Zámer národného projektu[1]

Názov národného projektu (ďalej aj „NP“): Národné laboratórium umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab)

Žiadateľ[2]:

Obchodné meno/názov	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Právna forma	Rozpočtová organizácia
Sídlo	Pribinova 25, 811 09 Bratislava
IČO	50349287

Poskytovateľ: Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Partner, ktorý sa bude zúčastňovať na implementácii aktivít NP (ak je to relevantné)

Obchodné meno/názov	N/A
Právna forma	N/A
Sídlo	N/A
IČO	N/A
Zdôvodnenie potreby partnera NP[3]	N/A
Kritériá pre výber partnera[4]	N/A
Má partner jedinečné postavenie na implementáciu týchto aktivít? Ak áno, na akom základe?	N/A

V prípade viacerých partnerov, doplňte údaje za každého partnera.

Sumárne informácie o NP

Celkové oprávnené výdavky NP (v EUR)	**5 011 236,35 EUR**
Miesto realizácie projektu (na úrovni kraja, resp. celé územie Slovenskej republiky)	Celé územie Slovenskej republiky
Identifikácia hlavných cieľových skupín (ak relevantné)	
Projekt so špecifickým určením pre marginalizované rómske komunity[5]	nie

[1] Formulár zámeru NP predstavuje minimálny obsahový štandard, ktorý je poskytovateľ oprávnený dopĺňať a rozširovať na základe svojich potrieb.

[2] Uviesť aj názov sekcie, ak je to relevantné. Žiadateľom je osoba, ktorá žiada o poskytnutie príspevku do nadobudnutia účinnosti zmluvy o poskytnutí nenávratného finančného príspevku alebo právoplatnosti rozhodnutia podľa § 13 ods. 2 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, alebo osoba, ktorá predkladá zámer NP.

[3] Pod partnerom sa rozumie partner ako je definovaný v § 3, písm. t) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[4] Uveďte, na základe akých kritérií bol partner vybraný, alebo ak boli kritériá zverejnené, uveďte odkaz na internetovú stránku, kde sú dostupné. Ako kritérium pre výber partnera môže byť tiež uvedená predchádzajúca spolupráca žiadateľa s partnerom, ktorá bude náležite opísaná a odôvodnená, avšak nejde o spoluprácu, ktorá by v prípade verejných prostriedkov spadala pod pôsobnosť zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[5] Zo zoznamu sa vyberie:

- "**áno**" – ak, projekt bude financovaný výhradne z alokácie so špecifickým určením pre marginalizované rómske komunity (ďalej len „MRK“) uvedenej v Programe Slovensko,
- "**nie**" - ak, projekt nebude v žiadnej miere financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko,
- "**čiastočne**" – ak, projekt bude z časti financovaný z alokácie so špecifickým určením pre MRK uvedenej v Programe Slovensko.

Spolufinancovaný Európskou úniou

Začlenenie národného projektu v štruktúre Programu Slovensko[6]

Cieľ politiky súdržnosti[7]	1 Konkurencieschopnejšia a inteligentnejšia Európa vďaka presadzovaniu inovatívnej a inteligentnej transformácie hospodárstva a regionálnej prepojenosti IKT
Priorita	1P3. Platforma strategických technológií pre Európu (STEP)
Špecifický cieľ	RSO1.6 Podpora investícií, ktoré prispievajú k cieľom Platformy strategických technológií pre Európu (platforma STEP) uvedeným v článku 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2024/795 (EFRR)
Opatrenie (ak relevantné)	N/A
Súvisiace typy akcií[8]	Podpora súvisiacich služieb, ktoré sú kritické a špecifické pre vývoj a výrobu kritických digitálnych technológií cez: a) zriadenie technologických centier (fablab) poskytujúcich služby pre výrobu fyzických elektronických zariadení v malých sériách; b) výskum a vývoj kvantovej kryptografie a algoritmov kvantovej distribúcie kľúčov (QKD); c) výskumné a vývojové laboratóriá umelej inteligesncie pre agentov umelej inteligencie.

Zákonné požiadavky

§ 23 ods. 3 zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

1. Dôvod určenia prijímateľa NP[9]

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej ako „MIRRI SR“) je ústredným orgánom štátnej správy pre centrálne riadenie informatizácie spoločnosti a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní verejných prostriedkov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti (ust. § 10 ods. 1 písm. d) zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov).

MIRRI SR zabezpečuje úlohy národného prevádzkovateľa centrálnej informačnej infraštruktúry a centrálnej komunikačnej infraštruktúry Slovenskej republiky pre verejnú správu (ust. § 4 písm. a) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov) a zároveň je orgánom vedenia ITVS.

