VPLIV UMETNE INTELIGENCE NA PREOBLIKOVANJE NALOG IN KOMPETENC V KIBERNETSKI VARNOSTI: PRELIMINARNA ZASNOVA REFERENČNEGA OKVIRA

Andreja Markun, Klemen Methans, Alenka Brezavšček
Fakulteta za organizacijske vede, Univerza v Mariboru, Kidričeva cesta 55a,4000 Kranj
andreja.markun@student.um.si, klemen.methans@um.si, alenka.brezavscek@um.si

Izvleček

Umetna inteligenca (UI) spreminja delo v kibernetski varnosti predvsem na ravni posameznih nalog, odgovornosti ter razmerja med avtomatizirano podporo in strokovno presojo. Prispevek je zasnovan kot konceptualni znanstveni članek, katerega namen je oblikovati preliminarno zasnovo referenčnega okvira za presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve pri zagotavljanju kibernetske varnosti. Predlagana zasnova temelji na strukturirani sintezi izbranih znanstvenih virov, kompetenčnih okvirov ter regulativnih in usmerjevalnih dokumentov. Analiza pokaže, da je vpliv UI smiselno obravnavati skozi štiri vloge: UI kot orodje za podporo varnostnim procesom, UI kot dejavnik spreminjanja groženj, UI kot predmet varovanja ter UI kot predmet upravljanja in skladnosti. Predlagani okvir povezuje te vloge s tremi vrstami učinkov na naloge: avtomatizacijo posameznih korakov naloge, prestrukturiranjem obstoječih nalog ter razširitvijo obstoječih oziroma nastankom novih nalog. Prispevek pokaže, da se kompetenčne zahteve ne oblikujejo kot splošna potreba po znanju o UI, temveč glede na konkretno nalogo, vlogo UI pri njeni izvedbi ter odgovornost, ki ostaja pri strokovnjaku oziroma organizaciji. Predstavljeni okvir je izhodišče za nadaljnje sistematično mapiranje literature, nadgradnjo referenčnega okvira ter njegovo empirično preverjanje v organizacijskem okolju.

Ključne besede: umetna inteligenca, kibernetska varnost, naloge v kibernetski varnosti, kompetenčne zahteve, odgovornost, referenčni okvir.

The impact of artificial intelligence on the transformation of tasks and competencies in cybersecurity: A preliminary reference framework

Abstract

Artificial intelligence (AI) is changing cybersecurity work primarily at the level of individual tasks, responsibilities, and the relationship between automated support and professional judgement. The paper is designed as a conceptual scientific article whose purpose is to propose a preliminary reference framework for assessing the impact of AI on tasks, responsibilities, and competency requirements in cybersecurity practice. The proposed framework is based on a structured synthesis of selected scientific sources, competency frameworks, and regulatory and guidance documents. The analysis shows that the impact of AI can be meaningfully examined through four roles: AI as a tool for supporting security processes, AI as a factor reshaping threats, AI as an object of protection, and AI as an object of governance and compliance. The proposed framework links these roles to three types of task-related effects: the automation of individual task steps, the restructuring of existing tasks, and the expansion of existing tasks or emergence of new ones. The paper shows that

competency requirements should not be understood as a general need for AI knowledge but should be assessed in relation to the specific task, the role of AI in its execution, and the responsibility that remains with the expert or the organisation. The framework provides a basis for further systematic mapping of the literature, further development of the reference framework, and empirical testing in organisational settings.

Keywords: artificial intelligence, cybersecurity, cybersecurity tasks, competency requirements, responsibility, reference framework.

1 UVOD

Kibernetska varnost se razvija v okolju hitro spreminjajočih se groženj, naraščajoče odvisnosti organizacij od digitalnih storitev in vse zahtevnejših regulativnih obveznosti [5], [22]. Zato kompetence v kibernetski varnosti niso omejene le na tehnično poznavanje sistemov, omrežij in ranljivosti, temveč vključujejo tudi analitično presojo, upravljanje tveganj, odzivanje na incidente, dokumentiranje odločitev in komunikacijo z vodstvom. Takšno širše razumevanje je razvidno tudi iz Evropskega okvira za kibernetske veščine (angl. European Cybersecurity Skills Framework, ECSF), ki med profili v kibernetski varnosti vključuje tako tehnične kot organizacijske in upravljavske vloge, kot so na primer vodja informacijske varnosti, strokovnjak za odzivanje na kibernetske incidente, arhitekt kibernetske varnosti, strokovnjak za upravljanje tveganj in osebe, odgovorne za zagotavljanje skladnosti [1].

Umetna inteligenca (angl. artificial intelligence, AI; v nadaljevanju UI) postaja pomemben dejavnik preoblikovanja dela v kibernetski varnosti, saj vpliva na izvajanje nalog, uporabo varnostnih orodij in razumevanje tveganj. Njena uporaba se povezuje z zaznavanjem groženj, obdelavo velikih količin varnostnih podatkov, razvrščanjem in prednostno obravnavo varnostnih opozoril, zaznavanjem anomalij, podporo odzivanju na incidente in izboljševanjem varnostno-operativnih procesov. Kaur idr. [2] razvrščajo uporabo UI v kibernetski varnosti po funkcijah ogrodja NIST Cybersecurity Framework, in sicer na identifikacijo, zaščito, zaznavanje, odzivanje in okrevanje. Novejša različica NIST CSF 2.0 tej logiki dodaja še funkcijo upravljanja (angl. govern), kar je pomembno tudi za razumevanje UI kot predmeta upravljanja, nadzora in skladnosti [3]. To kaže, da UI ne posega le v posamezna tehnična opravila, temveč v širši nabor nalog v kibernetski varnosti.

Poleg koristi vnaša UI na področje kibernetske varnosti tudi nova tveganja. Uporabljajo jo lahko napadalci, kar vpliva na pripravo zavajajočih vsebin, prilagajanje napadov in avtomatizacijo posameznih korakov napada. Poleg tega sistemi UI sami postajajo predmet varovanja. Njihova varnost ni odvisna le od klasične zaščite infrastrukture, temveč tudi od kakovosti podatkov, odpornosti modelov, nadzora vhodnih in izhodnih podatkov, varnosti vmesnikov ter obvladovanja ranljivosti, značilnih za strojno učenje in generativne modele. Macas idr. [4] opozarjajo, da so sistemi globokega učenja, uporabljeni v kibernetski varnosti, izpostavljeni napadom z namerno prilagojenimi vhodnimi podatki (angl. adversarial examples), kar lahko zmanjša zanesljivost varnostnih modelov in zahteva dodatne zaščitne pristope.

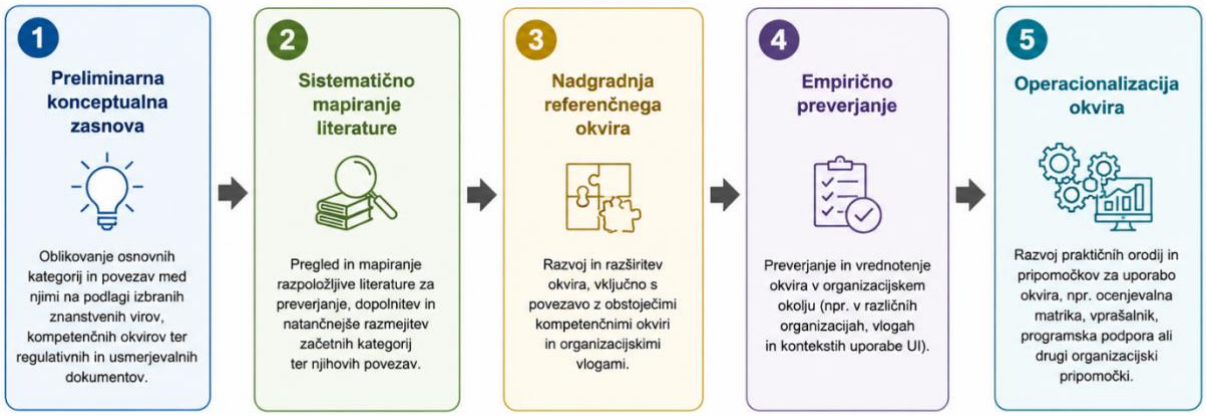
Pomen UI se razširi tudi na področje upravljanja in skladnosti. Akt o umetni inteligenci (angl. Artificial Intelligence Act, AI Act) oziroma Uredba (EU) 2024/1689 med drugim določa zahteve za sisteme UI z visokim tveganjem glede upravljanja tveganj, kakovosti podatkov, tehnične dokumentacije, vodenja zapisov, preglednosti, človeškega nadzora, robustnosti, točnosti in kibernetske varnosti [5]. Posebej pomembna je zahteva po človeškem nadzoru. Osebe, ki jim je tak nadzor dodeljen, morajo razumeti zmogljivosti in omejitve sistema, spremljati njegovo delovanje, pravilno interpretirati rezultate ter se zavedati tveganja pretiranega zanašanja na rezultate sistemov UI [5]. Za področje kibernetske varnosti to pomeni, da se kompetenčne zahteve širijo tudi na presojo, nadzor, dokumentiranje in odgovorno uporabo sistemov UI.

Pri presoji teh sprememb ni zadostno izhajati iz vprašanja, ali bo UI nadomestila posamezne poklice. Tak pogled je preveč poenostavljen, saj so vloge in profili v kibernetski varnosti sestavljeni iz različnih nalog, ki se razlikujejo po stopnji rutinskosti, obsegu podatkovne obdelave, zahtevani človeški presoji in ravni odgovornosti. Zato je pri analizi vpliva UI primerneje izhajati iz posameznih nalog kot iz formalnih profilov ali delovnih mest [11], [12]. UI lahko nekatere rutinske in ponovljive korake oziroma korake, ki zahtevajo obdelavo velikih količin podatkov, podpira ali avtomatizira, pri zahtevnejših analitičnih, komunikacijskih in odločitvenih nalogah pa predvsem spreminja način njihove izvedbe.

Uporaba UI v kibernetski varnosti zato ne pomeni preprostega nadomeščanja človekovega dela s tehnologijo. Bolj ustrezno je govoriti o preoblikovanju razmerja med izvedbo, podporo, nadzorom, razlago in odgovornostjo [13], [19], [20]. Sistem UI lahko na primer pripravi priporočilo, prednostno razvrsti varnostna opozorila ali pripravi povzetek ugotovitev o incidentu, vendar mora strokovnjak še vedno presoditi kontekst, preveriti ustreznost in zanesljivost rezultata, oceniti tveganje ter zagotoviti sledljivost in odgovornost za sprejeto odločitev.

Obstoječi kompetenčni okviri, kot sta okvir ECSF in NICE Workforce Framework for Cybersecurity (NICE Framework), so pomembno izhodišče za opredelitev profilov, nalog, znanj in spretnosti v kibernetski varnosti [1], [14], [15]. Njihova uporaba pa ne more ostati statična, saj UI spreminja način izvajanja posameznih nalog in s tem tudi pomen nekaterih kompetenc. Pri nekaterih nalogah se obstoječe kompetence predvsem nadgradijo, pri drugih pa se pojavi potreba po novih oziroma razširjenih kompetenčnih zahtevah, povezanih z uporabo, presojo, varovanjem in upravljanjem sistemov UI. Strokovnjak za odzivanje na kibernetske incidente tako ne potrebuje le znanja o postopkih odzivanja, temveč tudi zmožnost presoje priporočil sistemov UI, razumevanje omejitev orodij UI in sposobnost dokumentiranja odločitev, sprejetih ob njihovi podpori.

Širši raziskovalni cilj je razviti referenčni okvir za presojo, kako uporaba UI spreminja naloge, odgovornosti in kompetenčne zahteve pri zagotavljanju kibernetske varnosti. Tak okvir je potreben, ker vpliva UI na kompetence ni mogoče zanesljivo presojati zgolj na ravni splošnega poznavanja UI ali na ravni poklicev kot celote. Presoja mora izhajati iz konkretnih nalog, vloge UI pri njihovi izvedbi, sprememb v strokovni presoji, nadzoru in odgovornosti ter iz kompetenčnih zahtev, ki iz teh sprememb izhajajo. Takšna zasnova je skladna z razumevanjem konceptualnih okvirov kot sredstev za strukturiranje in komuniciranje kompleksnih raziskovalnih pojavov [36].



Slika 1: Večfazni razvoj referenčnega okvira za presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti
Vir: lastna zasnova avtorjev, grafično pripravljeno z uporabo ChatGPT (OpenAI).

Ta prispevek predstavlja prvo fazo širšega raziskovalnega procesa, prikazanega na sliki 1. V tej fazi oblikujemo preliminarno konceptualno zasnovo osnovnih kategorij in povezav med njimi. Nadaljnje faze vključujejo sistematično mapiranje literature, nadgradnjo referenčnega okvira, empirično preverjanje v organizacijskem okolju ter morebitno operacionalizacijo okvira v obliki ocenjevalne matrike, vprašalnika, programske podpore ali drugega praktičnega pripomočka za organizacije.

Namen prispevka je na podlagi strukturirane sinteze izbranih znanstvenih virov, kompetenčnih okvirov ter regulativnih in usmerjevalnih dokumentov oblikovati preliminarno zasnovo referenčnega okvira za presojo, kako UI vpliva na naloge, odgovornosti in kompetenčne zahteve pri zagotavljanju kibernetske varnosti. Pri tem izhajamo iz stališča, da kompetenčnih zahtev ni mogoče izpeljati zgolj iz splošnega poznavanja UI ali iz obstoječih seznamov znanj in spretnosti. Najprej je treba razumeti, v kateri vlogi se UI pojavlja, katere dele delovnih nalog spreminja, kako se s tem preoblikujejo strokovna presoja, nadzor in odgovornost ter katere kompetence iz teh sprememb izhajajo.

