5	4	4		**3,59**

Vir: lastno delo.

Zadnji stolpec v tabeli 44 predstavlja povprečno oceno pomembnosti posameznega ukrepa ob predpostavki nezaupanja ekspertizi implementatorjev in vzdrževalcev sistema UI. Predpostavka nezaupanja ekspertizi je, da organizacija ne more popolnoma zaupati

ekspertnemu mnenju implementatorjev, za katerega organizacija prosi, je potrebno, ali ga od njih zahteva.

Rezime odgovorov na dodatna vprašanja je zbran v tabeli 45. V celicah tabele 45, kjer sta številki 1 in 2 navedeni z modro in rdečo barvo, je potrebno pomen posamezne številke razbrati iz opisa v vrstici, ki se nahaja v drugem stolpcu tabele 45. Za dvopičjem v drugem stolpcu tabele 45 se izza vsake številke nahaja število intervjuvancev, ki so izbrali opcijo, ki jo številka pred dvopičjem predstavlja. V celicah petega vprašanja pod stolpcem »Št. številka« predstavlja število intervjuvancev, pod stolpcem »%« pa odstotek intervjuvancev, ki so izbrali posamezno človeško lastnost kot lastnost, ki dobro opisuje sistem UI. V stolpcu »Zap.« je označenih prvih pet najpogosteje izbranih človeških lastnosti.

Tabela 45: Rezultati - ostale relevantne zbrane informacije med intervjuji

	vrsta uporabnika		A	A	B	B	a	A	a	a	B	B	B	A	B	a	B	B	B	a	B	a	B	B	a	B	B		
	odločevalec da/sodelujem/ne		2	1	1	2	1	2	2	1	1	3	3	3	1	2	1	1	2	1	2	1	2	3	2	2	1	1	1		
	implementacija UI da/ne		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	stopnja seznanjenosti z analizo tveganj		2	1	2	5	1	3	2	1	1	3	5	4	1	5	1	3	5	2	3	2	2	3	2	2	3	2	1	2	
1	**Ali smatrate/obravnavate sistem UI kot tehnološki sistem (1: n=14), kot osebo (3: n=0) ali kot oboje (2: n=9) ?**				1	1	2	2	2	2	2	1	1		2	1		2		2	1	1	1	1	2	1	1	1	1	1		
2	**Ali smatrate metode in orodja, obravnavana pod točkami od E1 do E4 v večini primerov kot sestavni del sistema UI (1: n=11), ali ne (2: n=9) ?**				1	1	1	1	1	1	1	1	1		1	1		1		1	1	1	1	1	1	1	1	1	1	1		
3	**Ali bo služil sistem UI bolj kot pomoč posameznikom (1: n=17) ali kot pomoč organizaciji (2: n=6) ?**				2	1	2	1	1	1	1	1	1		1	1		2		1	2	2	1	2	1	1	1	1	1	1		
4	**Ali bo sistem UI v pravno formalnem in organizacijskem smislu delovni pripomoček (1: n=15) ali samostojna entiteta (2: n=8) ?**				1	1	2	2	2	2	2	1	1		2	1		2		1	1	1	1	1	2	1	1	1	1	1		
5	**S katerimi (človeškimi) lastnosti bi sistem UI najbolj poistovetili?**	**Zap.**																												**Št.**	**%**
	integriteta	**5**			1	0	0	1	0	1	1	0	0		1	0		1		0	1	0	0	1	1	0	0	1	1	0	**11**	**48**
	zanesljivost				1	0	0	0	0	0	0	0	0		1	0		1		0	1	0	0	1	0	0	0	0	0	0	**5**	**22**
	zglednost				0	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	0	**0**	**0**
	skupinsko delo				0	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	0	**0**	**0**
	komunikativnost	**2**			1	1	1	1	1	1	1	0	0		1	1		1		0	1	1	1	0	1	0	1	1	1	0	**17**	**74**
	zaupanje				1	0	0	0	0	0	0	0	0		0	0		0		0	1	0	0	0	0	0	0	0	0	0	**2**	**9**
	poštenost				1	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	**1**	**4**
	prilagodljivost	**4**			0	0	1	1	1	1	1	0	0		1	0		1		1	0	0	1	0	1	1	1	1	0	0	**13**	**57**
	pozornost na detajle				0	0	0	0	0	0	0	0	0		1	0		0		0	1	0	0	0	0	1	0	0	0	0	**3**	**13**
	kreativnost				0	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	**0**	**0**
	samokritičnost				0	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	**0**	**0**
	sodelovanje				0	0	0	1	0	1	1	0	0		1	0		0		0	1	1	0	1	1	0	0	0	1	0	**9**	**39**
	pozitivnost				0	1	0	0	0	0	0	0	0		0	0		1		0	0	0	0	1	0	0	0	0	0	0	**3**	**13**
	reševanje problemov	**3**			1	1	1	1	0	0	0	1	1		0	0		0		0	1	1	1	1	0	0	1	1	1	1	**14**	**61**
	čustvena inteligenca				0	0	0	0	0	0	0	0	0		0	0		1		0	0	0	0	1	1	0	1	0	1	0	**5**	**22**
	predanost				0	0	0	0	0	0	0	0	0		0	0		0		0	1	0	0	0	0	0	0	0	0	0	**1**	**4**
	samoiniciativnost				0	0	0	0	0	0	1	0	0		1	1		0		0	0	0	0	0	1	0	0	0	0	0	**4**	**17**
	učljivost	**1**			1	1	1	1	1	1	1	1	1		1	1		1		1	1	1	1	1	1	1	1	1	1	1	**23**	**100**
	ambicioznost				0	0	0	0	0	0	0	0	0		0	0		0		0	0	0	0	0	0	0	0	0	0	0	**0**	**0**
	neodvisnost				0	1	0	0	0	0	0	0	0		0	0		0		0	1	1	1	1	0	0	1	0	1	0	**7**	**30**
	delovne navade				1	0	0	1	0	1	1	0	0		1	0		0		0	0	0	0	1	1	0	0	1	1	1	**10**	**43**
6	**Ali imate pretežno dolgoletne IT partnerje: da (1: n=15) / ne (2: n=8) ?**				1	2	1	1	1	1	1	1	1		1	1		1		1	2	2	2	2	1	1	2	2	2	1		
7	**Ali je implementacija sistema UI enkraten projekt (1: n=12), ali je pričakovati neprestano nadgrajevanje sistema UI (2: n=11) ?**				2	1	1	2	2	2	2	1	1		2	1		2		1	1	1	2	1	2	2	1	2	1	1		

Vir: lastno delo.

Priloga 3: Podrobna analiza rezultatov po skupinah intervjuvancev

V prilogi 3 so prikazane podrobne tabele, iz katerih so oblikovani sklepi magistrskega dela. Za vsak sklop vprašanj (vprašanja so označena enako kot v prilogi 1 in v poglavju 4.1) so podane tabele zbranih odgovorov za vse različne zaznane skupine intervjuvancev.

Za vsak sklop vprašanj je v nadaljevanju podana tudi tabela po združenih skupinah intervjuvancev, kjer so skupine združene na naslednji način:

- ker se raziskava osredotoča na razlike med percepcijo specialistov poslovnih področij, ki nimajo računalniško – tehničnega ozadja in ekspertov informacijske tehnologije, sem analiziral tudi združene rezultate skupin UI-ekspertov in IT-ekspertov (v nadaljevanju tudi UI&IT strokovnjaki),
- ker se raziskava osredotoča tudi na vidik zmožnosti ocenjevanja tveganj, sem analiziral tudi združene rezultate vseh skupin uporabnikov, ki področje ocenjevanja tveganj poznajo.

Za vse tabele v prilogi 3 (razen za tabeli 63 in 64) velja enaka razlaga prvih treh vrstic:

- v prvi vrstici se nahajajo oznake skupin intervjuvancev, katerih podatki se nahajajo v določenem stolpcu (gre za oznake, ki so razložene v poglavju 4);
- v drugi vrstici se nahaja opis skupine ali skupin intervjuvancev, ki predstavljajo podatke posameznega stolpca;
- v tretji vrstici se nahaja podatek o številu intervjuvancev, ki predstavljajo podatke v posameznem stolpcu.

Pri vsaki tabeli se nahaja tudi vsebinska razlaga podatkov v številčnem delu tabele. Na koncu priloge 3, v tabeli 64, so po skupinah segmentirani tudi povzetki dodatnih informacij, zbranih med intervjuji, ki niso bile zajete v anketnem delu intervjujev.

