ZÁMER NÁRODNÉHO PROJEKTU OP EVS

na programové obdobie 2014 – 2020

Národný bezpečnostný úrad

Zvyšovanie efektívnosti riadenia procesov a posilnenie odborných kapacít Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti

Operačný program
Efektívna verejná správa

Európska únia
Európsky sociálny fond

Tento projekt je podporený z Európskeho sociálneho fondu.

Platnosť: 28.11.2017, účinnosť: 28.11.2017

Názov národného projektu:
Zvyšovanie efektívnosti riadenia procesov a posilnenie odborných kapacít Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti

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)

Kybernetická bezpečnosť je s neustále rastúcou mierou informatizácie a digitalizácie jednou z najexponovanejších oblastí, ktoré priamo ovplyvňujú fungovanie hospodárstva, verejnej správy ako aj života občanov v modernej spoločnosti. Aby politiku kybernetickej bezpečnosti bolo možné efektívne riadiť, potrebuje nielen strategické ukotvenie v systéme verejnej správy, kvalitný legislatívny a nelegislatívny rámec ale aj fundované personálne kapacity, či zodpovedajúce technické vybavenie. Komplexný prístup ku kybernetickej bezpečnosti s jasnými princípmi a cieľmi je základom pre dobre vyvinutý systém, ktorý dokáže flexibilne reagovať na aktuálne hrozby a zabezpečiť tak vysokú mieru bezpečnosti.

Podľa zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov je Národný bezpečnostný úrad ústredným orgánom štátnej správy pre kybernetickú bezpečnosť. Ako národná autorita preto z tejto pozície riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti, určuje štandardy a vydáva politiku bezpečného správania sa v kybernetickom priestore a plní úlohy regulačného orgánu pre túto oblasť. Úrad je hlavným kontaktným bodom pre zahraničie v oblasti kybernetickej bezpečnosti, spolupracuje s ústrednými orgánmi, prevádzkovateľmi základných služieb a prevádzkovateľmi digitálnych služieb a takisto plní úlohu národnej jednotky CSIRT (jednotky pre riešenie kybernetických bezpečnostných incidentov). Má teda osobitné postavenie v rámci organizácie činností ústrednej štátnej správy, ktoré nie je možné vykonávať prostredníctvom iného subjektu.

V rámci svojich úloh Národný bezpečnostný úrad vypracúva a realizuje koncepciu štátnej politiky vo vyššie uvedenej oblasti. V nadväznosti na túto skutočnosť bola dňa 7. januára 2021 vládou schválená Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá zakotvila smerovanie Slovenskej republiky prostredníctvom vymedzenia a implementácie reformných opatrení. Za účelom naplnenia tejto stratégie a jej cieľov bol zostavený Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Jednotlivé úlohy Akčného plánu, ktoré svojím účelom a cieľmi korešpondujú s hlavnými prioritami OP EVS, sa v predkladanom projekte týkajú analytických a strategických činností ako aj implementácie opatrení.

Mimo spomínaného akčného plánu a v kontexte napĺňania potrieb pre zvyšovanie úrovne kybernetickej bezpečnosti NBÚ vykonáva implementáciu súvisiacich strategických materiálov, o ktorých sa zmieňujeme nižšie ako aj dotknutého legislatívneho rámca. Aj tieto sa týkajú hlavného cieľa projektu a jeho hlavnej aktivity.

2. Príslušnosť národného projektu k relevantnej časti operačného programu

Prioritná os	1. Posilnené inštitucionálne kapacity a efektívna verejná správa
Investičná priorita	Investície do inštitucionálnych kapacít a do efektívnosti verejných správ a verejných služieb na národnej, regionálnej a miestnej úrovni v záujme reforiem lepšej právnej úpravy a dobrej správy.
Špecifický cieľ	1.2 Modernizované ľudské zdroje a zvýšené kompetencie zamestnancov
Miesto realizácie projektu (na úrovni kraja)	celé územie SR
Identifikácia hlavných cieľových skupín (ak relevantné)	Inštitúcie a subjekty verejnej správy Zamestnanci verejnej správy Právnické osoby a občania

3. Prijímateľ[1] národného projektu

Dôvod určenia prijímateľa národného projektu[2]	Národný bezpečnostný úrad, v zmysle zákona 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, je orgánom štátnej správy pre kybernetickú bezpečnosť. Predstavuje kľúčový subjekt v systéme riadenia informačnej a kybernetickej bezpečnosti.
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 Osobitné, jedinečné kompetencie na implementáciu národného projektu vychádzajú zo zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov uvedeného v dôvode určenia prijímateľa národného projektu.
Obchodné meno/názov (aj názov sekcie ak relevantné)	Národný bezpečnostný úrad
Sídlo	Budatínska 30, 851 06 Bratislava
IČO	36 061 701

[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.

[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).

