Európska únia
Európsky fond
regionálneho
rozvoja

Vzor CKO č. 34
verzia 1

Programové obdobie 2014 – 2020

Vec:	Zámer národného projektu
Určené pre:	Riadiace orgány Sprostredkovateľské orgány
Na vedomie:	Certifikačný orgán Orgán auditu Gestori horizontálnych princípov
Vydáva:	Centrálny koordinačný orgán Úrad podpredsedu vlády SR pre investície a informatizáciu v súlade s kapitolou 1.2, ods. 3, písm. a) Systému riadenia európskych štrukturálnych a investičných fondov
Záväznosť:	Vzor je pre subjekty, ktorým je určený záväzný. Subjekty, ktorým je vzor určený môžu vzor doplniť s ohľadom na špecifické potreby OP, pričom musí byť zachovaný minimálny obsah uvedený vo vzore.
Dátum vydania:	31.10.2017
Dátum účinnosti:	31.10.2017
Schválil:	JUDr. Denisa Žiláková generálna riaditeľka sekcie centrálny koordinačný orgán

Názov národného projektu: Dlhodobý strategický výskum v oblasti šifrovej ochrany a IT 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)

Národný bezpečnostný úrad (ďalej aj ako „NBÚ“) je ústredný orgán štátnej správy pre oblasť ochrany utajovaných skutočností, šifrovú ochranu informácií, kybernetickú bezpečnosť a dôveryhodné služby. V zmysle zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností úrad vykonáva a zabezpečuje výskum a vývoj v oblasti kryptológie, výskum a vývoj v oblasti šifrovej ochrany informácií (ďalej len „ŠOI“). Oblasť ŠOI je z vecného hľadiska veľmi špecifická a je jedným zo základných atribútov v oblasti informačnej bezpečnosti s dosahom ako na štátnu správu, tak aj na súkromný sektor s presahom na štruktúry EÚ a NATO. NBÚ disponuje odbornými kapacitami, ktoré sa podieľajú na plnení úloh výskumu a vývoja v oblasti ŠOI, na plnení úloh v oblasti nežiaduceho elektromagnetického vyžarovania (ďalej len „NEV“), a ďalších oblastiach majúcich vplyv na zabezpečenie ochrany utajovaných skutočností. NBÚ je taktiež ústredným orgánom štátnej správy pre kybernetickú bezpečnosť. Z pohľadu kompetencií Národného bezpečnostného úradu a jeho skúseností s riešením úloh v oblasti výskumu a vývoja, ktoré prispievajú k ochrane informačno-komunikačných technológií a boli riešené formou prepojenia vedeckých kapacít Slovenskej republiky v daných oblastiach s podnikateľským sektorom a zahraničnými partnermi, je vhodné realizovať navrhovaný projekt prostredníctvom národného projektu.

Prostredníctvom národného projektu bude zabezpečený výskum, vývoj, návrh a implementácia národnej technologickej platformy PKI spôsobilej na ochranu utajovaných skutočností, ktorá bude využitá aj pre potreby interoperability s PKI platformami EU/NATO. Cieľom je využívanie PKI infraštruktúry ako súčasti kontrolovaného prostredia, ktorým riadi prístup používateľov k zdrojom IS. Naplnenie tohto zámeru by s ohľadom na ochranu utajovaných skutočností prostredníctvom dopytovo orientovaného projektu nebolo možné.

Prostredníctvom národného projektu sa zabezpečí vytvorenie bezpečnostných nastavení pre operačné systémy mobilných zariadení, ktoré v súčasnosti predstavujú neoddeliteľnú súčasť IKT. Budú analyzované jednotlivé operačné systémy, ich zraniteľnosti a navrhnuté bezpečnostné nastavenia (šablóny) ktorých aplikáciou bude možné využívať mobilné zariadenia na prenos a uchovávanie utajovaných skutočností. Naplnenie tohto zámeru by s ohľadom na ochranu utajovaných skutočností prostredníctvom dopytovo orientovaného projektu nebolo možné.

Požiadavka prepojenia neutajovaných a utajovaných systémov zo dňa na deň rastie, preto v rámci národného projektu bude vyvinuté univerzálne VPN riešenie spôsobilé chrániť utajované skutočnosti stupňa utajenia „Vyhradené“ a „Dôverné“ v národných sieťach. Ďalším prínosom bude vyvinutie univerzálnej brány (gateway), pomocou ktorej bude možné bezpečné prepojenie komunikačných systémov spôsobilých chrániť utajované

skutočnosti rôzneho stupňa utajenia. Naplnenie tohto zámeru by s ohľadom na ochranu utajovaných skutočností prostredníctvom dopytovo orientovaného projektu nebolo možné.

