Zámer národného projektu[1]

Názov národného projektu (ďalej aj „NP“):
Výskum a vývoj systému pre komplexné zvládanie bezpečnostných hrozieb (AI Security Lab)

Žiadateľ[2]:

Obchodné meno/názov	Akadémia Policajného zboru v Bratislave – Inštitút bezpečnostných vied APZ v Bratislave
Právna forma	Rozpočtová organizácia – štátna vysoká škola
Sídlo	Sklabinská 1, 835 17 Bratislava 35
IČO	00735779

Poskytovateľ: Ministerstva školstva, výskumu, vývoja a mládeže SR

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

Obchodné meno/názov	Ministerstvo vnútra Slovenskej republiky
Právna forma	Rozpočtová organizácia
Sídlo	Pribinova 2, 812 72 Bratislava
IČO	00151866
Zdôvodnenie potreby partnera NP[3]	Ministerstvo vnútra Slovenskej republiky je ústredným orgánom štátnej správy zameraný okrem iného aj na ochranu vnútorného poriadku, bezpečnosti, krízového riadenia a koordináciu vzdelávania zamestnancov obcí a vyšších územných celkov plniacich úlohy štátnej správy. Vzhľadom na túto rozsiahlu kompetenčnú pôsobnosť projekt logicky spadá do jeho pôsobnosti a jeho priame riadenie a realizácia garantujú súlad s národnými bezpečnostnými prioritami, stratégiami a legislatívnymi rámcami. Je teda nevyhnutné realizovať národný projekt, ktorého hlavným realizátorom bude APZ v Bratislave v spolupráci s Ministerstvom vnútra SR. Národný projekt umožní centralizovaný, strategicky koordinovaný prístup, čím sa zníži riziko duplicít, rozdielov v kvalite alebo nekoordinovaných výstupov, ktoré by mohli vzniknúť pri rôznych prijímateľoch v dopytovo-orientovaných výziev. Ministerstvo vnútra Slovenskej republiky **prevádzkuje úložiská a systémy vládneho cloudu, výpočtový výkon, ktoré sú základným predpokladom realizácie projektu.**
Kritériá pre výber partnera[4]	Ústredný orgán štátnej správy zodpovedný za ochranu ústavného zriadenia, verejného poriadku, bezpečnosti osôb a majetku, koordináciu výkonu štátnej správy uskutočňovanej obcami, vyššími územnými celkami a orgánmi miestnej štátnej správy, Policajný zbor, koordináciu vzdelávania zamestnancov obcí a vyšších územných celkov plniacich úlohy štátnej správy.

[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.

	APZ v Bratislave v období od 04/2022 do 12/2023 v pozícií partnera sa spolupodieľala na implementácií národného projektu s názvom „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“ kód projektu ITMS2014+: 314011CDW7, ktorého hlavným cieľom bolo zvýšenie odolnosti Slovenska voči pôsobeniu hybridných hrozieb prostredníctvom realizácie komplexného súboru opatrení zahŕňajúcich optimalizáciu procesov v subjektoch verejnej správy, úpravou regulačného rámca, zvýšením kapacít, získaním nových kompetencií a zručností subjektami verejnej správy. Projekt bol realizovaný Ministerstvom vnútra Slovenskej republiky - Inštitút správnych a bezpečnostných analýz MVSR v spolupráci so štyrmi partnermi: APZ v Bratislave, Ministerstvom obrany Slovenskej republiky, Ministerstvom zahraničných vecí a európskych záležitostí Slovenskej republiky a Úradom vlády Slovenskej republiky.
Má partner jedinečné postavenie na implementáciu týchto aktivít? Ak áno, na akom základe?	Ministerstvo vnútra Slovenskej republiky Zákon č. 575/2001 Z. z. Zákon o organizácii činnosti vlády a organizácii ústrednej štátnej správy - § 11 Ministerstvo vnútra Slovenskej republiky je ústredným orgánom štátnej správy pre: a) ochranu ústavného zriadenia, verejného poriadku, bezpečnosti osôb a majetku, ochranu a správu štátnych hraníc, bezpečnosť a plynulosť cestnej premávky, ochranu bezpečnosti a plynulosti železničnej dopravy, veci zbraní a streliva, súkromné bezpečnostné služby, vstup na územie Slovenskej republiky a pobyt cudzincov na jej území, občianske preukazy, cestovné doklady a oprávnenia na vedenie motorových vozidiel, otázky azylantov a odídencov, evidenciu obyvateľov, evidenciu cestných motorových a prípojných vozidiel, integrovaný záchranný systém, civilnú ochranu a ochranu pred požiarmi, d) koordináciu vzdelávania zamestnancov obcí a vyšších územných celkov plniacich úlohy štátnej správy. V rámci národného projektu s názvom „Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“ kód projektu ITMS2014+: 314011CDW7 vzniklo v rámci Inštitútu správnych a bezpečnostných analýz MVSR - Centrum boja proti hybridným hrozbám.

Sumárne informácie o NP

Celkové oprávnené výdavky NP (v EUR)	12 999 525,29 EUR
Miesto realizácie projektu (na úrovni kraja, resp. celé územie Slovenskej republiky)	celé územie Slovenskej republiky
Identifikácia hlavných cieľových skupín (ak relevantné)	subjekty verejnej správy a nimi zriadené subjekty, vrátane subjektov územnej samosprávy
Projekt so špecifickým určením pre marginalizované rómske komunity[5]	nie

[5] Zo zoznamu sa vyberie:
- "**áno**" v prípade, ak sa projekt plánuje realizovať výhradne v lokalitách Atlasu rómskych komunít a bude financovaný z alokácie so špecifickým určením pre marginalizované rómske komunity,

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	1P1 Veda, výskum a inovácie
Špecifický cieľ	RSO1.1 Rozvoj a rozšírenie výskumných a inovačných kapacít a využívanie pokročilých technológií
Opatrenie (ak relevantné)	1.1.4 Podpora optimalizácie, rozvoja a modernizácie výskumnej infraštruktúry
Súvisiace typy akcií[8]	Dobudovanie výskumných infraštruktúr pre riešenie celospoločenských výziev a mimoriadnych situácií

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]

APZ v Bratislave je zriadená zákonným opatrením Predsedníctva Slovenskej národnej rady č. 370/1992, právne postavenie APZ v Bratislave ako štátnej vysokej školy univerzitného typu vychádza zo zákona č. 131/2002 Z. z. o vysokých školách a o zmene a doplnení niektorých zákonov, v znení neskorších predpisov. APZ v Bratislave v rámci svojho poslania rozvíja vedecké poznanie v akreditovaných študijnom odbore Bezpečnostné vedy a v dvoch študijných programoch Bezpečnostnoprávna ochrana osôb a majetku a Bezpečnostnoprávne služby vo verejnej správe, pripravuje vysokoškolsky kvalifikovaných a profesionálne zdatných odborníkov pre útvary Policajného zboru, odborné pracoviská Ministerstva vnútra Slovenskej republiky a ďalších štátnych a neštátnych bezpečnostných služieb, zabezpečuje ďalšie vzdelávanie a uskutočňuje vedeckú výchovu, rigorózne, habilitačné a inauguračné konanie.

Inštitút bezpečnostných vied APZ v Bratislave - hlavným cieľom Inštitútu bezpečnostných vied Akadémie PZ je vytváranie podmienok pre permanentný rozvoj kvality vzdelávania a vzdelávacích procesov v prepojení na vysokoškolské vzdelávanie vo vednom odbore Bezpečnostné vedy, v študijných programoch bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnoprávne

- "**nie**" v prípade, ak sa projekt neplánuje realizovať v lokalitách Atlasu rómskych komunít a nebude financovaný z alokácie so špecifickým určením pre marginalizované rómske komunity,
- "**čiastočne**" v prípade, ak sa celý projekt, resp. aj časť projektu plánuje realizovať v lokalitách Atlasu rómskych komunít a nebude financovaný z alokácie so špecifickým určením pre marginalizované rómske komunity,
- "**nepriamo**" v prípade, ak sa:
  - projekt plánuje realizovať bez potreby sledovať prepojenie na lokality Atlasu rómskych komunít, čiastočne bude financovaný z alokácie so špecifickým určením pre marginalizované rómske komunity a realizácia projektu predpokladá vplyv aj na marginalizované rómske komunity – tento vplyv sa bližšie uvádza v rámci rámcového popisu projektu.
  - projekt plánuje realizovať bez potreby sledovať prepojenie na lokality Atlasu rómskych komunít, nebude financovaný z alokácie so špecifickým určením pre marginalizované rómske komunity, ale realizácia projektu môže mať vplyv aj na marginalizované rómske komunity.