Na základe zákona o ITVS bola vydaná vyhláška č. 179/2020 Z. z. Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy. V zmysle uvedenej vyhlášky je potrebné, v rámci minimálnych bezpečnostných opatrení pre oblasť kybernetickej bezpečnosti vo

[6] V prípade zámeru NP, ktorý sa plánuje financovať z viacerých cieľov politiky súdržnosti / priorít / špecifických cieľov / opatrení sa vyberú zo zoznamu viaceré položky.
Zákon č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, Rámec implementácie fondov a metodický dokument č. 2 riadiaceho orgánu pre Program Slovensko neobmedzujú, resp. nevylučujú možnosť spojiť dva schválené zámery národných projektov do jednej výzvy, resp. na jeden schválený zámer národného projektu vyhlásiť dve výzvy na predloženie národných projektov. V takýchto prípadoch bude riadiaci orgán posudzovať výzvu tak, aby boli splnené všetky parametre schváleného/schválených zámeru/zámerov národného projektu berúc na zreteľ povolené odchýlky.

[7] V prípade Fondu na spravodlivú transformáciu sa vyberie "-".

[8] V súlade s informačným monitorovacím systémom.

[9] V prípade, ak ide o prijímateľa, ktorý nie je určený v Programe Slovensko, alebo ktorého kompetencie nevyplývajú z osobitných predpisov podľa zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, príslušná komisia pri Monitorovacom výbore pre Program Slovensko schválením zámeru NP schvaľuje aj prijímateľa NP. V opačnom prípade sa prijímateľ NP neposudzuje.

verejnej správe, okrem iného, „ustanoviť plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky.“

MIRRI SR je zároveň ústredným orgánom štátnej správy pre oblasť kybernetickej bezpečnosti v sektore verejná správa, podsektor informačné systémy verejnej správy podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti").

MIRRI SR ako ústredný orgán pre podsektor informačné systémy verejnej správy buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore (§ 9, ods. d) zákona o kybernetickej bezpečnosti).

MIRRI SR prevádzkuje, zákonom zriadenú, vládnu jednotku CSIRT (CSIRT.SK), ktorá poskytuje služby pre informačné systémy verejnej správy podľa zákona o kybernetickej bezpečnosti.

MIRRI SR je regulátorom a celoslovensky pôsobiacim orgánom pre oblasť bezpečnosti a riešenia kybernetických incidentov vo vzťahu k informačným systémom verejnej správy.

MIRRI SR poskytuje metodickú podporu povinným subjektom a zabezpečuje zvyšovanie spôsobilostí, vzdelávanie, skvalitnenie a rozvoj kybernetickej a informačnej bezpečnosti v sektore verejnej správy

2. Odôvodnenie využitia NP

V súčasnom dynamickom prostredí digitálnej transformácie a rýchleho vývoja umelej inteligencie (AI) je nevyhnutné, aby verejná správa reagovala na nové výzvy v oblasti kybernetickej bezpečnosti a efektívneho využívania dát. Slovenská republika, podobne ako iné krajiny, čelí rastúcim hrozbám spojeným s kybernetickými útokmi, manipuláciou s dátami a potrebou bezpečného nasadzovania AI modelov v kritických oblastiach štátnej správy. V súčasnosti však neexistuje centralizované riešenie, ktoré by umožňovalo systematický výskum a vývoj AI technológií špecificky zameraných na bezpečnostné aspekty ich nasadenia. Tento deficit spôsobuje, že inštitúcie verejnej správy nemajú jednotnú metodológiu a infraštruktúru na testovanie, validáciu a hodnotenie AI riešení v kontexte ich bezpečnosti a etických rizík.

Hlavnou motiváciou projektu je preto vytvorenie špecializovaného laboratória AI pre kybernetickú bezpečnosť, ktoré poskytne priestor pre experimentovanie, validáciu a rozvoj AI modelov s dôrazom na ich bezpečnostné a výkonnostné parametre. Cieľom je vybudovať platformu, ktorá bude slúžiť ako centrum pre výskum a vývoj v oblasti kybernetickej bezpečnosti, zabezpečovania kritických informačných systémov a aplikácie umelej inteligencie v bezpečnostných operáciách. Laboratórium poskytne inovatívne nástroje na testovanie odolnosti AI systémov voči adversariálnym útokom, vyhodnocovanie hrozieb spojených s generatívnymi modelmi a tvorbu metodológií na bezpečné nasadzovanie AI technológií do verejných infraštruktúr.

Rozsah projektu zahŕňa vývoj experimentálneho prostredia pre testovanie AI riešení, ktoré umožní detailnú analýzu bezpečnostných výziev a rizík spojených s ich používaním. Platforma bude poskytovať možnosti simulácie realistických kybernetických incidentov, hodnotenie odolnosti IT infraštruktúr voči AI-driven útokom a vývoj metodológií pre regulované nasadzovanie AI v kritických oblastiach štátnej správy.