Rezultati odgovorov na vprašanje A2)

Številka v celici tabele 46 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki je seznanjen s posamezno vrsto tveganj. Enako velja pri tabeli 47.

Tabela 46: Seznanjenost z vrstami tveganj po skupinah intervjuvancev

		Oznaka	A	a	B		1	2	3
		Opis	UI-strokovnjak	IT-strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja
	Vrsta tveganja	**Št. intervjujev**	4	8	16		13	11	4
1	Pristranskost in pravičnost		100	100	94		100	91	100
2	Zasebnost in kibernetska varnost		100	100	88		100	91	75
3	Transparentnost in odgovornost		100	100	63		100	73	25
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		100	88	44		77	64	25
5	Etični vidiki		100	100	100		100	100	100
6	Zanesljivost, integriteta in varnost uporabe		100	100	69		100	82	25
7	Upravljanje in regulacija		100	100	63		100	73	25
	Povprečje		**100**	**98**	**74**		**97**	**82**	**54**

		Oznaka	1	2	3	4	5
		Opis	Pogosto ocenjuje tveganja	Občasno ocenjuje tveganja	Sem vključen v proces	Sem seznanjen, a ne vključen	Nisem seznanjen
	Vrsta tveganja	**Št. intervjujev**	7	10	6	1	4
1	Pristranskost in pravičnost		100	100	100	100	75
2	Zasebnost in kibernetska varnost		100	100	83	100	75
3	Transparentnost in odgovornost		100	100	67	100	0
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		86	80	50	100	0
5	Etični vidiki		100	100	100	100	100
6	Zanesljivost, integriteta in varnost uporabe		100	100	67	100	25
7	Upravljanje in regulacija		100	100	67	100	0
	Povprečje		**98**	**97**	**76**	**100**	**39**

Vir: lastno delo.

Tabela 47: Seznanjenost z vrstami tveganj po zbirnih skupinah intervjuvancev

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Vrsta tveganja	**Št. intervjujev**	12	16		13	11	4		24	4
1	Pristranskost in pravičnost		100	94		100	91	100		100	75
2	Zasebnost in kibernetska varnost		100	88		100	91	75		96	75
3	Transparentnost in odgovornost		100	63		100	73	25		92	0
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		92	44		77	64	25		75	0
5	Etični vidiki		100	100		100	100	100		100	100
6	Zanesljivost, integriteta in varnost uporabe		100	69		100	82	25		92	25
7	Upravljanje in regulacija		100	63		100	73	25		92	0
	Povprečje		**99**	**74**		**97**	**82**	**54**		**92**	**39**

Vir: lastno delo.

Rezultati odgovorov na vprašanje B2)

Tabela 48: Seznanjenost s fazami ocenjevanja tveganj po skupinah intervjuvancev

		Oznaka	A	a	B		1	2	3
		Opis	UI-strokovnjak	IT-strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja
	Faza ocenjevanja tveganj	**Št. intervjujev**	4	8	16		13	11	4
1	Identifikacija tveganja		100	100	100		100	100	100
2	Ranljivosti in predpogoji za nastanek		100	88	56		85	73	25
3	Verjetnost nastanka		100	100	63		100	73	25
4	Resnost vpliva		100	100	94		100	100	75
5	Izračun ocene		75	88	50		77	64	25
6	Blaženje, preprečevanje		100	100	94		100	91	100
7	Upravljanje incidentov		100	88	31		69	55	25
	Povprečje		**96**	**95**	**70**		**90**	**79**	**54**

		Oznaka	1	2	3	4	5
		Opis	Pogosto ocenjuje tveganja	Občasno ocenjuje tveganja	Sem vključen v proces	Sem seznanjen, a ne vključen	Nisem seznanjen
	Faza ocenjevanja tveganj	**Št. intervjujev**	7	10	6	1	4
1	Identifikacija tveganja		100	90	100	100	100
2	Ranljivosti in predpogoji za nastanek		86	90	50	100	0
3	Verjetnost nastanka		100	90	67	100	0
4	Resnost vpliva		100	90	83	100	100
5	Izračun ocene		86	80	33	100	0
6	Blaženje, preprečevanje		100	90	100	100	75
7	Upravljanje incidentov		86	70	17	100	0
	Povprečje		**94**	**86**	**64**	**100**	**39**

Vir: lastno delo.

Številka v celici tabele 48 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki je seznanjen s posamezno fazo ocenjevanja tveganj. Enako velja pri tabeli 49.

Tabela 49: Seznanjenost s fazami ocenjevanja tveganj po zbirnih skupinah intervjuvancev

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Faza ocenjevanja tveganj	**Št. intervjujev**	12	16		13	11	4		24	4
1	Identifikacija tveganja		100	100		100	100	100		96	100
2	Ranljivosti in predpogoji za nastanek		92	56		85	73	25		79	0
3	Verjetnost nastanka		100	63		100	73	25		88	0
4	Resnost vpliva		100	94		100	100	75		92	100
5	Izračun ocene		84	50		77	64	25		71	0
6	Blaženje, preprečevanje		100	94		100	91	100		96	75
7	Upravljanje incidentov		100	31		69	55	25		63	0
	Povprečje		**97**	**70**		**90**	**79**	**54**		**84**	**39**

Vir: lastno delo.

Rezultati odgovorov na vprašanje C1)

Tabela 50: Percepcija sposobnosti ocenjevanja tveganj po skupinah intervjuvancev

		Oznaka	A	a	B		1	2	3
		Opis	UI-strokovnjak	IT-strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja
	Vrsta tveganja	**Št. intervjujev**	4	8	16		13	11	4
1	Pristranskost in pravičnost		100	50	25		38	55	25
2	Zasebnost in kibernetska varnost		100	75	56		77	73	25
3	Transparentnost in odgovornost		75	75	19		54	45	0
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		25	38	19		15	36	25
5	Etični vidiki		100	38	31		38	55	25
6	Zanesljivost, integriteta in varnost uporabe		100	75	44		69	64	25
7	Upravljanje in regulacija		75	50	25		46	45	0
	Povprečje		**82**	**57**	**31**		**48**	**53**	**18**

		Oznaka	1	2	3	4	5
		Opis	Pogosto ocenjuje tveganja	Občasno ocenjuje tveganja	Sem vključen v proces	Sem seznanjen, a ne vključen	Nisem seznanjen
	Vrsta tveganja	**Št. intervjujev**	7	10	6	1	4
1	Pristranskost in pravičnost		57	30	50	100	25
2	Zasebnost in kibernetska varnost		71	80	67	100	25
3	Transparentnost in odgovornost		71	40	33	0	25
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		14	20	33	100	25
5	Etični vidiki		29	50	50	100	25
6	Zanesljivost, integriteta in varnost uporabe		71	60	67	100	25
7	Upravljanje in regulacija		57	40	33	0	25
	Povprečje		**53**	**46**	**48**	**71**	**25**

Vir: lastno delo.

Številka v celici tabele 50 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna ocenjevati posamezno vrsto tveganj pri implementaciji sistema UI. Enako velja pri tabeli 51.

Tabela 51: Percepcija sposobnosti ocenjevanja tveganj po zbirnih skupinah intervjuvancev

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Vrsta tveganja	**Št. intervjujev**	12	16		13	11	4		24	4
1	Pristranskost in pravičnost		67	25		38	55	25		46	25
2	Zasebnost in kibernetska varnost		83	56		77	73	25		75	25
3	Transparentnost in odgovornost		75	19		54	45	0		46	25
4	Razumevanje možnosti in omejitev vhodnih podatkov in rezultatov		34	19		15	36	25		25	25
5	Etični vidiki		59	31		38	55	25		46	25
6	Zanesljivost, integriteta in varnost uporabe		83	44		69	64	25		67	25
7	Upravljanje in regulacija		58	25		46	45	0		42	25
	Povprečje		**66**	**31**		**48**	**53**	**18**		**50**	**25**

Vir: lastno delo.