[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.

služby vo verejnej správe a podľa požiadaviek a potrieb praxe. Inštitút bezpečnostných vied plní úlohu výskumno-vývojového lídra a garanta odbornej prípravy. Zabezpečuje metodiky, vedecké overenie použiteľnosti AI v bezpečnostných procesoch, návrh a realizáciu simulačných tréningov a digitálnej forenziky, ako aj vzdelávanie.

Poslaním Inštitútu bezpečnostných vied Akadémie PZ je podporovať pripravenosť vysokoškolsky kvalifikovaných a profesionálne zdatných odborníkov pre útvary Policajného zboru, odborné pracoviská Ministerstva vnútra Slovenskej republiky a ďalších štátnych a neštátnych bezpečnostných služieb; zabezpečovať ďalšie vzdelávanie, rozvíjať vedecké poznanie vo vednom odbore Bezpečnostné vedy a študijných odboroch bezpečnostnoprávna ochrana osôb a majetku a bezpečnostnoprávne služby vo verejnej správe, vykonávať expertnú a znaleckú činnosť, poskytovať súčinnosť pri uskutočňovaní vedeckej výchovy na stredných odborných školách Policajného zboru.

Hlavný cieľ a poslanie Inštitútu bezpečnostných vied Akadémie PZ bude napĺňané prostredníctvom profesionálnej angažovanosti vo vedeckej projektovej činnosti s podporou aktuálnych nástrojov informačno - komunikačných technológií a znaleckých aktivít s dôrazom na vzdelávacie procesy pre potreby rezortu Ministerstva vnútra SR ale aj externého prostredia.

2. Odôvodnenie využitia NP

Umelá inteligencia (AI) je kľúčová pre zvládanie dynamických bezpečnostných hrozieb, pretože umožňuje rýchlu analýzu veľkých dát, predikciu rizík a adaptívne rozhodovanie v reálnom čase. V prostredí verejnej bezpečnosti skracuje reakčný čas, zvyšuje presnosť detekcie incidentov a umožňuje štandardizovaný post-incidentný audit (logy, vysledovateľnosť, spätné učenie systémov). Projekt cieli na zodpovedné a právne súladné využitie AI, pri ktorom sú ústredné transparentnosť, kontrolovateľnosť a ochrana základných práv.

Realizácia navrhovaného riešenia prostredníctvom národného projektu je opodstatnená vzhľadom na jeho systémový, strategický a celospoločenský význam. Projekt rieši výskum a vývoj pre komplexné zvládanie bezpečnostných hrozieb s priamym dopadom na ochranu verejnosti a kľúčových inštitúcií – škôl, úradov a ďalších subjektov verejnej správy.

Prijímateľom a partnerom projektu sú organizácie, ktoré disponujú unikátnou kombináciou odborných, výskumných, vedeckých a legislatívnych kompetencií v oblasti bezpečnosti. Z pohľadu cieľov projektu je nevyhnutné, aby projekt:

- mal priamu väzbu na tvorbu národných bezpečnostných politík a stratégií,
- mal odborné kapacity na zabezpečenie výskumu a vývoja v oblasti bezpečnosti a AI,
- disponoval prepojením na Policajný zbor SR a záchranné zložky,
- bol schopný zabezpečiť vysokú mieru dôveryhodnosti výsledkov projektu pri implementácii do praxe.

Z uvedených dôvodov iný subjekt by nedisponoval zodpovedajúcim postavením, kapacitami ani oprávneniami na riešenie projektu v danom rozsahu.

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

Vzhľadom na národný charakter projektu s celoštátnym dosahom, ktorý má byť realizovaný ústredným orgánom štátnej správy nie je vhodné ani efektívne realizovať výber prijímateľa prostredníctvom súťažného postupu. Uvedeným spôsobom realizácie projektu dochádza aj k úspore administratívnych úkonov na strane žiadateľa pri súťažnom postupe prostredníctvom výzvy, a v konečnom dôsledku k efektívnejšiemu využitiu finančných prostriedkov.

Súťaž by zároveň viedla k roztfragmentovaniu riešení, ktoré by nebolo možné centrálne uplatniť ani garantovať ich interoperabilitu, pričom by sa zvyšovalo aj riziko duplicitných riešení.

4. **Uplatnenie princípu partnerstva pri príprave zámeru národného projektu**

   Ministerstvo vnútra Slovenskej republiky) ako strategický partner zohráva kľúčovú úlohu už v prípravnej fáze projektu. Jeho zapojenie zabezpečilo odborný a systémový rámec projektu, ako aj súlad so štátnymi prioritami v oblasti bezpečnosti.

Popis národného projektu

5. **Východiskový stav**

Slovensko ako aj iné štáty EU sú pod silným tlakom bezpečnostný hrozieb a čelia rôznym bezpečnostným výzvam. Objavujú sa incidenty, ktoré ohrozujú bezpečnosť štátu a jej obyvateľov. Tieto incidenty sú výsledkom rôznych aktivít, od kybernetických útokov cez násilie, destabilizačné aktivity a výtržnosti až po mimoriadne udalosti ako požiare, povodne či informačné operácie prostredníctvom sociálnych médií. Súčasné bezpečnostné procesy sú často viac reaktívne ako prediktíve, manuálne a nepripravené na dynamicky sa meniace podmienky. Známe predikcie globálneho vývoja (klíma, bezpečnostná situácia vo svete, vojna, resp. ozbrojené konflikty v susedstve, virtuálny svet sociálnych sietí) nevykazujú žiadne náznaky pre zlepšenie situácie v budúcnosti, naopak, skôr rátajú s nárastom rizík a následných možných incidentov. Reakcie zodpovedných orgánov Slovenskej republiky (ďalej len „SR“) na väčšie krízy v minulom období (Covid-19, zemetrasenie v Prešovskom kraji, utečenci z Ukrajiny a pod.) nepreukázali vysokú mieru pripravenosti (plány, postupy), či vôbec predikcie týchto rizík . Existuje preto významná príležitosť pre vytvorenie komplexného riešenia pre riadenie rizík bezpečnostných hrozieb Slovenskej republiky a zvládanie bezpečnostných hrozieb, ktoré spoja výhody umelej inteligencie, simulačných technológií a dátovej analytiky a to prostredníctvom cieleného výskumu a vývoja.

V oblasti digitálnych technológií a umelej inteligencie došlo v posledných rokoch k výraznému pokroku. AI riešenia sa využívajú v priemysle, zdravotníctve, doprave, ale aj v oblasti verejnej bezpečnosti. Tieto technológie umožňujú predikciu rizík, automatizované rozhodovanie, monitoring a analýzu veľkých dát a simuláciu rôznych scenárov. Zároveň sa rozvíjajú technológie ako IoT, inteligentné senzory, rozšírená a virtuálna realita (AR/VR) a mobilné aplikácie, ktoré môžu byť kľúčové pre bezpečné zvládnutie prírodných, ako aj antropogénných hrozieb.

Umelá inteligencia sa stáva čoraz dôležitejšou v oblasti bezpečnosti, pretože dokáže spracovávať obrovské množstvo dát, čo zlepšuje detekciu hrozieb následnú reakciu na jednotlivé hrozby a celkové zabezpečenie. Využíva strojové učenie a ďalšie techniky na analýzu rozsiahlych súborov údajov, identifikáciu vzorcov naznačujúcich hrozby a automatizáciu reakcií, čo vedie k proaktívnym a efektívnejším bezpečnostným opatreniam. Teda k:

- Pokročilej detekcii hrozieb a monitorovaniu v reálnom čase;
- Vylepšenej reakcii na incidenty,
- Vylepšenej správe zraniteľností,
- Detekcii phishingu a spamu,
- Autentifikácii a autorizáciu používateľov.