3. Zdôvodnenie vylúčenia „súťažného postupu“ výberu projektu prostredníctvom výzvy

Projekt je vhodnejšie realizovať formou NP ako využitie „súťažného postupu“ prostredníctvom výzvy, nakoľko navrhovaný spôsob realizácie projektu je efektívnejší, hospodárnejší a bezpečnejší, pretože umožňuje zabezpečiť jednotné bezpečnostné a technické štandardy, efektívne využívanie verejných

zdrojov, garantovať kvalitu a interoperabilitu výstupov, pružne reagovať na kybernetické hrozby a udržať kontrolu nad citlivou infraštruktúrou štátu. Vzhľadom na charakter projektu s cieľom vytvoriť experimentálne prostredie a jeho význam pre kritickú infraštruktúru a požiadavku na vysokú mieru centralizácie a bezpečnosti je zvolená forma národného projektu jednoznačné primeranejším a efektívnejším spôsobom realizácie.

4. Uplatnenie princípu partnerstva pri príprave zámeru národného projektu

Princíp partnerstva bol pri príprave NP zabezpečený realizáciou verejného pripomienkovania, prostredníctvom ktorého sa mohla zapojiť odborná verejnosť formou pripomienkovania projektového zámeru (vrátane príloh). Oznámenie o verejnom pripomienkovaní a samotná dokumentácia projektu boli transparentne zverejnené. Tento prístup zabezpečí nielen uplatnenie predmetného princípu partnerstva, ale prispeje k vysokej kvalite zámeru, zosúladeniu cieľov projektu s potrebami cieľových skupín a podporí vznik strategicky významného projektu, ktorý posilní kybernetickú bezpečnosť verejnej správy.

Verejné pripomienkovanie bolo vyhlásené oznámením na webovej stránke MIRRI SR s dátumom na predkladanie pripomienok do 5.3.2026. K predloženým pripomienkam boli zrealizované osobné stretnutia. Predložené pripomienky boli, resp. budú zapracované.

Popis národného projektu

5. Východiskový stav

Projekt prispieva k cieľom nariadenia Európskeho parlamentu a Rady (EÚ) 2024/795 vytvorením kapacít na výskum, vývoj a testovanie riešení umelej inteligencie, ktoré podporujú technologickú suverenitu EÚ, znižujú závislosť od mimoeurópskych poskytovateľov špičkových bezpečnostných nástrojov umelej inteligencie a umožňujú bezpečné využívanie umelej inteligencie v kritických oblastiach verejného sektora.

Riešenie tiež podporuje rozvoj európskych strategických technologických aktív poskytovaním experimentálneho prostredia kompatibilného s iniciatívami EÚ, ako sú centrá excelentnosti v oblasti umelej inteligencie, európske dátové priestory a iniciatívy v oblasti výskumu kybernetickej bezpečnosti. Projekt spĺňa požiadavky STEP na podporu investícií do pokrokových digitálnych technológií s vysokým strategickým vplyvom. Projekt je navrhnutý v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2024/795 o zriadení platformy Strategic Technologies for Europe Platform (STEP), pričom podporuje rozvoj kritických digitálnych technológií v oblasti umelej inteligencie a kybernetickej bezpečnosti.

Navrhovaný projekt Národné laboratórium umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab) vychádza z viacerých relevantných štatistík, analýz a odborných štúdií, ktoré identifikujú potrebu posilnenia kybernetickej bezpečnosti a výskumných kapacít v tejto oblasti. Medzi hlavné zdroje, na ktoré projekt nadväzuje, patria:

- Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023 (NBÚ SR)
- Národná stratégia kybernetickej bezpečnosti SR na roky 2021 – 2025
- Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025
- Štúdia Slovenskej technickej univerzity a MIRRI SR o zapojení SR do iniciatívy EÚ pre AI centrá excelentnosti
- Národná koncepcia informatizácie verejnej správy (NKIVS)
- Európsky akt o umelej inteligencii (AI Act)
- Európska smernica NIS2 o kybernetickej bezpečnosti (NIS2 Directive)