Prispevek odgovarja na naslednja raziskovalna vprašanja:

RV1: Katere vloge prevzema UI v kibernetski varnosti in kako so te povezane s spremembami nalog, odgovornosti in kompetenčnimi zahtevami?

RV2: Kako UI vpliva na naloge v kibernetski varnosti z vidika avtomatizacije posameznih korakov naloge, prestrukturiranja obstoječih nalog ter razširitve obstoječih oziroma nastanka novih nalog?

RV3: Katera kompetenčna področja izhajajo iz sprememb nalog in odgovornosti zaradi uporabe UI ter kako jih je mogoče povezati z izbranimi profili v kibernetski varnosti?

Prispevek je namenjen raziskovalcem, visokošolskim učiteljem in oblikovalcem študijskih programov s področja kibernetske varnosti ter strokovnjakom v organizacijah, ki načrtujejo uvajanje ali uporabo rešitev UI v varnostnih procesih. Uporabna vrednost prispevka je predvsem v tem, da ponuja podlago za sistematično presojo, katere naloge se z uporabo UI spreminjajo, katere odgovornosti ostajajo pri strokovnjakih oziroma organizaciji ter katere kompetenčne zahteve iz teh sprememb izhajajo.

2 TEORETIČNA IZHODIŠČA

2.1 Vloga umetne inteligence v kibernetski varnosti

V pričujočem prispevku UI ne obravnavamo kot enotne tehnologije z enim samim učinkom na kibernetsko varnost. Njena vloga je odvisna od tega, ali jo organizacija uporablja za podporo varnostnim procesom, ali jo uporabljajo napadalci, ali je sama sistem, ki ga je treba varovati, ali pa je predmet upravljanja, nadzora in skladnosti. Takšna razdelitev je pomembna, ker vsak od teh vidikov odpira drugačne naloge, odgovornosti in posledično drugačne kompetenčne zahteve.

Iz izbranih virov je mogoče razločiti štiri vsebinske vidike obravnave UI v kibernetski varnosti: uporabo UI za podporo varnostnim procesom, uporabo UI kot dejavnika spreminjanja groženj, obravnavo sistemov UI kot predmeta varovanja ter obravnavo UI kot predmeta upravljanja in skladnosti [2], [4], [5], [7], [8], [10], [23], [24]. Ti vidiki so v nadaljevanju članka uporabljeni kot podlaga za oblikovanje štirih analitičnih vlog UI v preliminarni zasnovi referenčnega okvira.

Prvi vidik je uporaba UI za podporo varnostnim procesom. Literatura kaže, da se UI uporablja pri zaznavanju anomalij, analizi varnostnih dogodkov, podpori odzivanju na incidente, odkrivanju zlonamernih aktivnosti in pripravi varnostnih poročil [2], [6]. Pri tem UI praviloma ne

nadomesti celotne naloge, temveč podpira obdelavo velikih količin podatkov, oblikovanje začetnih ocen in prednostno razvrščanje dogodkov. Za strokovnjake za kibernetsko varnost to pomeni, da morajo razumeti, kako takšna orodja delujejo, katere podatke uporabljajo, kakšne omejitve imajo in kako lahko preverijo njihove rezultate.

Drugi vidik je povezan z uporabo UI pri napadalnih dejavnostih. Literatura posebej opozarja na uporabo generativne UI pri pripravi zavajajočih vsebin, podpori socialnemu inženiringu, prilagajanju napadov in avtomatizaciji posameznih korakov procesa napada [7], [8]. Za namen tega članka je pomembno predvsem to, da takšna uporaba UI spreminja naloge spremljanja groženj, ozaveščanja uporabnikov, zaznavanja napadov in odzivanja na incidente. Strokovnjaki zato ne potrebujejo le tehničnega znanja o orodjih UI, temveč tudi zmožnost prepoznavanja sprememb v načinu izvedbe napadov in presoje tveganja za organizacijo.

Tretji vidik je povezan z varovanjem samih sistemov UI. Ti sistemi uvajajo posebna tveganja, povezana s podatki, modeli, vhodnimi in izhodnimi podatki, vmesniki in integracijami. Macas idr. [4] opozarjajo na ranljivost modelov globokega učenja za napade z namerno prilagojenimi vhodnimi podatki (angl. adversarial examples), Capuano idr. [9] pa poudarjajo, da razložljivost sistemov UI lahko izboljša razumevanje odločitev, hkrati pa odpira tudi dodatna tveganja. To pomeni, da se del nalog v kibernetski varnosti širi na vprašanja robustnosti modelov, varnosti podatkovnih tokov, nadzora nad uporabo modelov in zaščite celotnega življenjskega cikla sistemov UI.

Četrti vidik je povezan z upravljanjem in skladnostjo sistemov UI. Ta vidik izhaja iz tega, da uporaba UI v organizacijah zahteva obvladovanje tveganj, določanje odgovornosti, dokumentiranje odločitev, človeški nadzor in povezovanje varnostnih zahtev z regulativnimi obveznostmi. NIST Artificial Intelligence Risk Management Framework (NIST AI RMF) sistematizira obvladovanje tveganj pri uporabi sistemov UI skozi upravljanje, razumevanje konteksta, merjenje in ukrepanje [10], Akt o umetni inteligenci pa za sisteme UI z visokim tveganjem določa zahteve, ki vključujejo tudi dokumentacijo, preglednost, človeški nadzor, robustnost in kibernetsko varnost [5]. Za kompetence v kibernetski varnosti to pomeni širitev nalog na presojo tveganj pri uporabi sistemov UI, nadzor nad njihovo uporabo in zagotavljanje skladnosti.

2.2 Vpliv umetne inteligence na avtomatizacijo in preoblikovanje nalog

Presoja vpliva UI na delo je natančnejša, če izhaja iz posameznih nalog in ne iz poklicev ali delovnih mest kot celote. Acemoglu in Restrepo [11] razlagata tehnološke spremembe z vidika razporeditve nalog med človekom in tehnologijo. Avtomatizacija lahko posamezne korake naloge prenese na tehnologijo, hkrati pa tehnološki razvoj ustvarja tudi nove naloge, pri katerih ostaja človekova vloga pomembna. Podobno Arntz idr. [12] opozarjajo, da presoja na ravni poklicev ne pokaže dovolj natančno, katere naloge so dejansko izpostavljene avtomatizaciji.

Za kibernetsko varnost je tak pogled posebej pomemben, ker isti profil pogosto vključuje tehnične, analitične, dokumentacijske, komunikacijske in upravljavske naloge. Nekateri koraki so rutinski, ponovljivi ali zahtevajo obdelavo velikih količin podatkov, zato jih je mogoče podpreti z UI ali avtomatizirati na ravni posameznih korakov naloge. Druge naloge zahtevajo razumevanje konteksta, presojo tveganj, komunikacijo z deležniki in prevzem odgovornosti, zato jih UI praviloma ne odpravlja, temveč spreminja način njihove izvedbe.

Učinkov UI zato ne razumemo kot enostavnega nadomeščanja človekovega dela, temveč kot spremembo razmerja med izvedbo, podporo, nadzorom in odgovornostjo. Raisch in Krakowski [13] razlikujeta med avtomatizacijo, pri kateri stroj prevzame izvedbo naloge, in podporo

človekovemu delu, pri kateri človek in stroj sodelujeta pri izvedbi naloge. Hkrati opozarjata, da teh dveh procesov v organizacijah ni vedno mogoče jasno ločiti. V kibernetski varnosti lahko na primer sistem UI razvrsti opozorila, pripravi povzetek incidenta ali zazna odstopanja v obnašanju sistema, medtem ko presoja konteksta, sprejem odločitve, dokumentiranje in odgovornost ostanejo naloga strokovnjaka.

Za namen tega prispevka učinke UI na naloge v kibernetski varnosti na tej podlagi razvrščamo v tri skupine: (1) avtomatizacijo posameznih korakov naloge, (2) prestrukturiranje obstoječih nalog ter (3) razširitev obstoječih oziroma nastanek novih nalog. Prva skupina se nanaša na primere, ko UI podpira ali prevzame izvedbo posameznih, praviloma ponovljivih korakov oziroma korakov, ki zahtevajo obdelavo velikih količin podatkov. Druga skupina zajema naloge, ki ostanejo del dela strokovnjaka, vendar se spremeni način njihove izvedbe, zlasti zaradi večjega pomena nadzora, razlage, preverjanja in dokumentiranja. Tretja skupina vključuje naloge, ki nastajajo ali se bistveno razširijo zaradi uvajanja, uporabe, varovanja in upravljanja sistemov UI, na primer presojo ranljivosti modelov, spremljanje vhodnih in izhodnih podatkov sistemov UI, preverjanje zanesljivosti rezultatov, dokumentiranje uporabe UI, upravljanje tveganj pri uporabi sistemov UI in zagotavljanje skladnosti z zahtevami za uporabo UI.

2.3 Kompetence v kibernetski varnosti

Kompetence v kibernetski varnosti je smiselno razumeti kot povezavo med nalogami, znanji, spretnostmi in odgovornostmi, ki jih posamezniki oziroma organizacijske vloge potrebujejo za učinkovito delovanje v določenem varnostnem kontekstu. Takšno razumevanje je skladno z NICE Workforce Framework for Cybersecurity, ki delo v kibernetski varnosti strukturira prek nalog ter pripadajočih znanj in spretnosti [14]. Za ta prispevek je tak pristop pomemben, ker omogoča presojo, kako se spremembe posameznih nalog odražajo v novih oziroma razširjenih kompetenčnih zahtevah.

Podobno izhodišče ponuja Evropski okvir za kibernetske veščine (angl. European Cybersecurity Skills Framework, ECSF), ki opredeljuje profile v kibernetski varnosti ter z njimi povezane naloge, znanja, spretnosti in odgovornosti [1], [15]. ECSF je za ta prispevek uporaben predvsem kot referenčna podlaga za povezovanje prepoznanih sprememb z obstoječimi profili v kibernetski varnosti. Pri tem ni treba predpostaviti, da ima vsaka organizacija vse profile formalno vzpostavljene. Zlasti v manjših organizacijah so naloge pogosto združene ali prenesene na zunanje izvajalce.

Obstoječi kompetenčni modeli hkrati opozarjajo, da kompetenc v kibernetski varnosti ni mogoče razumeti izključno tehnično. Bendler in Felderer [16] ugotavljata, da številni modeli za informacijsko in kibernetsko varnost močno poudarjajo strokovno-tehnične kompetence, medtem ko so metodološke, socialne in osebne kompetence pogosto manj izrazito zastopane. Chowdhury in Gkioulos [17] podobno izpostavljata pomen tehničnih, izvedbenih, upravljavskih in komunikacijskih kompetenc pri kibernetski varnosti kritične infrastrukture. Na pomen širših kompetenc opozarjata tudi Dawson in Thomson [18], ki uspešnost prihodnje delovne sile v kibernetski varnosti povezujeta z zmožnostmi, ki presegajo ozko tehnično znanje, zlasti s presojo, prilagodljivostjo, komunikacijo in razumevanjem organizacijskega konteksta. To je pomembno tudi pri obravnavi UI, saj njena uporaba ne zahteva samo poznavanja orodij, temveč tudi presojo rezultatov sistemov UI, razumevanje omejitev, dokumentiranje odločitev, komunikacijo tveganj in odgovorno razporejanje nalog.

V tem prispevku kompetenc zato ne obravnavamo kot statičnega seznama znanj, temveč kot zmožnosti, vezane na spreminjajoče se naloge, odgovornosti in kontekst odločanja v kibernetski varnosti. Uvedba UI lahko okrepi pomen obstoječih kompetenc, na primer

analitične presoje, razumevanja tveganj in komunikacije z deležniki, hkrati pa odpira potrebo po novih oziroma razširjenih kompetencah, povezanih z uporabo, presojo, varovanjem in upravljanjem sistemov UI.

3 METODOLOGIJA

3.1 Metodološka umestitev prispevka

Prispevek je zasnovan kot konceptualni znanstveni članek. Pri takem tipu prispevka je osrednji rezultat oblikovanje nove konceptualne povezave, razlage, tipologije ali okvira na podlagi utemeljene izbire in argumentiranega povezovanja obstoječih konceptov, teorij oziroma raziskovalnih tokov. Konceptualni članki morajo imeti jasno raziskovalno zasnovo, utemeljeno izbiro konceptov ter pregledno prikazano logiko argumentacije [37].

Takšna metodološka zasnova je za obravnavano temo ustrezna, ker je vpliv UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti razmeroma novo in konceptualno še neustaljeno področje. Njegova obravnava zahteva povezovanje več raziskovalnih, strokovnih in regulativnih izhodišč: raziskav o uporabi UI in generativne UI v kibernetski varnosti, literature o avtomatizaciji in preoblikovanju dela, kompetenčnih okvirov za kibernetsko varnost, predvsem ECSF in NICE Framework, ter regulativnih in usmerjevalnih dokumentov s področja kibernetske varnosti, upravljanja tveganj in UI.

Prispevek se osredotoča na prvo fazo širšega raziskovalnega procesa, predstavljenega na sliki 1, tj. na oblikovanje preliminarne konceptualne zasnove referenčnega okvira. Namen te faze je izbrane znanstvene vire, kompetenčne okvire ter regulativne in usmerjevalne dokumente povezati v začetno zasnovo referenčnega okvira za presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti. Takšna zasnova je skladna z razumevanjem konceptualnih okvirov kot sredstev za strukturiranje, omejevanje in komuniciranje kompleksnih raziskovalnih pojavov v informacijskih sistemih [36].

