Zámer národného projektu[1]

Názov národného projektu (ďalej aj „NP“): Zvyšovanie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti u zamestnancov verejnej správy

Žiadateľ[2]:

Obchodné meno/názov	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
Právna forma	rozpočtová organizácia
Sídlo	Pribinova 25
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	
Právna forma	
Sídlo	
IČO	
Zdôvodnenie potreby partnera NP	
Kritériá pre výber partnera[3]	
Má partner jedinečné postavenie na implementáciu týchto aktivít? Ak áno, na akom základe?	

V prípade viacerých partnerov, doplňte údaje za každého partnera.

Sumárne informácie o národnom projekte

Celkové oprávnené výdavky NP (v EUR)	6 698 732,52 €
Miesto realizácie projektu (na úrovni kraja, resp. celá SR)	Celá SR
Identifikácia hlavných cieľových skupín (ak relevantné)	- zamestnanci verejnej správy[4], - odborní zamestnanci verejnej správy: a.) IT zamestnanci b.) zamestnanci v oblasti kybernetickej a informačnej bezpečnosti Zamestnancom verejnej správy sa rozumie: Zamestnanec – fyzická osoba len na ustanovený pracovný čas zamestnávateľa – pracovný pomer, služobný pomer, okrem dohôd o vykonaní prác mimo pracovného pomeru.

[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 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, alebo osoba, ktorá predkladá projektový zámer.

[3] 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 o verejnom obstarávaní.

[4] Verejnou správou sa rozumie: právnické osoby zapísané v registri organizácií vedenom Štatistickým úradom Slovenskej republiky v zmysle § 3 ods. 1 písmena a) až c) zákona č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

	Zamestnanci subjektov, ktorých činnosti nepodliehajú prieskumu čl. 107 (1) ZFEU (ak subjekt vykonáva zmiešané činnosti, tak oprávnení sú tí zamestnanci, ktorí sa podieľajú na činnostiach nespĺňajúcich podmienky pre uplatnenie čl. 107 (1) ZFEU
Projekt so špecifickým určením pre marginalizované rómske komunity[5]	nie

Začlenenie národného projektu v štruktúre Programu Slovensko 2021 – 2027[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	RSO1.2 Využívanie prínosov digitalizácie pre občanov, podniky, výskumné organizácie a orgány verejnej správy
Opatrenie (ak relevantné)	1.2.1 Podpora v oblasti informatizácie a digitálnej transformácie
Súvisiace typy akcií[8]	zlepšovanie technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti KIB v prostredí orgánov štátnej a verejnej správy

Zákonné požiadavky (§ 23 ods. 3 zákona č. 121/2022 Z. z.)

1. Dôvod určenia prijímateľa národného projektu[9]

Jednoznačne a stručne zdôvodnite výber prijímateľa NP ako jedinečnej osoby oprávnenej na realizáciu NP (napr. odkazom na Program Slovensko 2021 – 2027, v ktorom je priamo uvedený prijímateľ; odkazom na platné predpisy, podľa ktorých má prijímateľ osobitné, jedinečné / unikátne kompetencie na implementáciu aktivít NP priamo zo zákona; odkazom na národnú stratégiu, ktorá odôvodňuje jedinečnosť prijímateľa NP a pod.).

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

[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,
- "**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, Rámec implementácie fondov a metodický dokument č. 2 riadiaceho orgánu pre Program Slovensko 2021 – 2027 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 2021 – 2027, alebo ktorého kompetencie nevyplývajú z osobitných predpisov podľa zákona č. 121/2022 Z. z., príslušná komisia pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 schválením zámeru NP schvaľuje aj prijímateľa NP. V opačnom prípade sa prijímateľ NP neposudzuje.

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 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 národného projektu

Vysvetlite, prečo je nevyhnutné realizovať NP, prípadne ako budú využité výstupy projektu.

Podľa Správy o kybernetickej bezpečnosti v Slovenskej republike v roku 2023, Národného bezpečnostného úradu, vychádza že: „Sektor verejná správa má spomedzi všetkých sektorov najhoršie hodnotenia auditovaných požiadaviek. V tomto sektore je vykazovaných 47 % súladov a 16 % čiastočných súladov, počet nesúladov auditovaných položiek tvoril 26 %.“[10]

V správe sa tiež uvádza, že najvyšší počet hlásených kybernetických bezpečnostných incidentov v roku 2023 pochádzalo zo sektorov verejná správa, bankovníctvo a zdravotníctvo.