Identifikované nedostatky v súčasnom stave

- Súčasné systémy verejnej správy sú závislé na manuálnom vstupe, čo vedie k neefektívnosti a potenciálnej nesprávnosti údajov.
- Fragmentácia AI riešení naprieč verejnými inštitúciami
- Obmedzené analytické kapacity
- Chýba efektívne modelovanie potenciálnych kybernetických útokov na základe historických dát a simulácií, čo znemožňuje proaktívne opatrenia na ich elimináciu.
- Verejná správa nevyužíva potenciál strojového učenia a predikčných modelov na optimalizáciu procesov a rozhodovania.
- Absencia centrálneho AI riešenia spôsobuje nekoordinované implementácie AI modelov s nízkou mierou interoperability medzi rezortmi.
- Väčšina bezpečnostných systémov v štátnej správe stále funguje na statických pravidlách a signatúrnych metódach detekcie hrozieb, pričom nevyužíva pokročilé algoritmy strojového učenia na adaptívnu ochranu a anomálnu detekciu.
- Verejná správa nevyužíva systematické penetračné testy a červené tímy na hodnotenie odolnosti kritických systémov voči APT útokom, ransomvéru a iným pokročilým hrozbám.
- Súčasná IT infraštruktúra nie je kompatibilná s modernými nástrojmi na spracovanie údajov v reálnom čase, čo bráni efektívnemu využívaniu AI riešení.
- Zastarané technológie a chýbajúca integrácia s e-Government systémami

Realizátorom projektu bude Ministerstvo investícií, regionálneho rozvoja a informatizácie SR.

Vládna jednotka CSIRT, zameraná na kybernetickú bezpečnosť, bude využívať laboratórium na tvorbu riešení, ktoré im pomôžu analyzovať bezpečnostné hrozby, kontrolovať riziká a spracovávať bezpečnostné incidenty. Možnosti laboratória umožnia CSIRT-u vytvoriť modely na detekciu hrozieb alebo podporu pri reakciách na incidenty.

Laboratórium bude sprístupnené ďalším orgánom verejnej moci (OVM), ktoré umožní testovať a overovať vlastné aplikácie pred ich nasadením v prostredí verejnej správy.

Navrhovaný projekt bude organizačne a administratívne zabezpečený z vlastných kapacít z radov zamestnancov MIRRI SR.

5.1 Projekt AI CyberLab vytvára synergie s národným projektom Zvýšenie spôsobilostí vládnej jednotky CSIRT, ktorý rozširuje kapacity CSIRT-u v oblasti detekcie hrozieb a skenovania zraniteľností, pričom laboratórium poskytne nadstavbové AI prostredie na pokročilé simulácie a prediktívnu analýzu incidentov.Súlad projektu s nariadením o platforme STEP

Navrhovaný projekt je v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2024/795 o zriadení platformy Strategic Technologies for Europe Platform (STEP) a spĺňa podmienky podpory strategických technológií v EÚ.

Odvetvia platformy STEP

Projekt spadá primárne do odvetvia digitálnych a špičkových technológií, konkrétne do oblasti umelej inteligencie, pokročilej analytiky dát a technológií kybernetickej bezpečnosti. Laboratórium umelej inteligencie pre kybernetickú bezpečnosť bude poskytovať infraštruktúru na výskum, vývoj a testovanie pokročilých algoritmov strojového učenia, systémov detekcie anomálií, modelovania kybernetických útokov a analytických nástrojov pre spracovanie veľkých objemov dát v reálnom čase. Tieto technológie patria medzi strategické digitálne technológie podporované platformou STEP.

Spolufinancovaný Európskou úniou

Ciele platformy STEP

Projekt prispieva k napĺňaniu cieľov platformy STEP tým, že podporuje vývoj a testovanie kritických digitálnych technológií v oblasti umelej inteligencie a kybernetickej bezpečnosti a posilňuje európske technologické kapacity v oblasti ochrany digitálnej infraštruktúry. Súčasne prispieva k rozvoju odborných kapacít a zručností v oblasti AI a kybernetickej bezpečnosti vo verejnom sektore a podporuje spoluprácu medzi verejnou správou, výskumnými organizáciami a odbornými komunitami. Projekt tak prispieva k posilneniu európskych hodnotových reťazcov v oblasti digitálnej bezpečnosti a znižovaniu závislosti od mimoeurópskych technologických riešení.

Podmienky platformy STEP – kritické technológie

Technológie rozvíjané v rámci projektu predstavujú kritické technológie v zmysle nariadenia o platforme STEP, keďže prinášajú inovatívne a pokročilé prvky v oblasti umelej inteligencie aplikovanej na kybernetickú bezpečnosť a majú významný hospodársky a strategický potenciál. Zároveň prispievajú k znižovaniu strategickej závislosti Európskej únie v oblasti pokročilých bezpečnostných technológií, najmä v oblasti detekcie kybernetických hrozieb, analýzy incidentov a ochrany kritickej digitálnej infraštruktúry verejnej správy.