Podrobna analiza vprašanja C2) je predstavljena v tabelah 52 in 53

Tabela 52: Percepcija sposobnosti izvedbe faz ocenjevanja tveganj po skupinah intervjuvancev

	Oznaka	A	a	B	1	2	3	1	2	3	4	5
	Opis	UI-strokovnjak	IT-strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja	Pogosto ocenjuje	Občasno ocenjuje	Sem vključen v proces	Sem seznanjen, a	Nisem seznanjen
Vi	Št. intervjujev	4	8	16	13	11	4	7	10	6	1	4
1	**Pristranskost in pravičnos**	**50**	**25**	**17**	**22**	**30**	**14**	**29**	**23**	**21**	**57**	**14**
	Identifikacija tveganja	100	63	69	69	91	25	57	80	67	100	75
	Ranljivosti in predpogoji za nastanek	25	0	0	8	0	0	14	0	0	0	0
	Verjetnost nastanka	50	25	13	23	18	25	43	10	4	100	0
	Resnost vpliva	75	50	25	31	55	25	43	40	33	100	25
	Izračun ocene	25	38	13	8	36	25	14	20	7	100	0
	Blaženje, preprečevanje	25	0	0	8	0	0	14	0	0	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
2	**Zasebnost in varnost**	**61**	**38**	**22**	**30**	**42**	**14**	**31**	**41**	**26**	**57**	**14**
	Identifikacija tveganja	100	88	69	77	100	25	71	90	67	100	75
	Ranljivosti in predpogoji za nastanek	25	0	0	8	0	0	14	0	0	0	0
	Verjetnost nastanka	75	38	25	31	45	25	29	50	7	100	0
	Resnost vpliva	75	50	38	38	64	25	43	60	33	100	25
	Izračun ocene	50	63	25	23	64	25	14	60	11	100	0
	Blaženje, preprečevanje	50	25	0	23	9	0	29	20	0	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
3	**Transparentnost in odgovo**	**43**	**38**	**16**	**27**	**29**	**14**	**31**	**31**	**14**	**57**	**14**
	Identifikacija tveganja	100	88	75	85	100	25	71	100	67	100	75
	Ranljivosti in predpogoji za nastanek	25	0	0	8	0	0	14	0	0	0	0
	Verjetnost nastanka	25	38	6	23	9	25	29	20	0	100	0
	Resnost vpliva	50	50	25	31	45	25	43	40	17	100	25
	Izračun ocene	0	63	6	15	27	25	14	30	4	100	0
	Blaženje, preprečevanje	50	25	0	23	9	0	29	20	0	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
4	**Razumevanje možnosti in o**	**50**	**18**	**12**	**14**	**26**	**14**	**18**	**20**	**14**	**57**	**14**
	Identifikacija tveganja	100	75	50	54	91	25	57	60	67	100	75
	Ranljivosti in predpogoji za nastanek	25	0	0	8	0	0	14	0	0	0	0
	Verjetnost nastanka	50	0	6	8	9	25	14	10	0	100	0
	Resnost vpliva	50	25	19	15	36	25	14	30	17	100	25
	Izračun ocene	25	25	6	0	27	25	0	20	4	100	0
	Blaženje, preprečevanje	50	0	0	8	9	0	14	10	0	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
5	**Etični vidiki**	**61**	**23**	**14**	**16**	**35**	**14**	**18**	**29**	**21**	**57**	**14**
	Identifikacija tveganja	100	75	69	69	100	25	57	90	67	100	75
	Ranljivosti in predpogoji za nastanek	50	0	0	8	9	0	14	0	17	0	0
	Verjetnost nastanka	75	13	6	8	27	25	14	20	4	100	0
	Resnost vpliva	50	38	19	15	45	25	14	40	17	100	25
	Izračun ocene	50	38	6	0	45	25	0	30	7	100	0
	Blaženje, preprečevanje	50	0	0	8	9	0	14	10	0	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
6	**Zanesljivost, integriteta in**	**68**	**38**	**20**	**30**	**40**	**14**	**31**	**37**	**31**	**57**	**14**
	Identifikacija tveganja	100	88	69	77	100	25	71	90	67	100	75
	Ranljivosti in predpogoji za nastanek	50	0	0	8	9	0	14	0	17	0	0
	Verjetnost nastanka	75	38	19	31	36	25	29	40	7	100	0
	Resnost vpliva	75	50	31	38	55	25	43	50	33	100	25
	Izračun ocene	50	63	19	23	55	25	14	50	11	100	0
	Blaženje, preprečevanje	75	25	0	23	18	0	29	20	17	0	0
	Upravljanje incidentov	50	0	0	8	9	0	14	10	0	0	0
7	**Upravljanje in regulacija**	**29**	**21**	**17**	**22**	**19**	**14**	**24**	**19**	**14**	**57**	**14**
	Identifikacija tveganja	75	88	63	69	91	25	71	70	67	100	75
	Ranljivosti in predpogoji za nastanek	25	0	0	8	0	0	14	0	0	0	0
	Verjetnost nastanka	25	0	13	15	0	25	14	10	0	100	0
	Resnost vpliva	25	38	31	38	27	25	43	30	17	100	25
	Izračun ocene	0	25	13	8	18	25	0	20	4	100	0
	Blaženje, preprečevanje	25	0	0	8	0	0	14	0	0	0	0
	Upravljanje incidentov	25	0	0	8	0	0	14	0	0	0	0
	Povprečje	**52**	**29**	**17**	**23**	**32**	**14**	**26**	**29**	**20**	**57**	**14**

Vir: lastno delo.

Številka v celici tabele 52 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna izvesti posamezno fazo ocenjevanja tveganj (prikazano za vsako posamezno vrsto tveganj) pri implementaciji sistema UI. Enako velja pri tabeli 53.

Tabela 53: Percepcija sposobnosti izvedbe faz ocenjevanja tveganj po zbirnih skupinah intervjuvancev

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Vrsta tvegar	**Št. intervjujev**	12	16		13	11	4		24	4
	Tveganje	**Proces obdelave tveganja**									
1	Pristranskost in pravičnost		33	17		22	30	14		26	14
		Identifikacija tveganja	75	69		69	91	25		71	75
		Ranljivosti in predpogoji za nastanek	8	0		8	0	0		4	0
		Verjetnost nastanka	33	13		23	18	25		22	0
		Resnost vpliva	58	25		31	55	25		42	25
		Izračun ocene	34	13		8	36	25		18	0
		Blaženje, preprečevanje	8	0		8	0	0		4	0
		Upravljanje incidentov	17	0		8	9	0		8	0
2	Zasebnost in varnost		46	22		30	42	14		35	14
		Identifikacija tveganja	92	69		77	100	25		79	75
		Ranljivosti in predpogoji za nastanek	8	0		8	0	0		4	0
		Verjetnost nastanka	50	25		31	45	25		35	0
		Resnost vpliva	58	38		38	64	25		50	25
		Izračun ocene	59	25		23	64	25		36	0
		Blaženje, preprečevanje	33	0		23	9	0		17	0
		Upravljanje incidentov	17	0		8	9	0		8	0
3	Transparentnost in odgovornost		40	16		27	29	14		28	14
		Identifikacija tveganja	92	75		85	100	25		83	75
		Ranljivosti in predpogoji za nastanek	8	0		8	0	0		4	0
		Verjetnost nastanka	34	6		23	9	25		21	0
		Resnost vpliva	50	25		31	45	25		38	25
		Izračun ocene	42	6		15	27	25		22	0
		Blaženje, preprečevanje	33	0		23	9	0		17	0
		Upravljanje incidentov	17	0		8	9	0		8	0
4	Razumevanje možnosti in omejitev vhodni		29	12		14	26	14		19	14
		Identifikacija tveganja	83	50		54	91	25		63	75
		Ranljivosti in predpogoji za nastanek	8	0		8	0	0		4	0
		Verjetnost nastanka	17	6		8	9	25		12	0
		Resnost vpliva	33	19		15	36	25		25	25
		Izračun ocene	25	6		0	27	25		14	0
		Blaženje, preprečevanje	17	0		8	9	0		8	0
		Upravljanje incidentov	17	0		8	9	0		8	0
5	Etični vidiki		36	14		16	35	14		25	14
		Identifikacija tveganja	83	69		69	100	25		75	75
		Ranljivosti in predpogoji za nastanek	17	0		8	9	0		8	0
		Verjetnost nastanka	34	6		8	27	25		18	0
		Resnost vpliva	42	19		15	45	25		29	25
		Izračun ocene	42	6		0	45	25		18	0
		Blaženje, preprečevanje	17	0		8	9	0		8	0
		Upravljanje incidentov	17	0		8	9	0		8	0
6	Zanesljivost, integriteta in varnost		48	20		30	40	14		35	14
		Identifikacija tveganja	92	69		77	100	25		79	75
		Ranljivosti in predpogoji za nastanek	17	0		8	9	0		8	0
		Verjetnost nastanka	50	19		31	36	25		31	0
		Resnost vpliva	58	31		38	55	25		46	25
		Izračun ocene	59	19		23	55	25		32	0
		Blaženje, preprečevanje	42	0		23	18	0		21	0
		Upravljanje incidentov	17	0		8	9	0		8	0
7	Upravljanje in regulacija		24	17		22	19	14		21	14
		Identifikacija tveganja	84	63		69	91	25		71	75
		Ranljivosti in predpogoji za nastanek	8	0		8	0	0		4	0
		Verjetnost nastanka	8	13		15	0	25		12	0
		Resnost vpliva	34	31		38	27	25		33	25
		Izračun ocene	17	13		8	18	25		14	0
		Blaženje, preprečevanje	8	0		8	0	0		4	0
		Upravljanje incidentov	8	0		8	0	0		4	0
		Povprečje	**37**	**17**		**23**	**32**	**14**		**27**	**14**

Vir: lastno delo.