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

Zdôvodnenie potreby partnera národného projektu (ak relevantné)[3]	N/A
Kritériá pre výber partnera [4]	N/A
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	N/A
Obchodné meno/názov	N/A
Sídlo	N/A
IČO	N/A

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	7/2022
Uveďte plánovaný štvrťrok podpísania zmluvy o NFP s prijímateľom	3Q/2022
Uveďte plánovaný štvrťrok spustenia realizácie projektu	3Q/2022
Predpokladaná doba realizácie projektu v mesiacoch	7/2022 – 11/2023

6. Finančný rámec

Alokácia na vyzvanie (zdroj EÚ a ŠR)	724 500,00 EUR
Celkové oprávnené výdavky projektu	724 500,00 EUR
Vlastné zdroje prijímateľa	0,00 EUR

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

Východiskovým dokumentom realizácie národného projektu je Národná stratégia kybernetickej bezpečnosti na roky 2021 až 2025, ktorá bola schválená vládou Slovenskej republiky 7. januára 2021 uznesením č.5/2021. Ide o východiskový strategický dokument, ktorý komplexne určuje strategický prístup Slovenskej republiky

[3] Uveďte dôvody pre výber partnerov (ekonomickí, sociálni, profesijní...). Odôvodnite dôvody vylúčenia akejkoľvek tretej strany ako potenciálneho realizátora.

[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 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 VO.

k zabezpečeniu kybernetickej bezpečnosti s víziou posilnenia a vytvorenia otvoreného, slobodného a bezpečného kybernetického priestoru pre všetkých. Za účelom dosiahnutia jednotlivých cieľov stanovených národnou stratégiou bol vytvorený Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti, ktorý vymedzuje konkrétne úlohy a aktivity spolu s identifikovaním jasných kompetencií a zodpovedností jednotlivých aktérov participujúcich na jeho realizácii. Strategické postavenie zohráva NBÚ, ktorý plní úlohu gestora vo veľkej časti úloh, respektíve zastáva úlohu súčinného subjektu.

Schválený Akčný plán koordinácie boja proti hybridným hrozbám taktiež vymedzuje úlohy pre NBÚ v oblasti kybernetickej bezpečnosti. Reakciou na slabé povedomie spoločnosti v oblasti kybernetických hrozieb v gescii NBÚ je vytvorenie konceptu a kampane pre zvyšovanie bezpečnostného povedomia pri identifikácii nástrojov hybridného pôsobenia v kybernetickom priestore. Ďalšou dôležitou aktivitou je účasť expertov z radov NBÚ na prezentáciách a diskusiách s odbornou verejnosťou týkajúcich sa aktuálnych výziev a riešení informačných operácií v doméne kybernetickej bezpečnosti. V neposlednej rade je to aj aktívna účasť NBÚ na operatívnom, taktickom a strategickom riadení a výkone aktivít smerujúcich k zastaveniu alebo obmedzeniu šírenie škodlivého obsahu, závažných dezinformácií v širšom kontexte hybridných hrozieb.

Kľúčový nástroj smerovania SR predstavuje Programové vyhlásenie vlády SR (ďalej „PPV“) na obdobie rokov 2020 – 2024, kde si vláda SR dala za cieľ podporiť posilnenie kompetencií NBÚ, jej finančného zabezpečenia a zodpovednosti za ochranu všetkých sektorov kybernetického priestoru. PVV deklaruje vybudovanie účinného systému detekcie a ochrany kybernetického priestoru SR, skvalitnenie a zrýchlenie schopnosti reakcie na incidenty, vytvorenie moderných a efektívnych foriem spolupráce štátu s verejným i súkromným sektorom v oblasti kybernetickej bezpečnosti, najmä pri riešení bezpečnostných incidentov, výmene skúseností a vzdelávaní. Zároveň za dôležité považuje vláda SR aj zjednotenie existujúcich regulácií v oblasti kybernetickej bezpečnosti pod spoločnú reguláciu, s cieľom zabezpečiť komplexnosť legislatívy a zvýšiť kvalitu podnikateľského prostredia a verejného sektora.

Významným legislatívnym dokumentom je zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, ktorý predstavuje regulačný rámec komplexne upravujúci oblasť kybernetickej a informačnej bezpečnosti v Slovenskej republike. Na základe tohto zákona NBÚ riadi a koordinuje výkon štátnej správy ako i určuje štandardy, operačné postupy, vydáva metodiku a politiku správania sa v kybernetickom priestore. Zároveň je zodpovedný za vypracovanie národnej stratégie kybernetickej bezpečnosti a ročnej správy o stave kybernetickej bezpečnosti v Slovenskej republike v spolupráci s príslušnými štátnymi orgánmi. Významné miesto zohráva aj v rámci medzinárodných vzťahov a zahraničnej politiky, kde zastáva úlohu národného kontaktného miesta pre kybernetickú bezpečnosť pre zahraničie a zabezpečuje spoluprácu s jednotnými kontaktnými miestami členských štátov EÚ a NATO. K predmetu a rozsahu plánovaných aktivít tohto projektu má priamy vzťah osobitne aj §27a, §27b, §27c, ktoré si kladú za cieľ ochranu bezpečnostných záujmov SR.