Nežiaduce elektromagnetické vyžarovanie (ďalej ako „NEV“) predstavuje z hľadiska fyzikálnych princípov jeden z možných spôsobov úniku utajovaných skutočností. V Slovenskej republike ani vo väčšine krajín EÚ a NATO v súčasnosti neexistuje komplexný systém ochrany pred NEV, ktorý by bol schopný dostatočne rýchlo reagovať na nové hrozby. Účelom národného projektu je takýto systém v SR zrealizovať, pričom naplnenie tohto zámeru by s ohľadom na ochranu utajovaných skutočností prostredníctvom dopytovo orientovaného projektu nebolo možné.

2. Príslušnosť národného projektu k relevantnej časti operačného programu

Prioritná os	PO 1 Podpora výskumu, vývoja a inovácií
Investičná priorita	1.1 Rozšírenie výskumnej a inovačnej infraštruktúry a kapacít na rozvoj excelentnosti v oblasti výskumu a inovácií a podpora kompetenčných centier 1.2 Podpora investovania podnikov do výskumu a inovácie a vytvárania prepojení a synergií medzi podnikmi, centrami výskumu a vývoja a vysokoškolským vzdelávacím prostredím, najmä podpory investovania do vývoja produktov a služieb, prenosu technológií, sociálnej inovácie, ekologických inovácií, aplikácií verejných služieb, stimulácie dopytu, vytvárania sietí, zoskupení a otvorenej inovácie prostredníctvom inteligentnej špecializácie za podpory technologického a aplikovaného výskumu, pilotných projektov, opatrení skorého overovania výrobkov, rozšírených výrobných kapacít, prvej výroby, najmä v základných podporných technológiách, a šírenia technológií na všeobecný účel
Špecifický cieľ	1.1.3 Zvýšenie výskumnej aktivity prostredníctvom zlepšenia koordinácie a konsolidácie VaV potenciálu výskumných inštitúcií nevykonávajúcich hospodársku činnosť 1.2.1 Zvýšenie súkromných investícií prostredníctvom spolupráce výskumných inštitúcií a podnikateľskej sféry
Miesto realizácie projektu (na úrovni kraja)	VÚC: Košický kraj, Bratislavský kraj, Žilinský kraj, Trenčiansky kraj
Identifikácia hlavných cieľových skupín (ak relevantné)	Výskumné inštitúcie Akademický sektor Podnikateľský sektor vrátane podnikateľov spracúvajúcich utajované skutočnosti Zamestnanci orgánov verejnej moci

3. Prijímateľ[1] národného projektu

Dôvod určenia prijímateľa národného projektu[2]	Národný bezpečnostný úrad (ďalej aj ako „NBÚ“) je ústredný orgán štátnej správy pre oblasť ochrany utajovaných skutočností, šifrovú ochranu informácií, kybernetickú bezpečnosť a dôveryhodné služby. Úrad plní úlohy vyplývajúce zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností v znení neskorších predpisov. V zmysle zákona úrad vykonáva a zabezpečuje výskum a vývoj v oblasti kryptológie, výskum a vývoj v oblasti šifrovej ochrany informácií (ďalej len „ŠOI“). Oblasť ŠOI je z vecného hľadiska veľmi špecifická a je jedným zo základných atribútov v oblasti informačnej bezpečnosti s dosahom ako na štátnu správu, tak aj na súkromný sektor s presahom na štruktúry EÚ a NATO.
Má prijímateľ osobitné, jedinečné kompetencie na implementáciu aktivít národného projektu priamo zo zákona, osobitných právnych predpisov, resp. je uvedený priamo v príslušnom operačnom programe?	V súlade so zákonom o ochrane utajovaných skutočností je úrad ústredným šifrovým orgánom Slovenskej republiky. Medzi jeho hlavné úlohy v oblasti šifrovej ochrany patrí certifikácia prostriedkov a uznávanie zahraničných certifikátov, kontrola bezpečnosti prostriedkov, vydávanie bezpečnostných štandardov, koordinácia výskumu a vývoja, riadenie a koordinácia rezortných šifrových orgánov a zabezpečovanie vládneho a zahraničného spojenia. Úrad sa stal ústredným orgánom štátnej správy pre kybernetickú bezpečnosť.
Obchodné meno/názov (aj názov sekcie ak relevantné)	Národný bezpečnostný úrad
Sídlo	Bratislava, Budatínska 30, 851 06
IČO	36 061 701

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

Zdôvodnenie potreby partnera národného projektu (ak relevantné)[3]	Profesijný partner prijímateľa v oblasti bezpečnosti informačných systémov a oblasti elektromagnetického vyžarovania
Kritériá pre výber partnera [4]	Partner bol vybratý na základe požiadavky na

[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).