Podrobna analiza vprašanja D2) je predstavljena v tabelah 54, 55, 56, 57 in 58. V teh tabelah so vprašanja skrajšana, v celoti pa so razvidna iz tabele 36 (priloga 1).

Tabela 54: Odstotkovno izražena percepcija sposobnosti pridobitve odgovorov na vprašanja, ki povečujejo zmožnost ocenjevanja tveganj (po skupinah intervjuvancev)

	Oznaka	A	a	B	1	2	3	1	2	3	4	5
	Opis	UI-stro-njak	IT-stro-kovnjak	Domenski specialist	Odločeva-lec	Udeleže-nec odločanja	Ni vključen v odločanja	Pogosto ocenjuje tveganja	Občasno ocenjuje tveganja	Sem vklju-čen v proces	Sem seznanjen, a ne	Nisem seznanjen
	Št. int.	4	8	16	13	11	4	7	10	6	1	4
	Vprašanja - zmožnost odgovarjanja nanje/ preverjanja / pridobivanja prisotnosti koristnih dejavnikov in informacij											
1	sistem umetne inteligence?	100	75	63	85	73	25	100	70	33	100	75
2	podpora vodstva in rešitve za upravljanje poslovnih sprememb?	75	38	56	77	45	0	100	40	17	0	75
3	regulativne spodbude ali pritisk uporabnikov/javnosti/kulture za začetek	100	75	50	85	55	25	100	70	67	0	0
4	uporabnikov?	100	88	100	100	91	100	100	90	100	100	100
5	odkrivanje pristranskosti?	100	13	6	31	18	0	43	20	17	0	0
6	vhodnih/izhodnih podatkov umetne inteligence?	50	0	6	8	9	25	14	10	0	100	0
7	inteligence?	100	75	44	69	64	25	86	70	50	4	0
8	filtriranje občutljivosti podatkov?	50	25	6	15	18	25	29	20	0	100	0
9	občutljivih podatkov?	75	50	38	54	45	25	57	60	33	4	0
10	odkrivanje občutljivosti podatkov?	75	0	6	15	9	25	29	10	0	100	0
11	odobravanja podatkov in kršitev podatkov?	75	38	38	46	45	25	43	60	33	4	0
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	100	63	13	38	55	0	43	70	17	0	0
13	za interpretabilnost?	100	50	19	54	27	25	71	30	33	4	0
14	v zvezi z umetno inteligenco?	100	75	94	85	91	100	86	80	100	100	100
15	v fazi delovanja umetne inteligence?	100	75	81	77	91	75	86	70	100	0	100
16	odgovornosti deležnikov?	25	50	6	23	27	0	29	40	0	0	0
17	pismenosti na področju umetne inteligence, tehničnega znanja in	50	13	0	15	9	0	29	10	0	0	0
18	razumevanju rezultatov umetne inteligence?	50	13	6	15	18	0	29	20	0	0	0
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	50	13	0	15	9	0	29	10	0	0	0
20	uporabniške profile?	50	0	0	8	9	0	14	10	0	0	0
21	inteligence?	50	13	6	15	9	25	29	10	0	4	0
22	niso odgovori v obliki dialoga, kot so dokumenti, e-pošta, fizična dejanja	50	13	6	15	9	25	29	10	0	100	0
23	inteligence?	50	13	6	15	9	25	29	10	0	4	0
24	podpira umetna inteligenca?	50	13	6	15	9	25	29	10	0	100	0
25	razumejo rezultatov umetne inteligence?	25	0	0	0	9	0	0	10	0	0	0
26	predpisi za vsak posamezen izid?	50	13	6	15	9	25	29	10	0	100	0
27	rezultate UI?	50	13	6	15	9	25	29	10	0	4	0
28	primerov uporabe umetne inteligence?	75	13	0	23	9	0	43	10	0	0	0
29	kritičnih domenah aplikacij?	100	63	31	77	36	0	86	60	33	0	0
30	umetne inteligence ustvari napačne, pristranske ali slabo razumljene	75	25	19	38	18	25	43	30	17	100	0
31	značilnosti, protidejstva ali posamezne primere?	75	13	0	23	9	0	43	10	0	0	0
32	uporabnika (poenostavljeni vmesniki, vizualne predstavitve, odločitvena	100	13	25	38	27	25	57	20	50	0	0
33	jasnosti, podrobnosti in uporabnosti?	100	63	75	69	82	75	71	60	83	4	100
34	upravljanja podatkov in multidisciplinarne ekipe z zahtevanimi veščinami	100	25	38	54	36	25	71	30	33	100	25
35	delovne sile za razumevanje in učinkovito sodelovanje s sistemi umetne	100	63	44	69	45	50	86	60	50	4	0
36	pravičnosti in pravic do podatkov?	75	38	25	62	9	25	71	30	17	100	0
37	preverjanje skladnosti z uveljavljenimi etičnimi smernicami in standardi?	25	0	0	0	9	0	0	10	0	0	0
38	umetne inteligence?	50	13	6	15	9	25	29	10	0	100	0
39	standardi?	75	38	25	46	27	25	57	30	33	4	0
40	potrebe UI sistema?	100	17	27	38	14	33	40	20	0	100	33
41	tudi druge organizacije?	100	50	45	63	43	33	60	60	25	100	33
42	zunanjega okolja (izven organizacije)	0	17	18	25	14	0	20	20	0	0	33
43	bazo prednaučenega znanja?	0	0	18	13	14	0	0	20	0	0	33
44	znanja?	4	33	64	50	71	33	20	80	75	100	33
45	posledic delovanja sistema UI med ponudnikom sistema,	0	0	0	0	0	0	0	0	0	0	0
46	deležnikov v organizaciji in izven nje?	4	33	18	25	43	0	40	20	50	0	0
47	aplikacij)?	100	50	55	50	71	33	40	80	50	100	33
48	uglaševanje in kontekstualizacijo UI?	0	0	18	13	14	0	0	20	0	0	33
49	sistema UI, njegove zanesljivosti in varnosti?	100	33	0	25	14	0	40	20	0	0	0
50	uporabe in upravljanja umetne inteligence v realnem času?	0	17	0	13	0	0	20	0	0	0	0
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	100	17	9	25	14	0	20	20	25	0	0
	Povprečje	**65**	**30**	**24**	**36**	**29**	**21**	**44**	**32**	**22**	**34**	**16**

Vir: lastno delo.

Številka v celici tabele 54 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki ocenjujejo, da je njihova organizacija sposobna z uporabo svojega ali zunanjega znanja pridobiti odgovor na posamezno vprašanje v tabeli. V vrstici »Št. int.« je prikazano število intervjuvancev, ki sestavljajo posamezno skupino v stolpcu tabele. V vrstici »Povprečje« je izražen povprečni odstotek intervjuvancev znotraj skupine v stolpcu tabele, ki ocenjujejo, da bi njihova organizacija lahko pridobila odgovor na vprašanja. Enako velja pri tabeli 55.