V tej fazi raziskave je uporabljen namenski izbor virov, saj je cilj prispevka oblikovati začetne elemente referenčnega okvira in povezave med njimi, ne pa izčrpno mapirati vseh znanstvenih objav o UI in kibernetski varnosti. Izsledki te faze bodo podlaga za naslednjo raziskovalno fazo, tj. sistematično mapiranje literature, s katerim bo mogoče začetne elemente okvira preveriti, dopolniti in natančneje razmejiti.

3.2 Izbor virov

V analizo so bili vključeni viri, ki omogočajo povezavo med UI, nalogami, odgovornostmi in kompetenčnimi zahtevami v kibernetski varnosti. Namen izbora ni bil zajeti vseh objav o UI v kibernetski varnosti, temveč vključiti vire, ki prispevajo k razumevanju različnih vlog UI, vrst sprememb nalog, sprememb odgovornosti ter iz njih izpeljanih kompetenčnih zahtev. Izbor virov je bil zato namenski in usmerjen v oblikovanje preliminarne zasnove referenčnega okvira.

Iskanje znanstvenih virov je bilo opravljeno v obdobju junij–julij 2026. Iskanje ni bilo zasnovano kot sistematični pregled literature, zato niso bili uporabljeni formalni postopki izločanja in vključevanja virov po protokolu PRISMA. Namen iskanja je bil identificirati vsebinsko relevantne vire, ki omogočajo oblikovanje začetnih elementov referenčnega okvira ter povezav med UI, nalogami, odgovornostmi in kompetenčnimi zahtevami v kibernetski varnosti.

Znanstveni viri so bili razdeljeni v dve skupini. Prvo skupino so predstavljali znanstveni viri o UI v kibernetski varnosti. Ti so bili identificirani z namenskim iskanjem v podatkovnih bazah Scopus, Web of Science, IEEE Xplore in ACM Digital Library, dopolnilno pa tudi prek Google Scholar. Iskanje je bilo usmerjeno v novejše pregledne in raziskovalne prispevke, predvsem iz obdobja 2020–2026, ki obravnavajo uporabo UI pri zaznavanju, analizi in odzivanju na

grožnje, uporabo generativne UI v kibernetski varnosti, ranljivosti sistemov UI, varovanje modelov, upravljanje tveganj ter razvoj kompetenc in izobraževanja na področju kibernetske varnosti. Pri iskanju so bile uporabljene kombinacije izrazov, kot so *artificial intelligence*, *generative AI*, *machine learning*, *cybersecurity*, *cyber security*, *threat detection*, *incident response*, *threat intelligence*, *AI governance*, *cybersecurity skills*, *cybersecurity competences* in *cybersecurity education*. Iskalni izrazi so bili prilagojeni posameznim podatkovnim bazam. Pri začetni identifikaciji relevantnih znanstvenih virov je bilo kot podporno orodje uporabljeno tudi orodje Consensus. Uporabljeno je bilo za orientacijsko iskanje literature, prepoznavanje relevantnih raziskovalnih izhodišč in usmerjanje nadaljnjega pregleda virov. Orodje ni bilo uporabljeno za avtomatizirano odločanje o vključitvi virov v analizo. Končni izbor virov je temeljil na vsebinski presoji avtorjev glede njihove relevantnosti za oblikovanje preliminarne zasnove referenčnega okvira.

Drugo skupino so predstavljali znanstveni viri o avtomatizaciji in preoblikovanju dela. Ti viri niso bili vključeni kot rezultat izčrpnega pregleda literature o avtomatizaciji, temveč kot namensko izbrana konceptualna podlaga za razumevanje vpliva tehnologije na izvajanje nalog, razmerje med avtomatizacijo in podporo človekovemu delu, zaupanje v avtomatizirane sisteme ter nastajanje novih nalog zaradi tehnoloških sprememb. V prispevku služijo kot podlaga za razvrstitev učinkov UI na avtomatizacijo posameznih korakov naloge, prestrukturiranje obstoječih nalog ter razširitev obstoječih oziroma nastanek novih nalog. Pri tej skupini virov časovna omejitev ni bila uporabljena strogo, saj so bili vključeni tudi temeljni prispevki, pomembni za razumevanje avtomatizacije in preoblikovanja dela.

Poleg znanstvenih virov so bili vključeni tudi kompetenčni okviri ter regulativni in usmerjevalni dokumenti. Kompetenčni okviri so bili izbrani zato, ker predstavljajo uveljavljeno referenčno podlago za opis profilov, nalog, znanj, spretnosti in odgovornosti v kibernetski varnosti. Regulativni in usmerjevalni dokumenti so bili vključeni zato, ker uporaba UI v kibernetski varnosti odpira vprašanja upravljanja tveganj, človeškega nadzora, dokumentiranja, sledljivosti, odgovornosti, skladnosti in varovanja sistemov UI.

Vključeni so bili viri, ki so prispevali k vsaj enemu od naslednjih vidikov: razumevanju vlog UI v kibernetski varnosti, razumevanju sprememb nalog zaradi uporabe UI, razumevanju odgovornosti, nadzora ali odločanja pri uporabi UI, opredelitvi kompetenčnih zahtev ali povezovanju kompetenc s profili oziroma funkcijami v kibernetski varnosti. Izključeni so bili predvsem tehnično usmerjeni prispevki, ki obravnavajo razvoj ali primerjavo algoritmov brez povezave z delovnimi nalogami, odgovornostjo, kompetencami ali organizacijskim kontekstom.

Skupine virov, način njihove identifikacije oziroma izbora, uporabljeni viri in njihova vloga v analizi so prikazani v tabeli 1.

Tabela 1: Skupine izbranih virov, način izbora in njihova vloga v analizi

Skupina virov	**Način identifikacije oziroma izbora**	**Uporabljeni viri oziroma dokumenti**	**Vloga v prispevku**
Znanstveni viri o UI v kibernetski varnosti	Namensko iskanje, opravljeno v obdobju junij–julij 2026, v bazah Scopus, Web of Science, IEEE Xplore in ACM Digital Library, dopolnilno tudi prek Google Scholar in z uporabo orodja Consensus kot	Pregledni in raziskovalni prispevki, predvsem iz obdobja 2020–2026, ki obravnavajo uporabo UI v kibernetski varnosti, generativno UI, varovanje sistemov UI, analizo podatkov	Prepoznavanje nalog, tveganj, ranljivosti, novih področij dela in sprememb odgovornosti, ki vplivajo na kompetenčne zahteve v kibernetski varnosti.

	podpornega orodja za orientacijsko identifikacijo virov. Izbrani so bili viri, ki obravnavajo uporabo UI pri zaznavanju, analizi ali odzivanju na grožnje, uporabo UI kot dejavnika spreminjanja groženj, ranljivosti sistemov UI ter nove naloge, povezane z uporabo, upravljanjem in varovanjem sistemov UI.	o grožnjah, kompetenčne zahteve in izobraževanje na področju kibernetske varnosti. Celoten nabor uporabljenih znanstvenih virov je razviden iz seznama literature.	
Znanstveni viri o avtomatizaciji in preoblikovanju dela	Namenski izbor znanstvenih virov, ki pojasnjujejo vpliv tehnologije na izvajanje nalog, razmerje med avtomatizacijo in podporo človekovemu delu, zaupanje v avtomatizirane sisteme ter nastajanje novih nalog zaradi tehnoloških sprememb.	Acemoglu in Restrepo [11]; Arntz idr. [12]; Raisch in Krakowski [13]; Lee in See [19]; Parasuraman in Manzey [20]; Parker in Grote [21].	Konceptualna utemeljitev analize na ravni nalog ter oblikovanje kategorij učinkov UI: avtomatizacija posameznih korakov naloge, prestrukturiranje obstoječih nalog ter razširitev obstoječih oziroma nastanek novih nalog.
Kompetenčni okviri	Namenski izbor uveljavljenih kompetenčnih okvirov, ki opredeljujejo profile, naloge, znanja, spretnosti in odgovornosti v kibernetski varnosti.	NICE Framework [14]; European Cybersecurity Skills Framework – Role Profiles [1]; European Cybersecurity Skills Framework – User Manual [15].	Povezovanje prepoznanih sprememb nalog, odgovornosti in kompetenčnih zahtev z obstoječimi profili, nalogami in kompetencami v kibernetski varnosti.
Regulativni in usmerjevalni dokumenti	Namenski izbor dokumentov, ki določajo ali usmerjajo upravljanje tveganj, človeški nadzor, dokumentiranje, sledljivost, skladnost, kibernetsko varnost sistemov UI in poročanje o incidentih.	Akt o umetni inteligenci oziroma Uredba (EU) 2024/1689 [5]; Zakon o informacijski varnosti [22]; NIST Artificial Intelligence Risk Management Framework [10]; NIST Cybersecurity Framework 2.0 [3]; ENISA Threat Landscape 2024 [23]; MITRE ATLAS [24].	Prepoznavanje zahtev in usmeritev, ki vplivajo na odgovornosti, nadzor, odločanje, skladnost in kompetenčne zahteve organizacij ter strokovnjakov za kibernetsko varnost.

3.3 Analitični postopek in sinteza virov

V prispevku je uporabljena strukturirana sinteza izbranih virov. Sinteza ima integrativni značaj, ker povezuje različne vrste virov in jih uporablja za oblikovanje skupnih analitičnih kategorij:

vloge UI v kibernetski varnosti, spremembe nalog, spremembe odgovornosti oziroma nadzora ter kompetenčne zahteve. Tak pristop je primeren, kadar je znanje o obravnavanem pojavu razpršeno med različnimi raziskovalnimi skupnostmi, disciplinami ali vrstami virov ter kadar namen ni zgolj opisati obstoječe literature, temveč povezati različne poglede v začetno konceptualno razumevanje [38], [39].

Izbrani viri so bili analizirani z vidika povezave med UI, nalogami, odgovornostmi in kompetenčnimi zahtevami v kibernetski varnosti. Enota analize je bila relevantna navedba ali ugotovitev iz vira, ki se je nanašala na vlogo UI, spremembo naloge, tveganje, povezano z UI, spremembo odgovornosti oziroma nadzora ali kompetenčno zahtevo v kibernetski varnosti. Pri analizi niso bile upoštevane le neposredne navedbe kompetenc, temveč tudi opisi nalog, tveganj in odgovornosti, iz katerih je bilo mogoče utemeljeno izpeljati kompetenčne zahteve.

Analiza virov je bila vodena z enotnimi analitičnimi vprašanji. Pri vsakem viru je bilo preverjeno, na katero vlogo UI v kibernetski varnosti se nanaša, katere naloge oziroma odgovornosti opisuje, kakšen učinek ima UI na izvedbo teh nalog, kako se spreminjajo nadzor, odločanje ali odgovornost ter katere kompetenčne zahteve je mogoče iz tega neposredno povzeti ali utemeljeno izpeljati. Namen analize ni bil šteti pogostosti posameznih kompetenc v literaturi, temveč oblikovati sledljivo povezavo med izbranimi viri, spremembami nalog, odgovornostmi in kompetenčnimi zahtevami. Pregled uporabljenih elementov analize je prikazan v tabeli 2.

Tabela 2: Pregled elementov analize virov

Element analize	Namen elementa	Primer vrednosti
Vrsta vira	Opredelitev podlage, iz katere izhaja ugotovitev.	znanstveni vir; kompetenčni okvir; regulativni dokument; usmerjevalni dokument
Vloga UI	Določitev, v kateri vlogi se UI pojavlja v kibernetski varnosti.	UI kot orodje za podporo varnostnim procesom; UI kot dejavnik spreminjanja groženj; UI kot predmet varovanja; UI kot predmet upravljanja in skladnosti
Naloga v kibernetski varnosti	Opredelitev naloge, na katero se nanaša ugotovitev oziroma sprememba.	npr. razvrščanje opozoril; analiza incidenta; spremljanje groženj; varovanje modela; upravljanje tveganj
Učinek UI na nalogo	Razvrstitev vrste spremembe naloge.	avtomatizacija posameznih korakov naloge; prestrukturiranje obstoječih nalog; razširitev obstoječih oziroma nastanek novih nalog
Sprememba odgovornosti, nadzora ali odločanja	Opredelitev, kako uporaba UI vpliva na razmerje med avtomatizirano podporo, strokovno presojo, nadzorom, odločanjem in odgovornostjo.	potreba po preverjanju rezultatov UI; odločitev ostane pri strokovnjaku; dodatno dokumentiranje; določitev odgovornosti za uporabo UI
Kompetenčna zahteva	Opredelitev znanja, spretnosti ali zmožnosti, ki jo zahteva sprememba naloge oziroma odgovornosti.	presoja rezultatov sistemov UI; razumevanje omejitev modelov; dokumentiranje odločitev; upravljanje tveganj pri uporabi sistemov UI
Način utemeljitve kompetenčne zahteve	Označuje, ali je kompetenčna zahteva v viru navedena neposredno ali	neposredna navedba naloge, kompetence ali odgovornosti v viru;

	pa je izpeljana iz opisa naloge, tveganja oziroma odgovornosti.	izpeljava iz opisa naloge, tveganja ali odgovornosti

Vsebinska izhodišča za razvrščanje ugotovitev iz virov izhajajo iz teoretične obravnave v poglavju 2.1. V postopku sinteze so bila ta izhodišča oblikovana v štiri analitične vloge UI v kibernetski varnosti: UI kot orodje za podporo varnostnim procesom, UI kot dejavnik spreminjanja groženj, UI kot predmet varovanja ter UI kot predmet upravljanja in skladnosti. V prvem koraku analize so bile ugotovitve iz virov razvrščene glede na navedene vloge UI. V drugem koraku so bili primeri sprememb nalog razvrščeni glede na vrsto učinka UI na nalogo, pri čemer so bila upoštevana izhodišča iz poglavja 2.2: avtomatizacija posameznih korakov naloge, prestrukturiranje obstoječih nalog ter razširitev obstoječih oziroma nastanek novih nalog. V tretjem koraku je bilo preverjeno, ali ugotovitev vključuje tudi spremembo odgovornosti, nadzora ali odločanja.