Dlhodobé zanedbanie sa podpísalo na kritickom stave kybernetickej bezpečnosti v sektore verejná správa. Jej podstatnosť si neuvedomujú najmä malé samosprávy a menší prevádzkovatelia a prenášajú zodpovednosť na externé firmy, avšak výnimkou nie sú ani veľkí prevádzkovatelia v tomto podsektore vrátane štátnych inštitúcií „Celkové riadenie kybernetickej bezpečnosti chýba, je chaotické alebo neúplné.“[11]

[10] *SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI v Slovenskej republike v roku 2023, str. 36,* sprava-o-kybernetickej-bezpecnosti-v-sr-2023.pdf

[11] *SPRÁVA O KYBERNETICKEJ BEZPEČNOSTI v Slovenskej republike v roku 2023, str. 13-17*

Ďalej sa v dokumente Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 spomína: „Kybernetická bezpečnosť nemôže fungovať bez existencie mechanizmov na národnej úrovni, ktoré určujú politiku kybernetickej bezpečnosti, systém jej riadenia, ale aj procesy na detekciu a riešenie kybernetických bezpečnostných incidentov, **budovanie odborných kapacít a šírenie situačného a bezpečnostného povedomia**."

Preto je podľa uvedenej stratégie nutné **„Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti nielen na národnej, ale aj sektorovej úrovni."** Tento cieľ sa dosiahne pomocou „Vypracovania koncepcie vzdelávania personálu vo verejnej správe zameranú na prijímanie, udržanie, zabezpečenie a kariérny rast, ako aj zvyšovanie a udržiavanie jeho odbornej spôsobilosti."

„Vzdelávanie zamestnancov verejnej správy nie je systematické, neexistuje systém základného bezpečnostného vzdelávania pre úradníkov verejnej správy, ktorí denne pracujú s informačnými systémami verejnej správy a prichádzajú do kontaktu s citlivými a osobnými údajmi."

Národná stratégia kybernetickej bezpečnosti na roky 2021 – 2025 označuje doplnenie odborných kapacít vo verejnej správe za základnú súčasť zvyšovania kybernetickej bezpečnosti verejnej správy. [12]

Cieľový stav: Vzdelaní zamestnanci verejnej správy, ktorí vedia bezpečne poskytovať služby a používať systémy verejnej správy bez vzniku kybernetických bezpečnostných incidentov, ktoré vznikli kvôli ich nízkemu bezpečnostnému povedomiu.

Cieľ je dosiahnuteľný prostredníctvom:

a) vytvorenia systému odborného špecializovaného vzdelávania pre odborníkov v oblasti kybernetickej a informačnej bezpečnosti,
b) vytvorenia systému vzdelávania zamestnancov verejnej správy tak, aby spĺňali minimálne vedomostné štandardy v oblasti kybernetickej a informačnej bezpečnosti.[13]

Okrem spomenutého, Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 potvrdzuje, že vzdelaní odborníci a verejnosť sú jedným z hlavných cieľov Slovenskej republiky v oblasti kybernetickej bezpečnosti. Úlohou v tomto cieli je vzdelávanie a zvyšovanie bezpečnostného povedomia zamestnancov verejnej správy. Obsahom tejto úlohy je okrem iného zvyšovanie bezpečnostného povedomia pre pracovníkov verejnej správy v oblasti získavania odborných kompetencií a minimálnych vedomostných štandardov v oblasti kybernetickej bezpečnosti vrátane doplnkového vzdelávania špecialistov kybernetickej bezpečnosti. Zodpovedným subjektom pre túto úlohu je MIRRI SR.[14]

Na základe vyššie uvedeného je potrebné vzdelávať zamestnancov v sektore verejná správa od úrovne laika - základných znalostí až po úroveň odborného zamestnanca v relevantných oblastiach týkajúcich sa kybernetickej a informačnej bezpečnosti (legislatívna, prevádzková, riadiaca, technická/technologická a pod.)

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

Zdôvodnite, prečo je vhodnejšie realizovať NP ako využitie „súťažného postupu prostredníctvom výzvy (napr. porovnanie oboch spôsobov realizácie projektu, efektívnejšie a hospodárnejšie využitie finančných prostriedkov, efektívnosť služby poskytovanej cieľovej skupine, zabezpečenie štandardov kvality a pod.).

---

[13] *Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025 str. 11 – 20,* 2759.pdf (gov.sk)
[14] *Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 str.25,* 397.pdf (gov.sk)

Tento projekt súvisí najmä s naplnením povinností definovanými v zákone č.69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a v zákone č.95/2019 Z. z. Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.

Aktuálne nie je k dispozícii jednotný a centrálny školiaci systém, ktorý by umožnil celoplošné školenia zamestnancov verejnej správy až po úroveň odborného zamestnanca v relevantných oblastiach týkajúcich sa kybernetickej a informačnej bezpečnosti (legislatívna, prevádzková, riadiaca, technická/technologická a pod.).