Tabela 55: Odstotkovno izražena percepcija sposobnosti organizacije, da pridobi odgovore na vprašanja, ki povečujejo zmožnost ocenjevanja tveganj (po zbirnih skupinah intervjuvancev)

	Oznaka	A, a	B		1	2	3		1-4	5
	Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev.	Nisem seznanjen
	Št. int.	12	16		13	11	4		24	4
	Vprašanja - zmožnost odgovarjanja nanje/ preverjanja / pridobivanja prisotnosti koristnih dejavnikov in informacij									
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	83	63		85	73	25		71	75
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za	50	56		77	45	0		50	75
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali	83	50		85	55	25		75	0
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	92	100		100	91	100		96	100
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	42	6		31	18	0		25	0
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov	17	6		8	9	25		12	0
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	83	44		69	64	25		67	0
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti	33	6		15	18	25		21	0
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	58	38		54	45	25		50	0
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti	25	6		15	9	25		17	0
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev	50	38		46	45	25		46	0
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	75	13		38	55	0		46	0
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	67	19		54	27	25		42	0
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno	83	94		85	91	100		88	100
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne	83	81		77	91	75		79	100
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	42	6		23	27	0		25	0
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju	25	0		15	9	0		13	0
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne	25	6		15	18	0		17	0
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	25	0		15	9	0		13	0
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	17	0		8	9	0		8	0
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	25	6		15	9	25		13	0
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki	25	6		15	9	25		17	0
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	25	6		15	9	25		13	0
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna	25	6		15	9	25		17	0
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne	8	0		0	9	0		4	0
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen	25	6		15	9	25		17	0
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	25	6		15	9	25		13	0
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne	34	0		23	9	0		17	0
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah	75	31		77	36	0		58	0
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence	42	19		38	18	25		33	0
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali	34	0		23	9	0		17	0
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni	42	25		38	27	25		37	0
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in	75	75		69	82	75		67	100
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in	50	38		54	36	25		46	25
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje	75	44		69	45	50		63	0
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do	50	25		62	9	25		42	0
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z	8	0		0	9	0		4	0
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	25	6		15	9	25		17	0
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	50	25		46	27	25		38	0
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?	45	27		38	14	33		24	33
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?	67	45		63	43	33		53	33
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven	11	18		25	14	0		14	33
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega	0	18		13	14	0		8	33
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?	23	64		50	71	33		62	33
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja	0	0		0	0	0		0	0
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji	23	18		25	43	0		33	0
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?	67	55		50	71	33		62	33
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo	0	18		13	14	0		8	33
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove	55	0		25	14	0		20	0
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja	11	0		13	0	0		6	0
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	45	9		25	14	0		20	0
	Povprečje	**42**	**24**		**36**	**29**	**21**		**33**	**16**

Vir: lastno delo.

V tabeli 55 so prikazani odstotki intervjuvancev znotraj posamezne skupine (opredeljene v stolpcu tabele), ki so ocenili, da bi njihova organizacija lahko pridobila odgovor na posamezno vprašanje.

Tabela 56: Percepcija sposobnosti pridobitve odgovorov na vprašanja, ki povečujejo zmožnost ocenjevanja tveganj po zbirnih skupinah intervjuvancev (20 % / 80 %)

	Oznaka	A, a	B	1	2	3	1-4	5
	Opis	UI ali IT strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja	Seznanjen sem z ocenjev.	Nisem seznanjen
	Št. int.	12	16	13	11	4	24	4
	Vprašanja - zmožnost odgovarjanja nanje/ preverjanja / pridobivanja prisotnosti koristnih dejavnikov in informacij							
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	83	63	85	73	25	71	75
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za	50	56	77	45	0	50	75
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali	83	50	85	55	25	75	0
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	92	100	100	91	100	96	100
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	42	6	31	18	0	25	0
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov	17	6	8	9	25	12	0
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	83	44	69	64	25	67	0
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti	33	6	15	18	25	21	0
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	58	38	54	45	25	50	0
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti	25	6	15	9	25	17	0
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev	50	38	46	45	25	46	0
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	75	13	38	55	0	46	0
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	67	19	54	27	25	42	0
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno	83	94	85	91	100	88	100
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne	83	81	77	91	75	79	100
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	42	6	23	27	0	25	0
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju	25	0	15	9	0	13	0
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne	25	6	15	18	0	17	0
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	25	0	15	9	0	13	0
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	17	0	8	9	0	8	0
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	25	6	15	9	25	13	0
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki	25	6	15	9	25	17	0
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	25	6	15	9	25	13	0
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?	25	6	15	9	25	17	0
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne	8	0	0	9	0	4	0
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen	25	6	15	9	25	17	0
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	25	6	15	9	25	13	0
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne	34	0	23	9	0	17	0
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah	75	31	77	36	0	58	0
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence	42	19	38	18	25	33	0
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali	34	0	23	9	0	17	0
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni	42	25	38	27	25	37	0
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in	75	75	69	82	75	67	100
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in	50	38	54	36	25	46	25
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje	75	44	69	45	50	63	0
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do	50	25	62	9	25	42	0
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z	8	0	0	9	0	4	0
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	25	6	15	9	25	17	0
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	50	25	46	27	25	38	0
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?	45	27	38	14	33	24	33
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?	67	45	63	43	33	53	33
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven	11	18	25	14	0	14	33
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega	0	18	13	14	0	8	33
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?	23	64	50	71	33	62	33
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema	0	0	0	0	0	0	0
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in	23	18	25	43	0	33	0
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?	67	55	50	71	33	62	33
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo	0	18	13	14	0	8	33
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove	55	0	25	14	0	20	0
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja	11	0	13	0	0	6	0
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	45	9	25	14	0	20	0
	Povprečje	42	24	36	29	21	33	16

Vir: lastno delo.

V tabeli 56 so zeleno obarvane celice, kjer je odstotkovno izražena percepcija skupine v stolpcu, da je organizacija sposobna pridobiti odgovor na vprašanje v vrstici, večja od 80 %, v tabelah 57 in 58 pa večja od 90 %.

V tabeli 56 so rdeče obarvane celice, kjer je odstotkovno izražena percepcija skupine v stolpcu, da je organizacija sposobna pridobiti odgovor na vprašanje v vrstici, manjša od 20 %, v tabelah 57 in 58 pa manjša od 10 %.

Tabela 57: Percepcija sposobnosti pridobitve odgovorov na vprašanja, ki povečujejo zmožnost ocenjevanja tveganj po zbirnih skupinah intervjuvancev (10 % /90 %)

	Oznaka	A, a	B	1	2	3	1-4	5
	Opis	UI ali IT strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja	Seznanjen sem z ocenjev.	Nisem seznanjen
	Št. int.	12	16	13	11	4	24	4
	Vprašanja - zmožnost odgovarjanja nanje/ preverjanja / pridobivanja prisotnosti koristnih dejavnikov in informacij							
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	83	63	85	73	25	71	75
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za	50	56	77	45	0	50	75
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali	83	50	85	55	25	75	0
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	92	100	100	91	100	96	100
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	42	6	31	18	0	25	0
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov	17	6	8	9	25	12	0
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	83	44	69	64	25	67	0
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti	33	6	15	18	25	21	0
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	58	38	54	45	25	50	0
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti	25	6	15	9	25	17	0
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev	50	38	46	45	25	46	0
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	75	13	38	55	0	46	0
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	67	19	54	27	25	42	0
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno	83	94	85	91	100	88	100
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne	83	81	77	91	75	79	100
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	42	6	23	27	0	25	0
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju	25	0	15	9	0	13	0
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne	25	6	15	18	0	17	0
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	25	0	15	9	0	13	0
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	17	0	8	9	0	8	0
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	25	6	15	9	25	13	0
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki	25	6	15	9	25	17	0
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	25	6	15	9	25	13	0
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?	25	6	15	9	25	17	0
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne	8	0	0	9	0	4	0
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen	25	6	15	9	25	17	0
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	25	6	15	9	25	13	0
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne	34	0	23	9	0	17	0
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah	75	31	77	36	0	58	0
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence	42	19	38	18	25	33	0
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali	34	0	23	9	0	17	0
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni	42	25	38	27	25	37	0
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in	75	75	69	82	75	67	100
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in	50	38	54	36	25	46	25
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje	75	44	69	45	50	63	0
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do	50	25	62	9	25	42	0
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z	8	0	0	9	0	4	0
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	25	6	15	9	25	17	0
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	50	25	46	27	25	38	0
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?	45	27	38	14	33	24	33
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?	67	45	63	43	33	53	33
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven	11	18	25	14	0	14	33
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega	0	18	13	14	0	8	33
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?	23	64	50	71	33	62	33
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema	0	0	0	0	0	0	0
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in	23	18	25	43	0	33	0
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?	67	55	50	71	33	62	33
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo	0	18	13	14	0	8	33
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove	55	0	25	14	0	20	0
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja	11	0	13	0	0	6	0
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	45	9	25	14	0	20	0
	Povprečje	42	24	36	29	21	33	16

Vir: lastno delo.