6. Hlavné ciele NP (stručne):

Ciele projektu:

- Laboratórium umelej inteligencie pre kybernetickú bezpečnosť poskytne platformu na výskum a vývoj nových bezpečnostných technológií, pričom budú slúžiť ako testovacie prostredie pre pokročilé AI riešenia na detekciu a prevenciu kybernetických hrozieb.
- Implementácia systémov na monitorovanie, analýzu a predikciu bezpečnostných hrozieb s cieľom zvýšiť schopnosť verejných inštitúcií reagovať na bezpečnostné incidenty v reálnom čase.
- Vzdelanosť pracovníkov ohľadom kybernetickej bezpečnosti.
- Využitie strojového učenia a pokročilých analytických nástrojov na identifikáciu zraniteľností v IT infraštruktúre a na modelovanie dopadu rôznych druhov kybernetických útokov.
- Organizovanie pravidelných testov, penetračných skúšok a simulovaných kybernetických incidentov na zlepšenie schopností vládnych inštitúcií reagovať na rôzne bezpečnostné scenáre.

Projekt AI CyberLab nadväzuje najmä na plánované aktivity výskumu a vývoja realizované v rámci projektov Ministerstva školstva, výskumu, vývoja a mládeže SR, Ministerstva vnútra SR (projekt APZ) a akademických inštitúcií STU a TUKE v oblasti AI. Výskumné organizácie vyvíjajú nové poznatky, modely a metodiky, pričom AI CyberLab zabezpečí ich overenie, testovanie a implementačnú podporu pri zavádzaní do informačných systémov verejnej správy z pohľadu kybernetickej bezpečnosti. Laboratórium zároveň umožní orgánom verejnej moci testovať bezpečnosť a robustnosť AI riešení pred ich nasadením, čím vytvára prirodzené pokračovanie výskumno vývojového cyklu smerom k reálnej prevádzke vo verejnej správe. Projekt posilňuje spoluprácu medzi verejnou správou, akademickým prostredím a výskumnými tímami relevantných rezortov a subjektov VS, pričom vytvára trvalý mechanizmus pre transláciu výsledkov výskumu do štandardných bezpečnostných procesov štátu.

Projekt priamo súvisí so strategickými technologickými prioritami Európskej únie, najmä v oblasti umelej inteligencie, kybernetickej bezpečnosti a dátovej infraštruktúry. Zriadením národného laboratória pre umelú inteligenciu v oblasti kybernetickej bezpečnosti posilní Slovenská republika svoju

schopnosť aktívne prispievať k európskemu ekosystému excelentnosti v oblasti umelej inteligencie, čím splní ciele Platformy strategických technológií pre Európu (STEP).

7. Merateľné ukazovatele NP a iné údaje

Zoznam merateľných ukazovateľov projektu

Typ merateľného ukazovateľa projektu	Kód merateľného ukazovateľa projektu[10]	Názov merateľného ukazovateľa projektu	Merná jednotka merateľného ukazovateľa projektu	Indikatívna cieľová hodnota[11]
výstup	PSKPSOI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií	1
výsledok	PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	používatelia / rok	10

Zoznam iných údajov projektu (ak relevantné)

Kód iného údaja[12]	Názov iného údaja	Merná jednotka iného údaja
DPSK033	Počet nástrojov zabezpečujúcich prístupnosť pre osoby so zdravotným postihnutím	počet
DPSK034	Priemerná hrubá mesačná mzda financovaná z projektu za rok	EUR/rok
DPSK035	Medián priemerných hrubých mesačných miezd financovaných z projektu	EUR/rok

8. Prínosy, ktoré sa dajú očakávať pre cieľové skupiny (ak je to relevantné)

Cieľová skupina	Počet[13]	Prínos

V prípade viacerých cieľových skupín doplňte prínos pre každú z nich.

[10] Uvádza sa kód merateľného ukazovateľa projektu, nie kód spoločného, resp. špecifického merateľného ukazovateľa programu. Ak merateľný ukazovateľ projektu ešte nemá pridelený kód, uvádza sa „n/a“.

[11] V zmysle zmluvy o poskytnutí nenávratného finančného príspevku sa pre typ merateľného ukazovateľa projektu – výstup štandardne cieľová hodnota nastavuje ku koncu realizácie národného projektu. Pre typ merateľného ukazovateľa projektu – výsledok sa štandardne cieľová hodnota nastavuje na obdobie udržateľnosti národného projektu.

[12] Ak iný údaj ešte nemá pridelený kód, uvádza sa „n/a“.

[13] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

Spolufinancovaný Európskou úniou

9. Aktivity národného projektu

a. V tabuľke nižšie uveďte rámcový popis aktivít, ktoré budú v rámci identifikovaného národného projektu realizované.

Názov aktivity	Čo sa má aktivitou dosiahnuť	Spôsob realizácie (žiadateľ a / alebo partner)	Predpokladaný počet mesiacov realizácie aktivity
Vybudovanie národného laboratória umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab)	Projekt je kľúčovým krokom k posilneniu kybernetickej bezpečnosti na národnej aj medzinárodnej úrovni. Svojou unikátnou koncepciou, kombináciou výskumu, testovania a praktickej aplikácie AI technológií ponúka významný potenciál na riešenie súčasných aj budúcich bezpečnostných výziev. Realizácia tohto projektu prispeje k zlepšeniu celkovej bezpečnostnej infraštruktúry, ochrane citlivých údajov a posilneniu digitálnej suverenity krajiny.	Žiadateľ (realizácia prostredníctvom dodávateľa, na základne zrealizovaného verejného obstarávania)	36

V prípade viacerých aktivít, doplňte informácie za každú z nich.