Pri izpeljavi kompetenčnih zahtev je bila ločena neposredna navedba v viru od utemeljene izpeljave avtorjev. Neposredna navedba pomeni, da vir izrecno opredeli nalogo, znanje, spretnost, kompetenco ali odgovornost. Utemeljena izpeljava pa je bila uporabljena tam, kjer vir opisuje spremembo naloge, novo tveganje ali odgovornost, iz česar je bilo mogoče smiselno izpeljati kompetenčno zahtevo. Takšna razmejitev je pomembna, ker prispevek ne meri kompetenc empirično in ne šteje njihove pojavnosti v literaturi, temveč oblikuje sledljivo povezavo med izbranimi viri, spremembami nalog, odgovornostmi in kompetenčnimi zahtevami.

Sinteza rezultatov analize je potekala postopno. Najprej so bile opredeljene vloge UI in z njimi povezane spremembe nalog. Nato so bile prepoznane spremembe odgovornosti, nadzora in odločanja. V naslednjem koraku so bila iz teh sprememb izpeljana kompetenčna področja, v zadnjem koraku pa so bila ta področja povezana z izbranimi profili oziroma funkcijami v kibernetski varnosti. Na tej podlagi je bila oblikovana preliminarna zasnova referenčnega okvira, predstavljena v naslednjem poglavju.

4 PRELIMINARNA ZASNOVA REFERENČNEGA OKVIRA

V tem poglavju je predstavljena preliminarna zasnova referenčnega okvira, oblikovana na podlagi analitičnega postopka, opisanega v poglavju 3.3. Zasnova povezuje vloge UI v kibernetski varnosti, učinke UI na naloge, spremembe odgovornosti, nadzora in odločanja ter iz njih izpeljane kompetenčne zahteve. Ne gre za dokončen kompetenčni model ali validiran merski instrument, temveč za preliminarno zasnovo referenčnega okvira, ki omogoča sistematično presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti ter predstavlja podlago za nadaljnje sistematično mapiranje literature in empirično preverjanje.

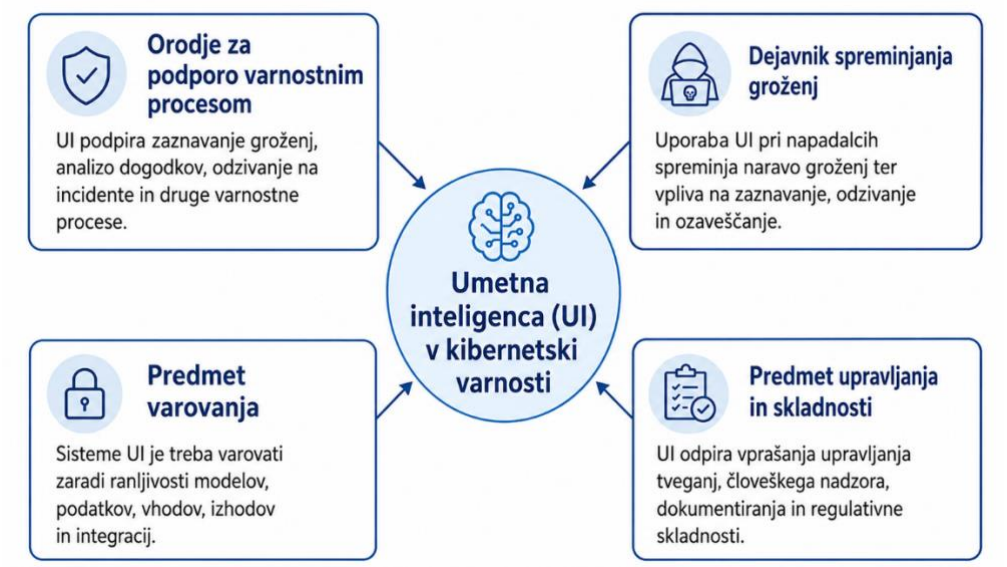
V nadaljevanju so elementi okvira predstavljeni v zaporedju, ki sledi raziskovalnim vprašanjem: najprej so opredeljene analitične vloge UI v kibernetski varnosti, nato učinki UI na naloge in odgovornosti, zatem kompetenčna področja, ki iz teh sprememb izhajajo, na koncu pa njihova povezava z izbranimi profili oziroma funkcijami v kibernetski varnosti.

4.1 Analitične vloge UI v kibernetski varnosti

Prvi element preliminarne zasnove referenčnega okvira so analitične vloge UI v kibernetski varnosti. Na podlagi vsebinskih vidikov, predstavljenih v poglavju 2.1, v tem poglavju razlikujemo štiri analitične vloge UI: UI kot orodje za podporo varnostnim procesom, UI kot dejavnik spreminjanja groženj, UI kot predmet varovanja ter UI kot predmet upravljanja in skladnosti. Te vloge predstavljajo avtorsko sintezo izbranih virov in pojasnjujejo, zakaj UI ne

vpliva enotno na vse naloge, odgovornosti in kompetenčne zahteve. Spremembe nalog in iz njih izpeljane kompetenčne zahteve se zato razlikujejo glede na vlogo, ki jo ima UI v posameznem varnostnem procesu. Štiri analitične vloge UI so prikazane na sliki 2.

Slika 2 prikazuje štiri analitične vloge UI kot prvi element preliminarne zasnove referenčnega okvira, tabela 3 pa te vloge povezuje s spremembami nalog in izpeljanimi kompetenčnimi zahtevami.



Slika 2: Štiri analitične vloge UI v kibernetski varnosti
Vir: lastna sinteza avtorjev na podlagi izbranih virov; grafično pripravljeno z uporabo ChatGPT (OpenAI).

Tabela 3: Analitične vloge UI, spremembe nalog in izpeljane kompetenčne zahteve v kibernetski varnosti

Vloga UI	**Spremembe nalog v kibernetski varnosti**	**Izpeljane kompetenčne zahteve**	**Podlaga v virih**
UI kot orodje za podporo varnostnim procesom	Sistemi UI lahko podprejo ali avtomatizirajo posamezne korake pri obdelavi varnostnih podatkov, zlasti pri zaznavanju anomalij, analizi varnostnih dogodkov, prednostnem razvrščanju varnostnih opozoril, analizi podatkov o grožnjah in podpori odzivanju na incidente. Težišče dela strokovnjaka se pri tem premika od ročne obdelave podatkov k preverjanju, razlagi in uporabi rezultatov sistema UI.	Zmožnost presoje rezultatov sistemov UI, razumevanje omejitev orodij, interpretacija varnostnih opozoril ter umeščanje rezultatov v varnostni in organizacijski kontekst.	Kaur idr. [2]; Uddin idr. [6]; Sai idr. [25]; Ferrag idr. [8]
UI kot dejavnik	Naloge spremljanja groženj, zaznavanja napadov, ozaveščanja	Razumevanje z UI spremenjenih vzorcev groženj,	Gupta idr. [7]; Yigit idr. [26]; Ferrag idr. [8]; ENISA [23];

spreminjanja groženj	uporabnikov in odzivanja se prilagajajo možnosti, da napadalci UI uporabljajo za pripravo zavajajočih vsebin, prilagajanje napadov ali avtomatizacijo posameznih korakov napadalnega procesa.	prepoznavanje zavajajočih vsebin, prilagajanje ozaveščanja uporabnikov, komunikacija tveganj ter posodabljanje postopkov zaznavanja in odzivanja.	MITRE Corporation [24]
UI kot predmet varovanja	Naloge se širijo na varovanje sistemov UI, vključno z varovanjem podatkov, modelov, vhodnih in izhodnih podatkov, vmesnikov, integracij in življenjskega cikla sistema.	Razumevanje ranljivosti sistemov UI, presoja odpornosti modelov, varovanje podatkovnih tokov, nadzor nad uporabo modelov, preverjanje zanesljivosti rezultatov sistemov UI ter varnostna presoja vmesnikov in integracij.	Macas idr. [4]; Capuano idr. [9]; Ferrag idr. [8]; MITRE Corporation [24]
UI kot predmet upravljanja in skladnosti	Naloge se širijo na upravljanje tveganj, dokumentiranje uporabe sistemov UI, zagotavljanje človeškega nadzora, določanje odgovornosti, spremljanje skladnosti in povezovanje tehničnih odločitev z regulativnimi zahtevami.	Upravljanje tveganj pri uporabi sistemov UI, dokumentiranje odločitev, razumevanje zahtev glede človeškega nadzora, zagotavljanje skladnosti z regulativnimi in organizacijskimi zahtevami, zagotavljanje sledljivosti odločitev in odgovorne uporabe sistemov UI.	NIST [10]; NIST [3]; European Parliament and Council [5]; ZInfV-1 [22]

Iz tabele 3 je razvidno, da se kompetenčne zahteve ne razlikujejo le po tehnični zahtevnosti, temveč predvsem po vlogi, ki jo ima UI v posameznem varnostnem procesu. Kadar UI podpira varnostne procese, je ključna presoja rezultatov sistemov UI v konkretnem varnostnem kontekstu. Kadar UI spreminja grožnje ali postane predmet varovanja, se kompetenčne zahteve širijo na razumevanje novih vzorcev napadov, ranljivosti modelov, podatkovnih tokov, vmesnikov in integracij. Pri upravljanju in skladnosti pa se poudarek premakne k človeškemu nadzoru, dokumentiranju, sledljivosti in upravljanju tveganj pri uporabi sistemov UI. Tabela tako pokaže, da ista tehnologija ustvarja različne kompetenčne zahteve glede na to, ali je uporabljena kot orodje, vir sprememb v grožnjah, predmet varovanja ali predmet upravljanja.

4.2 Učinki UI na naloge in odgovornosti v kibernetski varnosti

Drugi element preliminarne zasnove referenčnega okvira so učinki UI na naloge in odgovornosti v kibernetski varnosti. Analiza izbranih virov kaže, da vpliva UI na naloge ni smiselno obravnavati kot enoten proces. Učinki se razlikujejo glede na naravo naloge, stopnjo avtomatizirane podpore, potrebo po strokovni presoji, raven odgovornosti in vlogo, ki jo ima UI

v posameznem varnostnem procesu. Zato so bili učinki UI na naloge razvrščeni v tri skupine: avtomatizacija posameznih korakov naloge, prestrukturiranje obstoječih nalog ter razširitev obstoječih oziroma nastanek novih nalog. Pregled teh učinkov, značilnih sprememb, primerov nalog in vpliva na kompetenčne zahteve je prikazan v tabeli 4.

Tabela 4: Učinki UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti

Vidik primerjave	**Avtomatizacija posameznih korakov naloge**	**Prestrukturiranje obstoječih nalog**	**Razširitev obstoječih oziroma nastanek novih nalog**
Značilnost spremembe	Sistem UI lahko prevzame ali podpira posamezne korake naloge, zlasti pri obdelavi večjih količin varnostnih podatkov, ponavljajočih se postopkih, začetnem razvrščanju informacij ali pripravi osnutkov. Tak učinek je skladen z razumevanjem avtomatizacije kot prenosa posameznih nalog oziroma korakov naloge na tehnologijo [11], [12].	Naloga ostane del dela strokovnjaka, vendar se spremeni način njene izvedbe. Poudarek se premakne od ročne izvedbe k nadzoru, razlagi, presoji, dokumentiranju in odgovorni uporabi rezultatov sistemov UI. Tak premik je skladen z razumevanjem UI kot podpore človekovemu delu, ne zgolj kot nadomestitve dela [13], ter z literaturo o zaupanju in pristranskosti pri uporabi avtomatiziranih sistemov [19], [20].	Uvajanje, uporaba, upravljanje in varovanje sistemov UI širijo obseg nalog v kibernetski varnosti na področja, ki prej niso bila standardni del dela ali pa so bila manj izrazita. To vključuje varovanje modelov, podatkovnih tokov, vmesnikov in integracij [4], [8], [9], [24] ter upravljanje tveganj, človeški nadzor, dokumentiranje in skladnost pri uporabi sistemov UI [5], [10], [22].
Primeri nalog v kibernetski varnosti	Prednostno razvrščanje varnostnih opozoril, začetna analiza varnostnih dogodkov, zaznavanje anomalij, povzemanje informacij o grožnjah in priprava osnutkov poročil o incidentih [2], [6], [25].	Analiza incidentov, analiza podatkov o grožnjah, presoja varnostnih priporočil, presoja, ali je varnostni dogodek potrebno predati v nadaljnjo obravnavo, priprava odzivnih ukrepov ter komunikacija z vodstvom ali uporabniki [2], [6], [13], [19].	Varovanje sistemov UI, presoja ranljivosti modelov, varovanje podatkovnih tokov in integracij, nadzor nad uporabo modelov, upravljanje tveganj pri uporabi sistemov UI, zagotavljanje človeškega nadzora, dokumentiranje uporabe sistemov UI in zagotavljanje skladnosti z regulativnimi zahtevami [4], [5], [8], [9], [10], [22], [24].
Sprememba odgovornosti, nadzora ali odločanja	Odgovornost praviloma ostane pri strokovnjaku oziroma organizaciji, čeprav sistem UI podpira ali izvede posamezen korak naloge. Potrebno je preverjanje rezultatov in odločanje o njihovi	Poveča se pomen nadzora, razlage in utemeljevanja odločitev, ker strokovnjak ne izvaja več vseh korakov ročno, vendar ostaja odgovoren za presojo in ukrepanje. Pri tem	Nastanejo dodatne odgovornosti za upravljanje, varovanje, dokumentiranje, nadzor in skladnost pri uporabi sistemov UI. Posebej pomembne so odgovornosti glede človeškega nadzora,