Bezpečnostná stratégia SR taktiež poukazuje na dôležitosť zaistiť bezpečnosť v Slovenskej republike. Kybernetický priestor je osobitnou operačnou doménou, v ktorej

útočník môže závažne poškodiť bezpečnostné záujmy Slovenskej republiky. Kybernetické útoky sa stali súčasťou regionálnych konfliktov a mocenského súperenia a pri raste napätia medzi štátmi sa bude ich počet zvyšovať. V súvislosti s rozširovaním škály civilných cieľov môžu kybernetické útoky zapríčiniť škody porovnateľné s následkami ozbrojených útokov. Môžu totiž zásadným spôsobom ohroziť chod štátu, spoločnosti a bezpečnosť občana, poškodiť a ochromiť nosné komunikačné, energetické a finančné systémy, spôsobiť významné ekonomické škody, narušiť spoločenskú stabilitu a verejný poriadok a oslabiť základné funkcie štátu. V danej spojitosti do problematiky vstupujú aj princípy a ciele Obrannej stratégie SR a to najmä v spojitosti s efektívnym kybernetickým zabezpečovaním informačných systémov a sietí.

V rámci medzinárodných dokumentov poukazuje na nebezpečenstvo kybernetických hrozieb a ich nepriaznivých dopadov na prepojené hospodárstvo a spoločnosť nariadenie Európskeho parlamentu a Rady EÚ 2019/881 o agentúre ENISA a certifikácií kybernetickej bezpečnosti informačných a komunikačných technológií. Následky rozsiahlych incidentov by mohli narušiť poskytovanie základných služieb v celej EÚ. Keďže kybernetické hrozby sú globálnym problémom je nevyhnutná užšia medzinárodná spolupráca, v rámci ktorej je strategickým subjektom zastupujúcim Slovenskú republiku NBÚ, s cieľom zlepšiť kybernetické bezpečnostné normy vrátane potreby definovania spoločných regulačných noriem správania sa, prijatia kódexov správania, implementácie medzinárodných noriem a výmeny informácií, presadzovania rýchlejšej medzinárodnej spolupráce pri reakcii na problémy týkajúce sa sieťovej a informačnej bezpečnosti ako aj presadzovania spoločného globálneho prístupu k týmto problémom.

Dôležitosť problematiky boja s kybernetickými hrozbami vydvihuje aj nariadenie Európskeho parlamentu a Rady EÚ 2021/887, ktorým bolo zriadené Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier. Nariadenie deklaruje, že výrazné narušenie sietí a informačných systémov môže mať dosah na jednotlivé členské štáty i EÚ ako celok. Je nevyhnutné zabezpečenie a rozvoj základných výskumných a technologických kapacít v oblasti kybernetickej bezpečnosti.

Vzhľadom ku skutočnosti, že kybernetická bezpečnosť je horizontálna problematika, ktorá vstupuje do viacerých národných a európskych politík, časť úloh projektu sa týka aj podpory implementácie nariadenia EP a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027. Nariadenie predstavuje rámec priamo riadenej finančnej podpory pre digitálne technológie, najmä so zameraním na systémy HPC, umelú inteligenciu, kybernetickú bezpečnosť, pokročilých digitálnych zručností a všeobecnej podpory aplikácie IKT do spoločnosti a ekonomiky. Nariadenie zavádza do praxe v členských štátoch v zmysle čl. 16 sieť európskych digitálnych inovačných centier (EDIH) orientovaných najmä na podporu digitálnej konkurencieschopnosti priemyslu, osobitne malých a stredných spoločností, fungujúce ako tzv. one stop shops. Od EDIHov sa očakáva, že poskytnú spoločnostiam prístup k technickej expertíze a k možnostiam testovania (*test before invest*). V zmysle požiadaviek EK sa predpokladá, že EDIHy budú poskytovať služby z portfólia kybernetickej bezpečnosti.

Národný bezpečnostný úrad ako ústredný orgán štátnej správy zodpovedný za oblasť kybernetickej bezpečnosti tieto nariadenia vo svojej vecnej príslušnosti implementuje.

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

Ciele NP a s nimi spojené aktivity nadväzujú primárne na Koncepciu kybernetickej bezpečnosti Slovenskej republiky na obdobie 2015 - 2020, ktorá predstavovala prvý ucelený dokument identifikujúci princípy, zásady, ciele kybernetickej bezpečnosti. Na koncepciu nadväzoval Akčný plán realizácie. Výsledkom bolo vytvorenie stabilného inštitucionálneho rámca riadenia, ako i prijatie komplexnej legislatívy zastrešujúcej problematiku kybernetickej bezpečnosti a vytvorenie špeciálnych entít na riešenie kybernetických útokov.

Nová stratégia, ktorej jednotlivé aktivity sú súčasťou NP, má ambíciu nadviazať na zrealizované úlohy a flexibilne reagovať na neustále sa meniace bezpečnostné hrozby, zadefinovať princípy systému kybernetickej bezpečnosti a vymedziť strategické ciele a v konečnom dôsledku naplniť víziu posilnenia a vytvorenia otvoreného, slobodného a bezpečného kybernetického priestoru pre všetkých.