Tabela 58: Percepcija odločevalcev, da je organizacija sposobna pridobiti odgovore na vprašanja, ki povečujejo zmožnost ocenjevanja tveganj

	Oznaka	A, a	B
	Opis	UI ali IT strokovnjak	Domenski specialist
	Št. int.	12	12
	Uporabna vprašanja pri ocenjevanju tveganj in sposobnost organizacije pridobiti odgovore nanje, izraženo v %		
1	Ali obstajajo jasne tehnične zahteve (strojna in programska oprema) za sistem umetne inteligence?	83	75
2	Ali obstaja usklajenost z obstoječimi strategijami in cilji, ali obstaja podpora vodstva in rešitve za upravljanje	50	75
3	Ali obstaja gonilna sila prednosti konkurence, ali obstajajo pravne ali regulativne spodbude ali pritisk	83	58
4	Ali obstajajo jasne zahteve po dodatnem usposabljanju in izobraževanju uporabnikov?	92	100
5	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje pristranskosti?	42	8
6	Katere potencialne pristranskosti se obravnavajo v procesu filtriranja vhodnih/izhodnih podatkov umetne	17	0
7	Ali obstajajo uradne politike o pristranskosti v zvezi s sistemom umetne inteligence?	83	50
8	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za filtriranje občutljivosti podatkov?	33	0
9	Ali je na voljo zaledni sistem za filtriranje, predlaganje in odobravanje občutljivih podatkov?	58	42
10	Ali so v operativni fazi umetne inteligence na voljo kakšna orodja za odkrivanje občutljivosti podatkov?	25	0
11	Ali obstaja dnevnik dostopa za spremljanje filtriranja podatkov, odobravanja podatkov in kršitev podatkov?	50	42
12	Ali obstajajo metode šifriranja za prenos občutljivih podatkov?	75	17
13	Kakšna je raven interpretabilnosti modela, ali so na voljo kakšna orodja za interpretabilnost?	67	17
14	Ali obstaja celovita dokumentacija v zvezi z razvojem in procesi odločanja v zvezi z umetno inteligenco?	83	92
15	Ali so na voljo kakšna orodja za zbiranje povratnih informacij deležnikov v fazi delovanja umetne inteligence?	83	83
16	Ali obstaja sistem za vzpostavitev preglednosti in dojemanja odgovornosti deležnikov?	42	8
17	Ali obstaja sistem za upoštevanje značilnosti, potreb, pričakovanj, ravni pismenosti na področju umetne inteligence,	25	0
18	Ali obstaja sistem za upravljanje ciljev in potreb deležnikov po razumevanju rezultatov umetne inteligence?	25	8
19	Ali obstaja sistem za določanje obsega delovanja za uporabniške profile?	25	0
20	Ali obstaja sistem za upravljanje obsega dostopa do znanja za uporabniške profile?	17	0
21	Ali obstaja sistem za upravljanje omejitev rezultatov sistema umetne inteligence?	25	0
22	Ali obstaja sistem beleženja vseh rezultatov sistema umetne inteligence, ki niso odgovori v obliki dialoga, kot so	25	0
23	Ali obstaja sistem za upravljanje avtomatiziranih nalog za sistem umetne inteligence?	25	0
24	Ali je mogoče določiti, kakšna je kritičnost odločitev, ki jih sprejme ali podpira umetna inteligenca?	25	0
25	Ali je mogoče določiti, kakšne so možne posledice, če uporabniki ne razumejo rezultatov umetne inteligence?	8	0
26	Ali so na voljo informacije, potrebne za odgovornost ali skladnost s predpisi za vsak posamezen izid?	25	0
27	Ali je na voljo razlaga, potrebna za spodbujanje ustrezne ravni zaupanja v rezultate UI?	25	0
28	Ali obstaja sistem za spremljanje razumevanja specifičnih internih primerov uporabe umetne inteligence?	34	0
29	Ali so navedeni vsi avtomatizirani procesi odločanja umetne inteligence v kritičnih domenah aplikacij?	75	42
30	Katere so možne posledice v specifičnem operativnem kontekstu, če sistem umetne inteligence ustvari napačne,	42	17
31	Ali se razlaga osredotoča tudi na proces sklepanja, pomembne značilnosti, protidejstva ali posamezne primere?	34	0
32	Ali so razlage predstavljene na dostopen in razumljiv način za ciljnega uporabnika (poenostavljeni vmesniki,	42	25
33	Ali vmesniki za razlago (XUI) izpolnjujejo zahteve deležnikov glede jasnosti, podrobnosti in uporabnosti?	75	75
34	Ali ima organizacija potrebno digitalno infrastrukturo, prakse upravljanja podatkov in multidisciplinarne ekipe z	50	42
35	Ali obstaja strategija za usposabljanje in razvoj zmogljivosti človeške delovne sile za razumevanje in učinkovito	75	42
36	Ali obstajajo jasne politike upravljanja glede odgovornosti, razložljivosti, pravičnosti in pravic do podatkov?	50	25
37	Ali obstaja sistem za izvajanje etičnih ocen z različnimi deležniki in za preverjanje skladnosti z uveljavljenimi	8	0
38	Ali obstaja sistem za spremljanje zanesljivosti in varnosti rezultatov umetne inteligence?	25	0
39	Ali obstaja sistem za ocenjevanje skladnosti z ustreznimi predpisi in standardi?	50	25
40	Ali je velikost in ažurnost baze prednaučenega znanja ustrezna glede na potrebe UI sistema?	45	17
41	Ali je baza prednaučenega znanja skupna baza, do katere lahko dostopajo tudi druge organizacije?	67	33
42	Ali se da del baze prednaučenega znanja popolnoma izolirati od zunanjega okolja (izven organizacije)	11	17
43	Ali sistem UI podatke (ki jih v sistem posredujejo uporabniki) integrira v bazo prednaučenega znanja?	0	17
44	Ali je na voljo informacija o kibernetski varnosti baze prednaučenega znanja?	23	50
45	Ali je mogoče opredeliti razmejitev odgovornosti za posledice škodljivih posledic delovanja sistema UI med	0	0
46	Ali je mogoče oceniti o stopnjo vpliva UI sistema na dobrobit skupnosti deležnikov v organizaciji in izven nje?	23	17
47	Ali obstaja katalog vseh entitet umetne inteligence (modelov, agentov in aplikacij)?	67	42
48	Ali je na voljo mapiranje podatkov, ki se uporabljajo za učenje, uglaševanje in kontekstualizacijo UI?	0	17
49	Ali obstaja uporabniški vmesnik za monitoring nemotenega delovanja sistema UI, njegove zanesljivosti in varnosti?	55	0
50	Ali obstaja uporabniški vmesnik za nadziranje in uveljavljanje politik uporabe in upravljanja umetne inteligence v	11	0
51	Ali je sistem v celoti skladen z regulativo v pravnem okolju organizacije	45	8
	Povprečje	**42**	**23**

Vir: lastno delo.

Rezultati odgovorov na vprašanje E2)

Številka v celici tabele 59 predstavlja odstotek intervjuvancev določene skupine ali skupin v stolpcu tabele, ki so izbrali metodo ali ukrep v vrstici tabele kot enega izmed treh najpomembnejših za povečevanje sposobnosti njihove organizacije, da izvede analizo tveganj pri implementaciji sistema UI. Enako velja pri tabeli 60.

Tabela 59: Percepcija pomembnosti ukrepov in orodij, ki povečujejo zmožnost ocenjevanja tveganj (po skupinah intervjuvancev)

		Oznaka	A	a	B	1	2	3
		Opis	UI-strokovnjak	IT-strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja
	Metode in ukrepi	**Št. intervjujev**	4	8	16	13	11	4
1	Omejitev obsega delovanja UI in omejitev uporabnikov		100	88	63	92	73	25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		25	25	13	15	18	25
3	Zmanjševanje nedoločljivosti AI-user interakcij		0	13	13	0	27	0
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		75	25	44	54	36	25
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		0	13	25	23	0	50
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		25	13	25	23	9	50
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		0	13	19	8	18	25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		0	13	0	0	9	0
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		0	0	0	0	0	0
10	Zaledni sistem nemenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		25	13	56	23	45	75
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		0	13	0	8	0	0
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		50	75	44	54	64	25

		Oznaka	1	2	3	4	5
		Opis	Pogosto ocenjuje tveganja	Občasno ocenjuje tveganja	Sem vključen v proces	Sem seznanjen, a ne vključen	Nisem seznanjen
	Metode in ukrepi	**Št. intervjujev**	7	10	6	1	4
1	Omejitev obsega delovanja UI in omejitev uporabnikov		100	90	33	100	50
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		29	10	17	0	25
3	Zmanjševanje nedoločljivosti AI-user interakcij		0	10	17	0	25
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		43	50	33	100	25
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		29	10	17	0	25
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		14	10	50	0	25
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		0	10	33	0	25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		0	0	17	0	0
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		0	0	0	0	0
10	Zaledni sistem nemenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		0	60	33	0	75
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		14	0	0	0	0
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		71	50	50	100	25

Vir: lastno delo.