Projekt pripravuje predpoklady pre: zabezpečenie zvyšovania bezpečnostného povedomia zamestnancov verejnej správy prostredníctvom školení a zabezpečenie špecializovaných školení v oblasti kybernetickej a informačnej bezpečnosti pre odborných zamestnancov verejnej správy v relevantných oblastiach týkajúcich sa kybernetickej a informačnej bezpečnosti (legislatívna, prevádzková, riadiaca, technická/technologická a pod.).

Hlavným cieľom tohto NP je zvýšenie povedomia, znalostí, praktickej a metodickej pripravenosti na kybernetické útoky a hrozby zamestnancov verejnej správy. Daný cieľ je efektívnejšie dosiahnuteľný prostredníctvom centralizovaného spôsobu, teda projektu zameraného na zvyšovanie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti, kde bude mať každý orgán verejnej moci (ďalej len „OVM“) možnosť využitia a nebude nutné daný cieľ realizovať v každom OVM separátne. Realizácia vzdelávacích aktivít jednotlivých OVM samostatne by priniesla nejednotnosť definovania vzdelávacích cieľov, nehomogénny prístup k vzdelávacím aktivitám na rôznych úrovniach a nebolo by možné vytvoriť jednotný systém vzdelávania zamestnancov verejnej správy. Z časového hľadiska je vyššie riziko nedosiahnutia stanovených cieľov, nakoľko by sa museli jednotlivé OVM venovať definovaniu opisu obstarávania služieb v ktorých mnohé z nich nemajú potrebnú skúsenosť a expertízu. Znamenalo by to násobné vyššie náklady na obstarávania a tiež riziko nenaplnenia definovaných cieľov.

4. Odôvodnenie rozhodnutia nezapojiť partnerov do implementácie aktivít

Ak nezapojíte do implementácie aktivít NP niektorého z partnerov podľa článku 8 nariadenia o spoločných ustanoveniach[15], zdôvodnite ich nezapojenie. V prípade, ak žiadateľ spolupracoval s partnermi už pri príprave zámeru NP, uvedie informáciu o ich zapojení v tejto časti.

Konkrétne ide o:

- *regionálne, miestne, mestské a ostatné orgány verejnej správy;*
- *hospodárskych a sociálnych partnerov;*
- *subjekty, ktoré zastupujú občiansku spoločnosť;*
- *výskumné organizácie a univerzity.*

Cieľ projektu je efektívnejšie dosiahnuteľný prostredníctvom centralizovaného spôsobu, teda tvorba projektu zameraného na zvyšovanie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti, kde bude mať každé OVM možnosť využitia a nebude nutné daný cieľ realizovať v každom OVM separátne.

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

Popis národného projektu

5. Východiskový stav

[15] *Nariadenie EP a Rady (EÚ) 2021/1060.*

a. Uveďte východiskové dokumenty na regionálnej, národnej a európskej úrovni, ktoré priamo súvisia s realizáciou NP:

1. Program Slovensko 2021 – 2027,

2. Národná stratégia kybernetickej bezpečnosti na roky 2021-2025,

3. Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025,

4. Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023,

5. Národná koncepcia informatizácie verejnej správy (ďalej ako „NKIVS"),

6. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov,

7. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

b. Uveďte predchádzajúce výstupy z dostupných analýz, na ktoré nadväzuje navrhovaný zámer NP (štatistiky, analýzy, štúdie,...):

Zámer NP nadväzuje na projekt „Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS", ďalej tiež ako „VaŠS". Jednou z aktivít bolo aj poskytovanie školení pre zamestnancov verejnej správy v oblasti kybernetickej a informačnej bezpečnosti. Daná aktivita bola úspešne ukončená a na základe vysokého záujmu o konkrétne školenia a zozbieranej spätnej väzby od účastníkov sme zistili, že realizácia vybraných školení je veľmi potrebná a vítaná zo strany zamestnancov verejnej správy. Rozpočet na danú aktivitu a merateľné ukazovatele boli splnené. Nakoľko záujem o predmetné školenia zo strany zamestnancov verejnej správy prevýšil očakávania, bol uskutočnený prieskum záujmu o ďalšie školenia v oblasti kybernetickej a informačnej bezpečnosti pre zamestnancov verejnej správy a to prostredníctvom dotazníka spätnej väzby, ktorý bol zaslaný na všetky orgány verejnej moci začiatkom roka 2024. Z daného dotazníka vyplynulo, že vysoký záujem pretrváva a taktiež je záujem o školenia pre odborných zamestnancov v oblasti kybernetickej a informačnej bezpečnosti. Oslovených bolo 7840 subjektov verejnej správy. Dotazník vyplnilo a odpoveď odoslalo 1086 subjektov verejnej správy. Z výstupov dotazníkov sme získali 10 najčastejšie sa opakujúcich tém, resp. typy školení, ktoré budú v tomto projekte realizované. OVM uvideli počty zamestnancov, ktorých považujú za nutné vzdelávať na rôznych úrovniach.