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):

NP Zvýšenie efektívnosti riadenia procesov a posilnenie odborných kapacít Národného bezpečnostného úradu v oblasti kybernetickej bezpečnosti nadväzuje a dopĺňa v súčasnosti realizovaný NP Zvyšovanie odolnosti Slovenska voči hybridným hrozbám pomocou zefektívnenia procesov posilnením kapacít verejnej správy, avšak rieši problematiku kybernetickej bezpečnosti, ktorá je úzko previazaná s oblasťou hybridných hrozieb.

Predložený NP má spoločné prvky aj s NP Budovanie a rozvoj kapacít analytických útvarov na vybraných ústredných orgánoch štátnej správy. V 3Q/2021 sa vytvoril v prostredí NBÚ nový útvar Inštitút pre bezpečnostné štúdie, ktorého agenda je zameraná na analytickú stránku, posudzovanie bezpečnostných rizík, vyhodnocovanie politík, tvorbu prognóz a stratégií. Predložený projekt prispeje k rozšíreniu inštitútu o nové expertné kapacity v špecifickej oblasti kybernetickej bezpečnosti.

d. Popíšte problémové a prioritné oblasti, ktoré rieši zámer národného projektu. (Zoznam známych problémov, ktoré vyplývajú zo súčasného stavu a je potrebné ich riešiť):
    - Nízka flexibilita reakcie na čoraz sofistikovanejšie kybernetické incidenty – neustály rozvoj nových techník a typov hrozieb vyžaduje promptnú reakciu. Odpoveď na útok môže v mnohých prípadoch prísť neskoro alebo v nedostatočnej sile. Príprava na útok, príprava vhodných nástrojov, prieskum prostredia môže trvať dlhší čas, než ktorý majú k dispozícii riešitelia incidentov pri reakcii na prebiehajúci útok.
    - Nedostatočné monitorovanie a analytické vyhodnocovanie kybernetických incidentov vrátane škodlivého obsahu a škodlivých aktivít v kontexte

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

hybridných hrozieb - prijímanie rozhodnutí bez hlbších analýz v sebe nesie riziko subjektívneho nesprávneho vyhodnotenia situácie. Analytické štúdie a hodnotenia nemôžu existovať bez kvalitného monitorovania a následného vyhodnocovania údajov v kybernetickom priestore.

- Absencia interných expertných kapacít – poddimenzovaný počet analytických kapacít pôsobiacich v oblasti kybernetickej bezpečnosti vzhľadom na vyvíjajúcu sa situáciu v kybernetickom priestore môže mať nežiadúce dopady na monitorovanie a analytické vyhodnocovanie údajov, čo sa v konečnom dôsledku môže odraziť na prijatých rozhodnutiach.
- Absencia resp. nedostatočné riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch národného hospodárstva – súčasný stav si vyžaduje vytvoriť rámec riadenia rizík v kybernetickej bezpečnosti pre prevádzkovateľov základných služieb, ako i systematické a kontinuálne riadenie rizík v jednotlivých sektoroch národného hospodárstva.
- Absencia procesu atribúcie kybernetických bezpečnostných incidentov – bez zadefinovania zodpovedných inštitúcií a právnych mechanizmov môže nastať nekoordinovaný postup riešenia bezpečnostných incidentov.
- Potreba úpravy a doplnenia existujúceho regulačného rámca vzhľadom k vývoju informačných a komunikačných technológií ako aj škály nových hrozieb v informačnej a kybernetickej bezpečnosti – nedostatočná legislatívna úprava a neprispôsobené procesy slúžiace na boj proti kybernetickým hrozbám môžu vytvoriť priestor pre ich napredovanie a rozmáhanie sa a tým ohroziť široké spektrum subjektov od prvkov kritickej infraštruktúry až po bežné obyvateľstvo.
- Nedostatočná prepojenosť implementácie strategických materiálov a iniciatív EÚ s národnými. Nedostatočná komplementarita opatrení na realizáciu politiky spoločného záujmu medzi EÚ a SR bude mať za následok pomalú, resp. žiadnu konvergenciu zamýšľaných stimulačných efektov na podporu daného cieľa (napr. vytvorené EDIHy v slovenskom prostredí napriek očakávaniam o poskytovaní služieb z portfólia kybernetickej bezpečnosti bez spolupráce vecne kompetentného orgánu nebudú poskytovať vôbec alebo v diskutabilnej kvalite).
- Nedostatočné vybudovanie povedomia v spoločnosti a priemysle v oblasti kybernetickej bezpečnosti – nedostatočný priestor venovaný kybernetickej hygiene vo vzdelávacom a pracovnom procese môže v súčasnej dobe mať výrazné ekonomické a sociálne dopady.