	uporabi, saj avtomatizacija posameznega koraka ne pomeni prenosa odgovornosti za celotno nalogo [11], [13].	sta pomembna ustrezno zaupanje v sistem in zavedanje tveganja pretiranega zanašanja na rezultate avtomatiziranih sistemov [19], [20].	sledljivosti, tehnične dokumentacije, obvladovanja tveganj in kibernetske varnosti sistemov UI [5], [10], [22].
Vpliv na kompetenčne zahteve	Strokovnjak mora razumeti namen, način delovanja in omejitve orodja UI, preveriti rezultat sistema UI, prepoznati napačne, nepopolne ali nerelevantne rezultate ter presoditi, ali je rezultat primeren za uporabo v konkretnem varnostnem in organizacijskem kontekstu [2], [6], [25].	Poveča se pomen analitične presoje, razumevanja konteksta, ustreznega zaupanja v rezultate sistemov UI, prepoznavanja tveganja pretiranega zanašanja na te rezultate ter dokumentiranja odločitev [19], [20], [21].	Potrebne so nove oziroma razširjene kompetence za razumevanje ranljivosti sistemov UI, razložljivosti in omejitev modelov, varovanje modelov in podatkovnih tokov, upravljanje tveganj pri uporabi sistemov UI, razumevanje regulativnih zahtev, zagotavljanje sledljivosti ter odgovorno uporabo sistemov UI [4], [5], [8], [9], [10], [22], [24].

Tabela 4 kaže, da avtomatizacija posameznih korakov naloge praviloma ne odpravi naloge kot celote, temveč spremeni razmerje med izvedbo naloge, strokovno presojo in odgovornostjo. Pri prestrukturiranju obstoječih nalog je ta premik še bolj izrazit: osrednja postane zmožnost nadzora, razlage, preverjanja, utemeljevanja in dokumentiranja odločitev, ki so podprte s sistemi UI. Tretji učinek je povezan z razširitvijo obstoječih oziroma nastankom novih nalog, zlasti pri varovanju modelov, upravljanju tveganj pri uporabi sistemov UI, zagotavljanju človeškega nadzora, določanju odgovornosti in spremljanju skladnosti. Zato vpliv UI na kompetence ne izhaja samo iz tehnične uporabe orodij, temveč tudi iz sprememb v nadzoru, odločanju in odgovornosti.

4.3 Kompetenčna področja, povezana s spremembami nalog in odgovornosti zaradi uporabe UI

Tretji element preliminarne zasnove referenčnega okvira so kompetenčna področja, ki izhajajo iz sprememb nalog, odgovornosti, nadzora in odločanja zaradi uporabe UI. Analiza kaže, da vpliv UI na kompetence v kibernetski varnosti ni omejen na uporabo novih orodij. Kompetenčne zahteve se oblikujejo predvsem tam, kjer se spremeni razmerje med sistemom UI in strokovno presojo, kjer UI prispeva k spremenjenim vzorcem groženj, kjer sistemi UI sami postanejo predmet varovanja ter kjer uporaba UI odpira vprašanja odgovornosti, nadzora, sledljivosti in skladnosti. Izpeljana kompetenčna področja so prikazana v tabeli 5.

Tabela 5: Kompetenčna področja, povezana s spremembami nalog in odgovornosti zaradi uporabe UI

Kompetenčno področje	Opis kompetenčnega področja	Povezava s spremembami nalog	Primer uporabe oziroma naloge
Presoja in preverjanje	Preverjanje rezultatov sistemov UI, prepoznavanje	Avtomatizacija posameznih korakov naloge pri razvrščanju	Preverjanje, ali je sistem UI pravilno prednostno

rezultatov sistemov UI	napačnih, nepopolnih ali nerelevantnih rezultatov ter umeščanje teh rezultatov v varnostni in organizacijski kontekst.	opozoril, začetni analizi dogodkov, zaznavanju anomalij in pripravi osnutkov poročil.	razvrstil varnostno opozorilo ali pripravil ustrezen povzetek incidenta.
Razumevanje omejitev sistemov UI in ustrezno zaupanje v njihove rezultate	Razumevanje omejitev orodij UI, tveganja pretiranega ali nezadostnega zanašanja na rezultate sistemov UI ter potrebe po človeški presoji.	Prestrukturiranje obstoječih nalog, pri katerih strokovnjak ne izvaja več vseh korakov ročno, vendar ostaja odgovoren za presojo, razlago in odločitev.	Presoja, ali se lahko analitik zanese na priporočilo sistema UI ali mora izvesti dodatno preverjanje.
Razumevanje z UI spremenjenih vzorcev groženj	Prepoznavanje z UI spremenjenih vzorcev groženj, zavajajočih vsebin, prilagojenih napadov ter sprememb v socialnih in tehničnih vidikih napadov.	Prestrukturiranje oziroma razširitev nalog spremljanja groženj, zaznavanja napadov, ozaveščanja uporabnikov in odzivanja.	Prepoznavanje zavajajočega elektronskega sporočila ali druge vsebine, pripravljene z generativno UI.
Varovanje sistemov UI	Razumevanje ranljivosti sistemov UI, varovanje podatkovnih tokov, modelov, vhodnih in izhodnih podatkov, vmesnikov in integracij ter presoja odpornosti sistemov UI.	Razširitev obstoječih oziroma nastanek novih nalog, povezanih z varovanjem sistemov UI kot posebnega predmeta varovanja.	Preverjanje varnosti podatkovnih tokov, vhodnih podatkov, izhodnih podatkov, vmesnikov ali integracij sistema UI.
Upravljanje tveganj pri uporabi sistemov UI in zagotavljanje skladnosti z zahtevami	Prepoznavanje, ocenjevanje in obvladovanje tveganj pri uporabi sistemov UI ter razumevanje zahtev glede človeškega nadzora, odgovornosti, sledljivosti in skladnosti z regulativnimi in organizacijskimi zahtevami.	Razširitev obstoječih oziroma nastanek novih nalog na področju upravljanja tveganj pri uporabi sistemov UI, nadzora nad njihovo uporabo in povezovanja tehničnih odločitev z regulativnimi in organizacijskimi zahtevami.	Ocena tveganj pred uvedbo sistema UI v varnostno-operativni center ali v postopke odzivanja na varnostne incidente.
Dokumentiranje, sledljivost in komunikacija odločitev	Dokumentiranje uporabe sistemov UI, utemeljevanje odločitev, zagotavljanje sledljivosti ter komunikacija tveganj vodstvu, uporabnikom in drugim deležnikom.	Prestrukturiranje nalog odločanja in odzivanja ter razširitev zahtev glede dokazljivosti, odgovorne uporabe in organizacijskega nadzora.	Dokumentiranje, zakaj je bil rezultat sistema UI sprejet, zavrnjen ali dodatno preverjen.

Iz tabele 5 je razvidno, da izpeljana kompetenčna področja niso splošna področja znanja o UI, temveč so vezana na konkretne spremembe nalog, odgovornosti in odločanja v kibernetski varnosti. Nekatera področja predvsem razširjajo že obstoječe kompetence, zlasti analitično presojo, razumevanje tveganj, dokumentiranje in komunikacijo. Druga so bolj specifično

povezana z značilnostmi sistemov UI, predvsem z razumevanjem njihovih omejitev, ranljivosti, podatkovnih tokov, modelov, vmesnikov, integracij in zahtev glede človeškega nadzora.

Kompetenčna področja niso enako pomembna za vse naloge in profile. Pri nalogah, kjer UI podpira obdelavo podatkov ali pripravo začetnih analiz, je ključna zmožnost preverjanja, razlage in varnostne presoje rezultatov sistemov UI. Pri nalogah, ki vključujejo varovanje sistemov UI, so izrazitejše tehnične kompetence, povezane z modeli, podatkovnimi tokovi, vhodnimi in izhodnimi podatki, vmesniki in integracijami. Na področju upravljanja tveganj pri uporabi sistemov UI in zagotavljanja skladnosti pa postanejo pomembnejše kompetence za dokumentiranje, zagotavljanje sledljivosti, razumevanje odgovornosti, človeški nadzor in povezovanje tehničnih odločitev z regulativnimi in organizacijskimi zahtevami.

Ta kompetenčna področja so podlaga za preliminarno zasnovo referenčnega okvira, v katerem so spremembe nalog povezane z izbranimi profili oziroma organizacijskimi vlogami v kibernetski varnosti.

4.4 Povezava kompetenčnih zahtev s profili oziroma funkcijami v kibernetski varnosti

Četrti element preliminarne zasnove referenčnega okvira je povezava kompetenčnih zahtev s profili oziroma funkcijami v kibernetski varnosti. Namen te povezave ni določiti univerzalnega seznama kompetenc za vse strokovnjake za kibernetsko varnost, temveč pokazati, kako se lahko spremembe nalog, odgovornosti in kompetenčnih zahtev razporedijo med različne organizacijske vloge. Na tej podlagi lahko organizacija presodi, kateri profili so vključeni v uporabo, uvajanje, varovanje ali upravljanje sistemov UI ter katere kompetence je treba dodatno razvijati. Preliminarna zasnova te povezave je prikazana v tabeli 6.

Tabela 6: Preliminarna zasnova referenčnega okvira za presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti

Profil oziroma funkcija v kibernetski varnosti	**Povezane vloge UI**	**Značilne spremembe nalog in odgovornosti**	**Ključna kompetenčna področja**
Analitik v varnostno-operativnem centru	UI kot orodje za podporo varnostnim procesom; UI kot dejavnik spreminjanja groženj	Prednostno razvrščanje opozoril, začetna analiza dogodkov, zaznavanje anomalij, preverjanje rezultatov sistemov UI in presoja, ali je treba varnostni dogodek predati v nadaljnjo obravnavo. Težišče odgovornosti analitika se pri uporabi UI premakne k preverjanju pravilnosti razvrstitve, presoji konteksta in utemeljitvi nadaljnje obravnave.	Presoja in preverjanje rezultatov sistemov UI; razumevanje omejitev sistemov UI; razumevanje z UI spremenjenih vzorcev groženj.
Strokovnjak za odzivanje na varnostne incidente	UI kot orodje za podporo varnostnim procesom; UI kot dejavnik spreminjanja groženj	Uporaba sistemov UI pri analizi varnostnih incidentov, pripravi odzivnih ukrepov in poročil ter prilagajanju odziva na napade, pri katerih je bila uporabljena UI. Odgovornost ostaja pri strokovnjaku oziroma odzivni ekipi, zlasti pri potrditvi ukrepov,	Presoja in preverjanje rezultatov sistemov UI; dokumentiranje in utemeljevanje odločitev; razumevanje z UI spremenjenih vzorcev

		presoji posledic, dokumentiranju odločitev in komunikaciji z vodstvom ali drugimi deležniki.	groženj; komunikacija tveganj.
Strokovnjak za analizo podatkov o grožnjah	UI kot orodje za podporo varnostnim procesom; UI kot dejavnik spreminjanja groženj	Analiza večjih količin podatkov o grožnjah, prepoznavanje novih vzorcev napadov, presoja relevantnosti informacij in posodabljanje scenarijev groženj. Odgovornost strokovnjaka se krepi pri preverjanju zanesljivosti virov, razlagi rezultatov sistemov UI ter presoji, katere informacije so pomembne za konkretni varnostni in organizacijski kontekst.	Razumevanje omejitev sistemov UI; presoja in preverjanje rezultatov sistemov UI; razumevanje z UI spremenjenih vzorcev groženj; povezovanje tehničnih in kontekstualnih informacij.
Strokovnjak za implementacijo rešitev s področja kibernetske varnosti	UI kot predmet varovanja; UI kot orodje za podporo varnostnim procesom	Vključevanje sistemov UI v obstoječe varnostne rešitve, preverjanje varnosti integracij, nadzor nad podatkovnimi tokovi, varovanje vmesnikov in spremljanje zanesljivosti rezultatov sistemov UI. Odgovornost strokovnjaka se krepi pri tehnični presoji varnosti integracij, preverjanju zanesljivosti delovanja sistema UI in zagotavljanju, da uvedba sistema UI ne ustvarja dodatnih ranljivosti.	Varovanje sistemov UI; razumevanje ranljivosti modelov, podatkovnih tokov, vmesnikov in integracij; presoja tehničnih omejitev sistemov UI; preverjanje zanesljivosti rezultatov sistemov UI.
Upravljavec tveganj oziroma odgovorna oseba za varnost	UI kot predmet upravljanja in skladnosti; UI kot predmet varovanja	Presoja tveganj pri uporabi sistemov UI, določanje odgovornosti, vključevanje teh tveganj v obstoječe procese upravljanja kibernetske varnosti in spremljanje nadzornih ukrepov. Odgovornost se krepi pri odločanju o sprejemljivosti tveganj, določanju kontrol, spremljanju njihove učinkovitosti ter povezovanju uporabe UI z organizacijskim sistemom upravljanja varnosti.	Upravljanje tveganj pri uporabi sistemov UI in zagotavljanje skladnosti z zahtevami; razumevanje zahtev glede človeškega nadzora; dokumentiranje, sledljivost in komunikacija odločitev.
Oseba oziroma enota, odgovorna za zagotavljanje skladnosti	UI kot predmet upravljanja in skladnosti	Spremljanje regulativnih zahtev, dokumentiranje uporabe sistemov UI, preverjanje skladnosti postopkov, sodelovanje s tehničnimi profili in priprava dokazil o odgovorni uporabi UI. Odgovornost se krepi pri zagotavljanju sledljivosti, presoji skladnosti uporabe UI z notranjimi pravili in zunanjimi zahtevami ter pri	Razumevanje regulativnih in organizacijskih zahtev; dokumentiranje in sledljivost; komunikacija odločitev; povezovanje tehničnih ukrepov z zahtevami glede skladnosti.

		pripravi dokazil za notranje ali zunanje preverjanje.	
Vodstvo oziroma odločevalci na področju informacijske varnosti	UI kot predmet upravljanja in skladnosti; UI kot orodje za podporo varnostnim procesom	Sprejemanje odločitev o uvedbi sistemov UI, določanje prioritet, razporejanje odgovornosti, zagotavljanje virov in vključevanje UI v strategijo kibernetske varnosti. Odgovornost vodstva se krepi pri presoji sprejemljivosti uporabe UI, določanju pravil za njeno uporabo, zagotavljanju nadzora ter usklajevanju tehničnih, organizacijskih in regulativnih vidikov.	Razumevanje organizacijskih tveganj, povezanih z uporabo UI; odgovorno odločanje; razporejanje odgovornosti; komunikacija tveganj; nadzor nad uporabo sistemov UI.

