Zámer národného projektu
Operačného programu Integrovaná infraštruktúra Prioritná os 7 Informačná spoločnosť

Názov národného projektu: Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe

1. Zdôvodnite čo najpodrobnejšie prečo nemôže byť projekt realizovaný prostredníctvom výzvy na predkladanie žiadostí o NFP?
   (napr. porovnanie s realizáciou prostredníctvom dopytovo orientovaného projektu vzhľadom na efektívnejší spôsob napĺňania cieľov OP, efektívnejšie a hospodárnejšie využitie finančných prostriedkov)

Hlavným cieľom národného systému riadenia incidentov kybernetickej bezpečnosti vo VS je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej aj „jednotky CSIRT“) pre podsektor Informačné systémy verejnej správy (ďalej aj „ISVS“) podľa prílohy č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti“). Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe predstavuje prvú strategickú fázu budovania celonárodného systému riadenia incidentov kybernetickej bezpečnosti. Prostredníctvom tejto fázy budovania celonárodného systému budú pokryté preventívne a reaktívne služby pre podsektor ISVS.
Projekt je navrhnutý ako národný projekt, ktorého cieľovou skupinou sú tieto zainteresované strany:

- prevádzkovatelia jednotiek CSIRT zapojené do národného systému,
- prevádzkovatelia informačných systémov verejnej správy v pôsobnosti jednotlivých jednotiek CSIRT.

Tento projekt v kontexte NKIVS prispieva k realizácii priority informatizácie verejnej správy „Formovanie infraštruktúry“ a je plne v súlade so všetkými tromi strategickými cieľmi „prevencia“, „pripravenosť“ a „udržateľnosť“ Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike, ktorú odkazuje NKIVS. V rámci OPII projekt prispieva k naplneniu výsledkov špecifického cieľa 7.9 „Zvýšenie kybernetickej bezpečnosti v spoločnosti“, ktorými sú:

- zníženie finančných dopadov a dopadov na inštitúcie verejnej správy pri bezpečnostných incidentoch,
- zvýšenie vyspelosti trhu s bezpečnostnými riešeniami zvýšením výdavkov na bezpečnosť verejného sektora,
- zvýšenie kybernetickej bezpečnosti a aplikovanie najnovších poznatkov v európskom priestore,
- zvýšenie miery inovácie v oblasti bezpečnostných opatrení,
- zvýšenie dôvery občanov a podnikateľov v digitálny priestor,
- zvýšenie transparentnosti pri riešení bezpečnostných incidentov a kybernetických útokov.

Projekt je taktiež plne v súlade i so zásadným dokumentom kybernetickej bezpečnosti Slovenskej republiky Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 schváleným vládou SR.

Komplexné zabezpečenie kybernetickej bezpečnosti v rámci jednotlivých vecných oblastí musí pokryť výkon verejnej moci a výkon odborných činností. Pre naplnenie tohto ambiciózneho a náročného cieľa je potrebné technicky a znalostne posilniť jednotky CSIRT, ktoré budú súčasťou národného systému a technicky i organizačne zabezpečiť ich komunikáciu. Úlohou jednotiek CSIRT je vykonávanie preventívnych a reaktívnych opatrení v oblasti svojho pôsobenia a poskytovanie relevantných informácií o kybernetických incidentoch národnej jednotke CSIRT a vládnej jednotke CSIRT. Štruktúra jednotiek CSIRT, ktoré budú súčasťou projektu bola navrhnutá tak, aby bolo možné efektívne poskytovať preventívne a reaktívne služby definované v § 15 zákona o kybernetickej bezpečnosti pre podsektor ISVS.
Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe budú tvoriť tieto jednotky CSIRT:

- SK-CERT – národná jednotka CSIRT, ktorej prevádzkovateľom je Národný bezpečnostný úrad,
- CSIRT.SK – vládna jednotka CSIRT v pôsobnosti ÚPPVII, ktorá je súčasne jednotkou CSIRT pre podsektor ISVS,
- CSIRT SIS – sektorová jednotka CSIRT v pôsobnosti Slovenskej informačnej služby, ktorá zabezpečuje spravodajské činnosti kybernetickej bezpečnosti pre podsektor ISVS,
- GOV CERT SK – jednotka CSIRT zriadená Národnou agentúrou pre sieťové a elektronické služby, prevádzkovateľom základnej služby zabezpečujúca činnosti kybernetickej bezpečnosti pre kľúčové stavebné prvky e-Governmentu, ktorými sú Ústredný portál verejnej správy a vládna sieť Govnet.