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

NBÚ je ústredným orgánom štátnej správy, ktorému zo zákona prináležia kompetencie v oblasti riadenia a koordinovania problematiky kybernetickej bezpečnosti v Slovenskej republike. Jednotlivé aktivity projektu budú zastrešované v rámci útvarov NBÚ, a to primárne Inštitútom pre bezpečnostné štúdie (IBŠ), Národným centrom kybernetickej bezpečnosti SK-CERT, Sekciou regulácie a dohľadu. Implementácia projektu bude spoločne realizovaná 12 expertami s podporou dvoch back-office pracovníkov, ktorí budú zabezpečovať projekt po organizačnej a finančnej stránke. Administratívna a prevádzková

kapacita NBÚ vzhľadom na charakter a aktivity spojené s realizáciou projektu je dostatočná. NBÚ má skúsenosť s implementáciou fondov EÚ, a to európskych štrukturálnych a investičných fondov ako aj priamo riadených fondov s technologickým zameraním.

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)

HLAVNÝ CIEĽ:
Efektívne riadenie procesov a nastavenie metodík pri implementácii kľúčových úloh z Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti v priebehu rokov 2022 a 2023, vrátane posilnenia a stabilizovania odborných kapacít.

ČIASTKOVÉ CIELE:
Analyticko-organizačné:

1. Posilnenie analytických kapacít v oblasti bezpečnostných hrozieb, zvýšená schopnosť pre posudzovanie rizík, analýz dopadov, bezpečnostných modelov a dátovej analytiky. Vybudovanie dostatočného odborného personálneho základu pre systém riadenia informačnej a kybernetickej bezpečnosti.
2. Tvorba ekonomického modelu politík v oblasti kybernetickej bezpečnosti v Slovenskej republike.
3. Tvorba procesu technickej a politickej atribúcie incidentov spolu s určením zodpovedných inštitúcií a právnych mechanizmov a mechanizmov kybernetickej diplomacie.
4. Príprava metodiky posúdenia rizík pre aplikovanie na sektory štátu, vybrané nové technológie, služby s cieľom poznať možné bezpečnostné dopady na základné a kritické aktíva štátu, prevádzkovateľov základných služieb a občanov.
5. Tvorba rámca riadenia rizík v kybernetickej bezpečnosti upotrebiteľného pre prevádzkovateľov základných služieb, systematické a kontinuálne riadenie rizík kybernetickej bezpečnosti v jednotlivých sektoroch na riadne zabezpečenie implementácie bezpečnostných opatrení.

Regulačné a strategické:
6. Príprava novelizácie vyhlášok vychádzajúcich zo zákona č.69/2018 o kybernetickej bezpečnosti v závislosti od dostupnosti schválenej EÚ legislatívy (k identifikačným kritériám prevádzkovanej služby alebo pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a k podrobnostiam hlásenia kybernetických bezpečnostných incidentov).

Preventívno-koncepčné:
7. Návrh metodiky v rámci indexu pravidelného merania stavu pre oblasť kybernetickej bezpečnosti a pravidelné vyhodnocovanie s cieľom získať reálny a aktuálny prehľad a informáciu o trendoch a stave kybernetickej bezpečnosti na národnej úrovni.

8. Zvýšenie dôveryhodnosti a transparentnosti štátnych inštitúcií. Zvýšená analytická schopnosť identifikácie škodlivého obsahu a škodlivých aktivít a realizácia efektívnych opatrení na operatívnej, taktickej a strategickej úrovni v boji proti hybridným hrozbám. Vytvorenie prostredia otvorenej komunikácie, budovanie kapacít a rozvoj spôsobilosti v oblasti hybridných operácií v kybernetickom prostredí. Účasť, prezentácia a diskusia s odbornou verejnosťou aktuálne výzvy a riešenia dopadov prvkov informačných operácií v kybernetickom priestore na pracovných stretnutiach, workshopoch, konferenciách a besedách pri okrúhlych stoloch.
9. Zvýšenie bezpečnostného povedomia spoločnosti pri identifikácii nástrojov hybridného pôsobenia v kybernetickom priestore. Vypracovanie koncepcie rozvoja bezpečnostného povedomia, budovania spôsobilosti a prevencie verejnosti v kybernetickej doméne ako aj vzdelávacej, informačnej kampane pre obyvateľov na identifikáciu hybridných vplyvov v kybernetickom priestore.
10. Tvorba plánu šírenia a zvyšovania bezpečnostného povedomia v oblasti kybernetickej bezpečnosti.
11. Podpora oprávnených EDIHov v zmysle legislatívnych a strategických materiálov EÚ vo vecne príslušnej kompetencii pre oblasť kybernetickej bezpečnosti v prípade naplnenia vhodných podmienok a kritérií spolupráce.