Tabela 60: Percepcija pomembnosti ukrepov in orodij*, ki povečujejo zmožnost ocenjevanja tveganj (po zbirnih skupinah intervjuvancev)*

		Oznaka	A, a	B		1	2	3		1-4	5
		Opis	UI ali IT strokovnjak	Domenski specialist		Odločevalec	Udeleženec odločanja	Ni vključen v odločanja		Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
	Metode in ukrepi	**Št. intervjujev**	12	16		13	11	4		24	4
1	Omejitev obsega delovanja UI in omejitev uporabnikov		92	63		92	73	25		79	90
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		25	13		15	18	25		17	10
3	Zmanjševanje nedoločljivosti AI-user interakcij		9	13		0	27	0		8	10
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		42	44		54	36	25		46	50
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za UI		9	25		23	0	50		17	10
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		17	25		23	9	50		21	10
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		9	19		8	18	25		12	10
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		9	0		0	9	0		4	0
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		0	0		0	0	0		0	0
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		17	56		23	45	75		33	60
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		9	0		8	0	0		4	0
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		67	44		54	64	25		58	50

Vir: lastno delo.

Rezultati odgovorov na vprašanji E3) in E4)

Številka v celici tabele 61 predstavlja povprečno oceno koristnosti posameznega ukrepa v vrstici tabele (od 1 do 5) z vidika intervjuvancev določene skupine ali skupin v stolpcu tabele. Ocenjevali so koristnost ukrepa za povečevanje sposobnosti njihove organizacije, da izvede analizo tveganj pri implementaciji sistema UI. Za vsako skupino intervjuvancev in vsak ukrep sta v tabeli navedeni dve oceni. Z modro barvo je navedena ocena za situacijo, ko bi njihova organizacija pri implementaciji sistema UI lahko zaupala UI ekspertizi, ki bi jo imela na voljo. Z rdečo barvo je navedena ocena, če ji organizacija ne bi mogla zaupati. Enako velja pri tabeli 62.

Tabela 61: Ocene pomembnosti ukrepov in orodij, ki povečujejo zmožnost ocenjevanja tveganj (po skupinah intervjuvancev)

		Oznaka	A		a		B	
		Opis	UI-strokovnjak		IT-strokovnjak		Domenski specialist	
		Št. inter.	4		8		16	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,75	5	4,5	4,63	4,25	4,25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,25	3,75	3,38	3,5	3,56	3,63
3	Zmanjševanje nedoločljivosti AI-user interakcij		2,75	3,25	2,88	3,75	3,07	3,27
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4,25	4,75	3,88	4	4	4
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		2,75	3,5	3,38	3,75	3,93	4,14
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,25	3,75	3,13	3,5	3,21	3,36
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in		2,25	3	3,13	3,38	3,06	3,25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,5	3,25	2,38	2,63	2	2,14
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti		3	3,25	2,63	2,88	2,33	2,57
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,25	4,25	3,63	4,13	4,07	4,47
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		2,75	2,75	2	2,13	1,33	1,47
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,5	3,5	4,5	3,38	4,4	3,73

se nadaljuje

Tabela 61: Ocene pomembnosti ukrepov in orodij, ki povečujejo zmožnost ocenjevanja tveganj (po skupinah intervjuvancev) (nad.)

		Oznaka	1		2		3	
		Opis	Odločevalec		Udeleženec odločanja		Ni vključen v odločanja	
		Št. inter.	13		11		4	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,69	4,85	4,45	4,45	4,45	4,45
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,38	3,62	3,64	3,64	3,64	3,64
3	Zmanjševanje nedoločljivosti AI-user interakcij		3,23	3,69	2,8	3,2	2,8	3,2
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4,15	4,31	4	4,1	4	4,1
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,67	4,17	3,3	3,5	3,3	3,5
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,67	3,92	2,7	3	2,7	3
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in		3,15	3,54	2,64	2,73	2,64	2,73
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,23	2,62	2,11	2,22	2,11	2,22
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti		2,77	3,08	2,4	2,5	2,4	2,5
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,69	4,15	3,8	4,4	3,8	4,4
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		1,77	2	1,7	1,7	1,7	1,7
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,77	3,69	4,3	3,4	4,3	3,4

		Oznaka	1		2		3		4		5	
		Opis	Pogosto ocenjuje tveganja		Občasno ocenjuje tveganja		Sem vključen v proces		Sem seznanjen, a ne vključen		Nisem seznanjen	
		Št. inter.	7		10		6		1		4	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,71	5	4,7	4,7	3,5	3,5	5	5	4,25	4,25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,43	3,86	3,3	3,3	3,67	3,67	3	4	3,75	3,75
3	Zmanjševanje nedoločljivosti AI-user interakcij		3,43	4	2,7	3,1	2,83	3,33	3	4	3	3
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4	4,29	4,2	4,3	4	4	5	5	3	3
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,33	4,17	3,6	3,8	3,83	4	2	3	4	4
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,67	4	2,9	3,2	3,5	3,67	2	3	3	3
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in		2,86	3,57	2,9	3	3,33	3,5	2	3	3	3
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,57	3	1,7	2	2,5	2,5	2	3	2,5	2,5
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti		3	3,29	2,1	2,4	2,67	2,67	2	0	2,67	3
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,43	3,86	4	4,7	3,67	4	4	4	4,33	5
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		2,29	2,57	1,6	1,7	1,33	1,33	4	4	1	1
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,86	3,57	4,3	3,3	4,17	3,67	5	5	4,33	4

Vir: lastno delo.

Tabela 62: Ocene pomembnosti ukrepov in orodij, ki povečujejo zmožnost ocenjevanja tveganj (po zbirnih skupinah intervjuvancev)

		Oznaka	A, a		B	
		Opis	UI ali IT strokovnjak		Domenski specialist	
		Št. inter.	12		16	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,58	4,75	4,25	4,25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,34	3,58	3,56	3,63
3	Zmanjševanje nedoločljivosti AI-user interakcij		2,84	3,58	3,07	3,27
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4	4,25	4	4
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,17	3,67	3,93	4,14
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,17	3,58	3,21	3,36
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		2,84	3,25	3,06	3,25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,42	2,84	2	2,14
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		2,75	3	2,33	2,57
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,5	4,17	4,07	4,47
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		2,25	2,34	1,33	1,47
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,5	3,42	4,4	3,73

se nadaljuje

Tabela 62: Ocene pomembnosti ukrepov in orodij*, ki povečujejo zmožnost ocenjevanja tveganj (po zbirnih skupinah intervjuvancev) (nad.)*

		Oznaka	1		2		3	
		Opis	Odločevalec		Udeleženec odločanja		Ni vključen v odločanja	
		Št. inter.	13		11		4	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,69	4,85	4,45	4,45	4,45	4,45
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,38	3,62	3,64	3,64	3,64	3,64
3	Zmanjševanje nedoločljivosti AI-user interakcij		3,23	3,69	2,8	3,2	2,8	3,2
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4,15	4,31	4	4,1	4	4,1
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,67	4,17	3,3	3,5	3,3	3,5
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,67	3,92	2,7	3	2,7	3
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		3,15	3,54	2,64	2,73	2,64	2,73
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,23	2,62	2,11	2,22	2,11	2,22
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		2,77	3,08	2,4	2,5	2,4	2,5
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,69	4,15	3,8	4,4	3,8	4,4
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		1,77	2	1,7	1,7	1,7	1,7
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,77	3,69	4,3	3,4	4,3	3,4

		Oznaka	1-4		5	
		Opis	Seznanjen sem z ocenjev. tveganj		Nisem seznanjen	
		Št. inter.	24		4	
	Metode in ukrepi		Zaupanje	Nezaupanje	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,42	4,5	4,7	4,7
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,42	3,59	3,3	3,3
3	Zmanjševanje nedoločljivosti AI-user interakcij		2,96	3,46	2,7	3,1
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4,13	4,25	4,2	4,3
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		3,51	3,92	3,6	3,8
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3,24	3,54	2,9	3,2
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		2,96	3,29	2,9	3
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,17	2,46	1,7	2
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		2,5	2,63	2,1	2,4
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3,75	4,25	4	4,7
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		1,83	1,96	1,6	1,7
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,46	3,54	4,3	3,3

Vir: lastno delo.