Bližší popis aktivít projektu:

Vytvorenie centrálnej drag-and-drop AI platformy:

• základné funkcie pre vytváranie a prepájanie AI modelov, modulov, konvertorov a konektorov.

Zabezpečenie a konfigurácia cloudovej infraštruktúry:

• zabezpečenie platformy a vytvorenie granulárneho prístupu,

• výber a prenájom vhodných cloudových služieb optimalizovaných pre AI workloady,

• konfigurácia cloudového prostredia pre maximálnu efektivitu a bezpečnosť,

• nastavenie škálovateľnosti a monitoringu využitia cloudových zdrojov.

Vývoj nástrojov:

• konektory pre interné a externé zdroje dát,

• konvertory pre preklápanie zdrojov dát do požadovaných formátov pre vytváranie znalostných databáz

b. V tabuľke nižšie uveďte, či v rámci národného projektu bude uplatnený inštitút užívateľa[14] podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[14] Užívateľ sa na rozdiel od partnera nepodieľa na realizácii projektu žiadateľa, ale môže využiť finančný príspevok na realizáciu aktivít definovaných poskytovateľom vo výzve (napr. nákup a inštalácia kotla). Podľa § 3 písm. u) zákona č. 121/2022 Z. z. o príspevkoch z fondov

Názov aktivity	Využitie inštitútu užívateľa (áno/nie)	Typ užívateľa[15]	Poskytovateľ príspevku užívateľovi (žiadateľ alebo partner)
Aktivita 1	nie		

V prípade viacerých aktivít, doplňte informácie za každú z nich.

c. Uveďte detailnejší popis aktivít.

Vytvorenie centrálnej drag-and-drop AI platformy:

- základné funkcie pre vytváranie a prepájanie AI modelov, modulov, konvertorov a konektorov.

Zabezpečenie a konfigurácia cloudovej infraštruktúry:

- zabezpečenie platformy a vytvorenie granulárneho prístupu,
- výber a prenájom vhodných cloudových služieb optimalizovaných pre AI workloady,
- konfigurácia cloudového prostredia pre maximálnu efektivitu a bezpečnosť,
- nastavenie škálovateľnosti a monitoringu využitia cloudových zdrojov.

Vývoj nástrojov:

- konektory pre interné a externé zdroje dát,
- konvertory pre preklápanie zdrojov dát do požadovaných formátov pre vytváranie znalostných databáz.

Personálne kapacity (FTE)

Projekt predpokladá využitie kombinácie interných a externých odborných kapacít počas realizácie, pričom celkový rozsah personálnych nárokov vychádza z pracovných výpočtov v Analýze nákladov a prínosov (M-05) a z definovaných rolí v projektovom zámere I-02.

Počet FTE počas realizácie projektu (36 mesiacov):

- Interné kapacity MIRRI SR: **cca 4,3 FTE**
  - projektový manažér – 0,25 FTE
  - IT architekt – 0,5 FTE
  - IT analytik – 0,5 FTE
  - manažér kybernetickej a informačnej bezpečnosti – 0,5 FTE
  - kľúčový používateľ / odborný garant – 1,5 FTE
  - tester / kvalita – 0,5 FTE
- Externé odborné kapacity: **cca 11,8 FTE**
  - vývoj a technická implementácia riešenia (AI dizajnér, vývojári, DevSecOps) – 7,5 FTE
  - odborné kapacity pre bezpečnosť, integráciu, testovanie – 4,3 FTE

Európskej únie a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, užívateľom je osoba, ktorej prijímateľ alebo partner poskytuje finančné prostriedky z príspevku na základe predchádzajúceho súhlasu poskytovateľa a v súlade so zmluvou uzavretou medzi prijímateľom a užívateľom alebo partnerom a užívateľom alebo iným obdobným právnym vzťahom medzi prijímateľom a užívateľom alebo partnerom a užívateľom.

[15] Uvádza sa typ subjektu/osôb (napr. neverejní poskytovatelia soc. služieb, dlhodobí uchádzači o zamestnanie), alebo právna forma.

Spolu: cca **16,1 FTE** počas trvania projektu.**Finančná udržateľnosť po ukončení projektu** Personálne náklady počas implementácie predstavujú 63 % rozpočtu projektu, keďže súvisia s vývojom AI platformy, MLOps, bezpečnostného testovania, integrácie a technického návrhu riešenia.