Najčastejšie požadované oblasti na školenia, o ktoré bol v rámci prieskumu najväčší záujem zo strany subjektov VS:

1. **Základy kybernetickej bezpečnosti:** Pre bežných užívateľov PC, ktorí nemajú IT v pracovnej náplni, sú len bežní užívatelia PC..

2. **Legislatíva a trendy v oblasti kybernetickej bezpečnosti:** Právne aspekty - aplikácia legislatívy v oblasti kybernetickej bezpečnosti pre laikov.

3. **Školenia týkajúce sa systémov, sietí a kybernetickej bezpečnosti, ktoré zahŕňajú aj certifikáciu:** Akékoľvek zo školení uvedených v ponuke, s dôrazom na ochranu osobných údajov alebo technické a personálne bezpečnostné opatrenia. Napríklad školenia od SANS inštitútu, napríklad FOR508: Advanced Incident Response, Threat Hunting a Digital Forensics.

4. **Informačná bezpečnosť a jej aplikácia v praxi vo verejnej správe:** Zamerané na ochranu osobných údajov, Nariadenia GDPR alebo aj technické a personálne bezpečnostné opatrenia.

5. **Bezpečnosť v cloude:** Zahrnuje aj manažéra kybernetickej bezpečnosti.

6. **Umelá inteligencia, Zraniteľnosti na strane aplikácií/klienta/serverov: Prevencia pred útokmi.**

7. **Projektové riadenie IT**: ITIL, TOGAF

8. **Etický hacking, analytické nástroje, kryptografia:** CHFI, CEH: Školenia z oblasti digitálnej forenziky a etického hackovania.

9. **Manažment riadenia rizík:** Dôležité pre prevádzkovateľov základnej služby.

10. **Certifikácie v oblasti IT bezpečnosti:** Comptia Network+, Comptia Security+, CISM, CISSP:

Z dotazníkov sme tiež vedeli určiť predpokladaný počet zamestnancov, ktorých jednotlivé OVM považujú za potrebné preškoliť. OVM uviedli počty zamestnancov potrebných preškoliť v oblasti kybernetickej a informačnej bezpečnosti, kumulatívne 15 500 zamestnancov VS.

Taktiež Zámer NP nadväzuje na projekty v oblasti kybernetickej bezpečnosti, ktoré dodávali hardvér a softvér tým, že zlepší zručnosti pracovníkov, ktorí tieto zariadenia obsluhujú. Tým sa lepšie zhodnotia už realizované a prebiehajúce investície v oblasti kybernetickej a informačnej bezpečnosti.

c. Popíšte problémové a prioritné oblasti, ktoré rieši zámer NP. (Zoznam známych problémov, ktoré vyplývajú zo súčasného stavu a je potrebné ich riešiť):

Cieľom kybernetickej a informačnej bezpečnosti je vybudovať také prostredie, ktoré je schopné čeliť rôznym kybernetickým hrozbám. Okrem hardvérového a softvérového zabezpečenia, ktoré je pevnou súčasťou kybernetickej a informačnej bezpečnosti, je práve ľudský faktor potrebným pilierom v celom tomto systéme. Ten je však častou príčinou incidentov. Preto podľa dokumentu Národná koncepcia informatizácie verejnej správy Slovenskej republiky (ďalej lem „NKIVS“) je jeden z hlavných cieľov „Posilniť ľudské kapacity a vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti“.

Dôvodom realizácie projektu je reakcia na riziko kybernetických incidentov v prostredí verejnej správy ako aj národného hospodárstva.

Na základe NKIVS: Orgán vedenia podľa zákona ITVS je MIRRI. Jeho poslaním je riadny a efektívny výkon riadenia a dosiahnutie cieľov informatizácie a rozvoja ITVS, ktoré vyplývajú z NKIVS a ďalších koncepčných a strategických dokumentov s celoštátnou pôsobnosťou. Zabezpečuje *pripravenosť širšieho IT prostredia vo verejnej správe. Koordinuje rezorty a vymáha ich súčinnosť.*[16]

Oblasť kybernetickej bezpečnosti je neustále v rýchlom trende zmien a neustále sa vyvíjajú nové hrozby kybernetických hrozieb, ako aj trendy na ich elimináciu, resp. zníženie rizík a dopadov na chod organizácie. Realizáciou projektu dôjde k zvýšeniu úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti vo verejnej správe prostredníctvom školení zamestnancov verejnej správy a zabezpečenie špecializovaných školení u príslušných zamestnancov verejnej správy po úroveň odborného zamestnanca v relevantných oblastiach týkajúcich sa kybernetickej a informačnej bezpečnosti (legislatívna, prevádzková, riadiaca, technická/technologická, a pod.)