Je dôležité poznamenať, že v ďalších fázach rozširovania celonárodného systému sa uvažuje so zapojením ďalších sektorových jednotiek CSIRT v gescii príslušných ústredných orgánov podľa zákona o kybernetickej bezpečnosti, ktoré môžu zvýšenie vlastnej vyspelosti riešiť či už prostredníctvom národných projektov alebo dopytovo-orientovaných výziev.

2. Príslušnosť národného projektu k relevantnej časti operačného programu

Prioritná os	7 Informačná spoločnosť
Investičná priorita	Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva
Špecifický cieľ	*7.9 Zvýšenie kybernetickej bezpečnosti v spoločnosti*
Miesto realizácie projektu (na úrovni kraja)	Banskobystrický kraj Bratislavský kraj Nitriansky kraj Košický kraj Prešovský kraj Trenčiansky kraj Trnavský kraj Žilinský kraj
Identifikácia hlavných cieľových skupín (ak relevantné)	Inštitúcie a subjekty verejnej správy

3. Prijímateľ[1] národného projektu **Úrad podpredsedu vlády SR pre investície a informatizáciu**

[1] V tomto dokumente je používaný pojem prijímateľ a žiadateľ. Je to tá istá osoba, no technicky sa žiadateľ stáva prijímateľom až po podpísaní zmluvy o NFP.

Dôvod určenia prijímateľa národného projektu[2]	Hlavnými dôvodmi pre určenie prijímateľa národného projektu sú: • ÚPPVII je ústredným orgánom štátnej správy pre oblasť riadenia bezpečnosti ISVS podľa kompetenčného zákona a zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisoch, • ÚPPVII je ústredným orgánom pre oblasť kybernetickej bezpečnosti v sektore ISVS podľa zákona o kybernetickej bezpečnosti, • prevádzkuje zo zákona zriadenú vládnu jednotku CSIRT, ktorá poskytuje služby pre ISVS podľa zákona o kybernetickej bezpečnosti, • v spojení s povinnosťami každého správcu ISVS je ÚPPVII svojho druhu regulátorom a celoslovensky pôsobiacim orgánom pre oblasť bezpečnosti a riešenia kybernetických incidentov vo vzťahu k ISVS.
Má prijímateľ osobitné, jedinečné kompetencie na implementáciu aktivít národného projektu priamo zo zákona, osobitných právnych predpisov, resp. je uvedený priamo v príslušnom operačnom programe?	Áno, viď vyššie. Prijímateľ národného projektu bude ÚPPVII v zmysle zákona o kybernetickej bezpečnosti a v zmysle zákona o ISVS.
Obchodné meno/názov (aj názov sekcie ak relevantné)	Úrad podpredsedu vlády SR pre investície a informatizáciu
Sídlo	Štefánikova 15, 811 05 Bratislava
IČO	50 349 287

4. Partner, ktorý sa bude zúčastňovať realizácie národného projektu (ak relevantné)

Zdôvodnenie potreby partnera národného projektu (ak relevantné)[3]	Partnermi národného projektu budú: • Národný bezpečnostný úrad (ďalej aj „NBÚ“), • Slovenská informačná služba (ďalej aj „SIS“), • Národná agentúra pre sieťové a elektronické služby (ďalej aj „NASES“). Rozhodujúcim faktorom pre určenie jednotlivých aktérov (jednotiek CSIRT) projektu je ich pôsobnosť v podsektore ISVS definovanom v prílohe č. 1 zákona o kybernetickej bezpečnosti: • SK-CERT (NBÚ) je jednotkou CSIRT, ktorá má v zmysle § 6 zákona o kybernetickej bezpečnosti

[2] Jednoznačne a stručne zdôvodnite výber prijímateľa NP ako jedinečnej osoby oprávnenej na realizáciu NP (napr. odkaz na platné predpisy, operačný program, národnú stratégiu, ktorá odôvodňuje jedinečnosť prijímateľa NP).
[3] Uveďte dôvody pre výber partnerov (ekonomickí, sociálni, profesijní...). Odôvodnite dôvody vylúčenia akejkoľvek tretej strany ako potenciálneho realizátora.