Umelá inteligencia (AI) sa ukázala ako kľúčový nástroj pri riešení problémov bezpečnosti a ponúka vývoj inteligentných agentov na efektívne riešenie špecifických bezpečnostných výziev. Inteligentný agent, či už vo forme hardvéru alebo softvéru, bude navrhnutý tak, aby optimalizoval pravdepodobnosť dosiahnutia definovaného cieľa prostredníctvom svojej schopnosti pozorovať, učiť sa a robiť informované rozhodnutia.

Pod povrchom inteligentní agenti spracovávajú obrovské množstvo údajov, aby sa učili a porozumeli vzorcom. Pri nasadení v obranných systémoch títo agenti uplatňujú svoje znalosti analýzou prichádzajúcich údajov vrátane predtým neidentifikovaných informácií. Umelá inteligencia v oblasti bezpečnosti pomáha bezpečnostným profesionálom rozpoznávaním zložitých vzorcov údajov, poskytovaním praktických odporúčaní a umožnením autonómneho zmierňovania. Zlepšuje detekciu hrozieb, podporuje rozhodovanie a urýchľuje reakciu na incidenty.

Umelá inteligencia využíva tri základné mechanizmy na riešenie zložitých bezpečnostných problémov:

- umelá inteligencia vyniká v rozpoznávaní a klasifikácii vzorcov údajov, ktoré môžu byť pre ľudí náročné na analýzu. Tieto vzory prezentuje bezpečnostným profesionálom na ďalšie preskúmanie a analýzu;
- Inteligentní agenti ponúkajú praktické odporúčania na základe identifikovaných vzorcov a poskytujú bezpečnostným profesionálom usmernenia o vhodných opatreniach;
- Niektorí inteligentní agenti môžu podniknúť priame kroky v mene bezpečnostných profesionálov na riešenie a nápravu bezpečnostných problémov. Zatiaľ čo organizácia už môže mať kvalifikovaných bezpečnostných profesionálov, pokročilé nástroje a dobre zavedené procesy, inteligentní agenti sa snažia vylepšiť a rozšíriť tieto existujúce zdroje, čím posilnia celkové obranné schopnosti.

Východiskové dokumenty na národnej a európskej úrovni

- V Bezpečnostnej stratégií SR sa v II kapitole 6.f píše: „Zvyšovanie odolnosti štátu voči bezpečnostným hrozbám, vrátane zaistenia riadneho fungovania ústavných orgánov; budovania bezpečného a odolného kybernetického priestoru; prevencie a minimalizácie prejavov extrémizmu a radikalizácie, posilňovania podpory a dôvery verejnosti k demokratickým inštitúciám a základnej orientácii zahraničnej a bezpečnostnej politiky; rozvíjania kompetentnej bezpečnostnej komunity; budovania demokratického povedomia a osobnej zodpovednosti u mladej generácie; posilnenie kvality a úlohy vzdelávacieho systému pri rozvoji demokracie a zaisťovaní bezpečnosti; posilňovania súdržnosti a kultúrneho rozvoja spoločnosti a rozvoja občianskej spoločnosti. Štát a spoločnosť musia byť schopné odolať krízovým situáciám bez toho, aby to ohrozilo ich základné fungovanie a tým aj bezpečnosť občanov.“
- Programové vyhlásenie vlády SR na roky 2023 - 2027 „Lepšie, pokojnejšie a bezpečnejšie žiť“
- Bezpečnostná stratégia SR 2021
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie. Súlad s európskym rámcom pre AI: Projekt sleduje požiadavky európskej regulácie.
- Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 schválená vládou SR dňa 7.1.2021 vytyčuje viacero strategických cieľov, medzi nimi „Vzdelaní odborníci a vzdelaná verejnosť“ a „Rozvoj výskumu a vývoja v oblasti kybernetickej bezpečnosti“. Navrhovaný spôsob dosiahnutia týchto cieľov zahŕňa vytvorenie viacerých systémov vzdelávania, zameraných na adresovanie vyššie identifikovaných a popísaných problémov. V čase vzniku tohto Programu bol vypracovávaný súvisiaci akčný plán. Národná stratégia kybernetickej bezpečnosti na roky 2021 – 2025, dostupné z: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf
- Príloha č.1 k Národnej stratégii riadenia rizík bezpečnostných hrozieb Slovenskej republiky. Dostupné tu: https://rokovania.gov.sk/RVL/Material/26865/1
- Koncepčná reforma krízového riadenia a civilnej ochrany v Slovenskej republike na obdobie 2025 – 2030. Dostupné tu: https://rokovania.gov.sk/RVL/Material/30933/1

Výstupy z ukončených národných projektov

V rámci národného projektu s názvom *„Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“* kód projektu ITMS2014+: 314011CDW7, ktorý bol financovaný z OP Efektívna verejná správa v programovom období 2014-2020, boli okrem iného zrealizované nasledovné výstupy:

- **Dotazník vnímania hybridných hrozieb -** jeho adresátmi boli študenti a pedagógovia policajných/vojenských vysokých škôl vo V4, vybraných univerzít v EÚ ako aj mimo EÚ. Dotazník obsahoval súhrn otázok, ktoré boli orientované na oblasť hybridných hrozieb v celej škále ich pôsobenia. Boli oslovené nasledovné univerzity:
  - Akadémia Policajného zboru v Bratislave
  - Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Liptovský Mikuláš
  - Slovenská technická univerzita Bratislava
  - Ekonomická univerzita v Bratislave
  - Prešovská univerzita v Prešove
  - *Trenčianska univerzita* Alexandra Dubčeka v Trenčíne
  - Policejní akademie České republiky v Praze, Praha, Česká republika
  - Západočeská univerzita v Plzni, Plzeň, Česká republika
  - Jihočeská univerzita v Českých Budějovicích, České Budějovice, Česká republika
  - University of public service Ludovika, Budapest, Maďarsko
  - Esterhazy Karoly katolic university, Eger, Maďarsko
  - Wyższa Szkoła Policji w Szczytnie, Szczytno, Poľsko
  - Krakovská akadémia Andrzeja Frycza Modrzewskiego, Krakov, Poľsko
  - Univesrity of Oradea, Oradea, Rumunsko
  - Uzhhorod National University, Užhorod, Ukrajina
  - İzmir Kâtip Çelebi Üniversitesi, Izmir, Turecko
  - University of Maribor, Maribor, Slovinsko
  - Fachhochschulle, Eisenstadt, Rakúsko
-
- **Dotazník pre expertov -** jeho adresátmi boli experti na policajných školách v krajinách V4. Experti sa vyjadrovali vo vzťahovej rovine (t. z. vzťah každej premennej ku každej ďalšej premennej) k následne uvádzaným parametrom.
- 43 publikačných výstupov, pričom niektoré z článkov boli publikované v prestížnych karentovaných časopisoch:
  - HDI INDEX DIMENSIONS IN THE CONTEXT OF HYBRID THREA
  - THE INFLUENCE OF EDUCATION ON THE ISSUE OF HYBRID THREATS
  - HYBRID THREATS AND THEIR IMPACT ON THE PERFORMANCE OF THE BUSINESS ENVIRONMENT
  - ENSURING FINANCIAL SYSTEM SUSTAINABILITY: COMBATING HYBRID THREATS THROUGH ANTI-MONEY LAUNDERING AND COUNTER- TERRORISM FINANCING MEASURES
  - THE RISKS OF MISUSING SOCIAL NETWORKS IN THE CONTEXT OF HYBRID THREAT
  - INTEGRATED SECURITY STRATEGIES IN THE CONTEXT OF HYBRID THREATS IN THE SLOVAK REPUBLIC

Administratívna, finančnú a prevádzkovú kapacitu žiadateľa a partnera

APZ v Bratislave a MVSR majú skúsenosti s implementáciou rôznych typov projektov (napr.: *Zvýšenie odolnosti Slovenska voči hybridným hrozbám pomocou posilnenia kapacít verejnej správy“* kód projektu ITMS2014+: 314011CDW7).

Žiadateľ a partner disponuje stabilným finančným zázemím a skúsenosťou s úspešnou realizáciou projektov financovaných z verejných a európskych zdrojov. Finančné riadenie je nastavené v súlade s princípmi transparentnosti a efektívneho hospodárenia s verejnými prostriedkami.