Z výstupov realizovaných dotazníkov vyplynulo, že až 66% z opýtaných subjektov VS neabsolvovalo žiadne školenie v oblasti KIB za posledné 2 roky. Na druhej strane pozitívne hodnotíme, že až 95% subjektov má záujem (vníma potrebu) o školenia v KIB.

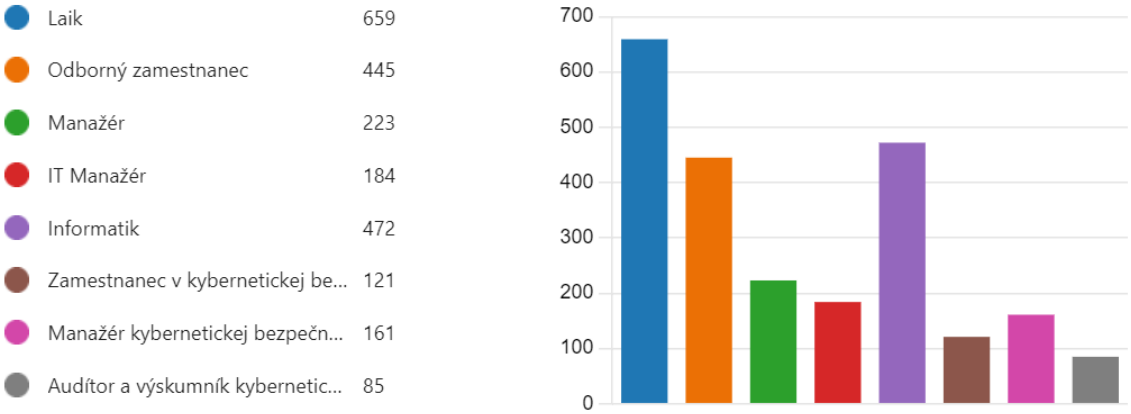
Jedným z cieľov NP je aj posilnenie konkrétnych odborných pozícii v oblasti kybernetickej a informačnej bezpečnosti (Architekt kybernetickej bezpečnosti, Špecialista riadenia rizík, Špecialista pre riešenie kybernetických incidentov, Analytik kybernetickej bezpečnosti, Tester kybernetickej bezpečnosti, Audítor kybernetickej bezpečnosti) z dôvodu že tieto pozície sú dlhodobo nedostatkové. Z vykonaných dotazov subjektov verejnej správy sme zistili, že najväčší záujem o vzdelávanie v oblasti kybernetickej a informačnej bezpečnosti majú 2 kategórie používateľov[17] a to „**laik“** (používateľ informačného systému, ktorý je najzraniteľnejší prvok z pohľadu existujúcich hrozieb a často využívaný prvok

[16] Národná koncepcia informatizácie verejnej správy Slovenskej republiky, str. 37, Microsoft Word - 03_Vlastný materiál_tlacba.docx (gov.sk)

[17] Kategórie používateľov v zmysle vyhlášky č. 492/2022 Z. z. NBÚ SR.

Financovaný Európskou úniou

z pohľadu útočníkov, resp. kybernetických útokov. Druhou najväčšou skupinou používateľov, ktorých vzdelávanie vnímajú OVM za najdôležitejšiu je skupina „**Informatik**“. Detailný pohľad na skupiny používateľov, ktorí majú záujem o školenia KIB:



Obrázok 1 Skupiny používateľov (zamestnancov VS) so záujmom o vzdelávacie aktivity v oblasti KIB

d. Uveďte, na ktoré z ukončených a prebiehajúcich národných projektov[18] zámer NP priamo nadväzuje, v čom je navrhovaný NP od nich odlišný, resp. na ktoré NP čiastočne nadväzuje / prelína sa s nimi v istej časti a ako sú v ňom zohľadnené (čiastkové) výsledky/dopady predchádzajúcich NP (ak je to relevantné):