9. Očakávaný stav a merateľné ciele

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]				
Cieľ národného projektu	Merateľný ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	Súvisiaci programový ukazovateľ[7]
Efektívne riadenie procesov a nastavenie metodík pri implementácii kľúčových úloh z Akčného plánu realizácie Národnej stratégie	P0178 Počet koncepčných, analytických a metodických materiálov	6	1	
	P0465 Počet ústredných orgánov štátnej správy, ktoré získali podporu na zavedenie a/alebo	1	1	O0058 Počet ústredných orgánov štátnej správy, ktoré získali

[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.

kybernetickej bezpečnosti v priebehu rokov 2022 a 2023, vrátane posilnenia a stabilizovania odborných kapacít.	posilnenie analytických jednotiek			podporu na zavedenie a/alebo posilnenie analytických jednotiek
	P0726 Počet zanalyzovaných legislatívnych noriem, metodických pokynov a usmernení	2	1	
	P0887 Počet novovzniknutých platforiem zameraných na zvyšovanie kvality verejných politík	1	1	
	O0057 Počet zamestnancov v analytických jednotkách v orgánoch štátnej správy na začiatku podpory	12	1	
	R0055 Počet zamestnancov, ktorí pracovali v novo zavedených a/alebo posilnených analytických jednotkách dva roky po ich vzniku	12	1	

Iné údaje, ktorými je možné sledovať napĺňanie cieľov národného projektu (ak relevantné)				
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[9]	P0178 Počet koncepčných, analytických a metodických materiálov
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať Monitorovacím výborom Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[10]	P0465 Počet ústredných orgánov štátnej správy, ktoré získali podporu na zavedenie a/alebo posilnenie analytických jednotiek
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať Monitorovacím výborom Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti.

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[11]	P0726 Počet zanalyzovaných legislatívnych noriem, metodických pokynov a usmernení
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať Monitorovacím výborom Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti.

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[12]	P0887 Počet novovzniknutých platforiem zameraných na zvyšovanie kvality verejných politík
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať osobitným interným orgánom na monitorovanie implementácie projektu.

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[13]	O0057 Počet zamestnancov v analytických jednotkách v orgánoch štátnej správy na začiatku podpory
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať osobitným interným orgánom na monitorovanie implementácie projektu.

[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] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.
[10] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.
[11] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.
[12] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.
[13] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[14]	R0055 Počet zamestnancov, ktorí pracovali v novo zavedených a/alebo posilnených analytických jednotkách dva roky po ich vzniku
Akým spôsobom sa budú získavať dáta?	Napĺňanie merateľných ukazovateľov sa bude sledovať a odpočtovať osobitným interným orgánom na monitorovanie implementácie projektu.

11. Očakávané dopady

Zoznam prínosov a prípadných iných dopadov, ktoré sa dajú očakávať pre jednotlivé cieľové skupiny		
Dopady	Cieľová skupina (ak relevantné)	Počet[15]
Udržanie rezortných analytických a odborných kapacít v procese realizácie Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025.	NBÚ	12
Identifikovanie trendov vývoja kybernetických hrozieb na národnej úrovni.	Verejnosť, miestna a štátna správa	Celá SR
Vypracovanie expertných štúdii internými kapacitami ako i zabezpečenie kvality údajov vstupujúcich do procesu vypracovania analýz a príslušných metodík prispeje k vyššej kvalite a suverénnosti rozhodnutí v oblasti kybernetickej bezpečnosti.	Tvorcovia verejných politík	Celá SR
Schopnosť predikcie dopadov kybernetických hrozieb a flexibilnej reakcie.	Tvorcovia verejných politík	Celá SR
Zabezpečenie prijatia a implementácie regulačného rámca, ktorý posilní odolnosť subjektov voči kybernetickým bezpečnostným incidentom.	Verejnosť, miestna a štátna správa	Celá SR
Lepšie manažovanie zahraničných vzťahov a medzinárodnej obchodnej politiky.	Štátna správa	Celá SR

[14] V prípade viacerých merateľných ukazovateľov, doplňte tabuľku za každý merateľný ukazovateľ.
[15] Ak nie je možné uviesť početnosť cieľovej skupiny, uveďte do tejto časti zdôvodnenie.

Zvýšenie bezpečnosti prvkov kritickej infraštruktúry ako i bezpečnosti občanov SR (spotrebiteľov).	Verejnosť, miestna a štátna správa	Celá SR
Zvýšenie bezpečnostného povedomia spoločnosti a priemyslu	Spoločnosť, priemysel	Celá SR
Zvýšenie kritického myslenia a overovania zdrojov informácií.	Verejnosť	Celá SR
Zvýšenie dôveryhodnosti a transparentnosti štátnych inštitúcií.	Miestna a štátna správa	Celá SR
Zabezpečenie kvality poskytovaných služieb EDIHov	Priemysel, miestna a štátna správa	Celá SR

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

12. Aktivity
    a) Uveďte detailnejší popis aktivít.

Hlavná aktivita projektu

1. Budovanie analytickej jednotky NBÚ a udržanie expertných kapacít v nadväznosti na implementáciu kľúčových úloh zo strategických dokumentov.