6. Hlavné ciele NP (stručne):

Cieľom projektu je vytvorenie excelentného pracoviska - Bezpečnostné centrum pre umelú inteligenciu (AI Security Lab) zameraného predovšetkým na aplikovaný výskum, vývoj a testovanie aplikácií riešení umelej inteligencie v oblasti verejnej bezpečnosti v súlade s transformačnými cieľmi domény 3 RIS3 Digitálna transformácia Slovenska.

- Prioritná oblasť 3-1: Inteligentné a prepojené systémy a zariadenia internetu vecí
  Transformačný cieľ 3-1 Zvýšiť v spoločnosti schopnosť rozhodovať sa na základe údajov od úrovne osobných rozhodnutí, cez automatizované pracoviská v podnikoch, až po úroveň kritickej infraštruktúry štátu, životného prostredia a mestskej infraštruktúry s využitím rôznych metód vrátane strojového učenia a umelej inteligencie.
- Prioritná oblasť č. 3-2: Zvýšenie úžitkovej hodnoty všetkých druhov údajov a databáz
  Transformačný cieľ 3-2 Využitím pokročilých informačných nástrojov zvýšiť využitie existujúcich dátových zdrojov na spracovanie údajov z existujúcich štruktúrovaných aj neštruktúrovaných zdrojov aj novovznikajúcich rozsiahlych báz údajov, ktoré budú základom riešení s vysokou pridanou hodnotou.
- Prioritná oblasť č. 3-4: Kybernetická bezpečnosť a kryptografia
  Transformačný cieľ 3-4 Vybudovať bezpečnú informačnú spoločnosť, ktorá využíva moderné technológie a dokáže sa brániť proti kybernetickým útokom a podporuje kybernetickú hygienu. Podniky aj ostatné subjekty by mali mať k dispozícii také digitálne riešenia, v ktorých bude bezpečnosť ich integrálnou súčasťou, aby nemuseli ochranu svojich údajov a sietí, kontinuitu výroby a ochranu pred kybernetickými útokmi riešiť ďalšími následnými projektmi.

Zameranie AI Security Lab sa sústredí najmä na:

1. Zber a konsolidáciu existujúcich vedeckých, technických a prakticky orientovaných bezpečnostných poznatkov, pre vytváranie a implementáciu scenárov pre bezpečnostné hrozby podporované aktuálnymi IT riešeniami.
2. Analýzu, predikciu a riadenie hrozieb: využívanie modelov od popredných svetových hráčov (Meta LLaMA, IBM Watson a ďalšie) pre predikciu a včasnú detekciu bezpečnostných incidentov.
3. Poskytovanie testovacieho Sandboxu (regulačného experimentálneho prostredia), ktoré umožni testovať vysokorizikové AI systémy v reálnych podmienkach.
4. Monitorovanie vysokorizkových systémov po uvedení na trh.
5. Digitálnu forenziku: AI nástroje pre identifikáciu, vyšetrovanie a analýzu dôkazov z digitálnych stôp (hlas, video, text).
6. Simulačný tréning: realistické scenáre s adaptívnym AI tréningovým modulom pre zásahové jednotky, bezpečnostný personál, ale aj širokú verejnosť s cieľom zlepšovať pripravenosť a zvyšovať odolnosť SR voči hrozbám.
7. Etické a právne aspekty AI: výskum a návrh etických a regulačných rámcov pre používanie umelej inteligencie vo verejnej bezpečnosti v súlade s regulačnými rámcami EÚ, napr. AI Act.
8. Budovanie znalostnej databázy hrozieb, za účelom popisu kľúčových postupov pre rozhodovanie AI modelov, pre implementáciu proaktívnej identifikácie a fixácie možnej hrozby.

9. Identifikáciu mladých a perspektívnych talentov, ich zapojenie do výskumnej a praktickej časti projektu riadenia bezpečnostných hrozieb.

SANDBOX: súbor pravidiel, protokolov a testovacích postupov (metodika), nie centrálny ISVS. Testovanie bude prebiehať v laboratórnom prostredí žiadateľa, resp. partnera podľa posúdenia, bez poskytovania elektronickej služby verejnosti.
Z kontextu definície **sandboxu,** vyplýva že ide o izolované prostredie, kde je možné bezpečne testovať alebo spúšťať IT aplikácie alebo systémy, bez rizika ovplyvnenia externého prostredia.

Definícia vysokorizikového AI systému vychádza z EU legislatívy o umelej inteligencii (AI Act), ktorá rozdeľuje AI systémy podľa rizika, ktoré môžu predstavovať pre ľudí a spoločnosť.

Nakoľko v rámci sandboxov budú testované rôzne kritické situácie, vektory útokov, ktoré môžu vytvárať potenciálne riziko, **daná infraštruktúra bude prístupná iba povereným a zaškoleným osobám**, ktoré sa budú aktívne zúčastňovať daného projektu a budú mať prístupové práva v zmysle bezpečnostným požiadaviek.

MONITORING: Z pohľadu praxe ide hlavne o sledovanie aktivít, výsledkov experimentov a bezpečnostných rizík spojených s AI systémami. Projekt nebude prevádzkovať centrálny monitorovací IS ani zbierať operačné logy OVM. Vytvorí sa „PMM metodika“ (post market monitoring podľa AI Act):

- katalóg metrík (výkonnosť, robustnosť, drift),
- šablónu PMM plánu pre poskytovateľov/používateľov HR AI,
- proces vyhodnocovania incidentov a oznamovacej povinnosti (definícia „závažného incidentu“ a spôsob reportingu podľa AI Act).

V rámci projektu bude implementované:

- Parametre na technické monitorovanie:
- Manažérske a procesné monitorovanie
- Etické a právne monitorovanie.

Metodika slúži správcom/poskytovateľom HR AI, ktorí si PMM realizujú u seba (alebo u svojho zhotoviteľa). AI Security Lab môže na žiadosť vykonať nezávislé hodnotenie v laboratórnych podmienkach alebo on site audit podľa protokolu – stále bez centrálneho zberu osobných alebo utajovaných údajov.

Laboratórium bude zároveň inkubátor pre tvorbu prototypov - produktov, ktoré vedia využiť štátne-verejné inštitúcie (napr. mestá a obce) alebo firmy na trhu. Jeden z príkladov je vyvinutie **digitálneho nástroja - platformy na zvládanie bezpečnostných hrozieb**, ktorý bude dostupný a prispôsobený potrebám všetkých zainteresovaných aktérov. Tento nástroj bude slúžiť na okamžité nahlasovanie incidentov, koordináciu reakcií, evidenciu udalostí, zdieľanie protokolov a komunikáciu počas kríz. Projekt podporí aj vývoj metodických rámcov, analytických modelov a bezpečnostných algoritmov (vrátane AI komponentov), ktoré umožnia prispôsobovať bezpečnostné systémy aktuálnym hrozbám. Dlhodobým cieľom je okrem iného zabezpečiť, aby verejné inštitúcie, napr. školy na Slovensku mali k dispozícii overený, efektívny a integrovaný systém bezpečnosti, ktorý pomáha predchádzať incidentom a zároveň znižuje ich následky.

Na základe výskumu a vývoja v rámci projektu sa vytvorí aj inovatívny, funkčný a komplexný systém pre zvládanie bezpečnostných hrozieb. V rámci projektu bude pripravený návrh a prebehne testovanie **prototypu simulačného centra**, ktoré umožní realizovať realistické tréningy, modelovanie hrozieb a

praktické nácviky reakcií na rôzne typy bezpečnostných incidentov vrátane násilných útokov, evakuácií, požiarov, kybernetických hrozieb či únikov nebezpečných látok a pod. Výhodou virtualizovania scenárov a bezpečnostných incidentov ma pozitívny dopad na životné prostredie.