Povprečno odstopanje ocene pozitivnosti ukrepov in orodij je prikazano v tabeli 63. V stolpcu »Abs. Razlika med 2 in 3« je prikazana absolutna razlika v povprečju ocen med skupino domenskih specialistov in skupino domenskih specialistov, ki posedujejo tudi UI&IT strokovna znanja, v stolpcu »Abs. Razlika med 1 in 2« pa absolutna razlika med

skupino UI&IT strokovnjakov in skupino domenskih specialistov, ki posedujejo tudi UI&IT strokovno znanje.

Tabela 63: Ocene pozitivnega vpliva ukrepov in orodij na zmožnost organizacijskega ocenjevanja tveganj z vidika treh skupin odločevalcev in povprečna razlika med ocenami skupin

		Opis	Zgolj UI&IT strokovnjak **skupina 1**			UI ali IT strokovnjak in hkrati domenski specialist			Domenski specialist **skupina 3**	
		Št. inter.	5			7			12	
	Ukrepi in orodja		Zaupanje	Nezaupanje	***Abs.razlika med 1 in 2***	Zaupanje	Nezaupanje	***Abs.razlika med 2 in 3***	Zaupanje	Nezaupanje
1	Omejitev obsega delovanja UI in omejitev uporabnikov		4,6	4,6	*0,12*	4,57	4,86	*0,47*	4,25	4,25
2	Postopno uvajanje funkcionalnosti UI in njenega vpliva		3,8	3,8	*0,73*	3	3,14	*0,53*	3,56	3,63
3	Zmanjševanje nedoločljivosti AI-user interakcij		3	3,2	*0,04*	2,71	3,57	*0,03*	3,07	3,27
4	Sistem za promocijo varovanih privatnih in osebnih podatkov		4,2	4,4	*0,3*	3,86	4,14	*0*	4	4
5	Večnivojska prezentacija možnih področij rezultatov sistema UI, prilagojeno razumljivosti za nestrokovnjake za umetno inteligenco		2,8	3,4	*0,62*	3,43	4	*0,32*	3,93	4,14
6	Večnivojska prezentacija uporabniških karakteristik, potreb in ciljev, skozi optiko poslovnih domen in specializacij sistema UI		3	3,2	*0,4*	3,29	3,71	*0,22*	3,21	3,36
7	Sistem za pomoč pri odpravljanju težav, razumljivosti in pristranskosti		2,6	3,2	*0,32*	3	3,43	*0,06*	3,06	3,25
8	Sistem za razlago logike in sklepanja algoritmov sistema UI		2,8	3,4	*0,75*	2,14	2,57	*0,29*	2	2,14
9	Sistem za uporabniško ocenjevanje razumljivosti in uporabnosti sistema UI		3,4	3,2	*0,8*	2,29	2,71	*0,05*	2,33	2,57
10	Zaledni sistem namenjen nestrokovnjakom za umetno inteligenco - za prilagajanje delovanja sistema umetne inteligence		3	4	*0,58*	3,86	4,29	*0,2*	4,07	4,47
11	Sistem za analizo nevsakdanjih scenarijev delovanja sistema UI		2,2	2,4	*0,06*	2,29	2,43	*0,96*	1,33	1,47
12	Neprestana optimizacija sistema umetne inteligence z vidika strokovnega znanja o umetni inteligenci na podlagi SOTA		4,2	3,6	*0,17*	4,71	3,43	*0*	4,4	3,73
	Povprečna razlika				***0,41***			***0,26***		

Vir: lastno delo.

Dodatne zabeležbe intervjujev

V celicah tabele 64, kjer so podatki navedeni kot npr. **1: n=0
2: n=0
3: n=2**, je potrebno pomen posamezne številke pred dvopičjem razbrati iz opisa v vrstici, ki se nahaja v prvem stolpcu tabele. Za dvopičjem se za vsako številko nahaja število intervjuvancev v skupini, ki so izbrali opcijo, ki jo številka pred dvopičjem predstavlja. V celicah, kjer se nahaja številka med 0 in 100, številka predstavlja odstotek intervjuvancev določene skupine v stolpcu tabele, ki je izbral posamezno človeško lastnost kot pričakovano lastnost sistema UI.

Tabela 64: Druga zbrana mnenja po zbirnih skupinah intervjuvancev

Oznaka	A, a	B	1	2	3	1-4	5
Opis	UI ali IT strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja	Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
Št. interv.	9	14	11	9	3	20	3
Ali smatrate/obravnavate sistem UI kot tehnološki sistem (1), kot osebo (3) ali kot oboje (2) ?	**1: n=4 2: n=0 3: n=5**	**1: n=10 2: n=0 3: n=4**	**1: n=5 2: n=0 3: n=6**	**1: n=6 2: n=0 3: n=3**	**1: n=3 2: n=0 3: n=0**	**1: n=11 2: n=0 3: n=9**	**1: n=3 2: n=0 3: n=0**
Ali smatrate metode in orodja, obravnavana pod točkami od E1 do E4 v večini primerov kot del sistema UI (1), ali ne (2) ?	**1: n=9 2: n=0**	**1: n=14 2: n=0**	**1: n=11 2: n=0**	**1: n=9 2: n=0**	**1: n=3 2: n=0**	**1: n=20 2: n=0**	**1: n=3 2: n=0**
Ali bo služil sistem UI bolj kot pomoč posameznikom (1) ali kot pomoč organizaciji (2) ?	**1: n=7 2: n=2**	**1: n=10 2: n=4**	**1: n=7 2: n=4**	**1: n=8 2: n=1**	**1: n=2 2: n=1**	**1: n=14 2: n=6**	**1: n=3 2: n=0**
Ali bo sistem UI v pravno formalnem in organizacijskem smislu delovni pripomoček (1) ali samostojna entiteta (2) ?	**1: n=4 2: n=5**	**1: n=11 2: n=3**	**1: n=6 2: n=5**	**1: n=6 2: n=3**	**1: n=3 2: n=0**	**1: n=12 2: n=8**	**1: n=3 2: n=0**

se nadaljuje

Tabela 64: Druga zbrana mnenja po zbirnih skupinah intervjuvancev (nad.)

Oznaka	A, a	B	1	2	3	1-4	5
Opis	UI ali IT strokovnjak	Domenski specialist	Odločevalec	Udeleženec odločanja	Ni vključen v odločanja	Seznanjen sem z ocenjev. tveganj	Nisem seznanjen
Št. interv.	9	14	11	9	3	20	3
S katerimi (človeškimi) lastnosti bi sistem UI najbolj poistovetili?							
integriteta	50	43	64	33	33	46	0
zanesljivost	21	21	27	11	33	21	0
zglednost	0	0	0	0	0	0	0
skupinsko delo	0	0	0	0	0	0	0
komunikativnost	75	64	82	89	0	63	67
zaupanje	8	7	9	11	0	8	0
poštenost	0	7	9	0	0	4	0
prilagodljivost	75	36	64	67	0	54	0
pozornost na detajle	29	0	9	22	0	13	0
kreativnost	0	0	0	0	0	0	0
samokritičnost	0	0	0	0	0	0	0
sodelovanje	42	36	45	33	33	37	0
pozitivnost	0	21	9	11	33	8	33
reševanje problemov	46	64	55	56	100	50	67
čustvena inteligenca	0	36	18	22	33	21	0
predanost	8	0	0	11	0	4	0
samoiniciativnost	13	21	18	22	0	12	33
učljivost	83	100	100	100	100	83	100
ambicioznost	0	0	0	0	0	0	0
neodvisnost	17	36	18	44	33	25	33
delovne navade	42	43	64	22	33	41	0
Ali imate pretežno dolgoletne IT partnerje: da (1) / ne (2) ?	**1: n=6** **2: n=3**	**1: n=9** **2: n=5**	**1: n=8** **2: n=3**	**1: n=5** **2: n=4**	**1: n=2** **2: n=1**	**1: n=13** **2: n=7**	**1: n=2** **2: n=1**
Ali je implementacija sistema UI enkraten projekt (1), ali je pričakovati neprestano nadgrajevanje sistema UI (2) ?	**1: n=2** **2: n=7**	**1: n=10** **2: n=4**	**1: n=5** **2: n=6**	**1: n=4** **2: n=5**	**1: n=3** **2: n=0**	**1: n=9** **2: n=11**	**1: n=3** **2: n=0**

Vir: lastno delo.