Účelom je efektívna implementácia kľúčových úloh z Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti v priebehu rokov 2022 a 2023 a súvisiacich strategických materiálov vrátane stabilizovania odborných kapacít. Pri realizácii úloh Akčného plánu Národnej stratégie kybernetickej bezpečnosti ako aj iných strategických materiálov je potrebné zabezpečiť efektívne riadenie procesov ako i nastavenie metodiky pri implementácii kľúčových úloh, čo si vyžaduje výkon kvalitnej analytickej činnosti založenej na údajoch ako i dobre vymedzený regulačný rámec. Aby jednotlivé aktivity mohli byť realizované je potrebné udržať a budovať predovšetkým interné expertné kapacity.

Na základe vyššie uvedených skutočností budú v rámci hlavnej aktivity realizované nasledujúce kľúčové činnosti:

1.1 Analytická činnosť zameraná na vybudovanie efektívneho systému reakcie na hybridné hrozby vrátane kybernetických incidentov
1.2 Posilnenie regulačného rámca v oblasti kybernetickej bezpečnosti
1.3 Analytická činnosť pre podporu budovania bezpečnostného povedomia spoločnosti a priemyslu

1.1 Analytická činnosť zameraná na vybudovanie efektívneho systému reakcie na hybridné hrozby vrátane kybernetických incidentov

Zvyšovanie úrovne kybernetickej bezpečnosti predstavuje neustály proces, ktorý musí komplexne reagovať na dynamický technologický rozvoj ako aj vyspelosť útočníkov. Neodmysliteľnou súčasťou pri identifikácii a následným riešením kybernetických incidentov sú odborné kapacity s pokročilými analytickými zručnosťami, na základe ktorých je možné nielen definovať zraniteľné miesta v kybernetickom priestore ale aj vytvoriť strategické, koncepčné a metodické materiály upravujúce proces reakcie na možnú hrozbu v kybernetickom priestore resp. reakciu na kybernetický incident. Zvýšená analytická schopnosť príslušníkov NBÚ identifikovať škodlivý obsah a škodlivé aktivity v kybernetickom priestore (vrátane webových sídiel, komunikačných kanálov sociálnych sietí a iných platforiem) povedie k realizácii efektívnejších opatrení na operatívnej, taktickej a strategickej úrovni v boji proti hybridným hrozbám.

Na naplnenie vyššie uvedeného cieľa si NBÚ v nasledujúcom období, najmä v súlade s Národnou stratégiou kybernetickej bezpečnosti, stanovilo špecifikovať ekonomický model dopadov kybernetických útokov na prevádzkovateľov základných služieb aj poskytovateľov digitálnych služieb. Odpoveďou na súčasnú absenciu jednotného procesu pre atribúciu kybernetických bezpečnostných incidentov bude vytvorenie koncepcie procesiu technickej a politickej atribúcie incidentov spolu s vymedzením zodpovedných inštitúcií, právnych mechanizmov a mechanizmov kybernetickej diplomacie ako i metodika posúdenia rizík pre vybrané sektory. Osobitnou kategóriou opatrení je tiež realizácie spomínaného Akčného plánu boja proti hybridným hrozbám, kde má aj NBÚ svoje vlastné úlohy.

Výstupy
- Špecifikácia ekonomického modelu politík v oblasti kybernetickej bezpečnosti
- Metodika posúdenia rizík pre vybrané sektory národného hospodárstva a prevádzkovateľov základných služieb
- Koncepcia technickej a politickej atribúcie incidentov
- Metodika vyhľadávania škodlivého obsahu a škodlivých aktivít v kybernetickom priestore s cieľom zabezpečenia zodpovedajúcich digitálnych stôp a dôkazov.

1.2 Posilnenie regulačného rámca v oblasti kybernetickej bezpečnosti

Vzhľadom k nutnosti zosúladenia národného legislatívneho rámca pre kybernetickú bezpečnosť s európskymi predpismi je treba pripraviť novelu zákona č. 69/2018 o kybernetickej bezpečnosti s cieľom zvýšenia odolnosti a vysokej úrovne bezpečnosti nielen sietí a informačných systémov ale tiež všetkých dotknutých prvkov pôsobiacich v kybernetickom priestore. Základom efektívne fungujúcich procesov sú dobre nastavené regulačné normy. Vychádzajúc z implementácie Koncepcie bezpečnostnej stratégie na roky 2016 -2020 a jej záverečného hodnotenia a odporúčaní pre ďalšie obdobie, je nevyhnutné pripraviť a zabezpečiť schválenie novely vyhlášky, ktorou sa určujú identifikačné kritériá prevádzkovateľom základnej služby a vyhlášky, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov.