Projekt sa zameriava na vytvorenie komplexného bezpečnostného systému a to prostredníctvom:

1. analýzy aktuálne existujúcich bezpečnostných protokolov a návrhov jednotných vzorových bezpečnostných protokolov;
2. prototypu simulačného centra - vývoj špičkového a moderného interaktívneho vzdelávacieho prostredia využívajúceho pokročilé technológie (AI, VR, AR, ML a IoT), v ktorom sa môžu všetci zainteresovaní aktéri pripraviť na rôzne bezpečnostné hrozby;
3. tvorby rôznych nástrojov a mobilných aplikácii, napr. digitálneho nástroja na nahlasovanie a zvládanie bezpečnostných hrozieb - vývoj systému, ktorý počas bezpečnostnej hrozby automaticky komunikuje so všetkými zainteresovanými aktérmi pomocou rôznych komunikačných kanálov (napr. integrácia cez Edupage);
4. činnosti a rozvoja Znaleckého ústavu pre identifikáciu, analýzu a predikciu prejavov radikalizmu a extrémizmu, ktorý súčasne bude vykonávať znaleckú činnosť v odbore Spoločenských a humanitných vied so zameraním na odvetvie politického extrémizmu a bude sa podieľať aj na vzdelávacej a publikačnej činnosti;
5. IoT riešení pre fyzickú bezpečnosť (napr.: inteligentné kamerové systémy s analýzou správania, detekčné senzory a varovné systémy a pod.);
6. vytvorením silného systému spolupráce medzi subjektami štátnej a verejnej , bezpečnostnými zložkami, psychológmi, zdravotníkmi a ďalšími relevantnými organizáciami, čím sa zlepší efektivita reakcií v prípade reálnej krízy;
7. vytvorením odporúčaní na riadenie bezpečnostných hrozieb, podporených AI modelmi;
8. aplikáciou talent manažment na identifikáciu a rozvoj mladých talentov v oblasti AI zameraných na bezpečnostné hrozby.

Tento projekt je orientovaný na **aplikovaný výskum**, čo jednoznačne dokumentuje hlavný cieľ projektu, ktorým je vývoj prakticky využiteľných nástrojov AI a digitálnych nástrojov, mobilných aplikácii, IoT riešení a metodík zameraných na oblasť verejnej bezpečnosti a bezpečnostnú politiku štátu. Dosiahnuté výsledky v aplikovanom výskume na teoretickej úrovni budú pripravené na postupnú implementáciu do praxe ako napríklad na kreovanie prototypu simulačného centra a digitálneho nástroja na riadenie bezpečnostných situácií, čo bude reflektovať a nadväzovať nielen na aktuálne, ale aj pripravované transformačné a reformné zámery v oblasti krízového riadenia na Slovensku.
Projekt zároveň **nezasahuje do hospodárskej súťaže**, keďže jeho výstupy nebudú komerčne využívané na trhu, ale budú slúžiť ako podklady pre tvorbu, nastavenie a aktualizáciu bezpečnostných politík štátu. Výsledky budú primárne smerované pre potreby verejnej a štátnej správy, čím sa zabezpečí ich celospoločenský prínos.

Projekt nebuduje, nenasadzuje ani neupravuje ISVS; výstupy sú metodického a informačného charakteru, štandardy, parametre, testovacie protokoly a referenčné prototypy v laboratórnom prostredí, ktoré budú určené napr. pre systémy krízového riadenia pre naturogénne a antropogénne hrozby alebo na zabezpečenie vnútornej bezpečnosti.

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	PSKPO165	Počet vytvorených dokumentácií, analýz, štúdií a správ v súvislosti s prípravou, implementáciou, monitorovaním a hodnotením	počet	15
výsledok	PSKPRCR08	Publikácie z podporovaných projektov	počet	15

Zoznam iných údajov projektu (ak relevantné)

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

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

Cieľová skupina	Počet[13]	Prínos
Subjekty verejnej správy a nimi zriadené subjekty, vrátane subjektov územnej samosprávy	Nie je možné vyčísliť presne vzhľadom na charakter projektu	Spoločensky prispeje k vyššej bezpečnostnej pripravenosti štátnych a verejných inštitúcií, čo môže viesť k zníženiu následkov bezpečnostných hrozieb. Projekt podporí digitalizáciu verejného sektora zavedením moderných nástrojov pre komunikáciu, koordináciu a simuláciu bezpečnostných hrozieb.

[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
Výskum a vývoj systému pre komplexné zvládanie bezpečnostných hrozieb	**Podaktivita 1** Prieskumy, analýzy, štúdie **Podaktivita 2** Vývoj prototypu simulačného centra využívajúceho poznatky z oblasti AI. **Podaktivita 3** Vývoj digitálnych nástrojov v oblasti bezpečnosti , napr. nástroja na zvládanie bezpečnostných hrozieb **Podaktivita 4** Vývoj IoT riešenia pre fyzickú bezpečnosť	**Aktivita** žiadateľ a partner **Podaktivita 1** žiadateľ a partner **Podaktivita 2** žiadateľ a partner **Podaktivita 3** žiadateľ a partner **Podaktivita 4** žiadateľ a partner	36

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.

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

c. Uveďte detailnejší popis aktivít.

Výskumné otázky a hypotézy

Cieľom výskumu je overiť prínosy integrácie umelej inteligencie (AI), senzorických systémov internetu vecí (IoT) a nástrojov na digitálne riadenie bezpečnostných incidentov. Predpokladá sa, že takto koncipovaný systém bude efektívnejší nielen v operatívnej fáze (rýchlosť a presnosť reakcie), ale aj v post-analytickej fáze (dokumentácia, vyhodnotenie, odporúčania pre legislatívu a prevenciu).

Výskum je postavený na **štyroch hypotézach**, ktoré systematicky pokrývajú jednotlivé vrstvy systému:

Hypotéza 1: Aplikácia modelov umelej inteligencie v simuláciách a bezpečnostných scenároch umožní vytvárať flexibilnejšie a realistickejšie postupy v porovnaní s manuálne vypracovanými plánmi.

🔍 *Zameranie:* Porovnanie AI generovaných bezpečnostných scenárov so statickými, expertnými plánmi.

📊 *Indikátory:* presnosť simulácie, schopnosť adaptácie, hodnotenie expertov.

[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 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.

Hypotéza 2: Elektronický nástroj na zvládanie bezpečnostných hrozieb dokáže znížiť reakčný čas o viac než 30 % v porovnaní s tradičnými metódami.

🔍 *Zameranie:* Efektívnosť digitálneho zásahového systému (napr. dashboard s odporúčaniami).

📊 *Indikátory:* reakčný čas, oneskorenia v komunikácii, koordinácia operácií.

Hypotéza 3: IoT senzory umiestnené v pilotných testovaných budovách dokážu detekovať a automaticky klasifikovať incident (vniknutie, výbuch, oheň) s presnosťou nad 85 % a aktivovať adekvátnu reakciu.

🔍 *Zameranie:* Výkon senzorickej a klasifikačnej vrstvy (IoT + AI).

📊 *Indikátory:* accuracy, precision, F1-score, počet falošných poplachov, rýchlosť aktivácie.

Hypotéza 4: Komplexný systém pre zvládanie bezpečnostných hrozieb dokáže podporiť nielen operatívne riadenie incidentov, ale aj následnú dokumentáciu, vyhodnotenie a legislatívnu odpoveď na zistené nedostatky.

🔍 *Zameranie:* Systém ako nástroj celostného zvládania incidentov – od detekcie po post-analýzu.

📊 *Indikátory:* pokrytie fáz incidentu, kvalita záznamov, spätná väzba do systému, využiteľnosť pre správne/trestné konania.

Stručný tematický rámec hypotéz

Hypotéza	Téma	Vrstva systému	Kľúčová otázka
H1	Realistickosť a adaptivita simulácií	AI modelovanie	Zlepšuje AI tvorbu scenárov?
H2	Skrátenie reakčného času	DSS (Decision Support)	Reagujeme rýchlejšie vďaka nástroju?
H3	Presnosť detekcie incidentov	IoT + AI klasifikácia	Dokáže systém spoľahlivo rozpoznať incidenty?
H4	Celkové riadenie a dokumentácia	Integrovaný systém	Pomáha systém aj po ukončení incidentu?

Výskumný dizajn

Hypotéza 1 (AI simulácie): *Aplikácia modelov umelej inteligencie v simuláciách a bezpečnostných scenároch umožní vytvárať flexibilnejšie a realistickejšie postupy v porovnaní s manuálne vypracovanými plánmi.*

📌 ***Testovanie:*** Porovnanie AI generovaných bezpečnostných scenárov (napr. pomocou reinforcement learning alebo agent-based simulácií) so statickými plánmi vytvorenými expertmi. Hodnotí sa realistickosť, variabilita, schopnosť adaptácie a akceptovateľnosť výstupov zo strany odborníkov.