Iz preliminarne zasnove referenčnega okvira je razvidno, da vpliv UI na naloge, odgovornosti in kompetenčne zahteve ni enak za vse profile oziroma organizacijske vloge. Pri operativnih profilih je poudarek predvsem na preverjanju rezultatov sistemov UI, razumevanju njihovih omejitev, presoji konteksta in odločitvi, ali je treba varnostni dogodek predati v nadaljnjo obravnavo. Pri profilih, ki sodelujejo pri uvajanju, integraciji ali varovanju sistemov UI, so izrazitejše naloge in odgovornosti, povezane z varovanjem modelov, podatkovnih tokov, vhodnih in izhodnih podatkov, vmesnikov in integracij. Pri upravljavskih, nadzornih in vodstvenih funkcijah pa se vpliv UI kaže predvsem v upravljanju tveganj pri uporabi sistemov UI, razporejanju odgovornosti, dokumentiranju, zagotavljanju sledljivosti, človeškem nadzoru in skladnosti z regulativnimi zahtevami.

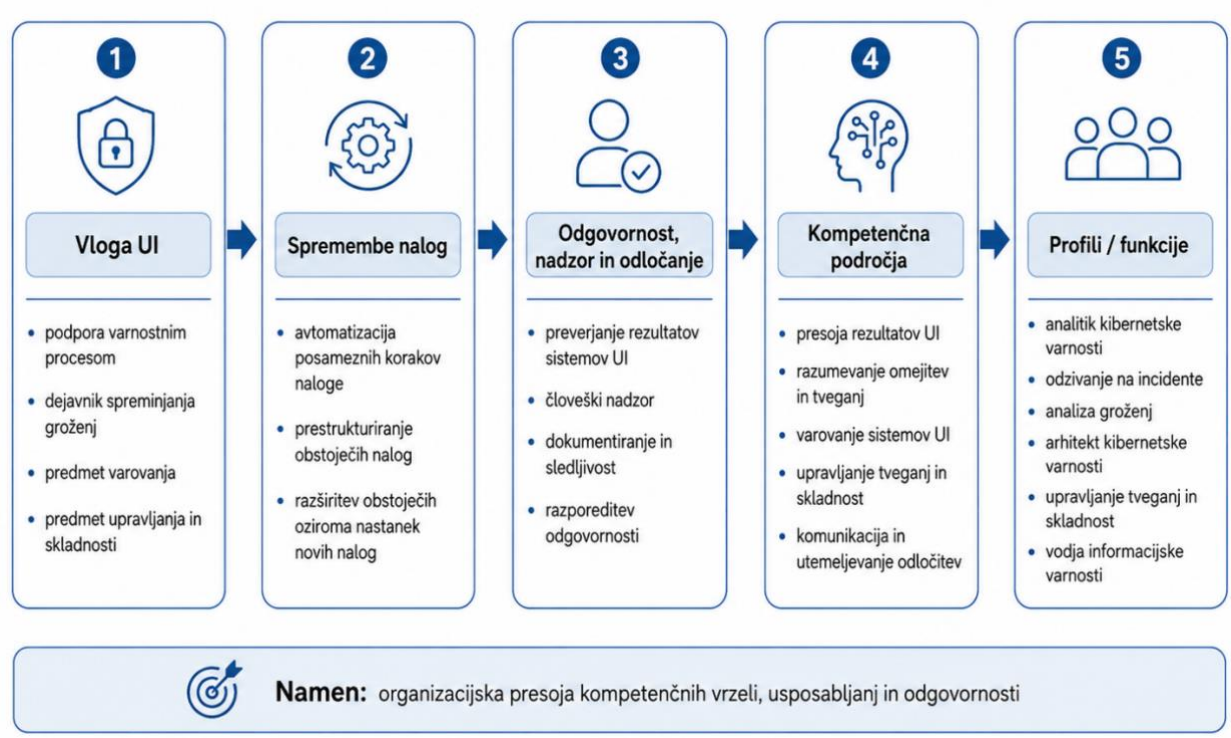
Preliminarna zasnova referenčnega okvira je zato uporabna kot pripomoček za organizacijsko presojo sprememb nalog, odgovornosti in kompetenčnih vrzeli. Organizacija lahko za posamezen profil oziroma funkcijo najprej opredeli, v kateri vlogi se UI pojavlja, nato presodi, katere naloge in odgovornosti se spreminjajo, in šele nato določi, katere kompetence je treba razvijati. Tak pristop preprečuje preširoko razumevanje kompetenc kot splošnega poznavanja UI in usmerja pozornost na konkretne naloge, odgovornosti in tveganja, ki nastajajo pri uporabi sistemov UI v kibernetski varnosti.

4.5 Konceptualna shema predlaganega referenčnega okvira

Na podlagi predhodnih podpoglavij je mogoče preliminarno zasnovo referenčnega okvira prikazati kot konceptualno shemo medsebojno povezanih elementov. Izhodišče presoje je vloga UI v posameznem varnostnem procesu. Iz te vloge izhajajo spremembe nalog, ki vplivajo na odgovornost, nadzor in odločanje. Na tej podlagi je mogoče opredeliti kompetenčna področja, ta pa povezati z izbranimi profili oziroma funkcijami v kibernetski varnosti.

Slika 3 prikazuje logiko presoje, na kateri temelji preliminarna zasnova referenčnega okvira. Kompetenčne zahteve niso obravnavane kot splošna posledica uporabe UI, temveč kot rezultat povezave med vlogo UI, spremembo konkretne naloge, spremembo odgovornosti oziroma nadzora ter profilom oziroma funkcijo, ki je vključena v izvedbo naloge.

Tako zasnovan okvir lahko organizacijam služi kot izhodišče za sistematično presojo kompetenčnih vrzeli, načrtovanje usposabljanj, posodabljanje opisov nalog in razporejanje odgovornosti pri uvajanju ali uporabi sistemov UI v kibernetski varnosti.



Slika 3: Povezava ključnih elementov predlaganega referenčnega okvira za presojo vpliva UI na naloge, odgovornosti in kompetenčne zahteve v kibernetski varnosti
Vir: lastna zasnova avtorjev, grafično pripravljeno z uporabo ChatGPT (OpenAI).

5 DISKUSIJA

5.1 Sinteza odgovorov na raziskovalna vprašanja

Rezultati analize potrjujejo, da je vpliv UI na delo v kibernetski varnosti smiselno presojati na ravni posameznih nalog, odgovornosti in kompetenčnih zahtev, ne le na ravni profilov oziroma delovnih mest kot celote. Tak pristop omogoča natančnejše razumevanje, katere naloge UI podpira ali pri njih avtomatizira posamezne korake, katere naloge se zaradi UI prestrukturirajo ter katere naloge se razširijo ali nastanejo zaradi uporabe, varovanja in upravljanja sistemov UI. Takšen pristop je skladen z izhodiščem, da so posamezne naloge primernejša enota analize učinkov avtomatizacije kot poklici oziroma delovna mesta kot celota [11], [12].

Prvo raziskovalno vprašanje se nanaša na vloge UI v kibernetski varnosti in njihovo povezavo s spremembami nalog, odgovornosti in kompetenčnih zahtev. Analiza pokaže, da se UI pojavlja v štirih analitičnih vlogah: kot orodje za podporo varnostnim procesom, kot dejavnik spreminjanja groženj, kot predmet varovanja ter kot predmet upravljanja in skladnosti. Ključna ugotovitev je, da vsaka od teh vlog odpira drugačne spremembe nalog, odgovornosti in kompetenčnih zahtev. Zato UI v kibernetski varnosti ni mogoče obravnavati kot enoten dejavnik sprememb, temveč kot tehnologijo, katere učinki so odvisni od njene konkretne vloge v varnostnem procesu.

Drugo raziskovalno vprašanje se nanaša na učinke UI na naloge v kibernetski varnosti z vidika avtomatizacije posameznih korakov naloge, prestrukturiranja obstoječih nalog ter razširitve obstoječih oziroma nastanka novih nalog. Analiza pokaže, da ta razvrstitev preprečuje poenostavljeno razumevanje UI kot tehnologije, ki naloge bodisi v celoti avtomatizira bodisi nanje nima vpliva. Pri številnih nalogah UI ne nadomesti človekovega dela v celoti, temveč podpira ali avtomatizira posamezne korake ter s tem spremeni razmerje med izvedbo, presojo, nadzorom in odgovornostjo. Takšna razlaga je skladna z razumevanjem avtomatizacije in podpore človekovemu delu kot prepletenih procesov ter z opozorili, da uporaba takšnih

sistemov zahteva ustrezno zaupanje, preverjanje rezultatov in zavedanje tveganja pretiranega zanašanja na njihove rezultate [13], [19], [20].

Tretje raziskovalno vprašanje se nanaša na kompetenčna področja, ki izhajajo iz sprememb nalog in odgovornosti, ter na njihovo povezavo z izbranimi profili oziroma funkcijami v kibernetski varnosti. Analiza pokaže, da kompetenčnih zahtev ni mogoče ustrezno opisati kot splošne potrebe po »znanju o UI«. Kompetence so odvisne od konkretne naloge, vloge UI pri njeni izvedbi ter odgovornosti, ki ostaja pri strokovnjaku oziroma organizaciji. Pri nalogah, kjer UI podpira obdelavo podatkov ali pripravo začetnih analiz, je v ospredju presoja rezultatov sistemov UI. Pri nalogah, ki se zaradi UI prestrukturirajo, postanejo pomembnejši nadzor, razlaga, dokumentiranje in utemeljevanje odločitev. Pri varovanju sistemov UI se kompetenčne zahteve širijo na razumevanje ranljivosti modelov, podatkovnih tokov, vhodnih in izhodnih podatkov, vmesnikov in integracij. Pri upravljanju in zagotavljanju skladnosti pa v ospredje stopijo človeški nadzor, sledljivost, dokumentiranje in jasna razporeditev odgovornosti.

Predlagana preliminarna zasnova referenčnega okvira tako dopolnjuje obstoječe kompetenčne okvire, kot sta ECSF in NICE Framework. Ti okviri opredeljujejo profile, naloge, znanja, spretnosti in odgovornosti v kibernetski varnosti [1], [14], [15], predlagana zasnova pa pokaže, kako se lahko obstoječe naloge, odgovornosti in kompetenčne zahteve spremenijo, kadar so v varnostne procese vključeni sistemi UI.

5.2 Teoretični prispevek članka

V teoretičnem smislu članek nadgrajuje splošno vprašanje, katera znanja o UI potrebujejo strokovnjaki za kibernetsko varnost, z razlago, da je kompetenčne zahteve treba izpeljevati iz sprememb konkretnih nalog, odgovornosti, nadzora in odločanja. Pri tem izhaja iz razumevanja, da tehnologija ne spreminja nujno poklicev kot celote, temveč predvsem posamezne naloge in razmerje med človekom in tehnologijo [11], [12], [13]. Predlagani referenčni okvir zato ni mišljen kot statičen seznam kompetenc, temveč kot konceptualna povezava med uporabo UI, spremembami nalog, odgovornostjo in kompetenčnimi zahtevami [36].

Osrednja teoretična dodana vrednost članka je v povezovanju treh sklopov literature, ki so pogosto obravnavani ločeno: literature o uporabi UI v kibernetski varnosti, literature o avtomatizaciji in preoblikovanju dela ter literature o kompetencah v kibernetski varnosti. Literatura o avtomatizaciji opozarja, da učinkov tehnologije ni mogoče ustrezno razumeti samo na ravni poklicev, temveč predvsem na ravni nalog [11], [12]. V kibernetski varnosti je to posebej pomembno, ker posamezni profili združujejo tehnične, analitične, komunikacijske, dokumentacijske in upravljavske naloge. Zato uporaba UI ne vodi nujno v odpravo celotnih profilov oziroma funkcij, temveč pogosteje v spremembo razmerja med izvedbo naloge, avtomatizirano podporo, strokovno presojo in odgovornostjo [13].