Výstupy
- Novelizácia zákona č. 39/2018 o kybernetickej bezpečnosti
- Novelizácia vyhlášok vychádzajúcich zo zákona č. 69/2018 o kybernetickej bezpečnosti

1.3 Analytická činnosť pre podporu budovania bezpečnostného povedomia spoločnosti a priemyslu

Jednotlivé úlohy reflektujú potrebu analyzovania úrovne vzdelávania, šírenia bezpečnostného povedomia ako aj poskytovania podpory v oblasti kybernetickej bezpečnosti. V zmysle Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025 je jedným zo strategických cieľov vzdelaná verejnosť. Za týmto účelom bude vypracovaná koncepcia rozvoja bezpečnostného povedomia, budovania spôsobilosti a prevencie verejnosti v kybernetickej doméne ako aj vzdelávacej, informačnej kampane pre obyvateľov na identifikáciu hrozieb a vplyvov pôsobiacich v kybernetickom priestore. Okrem toho budú vypracované analytické štúdie zamerané na výzvy a riešenia dopadov prvkov informačných operácií v kybernetickom priestore za účelom ich budúcej prezentácie a odbornej diskusie na pracovných stretnutiach, workshopoch, konferenciách a besedách pri okrúhlom stole. Čo sa týka poskytovania podpory pre oprávnené novovybudované EDIHy, úloha NBÚ bude najmä v posudzovaní bezpečnosti technickej infraštruktúry, prípravy na cvičenia z oblasti kybernetickej bezpečnosti, v asistencií pri vyhodnocovaní logov a udalostí z prvkov HW a SW v reálnom čase a ďalších opatreniach.

Nemenej dôležitou oblasťou bude vypracovanie indexu pravidelného merania stavu kybernetickej bezpečnosti a identifikácia zraniteľných miest štátnej, verejnej správy ako i verejných subjektov.

Výstupy

- Koncepcia rozvoja bezpečnostného povedomia, spôsobilosti a prevencie verejnosti
- Vypracovanie podkladov pre plán šírenia a zvyšovania bezpečnostného povedomia v oblasti kybernetickej bezpečnosti
- Index pravidelného merania stavu kybernetickej bezpečnosti
- Podpora oprávnených EDIHov v poskytovaní služieb z portfólia kybernetickej bezpečnosti

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
A.1 Budovanie analytickej jednotky NBÚ a udržanie expertných kapacít v nadväznosti na implementáciu kľúčových úloh zo	Efektívne riadenie procesov a nastavenie metodík pri implementácii kľúčových úloh z Akčného plánu realizácie Národnej stratégie kybernetickej bezpečnosti v priebehu rokov	Žiadateľ NBÚ	17

strategických dokumentov	2022 a 2023, vrátane posilnenia a stabilizovania odborných kapacít.		

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**
Aktivita 1		
521 Mzdové výdavky	630 000 EUR	Mzdové náklady spojené so zabezpečením a posilnením personálnych kapacít participujúcich na projekte v období 17 mesiacov realizácie. Odborná časť projektu: 12 expertov v oblasti kybernetickej bezpečnosti (fyzické osoby v služobnom pomere) z toho 6 expertov pracujúcich na 100% úväzok na projekte a 6 expertov na 60% úväzok na projekte, čo predstavuje 9,6 FTE. Podporná časť projektu: 2 zamestnanci (projektový a finančný manažér, v služobnom pomere) pracujúci na 40% úväzok na projekte, čo predstavuje 0,8 FTE. Výška priemernej mesačnej brutto mzdy na FTE predstavuje 2 616,00 EUR**.
Hlavné aktivity SPOLU	630 000 EUR	

Paušálna sadzba	94 500 EUR	Sadzba (15%) stanovená na základe Čl. 68 písm. b) nariadenia EP a Rady (EÚ) č. 1303/2013 - administratívno – technická podpora, materiálno-technické zabezpečenie, IKT podpora, školenia, cestovné náhrady a náklady na služobné cesty, služby spojené s používaním analytických nástrojov.
CELKOM	724 500,00 EUR	

*Rozpočet je zostavený na 17 mesiacov realizácie projektu
** Výpočet zohľadňuje vyššie odvody príslušníkov policajného zboru vo výške 36,2%

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

Národný projekt je v súlade s princípom doplnkovosti, definovanom v článku 95 Nariadenie Európskeho parlamentu Rady č. 1303/2013, ktorým sa stanovujú všeobecné ustanovenia o Európskom fonde regionálneho rozvoja, Európskom sociálnom fonde, Kohéznom fonde a Európskom námornom a rybárskom fonde, z čoho vyplýva, že implementácia projektu nenahrádza verejné alebo ekvivalentné štrukturálne výdavky členského štátu. Členský štát financuje činnosť štátneho orgánu pričom výdavky spojené s realizáciou národného projektu predstavujú minoritnú časť na zabezpečenie kapacít uskutočňujúcich činnosti s pridanou hodnotou v rámci reformných aktivít.

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

Áno – paušálna sadzba (15%) stanovená na základe Čl. 68 písm. b) nariadenia EP a Rady (EÚ) č. 1303/2013.

16. Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov
Informácie sa vypĺňajú iba pre investičné[16] typy projektov.

Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov	
Existuje relevantná štúdia uskutočniteľnosti[17] ? (áno/nie)	N/A
Ak je štúdia uskutočniteľnosti dostupná na internete , uveďte jej názov a internetovú adresu, kde je štúdia zverejnená	N/A

[16] 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.
[17] 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)

V prípade, že štúdia uskutočniteľnosti nie je dostupná na internete, uveďte webové sídlo a termín, v ktorom predpokladáte jej zverejnenie (mesiac/rok)	N/A