Hypotéza 2 (časová efektivita DSS): *Elektronický nástroj na zvládanie bezpečnostných hrozieb dokáže znížiť reakčný čas o viac než 30 % v porovnaní s tradičnými metódami.*

📌 ***Testovanie:*** Experimentálne porovnanie reakčnej doby v simulovaných scenároch – so systémom podporeným AI a bez neho. Merané metriky zahŕňajú čas aktivácie zásahu, prenos rozhodnutí a počet duplicít v činnostiach.

Hypotéza 3 (presnosť IoT detekcie): *IoT senzory umiestnené v pilotných testovaných budovách dokážu detekovať a automaticky klasifikovať incident (vniknutie, výbuch, oheň) s presnosťou nad 85 % a aktivovať adekvátnu reakciu.*

📌 ***Testovanie:*** Nasadenie IoT systému v testovacej alebo polorealistickej budove. Hodnotí sa presnosť klasifikácie pomocou supervised learning modelov (napr. Random Forest, CNN, LSTM), počet falošných poplachov (False Positives) a oneskorenie medzi detekciou a reakciou.

Hypotéza 4 (komplexný dopad systému): *Komplexný systém pre zvládanie bezpečnostných hrozieb dokáže podporiť nielen operatívne riadenie incidentov, ale aj následnú dokumentáciu, vyhodnotenie a legislatívnu odpoveď na zistené nedostatky.*

📌 ***Testovanie:*** Zhodnotenie celkového cyklu incidentu od detekcie po ukončenie – vrátane automatickej správy, logov, auditu a využiteľnosti záznamov pre správne alebo legislatívne konanie. Hodnotené expertmi a právnikmi na škále využiteľnosti (napr. 1–5).

Logická matica výskumu (Hypotézy 1–4)

Hypotéza	Premenné	Metóda	Indikátory	Nástroj / Technológia
H1: AI v simuláciách zlepší flexibilitu a realistickosť oproti manuálnym plánom	*Nezávislá:* typ modelu (AI vs. manuálny) *Závislá:* kvalita scenára	Experimentálne porovnanie, expertné hodnotenie	Hodnotenie realistickosti (škála 1–5), adaptívnosť scenára, počet možných reakcií	Agent-based modeling (Mesa, AnyLogic), LLM (GPT-like), expertný dotazník
H2: Elektronický nástroj zníži reakčný čas o viac ako 30 %	*Nezávislá:* typ zásahu (AI systém vs. tradičný) *Závislá:* reakčný čas	Simulovaný zásah, A/B testovanie	Reakčný čas (v s), percentuálna úspora, duplicita úloh	Decision Support Dashboard, logy systému, stopwatch recording
H3: IoT senzory detegujú incident s presnosťou nad 85 %	*Nezávislá:* typ senzora *Závislá:* klasifikácia incidentu	Reálne testy v simulovanom priestore, supervised learning	Accuracy, precision, F1-score, FP/FN pomer	IoT brána (Raspberry Pi, ESP32), AI model (Random Forest, CNN), confusion matrix
H4: Komplexný systém podporí aj dokumentáciu a právnu analýzu	*Nezávislá:* typ systému (s/bez automatickej dokumentácie) *Závislá:* kvalita výstupnej správy	Expertné vyhodnotenie incidentových záznamov	Kompletnosť správy, auditovateľnosť, legislatívna využiteľnosť	Záznamový modul DSS, právna analýza, kontrolný zoznam + hodnotiaca matica

Metodológia a technologický prístup

Výskum je postavený na **kombinovanom výskumnom dizajne**, ktorý spája **kvantitatívne experimentálne testovanie** s **kvalitatívnym hodnotením používateľskej skúsenosti a odborného posúdenia výsledkov**. Tento prístup je zvolený s cieľom zachytiť nielen technickú výkonnosť navrhovaného systému, ale aj jeho **sociálnu prijateľnosť, použiteľnosť a dôveryhodnosť** v kontexte verejnej bezpečnosti a civilnej ochrany.

Kvantitatívna časť výskumu sa zameriava na merateľné výstupy systému v podmienkach simulovaných a čiastočne reálnych incidentov. Budú testované nasledovné parametre:

- **Presnosť klasifikácie incidentov** (napr. požiar, vniknutie, výbuch) na základe IoT vstupov,
- **Reakčný čas systému** (latencia od detekcie po aktiváciu reakcie),
- **Efektívnosť reakčného algoritmu** navrhnutého AI modelom,
- **Miera úspory oproti tradičnému spôsobu zásahu** (v %),
- **Presnosť a adaptabilita simulácií bezpečnostných scenárov**.

Na získanie týchto údajov budú použité:

- **Real-time simulácie incidentov** (kybernetický útok, požiar, výbuch, evakuácia),
- **AI modelovanie** (napr. reinforcement learning, agent-based modeling),

- **Laboratórne a polorealistické testovanie presnosti IoT senzorov** (napr. PIR senzory, termokamery, dymové čidlá).

Doplňujúca kvalitatívna analýza bude slúžiť na zhodnotenie praktickej použiteľnosti systému zo strany koncových používateľov (napr. operátorov DSS, bezpečnostných zložiek) a expertov na krízové riadenie. Využité budú:

- **Expertné hodnotenia AI výstupov**, najmä v oblasti identifikácie, simulácií a odporúčaných reakcií,
- **Dotazníkové zisťovanie spokojnosti s používateľským rozhraním a systémom ako celkom**, vrátane aplikácie štandardizovaného nástroja **System Usability Scale (SUS)**,
- **Polostruktúrované rozhovory** s operátormi a odbornými hodnotiteľmi na vyhodnotenie dôveryhodnosti výstupov a kvality post-incidentovej dokumentácie.

Každá z formulovaných hypotéz bude overovaná kombináciou:

- **technických metód** (analýza senzorických dát, strojové učenie, spracovanie signálov, AI simulácie), a
- **sociálneho hodnotenia** (expertná spätná väzba, právna a procesná použiteľnosť výstupov, subjektívna spokojnosť).

Systém bude testovaný ako **celostný nástroj**, ktorý nielenže operatívne reaguje na identifikované incidenty, ale zároveň umožňuje generovať automatizované správy a odporúčania, vyhodnocovať chyby a podporovať **právne, organizačné a legislatívne zlepšenia** krízového manažmentu

Inovačný potenciál a výstupy projektu

Projekt prinesie inovatívne AI a IoT riešenia pre detekciu, simuláciu a zvládanie bezpečnostných hrozieb. Výstupmi budú:

- vývoj prototypu simulačného centra,
- softvér na zvládanie bezpečnostných hrozieb,
- AI modely pre analýzu správania a predikciu hrozieb,
- IoT bezpečnostné moduly,
- činnosť a rozvoj Znaleckého ústavu pre identifikáciu, analýzu a predikciu prejavov radikalizmu a extrémizmu, ktorý súčasne bude vykonávať znaleckú činnosť v odbore Spoločenských a humanitných vied so zameraním na odvetvie politického extrémizmu a bude sa podieľať aj na vzdelávacej a publikačnej činnosti,
- datasety a metodiky,
- výstupy aplikovaného výskumu bude potrebné chrániť prostredníctvom právnej ochrany (napr.: duševné vlastníctvo: Patentov, Úžitkových vzorov, Ochranné známky, Autorské právo) a zmluvnej ochrany (napr.: Licenčné zmluvy, Spoluautorské a vlastnícke dohody),
- open-source komponenty na ďalší výskum.

Inovačne projekt prekonáva existujúce riešenia tým, že kombinuje pokročilé technológie (AI, VR, AR, ML a IoT), bezpečnostnú politiku štátu a tréning v jedinom systéme.