	postavenie národnej jednotky CSIRT s pôsobnosťou pre SR a ktorá musí plniť úlohy jednotky CSIRT pre všetky sektory a podsektory a digitálne služby okrem tých sektorov a podsektorov, pre ktoré plní úlohy jednotky CSIRT ústredný orgán (§ 9 zákona o kybernetickej bezpečnosti), • CSIRT SIS – jednotka CSIRT v pôsobnosti Slovenskej informačnej služby, ktorá zabezpečuje spravodajské činnosti kybernetickej bezpečnosti pre podsektor ISVS, • GOV CERT SK – jednotka CSIRT zriadená Národnou agentúrou pre sieťové a elektronické služby, prevádzkovateľom základnej služby zabezpečujúca činnosti kybernetickej bezpečnosti pre kľúčové stavebné prvky e-Governmentu, ktorými sú Ústredný portál verejnej správy a vládna sieť Govnet.
Kritériá pre výber partnera [4]	Kritériá pre výber partnera vyplývajú zo zákona o kybernetickej bezpečnosti, detaily sú zdokumentované v ŠU. Rozhodujúcim faktorom pre určenie jednotlivých partnerov projektu (jednotiek CSIRT) je ich pôsobnosť v podsektore ISVS definovanom v prílohe č. 1 zákona o kybernetickej bezpečnosti.
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie.
Obchodné meno/názov	Úrad podpredsedu vlády SR pre investície a informatizáciu
Sídlo	Štefánikova 15, 811 05 Bratislava
IČO	50349287

V prípade viacerých partnerov, doplňte údaje za každého partnera.

5. Predpokladaný časový rámec
   Dátumy v tabuľke nižšie nie sú záväzné, ale predstavujú vhodný a žiadúci časový rámec pre zabezpečenie procesov, vedúcich k realizácii národného projektu.

Dátum vyhlásenia vyzvania vo formáte Mesiac/Rok	08/2018
Uveďte plánovaný štvrťrok podpísania zmluvy o NFP s prijímateľom	4 Q/2018
Uveďte plánovaný štvrťrok spustenia realizácie projektu	1 Q/2019
Predpokladaná doba realizácie projektu v mesiacoch	24 mesiacov

[4] Uveďte, na základe akých kritérií bol partner vybraný, alebo ak boli zverejnené, uveďte odkaz na internetovú stránku, kde sú dostupné. Ako kritérium pre výber - určenie partnera môže byť tiež uvedená predchádzajúca

6. Finančný rámec

Alokácia na vyzvanie (zdroj EÚ a ŠR)	44 960 647,00 EUR
Celkové oprávnené výdavky projektu	44 960 647,00 EUR
Vlastné zdroje prijímateľa	N/A

Rozdelenie na SW a HW v projekte je nasledovné:

Projekt	**Spolu za 10 rokov**	**t1**	**t2**
SW produkty - sumár obstaranie	17 783 144	10 752 577	7 030 566
SW produkty - sumár prevádzka	18 321 418	1 107 873	1 599 240
Aplikácie - sumár obstaranie	780 280	396 280	384 000
Aplikácie - sumár prevádzka	1 223 040	-	-
HW sumár obstaranie	37 989 907	17 213 704	1 781 250
HW sumár prevádzka	17 931 129	1 373 320	1 592 580
Riadenie projektu	1 729 256	1 729 256	-
Spolu	95 758 173	32 573 010	12 387 637

7. Východiskový stav

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

- smernica Európskeho parlamentu a rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii („smernica NIS“),
- vykonávacie nariadenie Komisie (EÚ) 2018/151 z 30. januára 2018, ktorým sa stanovujú pravidlá uplatňovania smernice Európskeho parlamentu a Rady (EÚ) 2016/1148, pokiaľ ide o bližšiu špecifikáciu prvkov, ktoré musia poskytovatelia digitálnych služieb zohľadňovať pri riadení rizík v oblasti bezpečnosti sietí a informačných systémov, a parametrov na posudzovanie toho, či má incident závažný vplyv,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- súvisiace vykonávacie predpisy k zákonu o kybernetickej bezpečnosti:
  - vyhláška Národného bezpečnostného úradu č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby),
  - vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov,
  - vyhláška Národného bezpečnostného úradu č. 166/2018 Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov,

- zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- zákon č. 45/2011 Z. z. o kritickej infraštruktúre v znení zákona č. 69/2018 Z. z.,
- koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020,
- akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020.