NP nadväzuje na projekt OPII s názvom „Výcvikové a školiace stredisko pre bezpečnosť prevádzky a správy IT pre sektor VS“. Deliaca línia je v časovom rozmedzí medzi projektami. (Operačný program integrovaná infraštruktúra končil v roku 2023). Projekt je rozšírenou verziou - rozšírenie aktivít, nakoľko boli definované vysoko žiadané oblasti *vzdelávacích aktivít v spomínanom* projekte VaŠS a tie, o ktoré nebol zo strany zamestnancov verejnej správy enormný záujem. Tento projekt nadväzuje na žiadané vzdelávacie aktivity a rozširuje úrovne vzdelania na odborné kapacity – Architekt kybernetickej bezpečnosti, Špecialista riadenia rizík, Špecialista pre riešenie kybernetických incidentov, Analytik kybernetickej bezpečnosti, Tester kybernetickej bezpečnosti a Audítor kybernetickej bezpečnosti. Zároveň je potrebné spomenúť, že vzdelávanie na úroveň Manažéra kybernetickej bezpečnosti nebude v tomto NP oprávnenou aktivitou. V NP môže ísť aj o opakované vzdelávanie tých istých osôb, nakoľko oblasť kybernetickej bezpečnosti je dynamicky sa meniaca a je žiadúce, resp. nevyhnutné, aby sa zamestnanci vzdelávali aj v rovnakých oblastiach s prihliadnutím na aktuálne trendy a aktualizácie.

e. Popíšte administratívnu, finančnú a prevádzkovú kapacitu žiadateľa a partnera (v prípade, ak je v projekte zapojený aj partner):

V projekte žiadateľ plánuje využiť interné kapacity na pozície projektového manažéra, finančného manažéra, administratívneho pracovníka a vedúceho projektovej kancelárie. Nakoľko žiadateľ okrem tohto projektu už v minulosti realizoval a tiež realizuje viacero projektov v oblasti kybernetickej a informačnej bezpečnosti a IT, je zrejmé, že disponuje dostatočnou administratívnou, organizačnou a finančnou kapacitou.

[18] V prípade, ak je to relevantné, uveďte aj ukončené národné projekty z programového obdobia 2014 – 2020.

6. Hlavné ciele NP (stručne):

V tejto časti popíšte očakávané ciele a očakávané výstupy / výsledky projektu. Popíšte prínos projektu pre napĺňanie cieľov a výsledkov príslušnej priority / špecifického cieľa / opatrenia Programu Slovensko 2021 – 2027, ako aj súvisiacich strategických dokumentov na národnej úrovni (ak je to relevantné).

Hlavným cieľom tohto NP je zvýšenie povedomia, znalostí, praktickej a metodickej pripravenosti na kybernetické útoky a hrozby zamestnancov verejnej správy. Daný cieľ je efektívnejšie dosiahnuteľný prostredníctvom centralizovaného spôsobu, teda projektu zameraného na zvyšovanie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti, kde bude mať každé OVM možnosť využitia poskytovaných vzdelávacích aktivít a nebude nutné daný cieľ realizovať v každom OVM separátne.

Zabezpečením širokého spektra vzdelávacích aktivít (od všeobecných až po špecializované školenia) zamestnancov verejnej správy na príslušnú úroveň, dôjde k zvýšeniu znalosti a zručnosti potrebných na posudzovanie a zvýšenie úrovne kybernetickej a informačnej bezpečnosti vo verejnej správe.

Zabezpečením pravidelného, zjednoteného a odborne zastrešeného vzdelávania zamestnancov verejnej správy, zvýšime schopnosť prípravy bezpečnostných opatrení na aktuálne hrozby a tiež relevantné reakcie na kybernetické hrozby. Realizácia NP zabezpečí spoľahlivejší výkon riadenia kybernetickej a informačnej bezpečnosti z pozície MIRRI, ako garanta pre sektor verejná správa a taktiež aj z pozície jednotlivých orgánov verejnej moci.

7. Merateľné ukazovatele NP a iné údaje

V tabuľke nižšie uveďte merateľné ukazovatele projektu a iné údaje. Poskytovateľ v spolupráci so žiadateľom uvádzajú povinne minimálne jeden merateľný ukazovateľ projektu – výstup a minimálne jeden merateľný ukazovateľ projektu výsledok[19]. Merateľné ukazovatele projektu musia byť definované tak, aby odrážali výstupy/výsledky projektu a predstavovali kvantifikáciu toho, čo sa realizáciou aktivít za požadované výdavky dosiahne[20].

Zoznam merateľných ukazovateľov projektu

Typ merateľného ukazovateľa projektu	Kód merateľného ukazovateľa projektu[21]	Názov merateľného ukazovateľa projektu	Merná jednotka merateľného ukazovateľa projektu	Indikatívna cieľová hodnota[22]
výstup	PSKPSOI12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	verejné inštitúcie	200
výsledok	PSKPxy	Účastníci, ktorí absolvovali vzdelávaciu aktivitu so	počet	7 430