Projekt je koncipovaný ako inovatívna výskumno-vývojová iniciatíva, ktorej cieľom je vytvárať nové metodiky, technologické riešenia a prototypy (AI a digitálne nástroje, simulačné centrum, mobilné aplikácie a IoT riešenia) s priamym prínosom pre posilnenie bezpečnostných politík štátu. Projekt nerieši udržiavanie existujúcich kapacít, ale systematickým zapájaním širokého spektra externých domácich a zahraničných odborných kapacít zabezpečuje rozvoj interdisciplinárneho výskumu v oblasti AI riešení pre zvládanie bezpečnostných a hybridných hrozieb.

Spolufinancovaný Európskou úniou

Zainteresovaní aktéri:

- zamestnanci štátnej a verejnej správy realizujúci bezpečnostné politiky a bezpečnostné služby realizované v mene štátu
- výskumno-vývojové kapacity Akadémie policajného zboru, študenti v rámci študijných odborov týkajúcich sa bezpečnostných politík

Hlavná aktivita projektu:

Výskum a vývoj systému pre komplexné zvládanie bezpečnostných hrozieb (01/2026 – 12/2028)

Podaktivita 1 Prieskumy, analýzy, štúdie (odborná podaktivita nevývojového charakteru)

- Analýza a identifikácia bezpečnostných rizík a analýza aktuálne existujúcich bezpečnostných protokolov a ich nedostatkov;
- Mapovanie zraniteľných miest (fyzické, psychologické, digitálne a pod.);
- Komparatívna analýza osvedčených postupov zo zahraničia, adaptácia na slovenský kontext a spolupráca **so zahraničnými inštitúciám a korporáciami (napr.: Europol a pod.);**
- Právny rozbor súladu s GDPR a inými reguláciami ochrany osobných údajov.
- Spolupráca **s odborníkmi** v oblasti v oblasti programovania, AI a IKT, polície, znalcov v oblasti extrémizmu, psychológov, bezpečnostných analytikov a pod.;
- Analýza psychologických a sociálnych aspektov bezpečnostných hrozieb (napr.: správanie zúčastnených osôb pri bezpečnostných hrozbách, efektívne metódy tréningu a prípravy rôznych aktérov a pod.);
- Vypracovanie jednotných bezpečnostných protokolov a metodík
- Vypracovanie expertných správ a znaleckých posudkov;
- Návrh modelov spolupráce, ktoré podporia rýchle a koordinované reakcie v krízach.

Podaktivita 2 Vývoj prototypu simulačného centra využívajúceho poznatky z oblasti AI (odborná podaktivita vývojového charakteru)

- Návrh a implementácia technickej architektúry centra využívajúceho pokročilé technológie (AI, VR, AR, ML a IoT);
- Tvorba základných scenárov v spolupráci s odborníkmi (psychológovia, polícia, hasiči, krízoví manažéri, znalcov v oblasti extrémizmu);
- Vývoj základných realistických interaktívnych simulácií s rôznymi scenármi bezpečnostných situácií (napr.: aktívny útočník, phishing, bombová hrozba);
- Nasadenie adaptívneho AI modulu pre analýzu rozhodnutí účastníkov a adaptívne učenie;
- Zabezpečenie použiteľnosti, škálovateľnosti a modulárnosti systému;
- Testovanie, spätná väzba a optimalizácia;
- Výstupy aplikovaného výskumu bude potrebné chrániť prostredníctvom právnej ochrany (napr.: duševné vlastníctvo: Patentov, Úžitkových vzorov, Ochranné známky, Autorské právo) a zmluvnej ochrany (napr.: Licenčné zmluvy, Spoluautorské a vlastnícke dohody).

Podaktivita 3 Vývoj digitálnych nástrojov v oblasti bezpečnosti, napr. nástroja na zvládanie bezpečnostných hrozieb (odborná podaktivita vývojového charakteru)

- Vývoj robustného multikanálového notifikačného systému (podpora SMS, e-mailov, push správ, hovorov, alertov, sirén a iných) s vysokou dostupnosťou a odolnosťou;
- Cielenie a segmentácia – na základe geolokácie, skupiny, organizačnej štruktúry alebo definovaných zón;
- Implementácia bezpečnej a šifrovanej komunikácie v reálnom čase;

- Riadenie incidentov s transparentným sledovaním – správa incidentov, eskalácia, priraďovanie zodpovedností a sledovanie ich riešenia;
- Identifikácia, analýza, dokazovanie a predikcia prejavov radikalizmu a extrémizmu v digitálnom prostredí;
- Reporty a audit – prehľad o doručených správach, odpovediach a stave incidentov.
- Integrácie – podpora pre AD, M365, API, webhooky, Cell Broadcast a ďalšie technológie;
- Mapový modul – vizualizácia používateľov v reálnom čase na mape s možnosťou interaktívneho filtrovania a lokalizačných zón;
- Šifrovaná komunikácia – obojsmerná hlasová a textová komunikácia medzi operátormi a používateľmi cez zabezpečené kanály;
- Zabezpečenie interoperability s existujúcimi štátnymi a verejnými systémami;
- Testovanie, spätná väzba a optimalizácia;
- Overenie odolnosti systému voči kybernetickým útokom;
- Výstupy aplikovaného výskumu bude potrebné chrániť prostredníctvom právnej ochrany (napr.: duševné vlastníctvo: Patentov, Úžitkových vzorov, Ochranné známky, Autorské právo) a zmluvnej ochrany (napr.: Licenčné zmluvy, Spoluautorské a vlastnícke dohody).

Podaktivita 4 Vývoj IoT riešenia pre fyzickú bezpečnosť (odborná podaktivita vývojového charakteru)

- Vývoj bezpečnostných algoritmov a AI komponentov (napr.: algoritmy pre detekciu anomálií a rizikových situácií na základe dát zo senzorov a systémov, AI pre adaptívne učenie simulačných scenárov podľa správania účastníkov, prediktívne modely pre včasné varovanie a riadenie kríz, návrh modelov spolupráce, ktoré podporia rýchle a koordinované reakcie v krízach a pod.);
- Vývoj a integrácia inteligentných senzorov, kamerových systémov a varovných zariadení a aplikácií;
- Implementácia pokročilých analytických nástrojov pre spracovanie dát z IoT;
- Prepojenie fyzických bezpečnostných systémov s digitálnymi nástrojmi, napr. nástrojom pre krízové riadenie.

Projekt počíta s otvorenou architektúrou systémov, čo umožní:

- škálovanie na ďalšie subjekty štátnej a verejnej správy,
- budúce rozšírenie o nové scenáre (napr. environmentálne hrozby, teroristické útoky a pod).
- prepojenie na formálne a neformálne vzdelávacie systémy.

Riziká a mitigácie:

Riziko: Výskumné a vývojové úlohy môžu byť náročnejšie, ako sa predpokladalo, čo spôsobí oneskorenie.
Mitigácia: Realistické časové plánovanie, fázy s jasnými míľnikmi, flexibilná projektová štruktúra, využitie metodík agilného vývoja.

Riziko: AI, softvér a senzory môžu byť cieľom kybernetických alebo fyzických útokov.
Mitigácia: Využitie bezpečnostných štandardov (napr. ISO/IEC 27001, OWASP), penetračné testovanie, šifrovanie, pravidelná aktualizácia systémov.

Etické a právne aspekty

Realizácia projektu si vyžaduje dôsledné zohľadnenie etických princípov a právnych noriem. Vzhľadom na prácu s citlivými údajmi, využívanie umelej inteligencie a pôsobenie v prostredí verejných inštitúcií je nutné, aby bol projekt postavený na princípoch dôvery, transparentnosti a súladu so zákonmi, a to predovšetkým:

- Ochrana osobných údajov (GDPR)

- Zodpovedné využitie umelej inteligencie
- Právne záväzky v oblasti bezpečnosti
- Etické používanie simulačných scenárov
- Licencovanie a duševné vlastníctvo

Dopad projektu
Projekt bude mať vedecký dopad prostredníctvom vývoja inovatívnych AI a IoT riešení pre zvládanie bezpečnostných hrozieb, čím prispeje k rozvoju interdisciplinárneho výskumu. Spoločensky prispeje k vyššej bezpečnostnej pripravenosti štátnych a verejných inštitúcií, čo môže viesť k zníženiu následkov bezpečnostných hrozieb. Projekt podporí digitalizáciu verejného sektora zavedením moderných nástrojov pre komunikáciu, koordináciu a simuláciu bezpečnostných hrozieb.