Po ukončení realizácie sa **personálne náklady zásadne znižujú**, pretože:

- interné kapacity MIRRI SR budú pokrývať iba **prevádzku a dohľad**, nie vývoj (cca 1,6 FTE),
- priamy vývoj a implementačné práce už nebudú financované zo štátneho rozpočtu,
- prevádzka bude zabezpečená prostredníctvom **SLA zmluvy**, na ktorú má MIRRI SR už dnes garantované financovanie v kapitole rozpočtu.

Hoci AI kompetenčné centrá STU a TUKE nie sú do tohto projektu zapojené ako partneri, napriek tomu sa vytvorí mechanizmus technickej koordinácie, najmä pokiaľ ide o bezpečnostné aspekty umelej inteligencie, a to vo forme odborných pracovných skupín, výmenných workshopov, zdieľania neprodukčných dátových súborov alebo konzultácií počas vypracovávania metodík.

NP bude realizovaný v súlade s horizontálnymi princípmi s povinnosťou dodržania súladu projektu s Chartou základných práv Európskej únie, rodovou rovnosťou, nediskrimináciou a prístupnosťou osôb so zdravotným postihnutím, ktoré sú definované v Partnerskej dohode SR na roky 2021 – 2027 a v čl. 9 nariadenie o spoločných ustanoveniach, berúc do úvahy Chartu základných práv Európskej únie a povinnosti vyplývajúce z Dohovoru OSN o právach osôb so zdravotným postihnutím a zabezpečenia prístupnosti v súlade s jeho článkom 9, ako horizontálne základné podmienky. Pri implementácii plánovaných aktivít projektu sa budú dodržiavať všetky články Charty ZP EÚ s dôrazom najmä na články Charty ZP EÚ, ktoré sa najviac vzťahujú k plánovaným intervenciám, aktivitám a cieľovým skupinám.

V súvislosti so všetkými plánovanými aktivitami bude zohľadnený v rámci NP:

- princíp rovnosti mužov a žien a princíp nediskriminácie tak, aby nedochádzalo k znevýhodneným podmienkam pre akúkoľvek skupinu osôb a aby boli vytvorené podmienky prístupnosti aj pre osoby so zdravotným postihnutím k fyzickému prostrediu, k informáciám a komunikácii vrátane informačných a komunikačných technológií a systémov, ako aj k ďalším prostriedkom a službám dostupným alebo poskytovaným verejnosti.

10. Predpokladaný časový rámec

Predpokladaný dátum vyhlásenia výzvy vo formáte mesiac/rok	9/2026
Predpokladaná doba realizácie NP v mesiacoch	36

Termíny v tabuľke nie sú záväzné.

11. Finančný rámec[16]

a) žiadateľa

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[17] (v EUR)	menej rozvinutý región	4 346 746,41 EUR
	viac rozvinutý región	664 489,94 EUR
Zdroj EÚ podľa kategórie regiónu[18] (v EUR)	menej rozvinutý región	4 346 746,41 EUR
	viac rozvinutý región	664 489,94 EUR

[16] Finančný rámec je potrebné uvádzať za celý NP spolu a v prípade financovania NP z viacerých priorít/špecifických cieľov, aj v rozdelení podľa špecifických cieľov.
[17] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[18] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

Zdroj ŠR podľa kategórie regiónu[19] (v EUR)	menej rozvinutý región	0,00 EUR
	viac rozvinutý región	0,00 EUR
Vlastné zdroje prijímateľa[20] podľa kategórie regiónu[21] (v EUR)	menej rozvinutý región	0,00 EUR
	viac rozvinutý región	0,00 EUR
Miera spolufinancovania (v %)	Zdroj EÚ	100 %
	Štátny rozpočet SR	0,00 %
	Prijímateľ	0,00 %
Uplatňovanie špecifického pravidla financovania[22] (ak relevantné)		
Zdroj pro-rata (v %)	neaplikuje sa	N/A
	neaplikuje sa	N/A
V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.	V zmysle čl. 63 ods. 3 prvá veta nariadenia o spoločných ustanoveniach, v projekte, ktorý zahŕňa / má prínos pre viac ako jednu kategóriu regiónu podľa článku 108 ods. 2 nariadenia o spoločných ustanoveniach v rámci členského štátu, sa celkové oprávnené výdavky spojené s projektom pridelia na príslušné kategórie regiónu na pomernom základe, a to podľa objektívnych kritérií. Objektívnym kritériom vzhľadom na povahu a zameranie projektu je podiel obyvateľov v bratislavskom regióne (NUTS II) k obyvateľom v SR (referenčným obdobím je rok 2021). Celkové oprávnené výdavky sa vyjadria pomerom podľa kategórie regiónu: menej rozvinutý región v pomere 86,74%, viac rozvinutý región v pomere 13,26%	

b) partnera (ak relevantné)

Fond	Vyberte položku.	
Celkové oprávnené výdavky NP podľa kategórie regiónu[23] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Zdroj EÚ podľa kategórie regiónu[24] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Zdroj ŠR podľa kategórie regiónu[25] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Vlastné zdroje partnera[26] podľa kategórie regiónu[27] (v EUR)	Vyberte položku.	
	Vyberte položku.	
Miera spolufinancovania (v %)	Zdroj EÚ	
	Štátny rozpočet SR	
	Partner	
Zdroj pro-rata (v %)	Vyberte položku.	
	Vyberte položku.	