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

- Hlavný dokument štúdie uskutočniteľnosti:
  (dostupný na https://wiki.finance.gov.sk/display/SU/SU-MD-su_132)
- Prílohy Agenda
  (dostupný na https://wiki.finance.gov.sk/pages/viewpage.action?pageId=28606631)
- CBA rozpočet
  (dostupný na https://metais.finance.gov.sk/studia/detail/6c434eaa-7a1f-d991-7a03-175c886106c5?tab=documents)

c. Uveďte, na ktoré z ukončených a prebiehajúcich národných projektov[5] zámer NP priamo nadväzuje, v čom je navrhovaný NP od nich odlišný a ako sú v ňom zohľadnené výsledky/dopady predchádzajúcich NP (ak relevantné):

Zámer NP priamo nenadväzuje na žiadny z ukončených ani prebiehajúcich národných projektov.

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

- neadekvátne technologické a znalostné vybavenie jednotiek CSIRT,
- nízka úroveň vyspelosti jednotlivých pracovísk jednotiek CSIRT zapojených do projektu (Capability Maturity Model),
- nízka miera detekcie prebiehajúcich bezpečnostných incidentov,
- vysoké riziko kybernetických bezpečnostných incidentov,
- nedostatočné plnenie požiadaviek zákona o kybernetickej bezpečnosti,
- preventívne a reaktívne služby nie sú poskytované na adekvátnej úrovni.

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

Žiadateľ

Administratívna kapacita interná – Požiadavky interných administratívnych rolí budú plnené internými zdrojmi.

Administratívna kapacita externá – Dodávateľsky sa plánujú zabezpečiť vybrané podporné aktivity.

[5] V prípade ak je to relevantné, uveďte aj ukončené národné projekty z programového obdobia 2007-2013.

Finančná kapacita – Obstarávacie náklady a prevádzkové náklady počas trvania projektu budú financované z fondov EÚ, po skončení projektu bude prevádzka riešenia financovaná zo štátneho rozpočtu.

Prevádzková kapacita – predpokladá sa zabezpečenie prevádzky riešenia internými pracovníkmi.

Partneri

Administratívna kapacita interná – Požiadavky interných administratívnych rolí budú plnené internými zdrojmi.

Administratívna kapacita externá – Dodávateľsky sa plánujú zabezpečiť vybrané podporné aktivity.

Finančná kapacita – Obstarávacie náklady a prevádzkové náklady počas trvania projektu budú financované z fondov EÚ, po skončení projektu bude prevádzka riešenia financovaná zo štátneho rozpočtu.

Prevádzková kapacita – predpokladá sa zabezpečenie prevádzky riešenia internými pracovníkmi.

8. Vysvetlite hlavné ciele NP (stručne):
   (očakávaný prínos k plneniu strategických dokumentov, k socio-ekonomickému rozvoju oblasti pokrytej OP, k dosiahnutiu cieľov a výsledkov príslušnej prioritnej osi/špecifického cieľa)

Hlavným cieľom NP je vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT schopnej zabezpečiť prevenciu a odhaľovanie kybernetických incidentov na celonárodnej úrovni, pričom v prípade realizácie projektu sa uvažuje s:

- efektívnejším predchádzaním a detekciou kybernetických incidentov v prostredí VS,
- efektívnejšou reakciou na kybernetické incidenty v prostredí celého hospodárstva.

Naplnenie uvedeného hlavného cieľa sa zabezpečí:

- monitorovaním a evidenciou kybernetických bezpečnostných incidentov,
- prijímaním včasných varovaní pred kybernetickými bezpečnostnými incidentami,
- zvýšením bezpečnosti vykonávaním penetračných testov,
- poskytovaním služieb potrebných pre zvládnutie bezpečnostných incidentov,
- zlepšením riadenia odozvy na incident a podporou pri zvládaní bezpečnostných incidentov,
- vykonávaním forenznej analýzy a analýzy škodlivého kódu,
- podporou pri odstraňovaní následkov,
- zvýšením spôsobilostí budovaním schopností a odbornosti zamestnancov,
- zvýšením bezpečnostného povedomia o kybernetickej bezpečnosti,
- zabezpečením adekvátnej úrovne kybernetickej a informačnej bezpečnosti vo verejnej správe,
- zvýšením ochrany pred škodlivým kódom,

- zaistením a vytváraním indiktárov kompromitácie,
- zvýšením vyspelosti v oblasti kybernetických hrozieb (threat intelligence a threat hunting).