Članek k povezovanju teh razprav dodaja razmejitev štirih analitičnih vlog UI v kibernetski varnosti. UI se lahko pojavlja kot orodje za podporo varnostnim procesom, kot dejavnik spreminjanja groženj, kot predmet varovanja ter kot predmet upravljanja in skladnosti. Ta razmejitev je teoretično pomembna zato, ker pokaže, da UI v kibernetski varnosti nima enotnega učinka. Kompetenčne zahteve se razlikujejo glede na to, ali UI podpira razvrščanje opozoril ali analizo dogodkov, spreminja načine izvedbe napadov, zahteva varovanje samih sistemov UI ali odpira vprašanja človeškega nadzora, dokumentiranja, odgovornosti in skladnosti [2], [4], [5], [6], [7], [8], [10], [23], [24].

Pomemben del teoretičnega prispevka je tudi vključitev odgovornosti, nadzora in odločanja kot povezovalnega elementa med spremembami nalog in kompetenčnimi zahtevami. Vpliv UI na

kompetence ne izhaja samo iz tega, kaj sistem tehnično omogoča, temveč tudi iz tega, kdo mora preveriti rezultat sistema, kdo sprejme odločitev, kdo jo dokumentira in kdo zanjo ostaja odgovoren. Literatura o zaupanju v avtomatizirane sisteme opozarja, da sta pri uporabi takšnih sistemov pomembna ustrezno zaupanje in zavedanje tveganja pretiranega zanašanja na njihove rezultate [19], [20]. V kibernetski varnosti ima to neposredne kompetenčne posledice, saj napačna ali nekritično sprejeta ocena sistema UI lahko vpliva na zaznavanje groženj, odzivanje na incidente, upravljanje tveganj in zagotavljanje skladnosti.

Predlagana zasnova zato dopolnjuje obstoječe kompetenčne okvire, kot sta ECSF in NICE Framework. Ti okviri so pomembna referenčna podlaga za opis profilov, nalog, znanj, spretnosti in odgovornosti v kibernetski varnosti [1], [14], [15]. Članek pa dodaja razlago, kako se lahko te naloge in odgovornosti spreminjajo, kadar so v varnostne procese vključeni sistemi UI. S tem ne nadomešča obstoječih kompetenčnih okvirov, temveč jih dopolnjuje z dinamično povezavo med tehnološko spremembo, spremembo naloge, spremembo odgovornosti in novo oziroma razširjeno kompetenčno zahtevo.

Na tej podlagi članek oblikuje povezovalno razlago vpliva UI na kompetence v kibernetski varnosti. Kompetenčne zahteve niso obravnavane kot neposredna posledica splošne uporabe UI, temveč kot rezultat konkretnih sprememb nalog, odgovornosti, nadzora in odločanja. Taka razlaga omogoča bolj sistematično razumevanje vpliva UI na delo v kibernetski varnosti in predstavlja izhodišče za nadaljnje sistematično mapiranje literature ter empirično preverjanje predlaganega referenčnega okvira.

5.3 Implikacije za organizacije in razvoj kompetenc

Rezultati analize imajo praktične implikacije za organizacije, ki uvajajo ali uporabljajo sisteme UI v procesih kibernetske varnosti. Organizacije naj kompetenčnih vrzeli ne presojajo zgolj na podlagi formalnih nazivov delovnih mest ali splošnih tehnoloških trendov, temveč na ravni konkretnih nalog. Pri tem morajo ugotoviti, v kateri vlogi se UI pojavlja, katere naloge se spreminjajo, kdo ostaja odgovoren za presojo in odločitev ter katere kompetence je zato treba razvijati.

Primer takšne uporabe je uvedba sistema UI za prednostno razvrščanje varnostnih opozoril v varnostno-operativnem centru. Sistem UI lahko podpre začetno razvrščanje opozoril, pripravi povzetek dogodka ali predlaga nadaljnjo obravnavo. Naloga analitika se s tem ne odpravi, temveč se prestrukturira: analitik mora preveriti pravilnost razvrstitve, presoditi kontekst, odločiti o nadaljnji obravnavi in po potrebi dokumentirati odločitev. Iz tega izhajajo kompetence za presojo rezultatov sistemov UI, razumevanje omejitev orodja, prepoznavanje napačnih ali nepopolnih rezultatov ter komunikacijo tveganj. Organizacijsko to pomeni, da morajo biti jasno določeni postopki preverjanja, predaje varnostnega dogodka v nadaljnjo obravnavo, dokumentiranja in odgovornosti.

Posebej pomembno je vprašanje odgovornosti. Če UI podpira posamezne korake naloge, to še ne pomeni, da prevzame odgovornost za odločitev. Odgovornost za presojo, ukrepanje, dokumentiranje in komunikacijo ostaja organizacijska in strokovna. Zato morajo biti pri uporabi UI v kibernetski varnosti jasno določeni postopki preverjanja rezultatov, odobritve ukrepov, predaje varnostnega dogodka v nadaljnjo obravnavo in dokumentiranja odločitev.

Organizacije morajo sisteme UI obravnavati tudi kot poseben predmet varovanja. Poleg običajnih informacijsko-varnostnih kontrol je treba upoštevati tveganja, povezana s podatkovnimi tokovi, modeli, vhodnimi in izhodnimi podatki, vmesniki in integracijami. Kompetence za varovanje sistemov UI zato niso vezane le na en profil, temveč se razporedijo med več organizacijskih vlog, vključno s strokovnjaki za kibernetsko varnost, podatkovnimi

strokovnjaki, razvijalci, upravljavci tveganj, pravnimi službami in osebami, odgovornimi za skladnost.

Povezava med kibernetsko varnostjo, upravljanjem tveganj in skladnostjo postaja vse pomembnejša. Analiza oglasov za delo kaže, da se povpraševanje po veščinah, povezanih z UI, že povezuje z nalogami, kot so analiza podatkov o grožnjah, zaznavanje anomalij in avtomatizirana podpora odzivanju na varnostne incidente [27]. Hkrati evropski regulativni okvir krepi zahteve glede varnosti, preglednosti, odgovornosti, človeškega nadzora, spremljanja in dokumentiranja uporabe UI. Bolgouras idr. [28] poudarjajo preplet zahtev Akta o umetni inteligenci, GDPR, NIS2 in drugih evropskih okvirov, Burns idr. [29] pa izpostavljajo potrebo po strukturiranem pristopu k upravljanju UI, ki vključuje razvrščanje tveganj, preglednost, odgovornost, spremljanje in kontrolne točke skladnosti. To pomeni, da razvoj kompetenc v kibernetski varnosti vse bolj vključuje tudi zmožnost povezovanja tehničnih, organizacijskih in regulativnih zahtev.

5.4 Implikacije za izobraževanje in usposabljanje

Ugotovitve imajo pomembne implikacije za izobraževanje in usposabljanje strokovnjakov za kibernetsko varnost. Če se kompetenčne zahteve spreminjajo glede na nalogo, vlogo UI in raven odgovornosti, potem vsebin o UI ni smiselno dodajati zgolj kot splošnega modula. Učne vsebine morajo biti povezane s konkretnimi nalogami, kot so zaznavanje anomalij, analiza podatkov o grožnjah, odzivanje na varnostne incidente, varovanje sistemov UI, upravljanje tveganj pri uporabi sistemov UI in zagotavljanje skladnosti. To pomeni, da je treba kompetenčna področja prevesti v učne izide, učne aktivnosti in načine preverjanja znanja.

Vsebine o UI je zato smiselno vključevati v obstoječe programe, predmete in učne enote s področja kibernetske varnosti tam, kjer UI spreminja način izvedbe nalog, odgovornosti in potrebne kompetence. Takšna usmeritev je skladna s predlogi za razvoj programov CyberAI, ki razlikujejo med področjem SecureAI, usmerjenim v varovanje življenjskega cikla sistemov UI, in področjem AICyber, usmerjenim v uporabo orodij in tehnik UI v kibernetski varnosti [30]. Podobno Brito idr. [31] kažejo, da je mogoče vsebine o UI vključevati v obstoječe predmete s področja kibernetske varnosti, vendar mora biti takšno vključevanje povezano s praktičnimi nalogami in preverjanjem znanja.

Posebno pozornost zahteva usposabljanje že zaposlenih strokovnjakov. Ker se naloge v kibernetski varnosti hitro spreminjajo, formalno izobraževanje samo ne more zagotoviti vseh potrebnih kompetenc. Programi stalnega strokovnega razvoja naj izhajajo iz konkretnih profilov, nalog in kompetenčnih vrzeli. Kallonas idr. [32] opozarjajo, da je usposabljanje učinkovitejše, kadar je prilagojeno vlogi, predznanju, ciljem in učnim potrebam posameznika.

Izobraževanje mora razvijati tudi kompetence za kritično uporabo orodij UI. Udeleženci morajo razumeti, da sistemi UI ne zagotavljajo samodejno pravilnih, popolnih ali kontekstualno ustreznih rezultatov. Zato morajo programi vključevati preverjanje rezultatov sistemov UI, razumevanje omejitev modelov, prepoznavanje napačnih ali nerelevantnih rezultatov, presojo zanesljivosti in dokumentiranje odločitev. Poleg tehničnih kompetenc so pomembni tudi etični, komunikacijski in organizacijski vidiki, vključno z odgovornostjo, razložljivostjo, varovanjem podatkov, človeškim nadzorom in komunikacijo tveganj [33], [34].

Izobraževanje in usposabljanje bi zato morala slediti isti logiki kot predlagana zasnova referenčnega okvira. Izhodišče naj ne bo splošno vprašanje, katera znanja o UI so koristna, temveč katera naloga se spreminja, kakšna je vloga UI pri tej nalogi, katera odgovornost ostaja pri človeku in katera kompetenca je potrebna za varno, kritično in odgovorno izvedbo naloge. Pri praktičnem usposabljanju so lahko koristni tudi scenariji in simulacije groženj, podprti z

generativno UI, saj omogočajo preverjanje odzivanja, analize incidentov in obrambnih postopkov v nadzorovanem učnem okolju [35].

5.5 Omejitve in možnosti nadaljnjih raziskav

Prispevek ima več omejitev, ki jih je treba upoštevati pri razlagi ugotovitev. Prva omejitev izhaja iz izbora virov. Analiza ni bila zasnovana kot sistematični pregled literature, temveč kot namenski izbor znanstvenih virov, kompetenčnih okvirov ter regulativnih in usmerjevalnih dokumentov, potrebnih za oblikovanje preliminarne zasnove referenčnega okvira. Zato ugotovitev ni mogoče razumeti kot celovit pregled vseh raziskav o uporabi UI v kibernetski varnosti ali kot oceno pogostosti posameznih kompetenčnih zahtev v literaturi.

Druga omejitev se nanaša na način izpeljave kompetenčnih področij. Del kompetenčnih zahtev je neposredno podprt z obravnavanimi viri, del pa je utemeljeno izpeljan iz opisanih sprememb nalog, tveganj in odgovornosti. Takšen pristop je primeren za začetno konceptualno ureditev področja, vendar ne omogoča sklepanja o tem, katere kompetence so v praksi najpomembnejše, najpogosteje zahtevane ali najtežje dosegljive.

Tretja omejitev se nanaša na stopnjo preverjenosti predlagane zasnove referenčnega okvira. Prispevek namenoma predstavlja preliminarno zasnovo okvira, ki še ni bila empirično preverjena v organizacijskem okolju. Prav tako še ni operacionalizirana v obliki podrobnega nabora nalog, kompetenc, ravni zahtevnosti, kazalnikov usposobljenosti ali ocenjevalnega instrumenta. Zato je ni mogoče razumeti kot dokončno orodje za merjenje kompetenčnih vrzeli, temveč kot analitično izhodišče za nadaljnji razvoj in preverjanje.

Četrta omejitev je povezana s hitro spreminjajočim se tehnološkim in regulativnim okoljem. Zmogljivosti sistemov UI, načini njihove uporabe v varnostnih procesih in pri napadih ter zahteve glede njihovega upravljanja se hitro spreminjajo. Zato je treba predlagano zasnovo razumeti kot analitično izhodišče, ki ga bo treba z razvojem področja dopolnjevati, preverjati in prilagajati.

Nadaljnje raziskave bi morale najprej vključiti sistematično mapiranje literature o vplivu UI na naloge, vloge in kompetence v kibernetski varnosti. Tak pregled bi omogočil preverjanje in dopolnitev kategorij, oblikovanih v tem prispevku. Naslednji korak bi bilo empirično preverjanje okvira, na primer z intervjuji s strokovnjaki, anketami med organizacijami, metodo Delphi ali študijami primerov. Takšne raziskave bi omogočile presojo, katere naloge se v praksi dejansko spreminjajo, katere kompetenčne vrzeli organizacije zaznavajo, kako se odgovornosti razporejajo med različne profile in katere kompetence so najpomembnejše za varno in odgovorno uporabo sistemov UI v kibernetski varnosti.

Pomembna smer nadaljnjih raziskav je tudi primerjava med kompetenčnimi okviri, študijskimi programi, programi usposabljanja in zahtevami trga dela. Analiza oglasov za zaposlitev, učnih načrtov in programov usposabljanja bi lahko pokazala, v kolikšni meri se kompetenčne zahteve, povezane z UI, že pojavljajo v praksi in kje nastajajo vrzeli. Takšna analiza bi bila koristna za oblikovanje študijskih programov, krajših usposabljanj in programov stalnega strokovnega razvoja za različne profile v kibernetski varnosti.