[19] Všeobecne v prípade merateľného ukazovateľa projektu – výsledok s výnimkou projektov technickej pomoci (okrem aktivít technickej pomoci zameraných na financovanie informačných systémov, CPV, vzdelávania administratívnych kapacít a materiálovo-technického zabezpečenia), projektov návratnej finančnej pomoci a projektov, ktorých cieľová skupina je totožná s účastníkom projektu, ktorá bude monitorovaná prostredníctvom spoločných merateľných ukazovateľov programu – výsledku v súlade s prílohou I nariadenia EP a Rady (EÚ) 2021/1057 o ESF+ (karta účastníka) a súčasne platí jedna z dvoch nasledujúcich pod podmienok: projekty sú financované z ESF+, alebo projekty sú financované FST v súlade s čl. 8 písm. k) až m) nariadenia EP a Rady (EÚ) 2021/1056 o FST. Povinnosť stanovenia minimálne jedného výsledkového merateľného ukazovateľa projektu s výnimkou zámerov národných projektov:
• nepredstavujúcich investíciu do výroby a infraštruktúry;
• v rámci, ktorých cieľová skupina je totožná s účastníkom projektu a súčasne platí jedna z dvoch nasledujúcich pod podmienok: projekty sú financované z ESF+, alebo projekty sú financované FST v súlade s článkom 8 písm. k) až m) nariadenia o FST.

[20] V odôvodnených prípadoch sa uvedená tabuľka nevypĺňa, pričom je nevyhnutné do tejto časti uviesť podrobné a jasné zdôvodnenie, prečo nie je možné uviesť požadované údaje.

[21] 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“.

[22] 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.

		zameraním na kybernetickú a informačnú bezpečnosť		

Zoznam iných údajov projektu (ak relevantné)

Kód iného údaja[23]	Názov iného údaja	Merná jednotka iného údaja

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

Cieľová skupina	Počet[24]	Prínos
1.) zamestnanci verejnej správy, 2.) odborní zamestnanci verejnej správy: a.) IT zamestnanci, b.) zamestnanci v oblasti kybernetickej a informačnej bezpečnosti	7 430	Zlepšenie kvality vedomostnej úrovne v oblasti kybernetickej a informačnej bezpečnosti

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

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)	Realizácia aktivity od – do[25]
Vyškolenie/školenia zamestnancov verejnej správy	Zvýšenie úrovne odbornosti v oblasti kybernetickej a informačnej bezpečnosti vo verejnej správe prostredníctvom školení zamestnancov verejnej správy a zabezpečenie špecializovaných školení u príslušných zamestnancov verejnej správy po úroveň odborného zamestnanca v relevantných oblastiach týkajúcich sa kybernetickej a informačnej bezpečnosti (legislatívna, prevádzková, riadiaca, technická/technologická, a pod.)	Realizácia prostredníctvom školení. Školenia: governacne, technické a špecializované školenia: Architekt kybernetickej bezpečnosti, Špecialista riadenia rizík, Špecialista pre riešenie kybernetických incidentov, Analytik kybernetickej bezpečnosti, Tester kybernetickej bezpečnosti, Audítor kybernetickej bezpečností	01/2025 – 06/2027

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

b. Uveďte detailnejší popis aktivít.

[23] Ak iný údaj ešte nemá pridelený kód, uvádza sa „n/a“.
[24] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.
[25] Údaj uveďte v mesiacoch, počítaných od začiatku realizácie projektu (napr. 3 – 24), alebo informáciou o realizácii aktivity počas celého projektu, aby bolo zrejmá časová nadväznosť aktivít (ak je to relevantné).

Okrem detailnejšieho popisu každej oprávnenej hlavnej aktivity uveďte, ako je v projekte zabezpečené dodržiavanie horizontálnych princípov podľa čl. 9 nariadenia o spoločných ustanoveniach, ako aj podľa uznesenia vlády SR č. 668 z 26. októbra 2022.

Ak po schválení zámeru NP komisiou pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 dôjde k podstatnej zmene v rozsahu hlavných aktivít NP uvedených vyššie (t. j. minimálne jedna hlavná aktivita nebude v rámci NP realizovaná, resp. má dôjsť k výraznému zväčšeniu alebo zmenšeniu rozsahu schválených aktivít, príp. doplneniu novej aktivity), riadiaci orgán / sprostredkovateľský orgán predloží pred vyhlásením výzvy na schválenie príslušnej komisii pri Monitorovacom výbore pre Program Slovensko 2021 – 2027 upravený zámer NP. Z dôvodu zabezpečenia overenia dodržania vyššie uvedenej zásady poskytovateľ vo výzve na predkladanie ŽoNFP v rámci relevantnej podmienky poskytnutia príspevku zadefinuje hlavné aktivity schváleného zámeru NP ako povinné hlavné aktivity projektu.