Naplnením hlavného cieľa NP sa dosiahnu tieto výsledky špecifického cieľa 7.9:

- zníženie finančných dopadov a dopadov na inštitúcie verejnej správy pri bezpečnostných incidentoch,
- zvýšenie vyspelosti trhu s bezpečnostnými riešeniami zvýšením výdavkov na bezpečnosť verejného sektora,
- zvýšenie kybernetickej bezpečnosti a aplikovanie najnovších poznatkov v európskom priestore,
- zvýšenie miery inovácie v oblasti bezpečnostných opatrení,
- zvýšenie dôvery občanov a podnikateľov v digitálny priestor.

Kódy intervencie, ku ktorým projekt prispieva:

- kód intervencie 78: Služby a aplikácie elektronickej verejnej správy.

9. Očakávaný stav a merateľné ciele

<table>
<tr><td colspan="5">V tejto časti popíšte očakávané výsledky projektu s konkrétnym prínosom vo vzťahu k rozvoju oblasti pokrytej operačným programom a zrealizovaniu aktivít. V tabuľke nižšie uveďte projektové ukazovatele a iné údaje. Projektové ukazovatele musia byť definované tak, aby odrážali výstupy/výsledky projektu a predstavovali kvantifikáciu toho, čo sa realizáciou aktivít za požadované výdavky dosiahne.[6]</td></tr>
<tr><td>Cieľ národného projektu</td><td>Merateľný ukazovateľ</td><td>Indikatívna cieľová hodnota</td><td>Aktivita projektu</td><td>Súvisiaci programový ukazovateľ[7]</td></tr>
<tr><td>Vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT schopnej zabezpečiť prevenciu a odhaľovanie kybernetických incidentov na celonárodnej úrovni</td><td>P0048 Dodatočný počet informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov</td><td>60 %</td><td>Nákup HW a krabicového softvéru</td><td>Pomer www serverov organizácii verejnej správy bez bezpečnostných nedostatkov na celkovej vzorke www serverov verejnej správy</td></tr>
<tr><td colspan="5">Iné údaje, ktorými je možné sledovať napĺňanie cieľov národného projektu (ak relevantné)</td></tr>
</table>

[6] 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.

[7] Národný projekt by mal obsahovať minimálne jeden relevantný projektový ukazovateľ, ktorý sa agreguje do programového ukazovateľa. Pri ostatných projektových ukazovateľoch sa uvedie N/A. Relevantný programový ukazovateľ je automaticky generovaný v ITMS2014+.

Cieľ národného projektu	Ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	

V prípade viacerých merateľných ukazovateľov, doplňte údaje za každý merateľný ukazovateľ.

10. Bližší popis merateľných ukazovateľov.[8]

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa	Dodatočný pomer informačných systémov verejnej správy s implementovaným nástrojom na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov
Akým spôsobom sa budú získavať dáta?	Dáta pre overenie dosiahnutia merateľného ukazovateľa sa budú získavať overením skutočného stavu implementovaných nástrojov na rozpoznávanie, monitorovanie a riadenie bezpečnostných incidentov.

V prípade viacerých merateľných ukazovateľov, doplňte údaje za každý z nich.

11. Očakávané dopady

Zoznam prínosov a prípadných iných dopadov, ktoré sa dajú očakávať pre jednotlivé cieľové skupiny		
Dopady	Cieľová skupina (ak relevantné)	Počet[9]
Prínosy z prevencie incidentov (t. j. rôzne zraniteľnosti odhalia jednotky CSIRT ešte pred samotným zneužitím)	Inštitúcie a subjekty verejnej správy	Zo súčasných 5 % na cieľových 20 %
Zabránenie škodám v prípade preventívne odhalených incidentov	Inštitúcie a subjekty verejnej správy	60 %
Prínosy zo zníženia dôsledkov incidentov, ktoré už nastali (odhalenie útoku ešte počas jeho priebehu, rýchle odstránenie chýb vedúcich k útoku a pod.)	Inštitúcie a subjekty verejnej správy	Zo súčasných 5 % na cieľových 20 %
Zabránenie škodám z incidentov, ktoré už nastali	Inštitúcie a subjekty verejnej správy	20 %

[8] 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.
[9] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

V prípade viacerých cieľových skupín, doplňte dopady na každú z nich.

12. Aktivity
a) Uveďte detailnejší popis aktivít.

V zmysle platnej Príručky pre žiadateľa pôjde o nasledujúce skupiny aktivít:

Hlavné aktivity:
- Nákup HW a krabicového softvéru

Podporné aktivity:
- Riadenie projektu

b) V tabuľke nižšie uveďte rámcový popis aktivít, ktoré budú v rámci identifikovaného národného projektu realizované a ich prepojenie so špecifickými cieľmi.