6 SKLEP

Prispevek je obravnaval vpliv umetne inteligence (UI) na preoblikovanje nalog, odgovornosti in kompetenčnih zahtev v kibernetski varnosti. Izhodišče analize je bilo, da teh sprememb ni mogoče ustrezno presojati zgolj na ravni poklicev ali profilov kot celote, temveč predvsem na ravni konkretnih nalog, odgovornosti in razmerja med strokovnjakom in sistemom UI. Tak pristop omogoča razlikovanje med nalogami, pri katerih UI podpira oziroma avtomatizira

posamezne korake naloge, nalogami, pri katerih se spremeni način izvedbe, ter nalogami, ki se razširijo ali nastanejo zaradi uporabe, varovanja in upravljanja sistemov UI.

Na podlagi strukturirane sinteze izbranih znanstvenih virov, kompetenčnih okvirov ter regulativnih in usmerjevalnih dokumentov so bile oblikovane štiri analitične vloge UI v kibernetski varnosti: UI kot orodje za podporo varnostnim procesom, UI kot dejavnik spreminjanja groženj, UI kot predmet varovanja ter UI kot predmet upravljanja in skladnosti. Vsaka od teh vlog vpliva na drugačen sklop nalog, odgovornosti in kompetenčnih zahtev. Pri uporabi UI za podporo varnostnim procesom je v ospredju preverjanje in interpretacija rezultatov sistemov UI. Pri z UI spremenjenih grožnjah postane pomembno razumevanje novih vzorcev napadov ter prilagajanje postopkov zaznavanja, ozaveščanja in odzivanja. Kadar je UI predmet varovanja, se naloge širijo na zaščito podatkov, modelov, vhodnih in izhodnih podatkov, vmesnikov in integracij. Kadar je UI predmet upravljanja in skladnosti, pa v ospredje stopijo upravljanje tveganj, človeški nadzor, dokumentiranje, sledljivost in odgovorna uporaba.

Ključna ugotovitev prispevka je, da se kompetenčne zahteve ne oblikujejo kot splošna potreba po znanju o UI, temveč glede na konkretno nalogo, vlogo UI pri njeni izvedbi in odgovornost, ki ostaja pri strokovnjaku oziroma organizaciji. UI lahko zmanjša obseg ročne obdelave podatkov ali priprave začetnih analiz, vendar hkrati okrepi potrebo po presoji, razlagi, nadzoru, dokumentiranju in utemeljevanju odločitev. Kompetenčne zahteve se zato pogosto preusmerjajo od neposredne izvedbe posameznih korakov k preverjanju rezultatov sistemov UI, razumevanju omejitev teh sistemov, presoji tveganj in zagotavljanju odgovorne uporabe.

Predlagana preliminarna zasnova referenčnega okvira povezuje vloge UI, učinke na naloge, spremembe odgovornosti in kompetenčna področja z izbranimi profili oziroma funkcijami v kibernetski varnosti. Njena vrednost je predvsem v tem, da organizacijam ponuja analitično podlago za presojo, katere naloge in odgovornosti se z uvedbo ali uporabo UI spreminjajo, kateri profili oziroma organizacijske vloge so pri tem vključeni in katere kompetence je treba razvijati. Okvir je zato uporaben pri načrtovanju usposabljanj, posodabljanju opisov nalog, razporejanju odgovornosti, presoji kompetenčnih vrzeli ter vključevanju tveganj pri uporabi sistemov UI v obstoječe procese upravljanja informacijske in kibernetske varnosti.

Zaključimo lahko, da UI ne odpravlja potrebe po strokovnjakih za kibernetsko varnost, temveč spreminja pogoje njihovega dela. Ključno vprašanje zato ni, ali bo UI nadomestila posamezne profile v kibernetski varnosti, temveč kako se spreminjajo naloge, odgovornosti in kompetence, ki tem profilom omogočajo varno, kritično in odgovorno delovanje v okolju vse širše uporabe UI.

Literatura

[1] European Union Agency for Cybersecurity, European Cybersecurity Skills Framework (ECSF): Role Profiles, ENISA, 2022. [Online]. Dostopno na: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

[2] R. Kaur, D. Gabrijelčič in T. Klobučar, “Artificial intelligence for cybersecurity: Literature review and future research directions,” Information Fusion, vol. 97, čl. 101804, 2023, doi: 10.1016/j.inffus.2023.101804.

[3] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024, doi: 10.6028/NIST.CSWP.29.

[4] M. Macas, C. Wu in W. Fuertes, “Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems,” Expert Systems with Applications, vol. 238, čl. 122223, 2024, doi: 10.1016/j.eswa.2023.122223.

[5] European Parliament and Council of the European Union, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union, L 2024/1689, 2024. [Online]. Dostopno na: http://data.europa.eu/eli/reg/2024/1689/oj

[6] M. Uddin idr., "Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations," Artificial Intelligence Review, vol. 58, čl. 236, 2025, doi: 10.1007/s10462-025-11219-5.

[7] M. Gupta, C. Akiri, K. Aryal, E. Parker in L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," IEEE Access, vol. 11, str. 80218–80245, 2023, doi: 10.1109/ACCESS.2023.3300381.

[8] M. A. Ferrag idr., "Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities," Internet of Things and Cyber-Physical Systems, vol. 5, str. 1–46, 2025, doi: 10.1016/j.iotcps.2025.01.001.

[9] N. Capuano, G. Fenza, V. Loia in C. Stanzione, "Explainable artificial intelligence in cybersecurity: A survey," IEEE Access, vol. 10, str. 93575–93600, 2022, doi: 10.1109/ACCESS.2022.3204171.

[10] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, 2023, doi: 10.6028/NIST.AI.100-1.

[11] D. Acemoglu in P. Restrepo, "Automation and new tasks: How technology displaces and reinstates labor," Journal of Economic Perspectives, vol. 33, št. 2, str. 3–30, 2019, doi: 10.1257/jep.33.2.3.

[12] M. Arntz, T. Gregory in U. Zierahn, "The risk of automation for jobs in OECD countries: A comparative analysis," OECD Social, Employment and Migration Working Papers, št. 189, OECD Publishing, 2016, doi: 10.1787/5jlz9h56dvq7-en.

[13] S. Raisch in S. Krakowski, "Artificial intelligence and management: The automation–augmentation paradox," Academy of Management Review, vol. 46, št. 1, str. 192–210, 2021, doi: 10.5465/amr.2018.0072.

[14] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel in G. Witte, Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181 Rev. 1, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-181r1.

[15] European Union Agency for Cybersecurity, European Cybersecurity Skills Framework (ECSF): User Manual, ENISA, 2022. [Online]. Dostopno na: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf-user-manual

[16] D. Bendler in M. Felderer, "Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model," ACM Transactions on Computing Education, vol. 23, št. 2, čl. 25, 2023, doi: 10.1145/3573205.

[17] N. Chowdhury in V. Gkioulos, "Key competencies for critical infrastructure cyber-security: A systematic literature review," Information & Computer Security, vol. 29, št. 5, str. 697–723, 2021, doi: 10.1108/ICS-07-2020-0121.

[18] J. Dawson in R. Thomson, "The future cybersecurity workforce: Going beyond technical skills for successful cyber performance," Frontiers in Psychology, vol. 9, čl. 744, 2018, doi: 10.3389/fpsyg.2018.00744.

[19] J. D. Lee in K. A. See, “Trust in automation: Designing for appropriate reliance,” Human Factors, vol. 46, št. 1, str. 50–80, 2004, doi: 10.1518/hfes.46.1.50_30392.

[20] R. Parasuraman in D. H. Manzey, “Complacency and bias in human use of automation: An attentional integration,” Human Factors, vol. 52, št. 3, str. 381–410, 2010, doi: 10.1177/0018720810376055.

[21] S. K. Parker in G. Grote, “Automation, algorithms, and beyond: Why work design matters more than ever in a digital world,” Applied Psychology, vol. 71, št. 4, str. 1171–1204, 2022, doi: 10.1111/apps.12241.

[22] Zakon o informacijski varnosti (ZInfV-1), Uradni list Republike Slovenije, št. 40/25, 2025. [Online]. Dostopno na: https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2025-01-1571

[23] European Union Agency for Cybersecurity, ENISA Threat Landscape 2024, ENISA, 2024. [Online]. Dostopno na: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[24] MITRE Corporation, “MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems,” 2024. [Online]. Dostopno na: https://atlas.mitre.org/

[25] S. Sai, U. Yashvardhan, V. Chamola in B. Sikdar, “Generative AI for cyber security: Analyzing the potential of ChatGPT, DALL-E, and other models for enhancing the security space,” IEEE Access, vol. 12, str. 53497–53516, 2024, doi: 10.1109/ACCESS.2024.3385107.

[26] Y. Yigit, W. J. Buchanan, M. G. Tehrani in L. A. Maglaras, “Review of generative AI methods in cybersecurity,” arXiv preprint arXiv:2403.08701, 2024, doi: 10.48550/arXiv.2403.08701.

[27] C. M. Graham, “AI skills in cybersecurity: Global job trends analysis,” Information & Computer Security, vol. 33, št. 5, str. 673–689, 2025, doi: 10.1108/ICS-09-2024-0235.

[28] V. Bolgouras, A. Zarras, C. Leka, I. Stylianou, A. Farao in C. Xenakis, “EU regulatory ecosystem for ethical AI,” AI and Ethics, vol. 5, str. 5063–5080, 2025, doi: 10.1007/s43681-025-00749-x.

[29] F. Burns, J. Edelberg, P. Kuivanen, E. Tuomi, J. Ylimaa in I. Tikanmäki, “AI governance: Achieving EU AI Act compliance in the Dynamo project,” v Proceedings of the 24th European Conference on Cyber Warfare and Security, 2025, str. 875–878, doi: 10.34190/eccws.24.1.3378.

[30] S. Kaza idr., “CyberAI: Knowledge area frameworks for cybersecurity programs in the age of artificial intelligence,” v Proceedings of the 26th ACM Annual Conference on Cybersecurity and Information Technology Education, 2025, doi: 10.1145/3769694.3771142.

[31] F. Brito, Y. Mekdad, M. Ross, M. A. Finlayson in S. Uluagac, “Enhancing cybersecurity education with artificial intelligence content,” v Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1, 2025, str. 158–164, doi: 10.1145/3641554.3701958.

[32] C. Kallonas, A. Piki in E. Stavrou, “Empowering professionals: A generative AI approach to personalized cybersecurity learning,” v Proceedings of the 2024 IEEE Global Engineering Education Conference (EDUCON), 2024, str. 1–10, doi: 10.1109/EDUCON60312.2024.10578894.

[33] R. Straight, “Beyond human-centric models in cybersecurity education: A pilot posthuman analysis of the NICE Workforce Framework for Cybersecurity,” Journal of Cybersecurity Education, Research and Practice, vol. 2024, št. 1, čl. 30, 2024, doi: 10.62915/2472-2707.1210.

[34] A. W. Z. Abidin, N. H. M. Ariffin, Z. A. Nasruddin, N. F. Habidin in M. Yusoff, “Evaluating and modelling artificial intelligence and emotional intelligence to improve cybersecurity employee ethical

competence model," Journal of Advanced Research Design, vol. 130, št. 1, str. 13–25, 2025, doi: 10.37934/ard.130.1.1325.

[35] R. Vadisetty in A. Polamarasetti, "Generative AI for cyber threat simulation and defense," v Proceedings of the 2024 12th International Conference on Control, Mechatronics and Automation (ICCMA), 2024, str. 272–278, doi: 10.1109/ICCMA63715.2024.10843938.

[36] Antunes, P., Johnstone, D., & Hoang Thuan, N. (2025). Construction of Conceptual Frameworks in Research: An Information Systems Design Perspective. Communications of the Association for Information Systems, 57, 53–84. https://doi.org/10.17705/1CAIS.05703.

[37] Jaakkola, E. (2020). Designing conceptual articles: four approaches. AMS Review, 10, 18–26. https://doi.org/10.1007/s13162-020-00161-0.

[38] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039.

[39] Cronin, M. A., & George, E. (2020). The Why and How of the Integrative Review. Organizational Research Methods, 26(1), 168–192. https://doi.org/10.1177/1094428120935507.

Andreja Markun je magistrica organizatorka informatičarka, zaposlena na področju informacijske varnosti. V svojih raziskavah se ukvarja s sistemskimi pristopi k razvoju kibernetskih kompetenc, vplivom regulative na kadrovske ukrepe ter dolgoročno odpornostjo organizacij v digitalnem okolju.

Klemen Methans je zaposlen kot sistemski inženir za Microsoftove sisteme v okviru operacij varnostno-operativnega centra v podjetju Nil, d.o.o. Je zunanji sodelavec Univerze v Mariboru, Fakultete za organizacijske vede, kjer kot asistent izvaja vaje pri predmetih s področja informacijske in kibernetske varnosti.

Alenka Brezavšček je izredna profesorica na Fakulteti za organizacijske vede Univerze v Mariboru, predstojnica Katedre za metodologijo. Doktorirala je na področju integralnega upravljanja kakovosti. Njeno raziskovalno delo vključuje operacijske raziskave, stohastične procese, zanesljivost in razpoložljivost sistemov, optimizacijo vzdrževanja ter informacijsko in kibernetsko varnost.