[19] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[20] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027
[21] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[22] Uveďte konkrétne číslo tabuľky a jej názvu podľa Stratégie financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027.
[23] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[24] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[25] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[26] Uveďte v súlade so Stratégiou financovania Európskeho fondu regionálneho rozvoja, Európskeho sociálneho fondu plus, Kohézneho fondu, Fondu na spravodlivú transformáciu a Európskeho námorného, rybolovného a akvakultúrneho fondu na programové obdobie 2021 – 2027
[27] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

V prípade uplatňovania systému pro-rata uveďte spôsob jeho stanovenia (pomer medzi VRR a MRR), ktorý sa uplatňuje v prípade realizácie operácií s prínosom pre oba kategórie regiónov, vrátane názvu dokumentu v akom bol stanovený.	

12.Rozpočet

Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu a ich výstižné zdôvodnenie

Predpokladané finančné prostriedky na aktivity NP	Celkové oprávnené výdavky (v EUR)	Plánované vecné vymedzenie
Hlavné aktivity		
Vybudovanie národného laboratória umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab)		
013 - Softvér	1 532 988,36	Výška výdavku bola stanovená na základe indikatívnych cenových ponúk na cloudové služby, SW licencie.
521 - Mzdové výdavky	3 150 410,10	Vývoj aplikácií. Analýza a dizajn, Implementácia a testovanie. pozície: IT analytik, IT architekt, špecialista pre bezpečnosť IT, projektový manažér IT projektu, špecialista pre databázy, IT/IS konzultant, IT tester Interné pozície: IT analytik, IT architekt, kľúčový používateľ, manažér kybernetickej a informačnej bezpečnosti, tester
Aktivita 2		
skupina výdavkov		
skupina výdavkov		
Hlavné aktivity spolu	4 683 398,46	
Podporné aktivity		
skupina výdavkov		
skupina výdavkov		
Podporné aktivity SPOLU		
907 Paušálna sadzba na nepriame výdavky podľa článku 54 písm. a) NSU v hodnote 7% z oprávnených výdavkov na hlavné aktivity	327 837,89	Riadenie projektu (projektový manažér, finančný manažér, administratívny pracovník), publicita a informovanosť (špecialista na publicitu).
CELKOM	5 011 236,35 EUR	

Indikatívny rozpočet bol pripravený na základe troch indikatívnych cenových ponúk. Na základe ponúk boli vypočítané artimetické priemery pre jednotlivé položky rozpočtu.

Spolufinancovaný Európskou úniou

Indikatívny rozpočet bol pripravený na základe expertných odhadov, analýzy historických výdavkov a dostupných trhových dát. Pri zostavovaní rozpočtu boli zohľadnené reálne potreby projektu, očakávané objemy prác a porovnanie s nákladmi z predchádzajúcich projektov implementovaných SKB v predmetnej oblasti.

Pri skupine 521 – Mzdové výdavky sme vychádzali z dlhodobých mzdových nákladov na porovnateľné pozície, čím je preukázaná primeranosť a hospodárnosť mzdových výdavkov, ako aj súlad s princípom „hodnota za peniaze“.

V prípade zvýšenia celkových oprávnených výdavkov NP (po jeho schválení komisiou pri Monitorovacom výbore pre Program Slovensko 2021 – 2027) o viac ako 15 % (a nejde o prípad, kedy je určenie alokácie výsledkom realizovanej štúdie uskutočniteľnosti), riadiaci orgán / sprostredkovateľský orgán predloží pred vyhlásením výzvy na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 upravený zámer NP.

Ostatné zmeny v rozpočte projektu (napr. doplnenie novej skupiny výdavkov, vypustenie skupiny výdavkov, zvýšenie alebo zníženie výšky oprávnených výdavkov v rámci skupín výdavkov a pod.) nie je potrebné predkladať na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027.

13.Ďalšie informácie o národnom projekte

Detailnejšie informácie ohľadom národného projektu sú dostupné v rámci Metainformačného systému Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky kde sa nachádza kompletná dokumentácia v súlade s Vyhláškou 401/2023 Z. z.

Detail položky Projekt rozvoja IT, Národné laboratórium umelej inteligencie pre kybernetickú bezpečnosť (AI CyberLab) | MetaIS