Doplňujúce informácie k zneniu vylučujúceho kritéria horizontálnych princípov:

Dodržiavanie horizontálnych princípov

V rámci projektu bude zabezpečené dodržiavanie horizontálnych princípov v súlade so Základným mechanizmom na zabezpečenie dodržiavania Horizontálnych princípov v Programovom období 2021 – 2027 a základných horizontálnych podmienok.

10. Predpokladaný časový rámec

Predpokladaný dátum vyhlásenia výzvy vo formáte mesiac/rok	09/2024
Predpokladaná doba realizácie NP v mesiacoch	30

Termíny v tabuľke nie sú záväzné.

11. Finančný rámec[26]

Fond	Európsky fond regionálneho rozvoja	
Celkové oprávnené výdavky NP podľa kategórie regiónu[27] (v EUR)	menej rozvinutý región	5 167 402,27 €
	viac rozvinutý región	1 531 330,25 €
Zdroj EÚ podľa kategórie regiónu[28] (v EUR)	menej rozvinutý región	4 392 291,92[29] €
	viac rozvinutý región	612 532,10 €
Vlastné zdroje prijímateľa[30] podľa kategórie regiónu[31] (v EUR)	neaplikuje sa	-
	neaplikuje sa	

12. Rozpočet

V tejto časti uveďte, ako bol pripravovaný indikatívny rozpočet a ako spĺňa kritérium „hodnota za peniaze“, t. j. akým spôsobom bola odhadnutá cena za každú položku, napr. prieskum trhu, analýza minulých výdavkov spojených s podobnými aktivitami, nezávislý znalecký posudok. V prípade, ak príprave projektu predchádza vypracovanie štúdie uskutočniteľnosti, ktorej výsledkom je, okrem iného aj určenie výšky alokácie, je potrebné uviesť túto štúdiu ako zdroj určenia výšky finančných prostriedkov. Skupiny výdavkov doplňte v súlade s Príručkou oprávnenosti výdavkov v platnom znení.

[26] 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.
[27] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[28] V prípade Kohézneho fondu vyberte „neaplikuje sa“.
[29] Vzhľadom na výšku alokácie zdrojov v prospech viac rozvinutého regiónu v opatrení 1.2.1 bude alokácia za viac rozvinutý región hradená z vlastných zdrojov žiadateľa/prijímateľa.
[30] 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
[31] V prípade Kohézneho fondu vyberte „neaplikuje sa“.

V prípade infraštruktúrnych projektov, ako aj projektov súvisiacich s obnovou mobilných prostriedkov, sa do ukončenia verejného obstarávania uvádzajú položky rozpočtu len do úrovne aktivít.

Uveďte, či bude v národnom projekte využité zjednodušené vykazovanie výdavkov a ak áno, ktorá forma. V prípade využitia paušálnej sadzby ktorej výška je stanovená v nariadení sa spôsob stanovenia sadzby nepožaduje.

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		
skupina výdavkov: 518 Ostatné služby: školenia	5 832 217,00 € (vrátane DPH)	Školenia – suma bola vypočítaná na základe indikatívneho prieskumu trhu a predpokladaných počtov účastníkov na jednotlivých školeniach. Školenia sú rozdelené na tzv. všeobecné a špecializované. Každé školenia má iný počet účastníkov a aj inú cenu za školenie / 1 účastník.
skupina výdavkov: 521 Mzdové náklady: priame výdavky	428 280,69 €	Cena práce – bola vypočítaná na základe predpokladaného počtu hodín (na obdobie 30 mesiacov – r. 2025 + r. 2026 + 6 mesiacov v r. 2027) a bežnej hodinovej sadzby zavedenej na MIRRI SR pri uzatváraní dohôd v zmysle ZP.
Hlavné aktivity spolu	6 260 497,69 €	
Podporné aktivity		
skupina výdavkov: 907: nepriame (paušálne) výdavky	438 234,83 €	Na financovanie nepriamych nákladov projektu sa použije paušálna sadzba v súlade s článkom 54 písm. a) Nariadenia Európskeho parlamentu a Rady (EÚ) 2021/1060, ktorým sa stanovujú spoločné ustanovenia o EFRR, ESF+, Kohéznom fonde, FST a ENRAF a rozpočtové pravidlá pre uvedené fondy, ako aj pre Fond pre azyl, migráciu a integráciu, Fond pre vnútornú bezpečnosť a Nástroj finančnej podpory na riadenie hraníc a vízovú politiku, t. j. na pokrytie nepriamych nákladov projektu sa použije paušálna sadzba až do výšky 7 % oprávnených priamych nákladov projektu, a to bez nutnosti vykonať výpočet na určenie uplatniteľnej sadzby.
Podporné aktivity SPOLU	438 234,83 €	
CELKOM	6 698 732,52 €	

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.

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 MIRRI SR https://metais.vicepremier.gov.sk/).

N/A