Šírenie, komunikácia a využitie výsledkov
Výsledky projektu budú aktívne komunikované prostredníctvom odborných konferencií, seminárov, vedeckých publikácií a digitálnych platforiem. Kľúčové výstupy – prototypy, softvérové nástroje, algoritmy a metodiky – budú sprístupnené cieľovým skupinám (štátna a verejná správa, záchranné zložky a pod.) prostredníctvom workshopov, školení a online portálu. Časť riešení bude dostupná ako open-source pre podporu ďalšieho výskumu a implementácie. Projekt bude mať aj popularizačný rozmer – zvýši povedomie o významnosti pripravenosti na bezpečnostné hrozby a prinesie praktické nástroje pre ich zvládanie v reálnom prostredí.

Dodržiavanie horizontálnych princípov
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	01/2026
Predpokladaná doba realizácie NP v mesiacoch	36

Termíny v tabuľke nie sú záväzné.

Spolufinancovaný Európskou úniou

11.Finančný rámec[16]

a) žiadateľa

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[17] (v EUR)	neaplikuje sa	
	viac rozvinutý región	8 680 304,18 EUR
Zdroj EÚ podľa kategórie regiónu[18] (v EUR)	neaplikuje sa	
	viac rozvinutý región	3 472 121,67 EUR
Zdroj ŠR podľa kategórie regiónu[19] (v EUR)	neaplikuje sa	
	viac rozvinutý región	5 208 182,51 EUR
Vlastné zdroje prijímateľa[20] podľa kategórie regiónu[21] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Miera spolufinancovania (v %)	Zdroj EÚ	40,00 %
	Štátny rozpočet SR	60,00 %
	Prijímateľ	0,00 %
Uplatňovanie špecifického pravidla financovania[22] (ak relevantné)		
Zdroj pro-rata (v %)	neaplikuje sa	
	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.	N/A	

b) partnera (ak relevantné)

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[23] (v EUR)	neaplikuje sa	
	viac rozvinutý región	4 319 221,11 EUR
Zdroj EÚ podľa kategórie regiónu[24] (v EUR)	neaplikuje sa	
	viac rozvinutý región	1 727 688,44 EUR
Zdroj ŠR podľa kategórie regiónu[25] (v EUR)	neaplikuje sa	
	viac rozvinutý región	2 591 532,67 EUR
Vlastné zdroje partnera[26] podľa kategórie regiónu[27] (v EUR)	neaplikuje sa	
	neaplikuje sa	
Miera spolufinancovania (v %)	Zdroj EÚ	40,00 %
	Štátny rozpočet SR	60,00 %

[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“.
[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“.

	Partner	0,00 %
Zdroj pro-rata (v %)	neaplikuje sa	
	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.	N/A	

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		
Aktivita 1	**Výskum a vývoj systému pre komplexné zvládanie bezpečnostných hrozieb**	

521 - Mzdové výdavky **(APZ v Bratislave)**	6 200 217,27 EUR	Skupina výdavkov zahŕňa výdavky na mzdové kapacity na realizáciu aktivít projektu (celková cena práce vrátane odmien v súlade podmienkami stanovenými v Príručke pre Prijímateľa) a to v nasledovnej predpokladanej štruktúre: **Odborný garant projektu (APZ v Bratislave)** Predpokladané zapojenie: 1 FTE Predpokladaná priemerná CCP: 33,39 €/hod. **Koordinátor odborných aktivít (APZ v Bratislave)** Predpokladané zapojenie: 2 FTE Predpokladaná priemerná CCP: 29,91 €/hod. **Expert (APZ v Bratislave)** Predpokladané zapojenie: 12 FTE (FTE bude rozdelené podľa potreby) Predpokladaná priemerná CCP: 40,79 €/hod. **Odborný zamestnanec – senior (APZ v Bratislave)** Predpokladané zapojenie: 6 FTE (FTE bude rozdelené podľa potreby) Predpokladaná priemerná CCP: 25,83 €/hod. **Odborný zamestnanec – junior (APZ v Bratislave)** Predpokladané zapojenie: 6 FTE (FTE bude rozdelené podľa potreby) Predpokladaná priemerná CCP: 21,75 €/hod. **Odborný zamestnanec na DoPMPP (APZ v Bratislave)** Predpokladané zapojenie: DoPMPP - 12 555 osobohodín Predpokladaná priemerná CCP: 54,38 €/hod. Kalkulácia mzdových nákladov pracovníkov vychádza na základe údajov z predchádzajúcich projektov podobného zamerania a mzdovej politiky APZ v Bratislave. Cena práce je obvyklá v danom mieste a čase. Indikatívny počet FTE/osobohodín predstavuje predpokladaný objem vykonávania činnosti na danej pozícii počas celej doby implementácie príslušnej aktivity projektu, so zohľadnením prípadného postupného obsadenia pracovných pozícií.

521 - Mzdové výdavky **(MV SR)**	3 085 157,94 EUR	Skupina výdavkov zahŕňa výdavky na mzdové kapacity na realizáciu aktivít projektu (celková cena práce vrátane odmien v súlade podmienkami stanovenými v Príručke pre Prijímateľa) a to v nasledovnej predpokladanej štruktúre: **Koordinátor odborných aktivít (MV SR)** Predpokladané zapojenie: 1 FTE Predpokladaná priemerná CCP: 33,99 €/hod. **Obsahový garant (MV SR)** Predpokladané zapojenie: 1 FTE Predpokladaná priemerná CCP: 33,99 €/hod. **Odborný zamestnanec – senior (MV SR)** Predpokladané zapojenie: 10 FTE (FTE bude rozdelené podľa potreby) Predpokladaná priemerná CCP: 28,00 €/hod. **Odborný zamestnanec na DoPMPP (MV SR)** Predpokladané zapojenie: DoPMPP – 9 975 osobohodín Predpokladaná priemerná CCP: 54,38 €/hod. Kalkulácia mzdových nákladov pracovníkov vychádza na základe údajov z predchádzajúcich projektov podobného zamerania a mzdovej politiky MV SR. Cena práce je obvyklá v danom mieste a čase. Indikatívny počet osobohodín predstavuje predpokladaný objem vykonávania činnosti na danej pozícii počas celej doby implementácie príslušnej aktivity projektu, so zohľadnením prípadného postupného obsadenia pracovných pozícií.
956 - Paušálna sadzba na pokrytie zostávajúcich oprávnených nákladov projektu podľa článku 56 NSU (nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1060) **(APZ v Bratislave)**	2 480 086,91 EUR	Paušálna sadzba na pokrytie zostávajúcich oprávnených výdavkov projektu podľa článku 56 NSU vo výške 40 % - predpokladáme, že bude využitá najmä na nasledovné typy skupín výdavkov: 013 – Softvér, 022 - Samostatné hnuteľné veci a súbor hnuteľných vecí, 112 – Zásoby, 512 - Cestovné náhrady, 518 - Ostatné služby, 521 - Mzdové výdavky.
956 - Paušálna sadzba na pokrytie zostávajúcich oprávnených nákladov projektu podľa článku 56 NSU (nariadenie Európskeho parlamentu a Rady (EÚ) 2021/1060) **(MV SR)**	1 234 063,18 EUR	Paušálna sadzba na pokrytie zostávajúcich oprávnených výdavkov projektu podľa článku 56 NSU vo výške 40 % - predpokladáme, že bude využitá najmä na nasledovné typy skupín výdavkov: 013 – Softvér, 022 - Samostatné hnuteľné veci a súbor hnuteľných vecí, 112 – Zásoby, 512 - Cestovné náhrady, 518 - Ostatné služby, 521 - Mzdové výdavky.
Hlavné aktivity spolu		
Podporné aktivity		
skupina výdavkov	N/A	N/A
skupina výdavkov	N/A	N/A

Podporné aktivity SPOLU	N/A	
CELKOM		

13.Ďalšie informácie o národnom projekte

Definuje riadiaci orgán / sprostredkovateľský orgán, ak je to relevantné, v nadväznosti na zameranie projektu (napr. v prípade IT projektov odkaz na dokumentáciu projektu dostupnú v Metainformačnom systéme Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky https://metais.vicepremier.gov.sk/).