Názov aktivity	Cieľ, ktorý má byť aktivitou dosiahnutý (podľa sekcie *Očakávaný stav*)	Spôsob realizácie (žiadateľ a/alebo partner)	Predpokladaný počet mesiacov realizácie aktivity
Nákup HW a krabicového vybavenia	Vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT schopnej zabezpečiť prevenciu a odhaľovanie kybernetických incidentov na celonárodnej úrovni	Žiadateľ Partneri	24
Riadenie projektu	Vytvorenie siete adekvátne odborne a technicky vybavených jednotiek CSIRT schopnej zabezpečiť prevenciu a odhaľovanie kybernetických incidentov na celonárodnej úrovni	Žiadateľ Partneri	24

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

13. Rozpočet
    Jasne 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, o. i. aj určenie výšky alokácie, je potrebné uviesť túto štúdiu ako zdroj určenia výšky finančných prostriedkov. Skupiny výdavkov doplňte v súlade s MP CKO č. 4 k číselníku oprávnených výdavkov v platnom znení. V prípade operačných programov implementujúcich infraštruktúrne projekty, ako aj projekty súvisiace s obnovou mobilných prostriedkov, sa do ukončenia verejného obstarávania uvádzajú položky rozpočtu len do úrovne aktivít.

Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu a ich výstižné zdôvodnenie		
Predpokladané finančné prostriedky na hlavné aktivity	**Celková suma**	**Uveďte plánované vecné vymedzenie**
Nákup HW a krabicového softvéru	43 231 391 €	Okrem nákupu HW a SW vybavenia, suma zahŕňa aj obstaranie licencií, licenčný poplatok na obdobie trvania projektu a odborné školenia.
Hlavné aktivity SPOLU	43 231 391 €	
Predpokladané finančné prostriedky na podporné aktivity	**Celková suma**	**Uveďte plánované vecné vymedzenie**
Riadenie projektu	1 729 256 €	Cena riadenia projektu predstavuje 4% z celkových nákladov projektu
Podporné aktivity SPOLU	1 729 256 €	
CELKOM	**44 960 647 €**	

14. Deklarujte, že NP vyhovuje **zásade doplnkovosti** (t. j. nenahrádza verejné alebo ekvivalentné štrukturálne výdavky členského štátu v súlade s článkom 95 všeobecného nariadenia).

    Príspevok z EŠIF v tomto projekte nebude mať za následok zníženie vnútroštátnych štrukturálnych výdavkov a bude doplnkom vnútroštátneho verejného financovania v zmysle zásady doplnkovosti.

15. Bude v národnom projekte využité zjednodušené vykazovanie výdavkov? Ak áno, aký typ?

    Nie.

16. Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov

Informácie sa vypĺňajú iba pre investičné[10] typy projektov.

Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov	
Existuje relevantná štúdia uskutočniteľnosti[11] ? (áno/nie)	áno
Ak je štúdia uskutočniteľnosti dostupná na internete , uveďte jej názov a internetovú adresu, kde je štúdia zverejnená	• Hlavný dokument štúdie uskutočniteľnosti: https://wiki.finance.gov.sk/display/SU/SU-MD-su_132 • Prílohy Agenda https://wiki.finance.gov.sk/pages/viewpage.action?pageId=28606631 • CBA https://metais.finance.gov.sk/studia/detail/6c434eaa-7a1f-d991-7a03-175c886106c5?tab=documents
V prípade, že štúdia uskutočniteľnosti nie je dostupná na internete, uveďte webové sídlo a termín, v ktorom predpokladáte jej zverejnenie (mesiac/rok)	N/A

[10] Investičný projekt – dlhodobá alokácia finančného aj nefinančného kapitálu na naplnenie investičného zámeru až do etapy, kedy projekt vstúpi do prevádzkovej etapy a prípadne začne generovať stabilné príjmy. Investičný projekt smeruje k: výstavbe stavby alebo jej technickému zhodnoteniu; nákupu pozemkov, budov, objektov alebo ich častí; nákupu strojov, prístrojov, tovarov a zariadení; obstaraniu nehmotného majetku vrátane softvéru. Zdroj: Uznesenie Vlády SR č. 300 z 21.6.2017 k návrhu Rámca na hodnotenie verejných investičných projektov v SR.

[11] Pozri aj Uznesenie Vlády SR č. 300 z 21.6.2017 k návrhu k návrhu Rámca na hodnotenie verejných investičných projektov v SR (dostupné na: http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=26598)