[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

	výskumné a vývojové aktivity v relevantnej oblasti. Podporuje sedem centier excelentného výskumu (napr. Centrum IKT pre znalostné systémy, Centrum excelentnosti výkonových elektronických systémov a materiálov pre ich komponenty, Centrum excelentnosti integrovaného výskumu a využitia progresívnych materiálov a technológií v oblasti automobilovej elektroniky), ktoré z pohľadu predkladaného národného projektu garantujú realizáciu výskumných a vývojových aktivít a projektov na vysokej úrovni a transfer získaných výsledkov výskumu do praxe.
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie.
Obchodné meno/názov	Technická univerzita v Košiciach
Sídlo	Letná 9, 04001 Košice - mestská časť Sever
IČO	00397610

Zdôvodnenie potreby partnera národného projektu (ak relevantné)	Profesijný partner prijímateľa v oblasti elektromagnetického vyžarovania a ochrany kritickej infraštruktúry.
Kritériá pre výber partnera	Partner bol vybratý na základe požiadavky na výskumné a vývojové aktivity v relevantnej oblasti. Na pôde ŽU bol zrealizovaný projekt Univerzitný vedecký park ŽU s nosnými témami zameranými aj na aplikovaný výskum v oblasti IKT. Medzi nosné vedecké aktivity sa radí vývoj nových materiálov a technológií využiteľných v oblasti ochrany proti NEV a ochrana kritickej infraštruktúry vrátane inovatívnych prvkov v monitorovaní tejto infraštruktúry.
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie.
Obchodné meno/názov	Žilinská univerzita v Žiline
Sídlo	Univerzitná 8215/1, 01026 Žilina
IČO	00397563

Zdôvodnenie potreby partnera národného projektu (ak relevantné)	Profesijný partner prijímateľa v oblasti bezpečnosti informačných systémov, PKI, šifrovej ochrany informácií a elektronického podpisu.
Kritériá pre výber partnera	Partner bol vybratý na základe požiadavky na výskumné a vývojové aktivity v relevantnej oblasti. UPJŠ sa podieľala na viacerých VaV projektoch, ktoré súviseli s infraštruktúrou PKI a EP (projekt

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.

	infraštruktúry PKI ako hlavnej technologickej platformy pilotného riešenia elektronických volieb). Partner disponuje skúseným odborným personálom, ktorý sa zaoberá návrhom a analýzou kryptografických algoritmov a protokolov a ich implementáciou v softvérovej a hardvérovej oblasti.
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie.
Obchodné meno/názov	Univerzita Pavla Jozefa Šafárika v Košiciach
Sídlo	Šrobárova 2, 04180 Košice - mestská časť Staré Mesto
IČO	00397768

Zdôvodnenie potreby partnera národného projektu (ak relevantné)	Profesijný partner prijímateľa v oblasti bezpečnosti a obrany SR. Prioritne rieši projekty výskumu a vývoja zamerané na kybernetickú bezpečnosť a oblasť komunikačných a informačných systémov vrátane sieťových protokolov.
Kritériá pre výber partnera	Partner bol vybratý na základe požiadavky na výskumné a vývojové aktivity v relevantnej oblasti. Partner má uzavretú zmluvu o spolupráci v oblasti vedy a techniky s prijímateľom. Má vybudované laboratórium elektromagnetického vyžarovania a susceptibility, ktoré je kompletne vybavené zariadením a prístrojmi slúžiacimi na experimentálne meranie a testovanie elektronických zariadení. Taktiež má laboratórium informačnej bezpečnosti. AOS je členom Slovenskej asociácie dodávateľov a užívateľov vojenských komunikačných a informačných systémov AFCEA, ktorá sa zaoberá najmä problematikou riadiacich systémov a informačných technológií pre použitie v štátnej správe.
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie.
Obchodné meno/názov	Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Sídlo	Liptovský Mikuláš, Demänová 393, 031 06
IČO	37910337

Zdôvodnenie potreby partnera národného projektu (ak relevantné)	Profesijný partner prijímateľa pri riešení úloh z oblasti IKT a elektromagnetického vyžarovania.
Kritériá pre výber partnera	STU, fakulta elektrotechniky a informatiky dlhodobo spolupracuje s prijímateľom na riešení úloh výskumu a vývoja. K riešeným úlohám patrí vývoj meracej aparatúry na zónové merania priestorov a programového vybavenia pre aparatúru

	na zónové merania a meranie útlmu tienených komôr (rok 2006), vytvorenie databázy konštrukčných materiálov z hľadiska hodnôt ich elektromagnetického útlmu (rok 2007) a simulácia elektromagnetických polí (roky 2008 až 2009).
Má partner monopolné postavenie na implementáciu týchto aktivít? (áno/nie) Ak áno, na akom základe?	Nie
Obchodné meno/názov	Slovenská technická univerzita v Bratislave
Sídlo	Bratislava, Vazovova 5. 812 43
IČO	00397 687

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	jún/2018
Uveďte plánovaný štvrťrok podpísania zmluvy o NFP s prijímateľom	IV/2018
Uveďte plánovaný štvrťrok spustenia realizácie projektu	IV/2018
Predpokladaná doba realizácie projektu v mesiacoch	48 mesiacov

6. Finančný rámec

Alokácia na vyzvanie (zdroj EÚ a ŠR)	39 000 000 eur
Celkové oprávnené výdavky projektu	39 000 000 eur
Vlastné zdroje prijímateľa	0

7. Východiskový stav

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

Priorita kybernetickej bezpečnosti je zdôraznená vo viacerých koncepčných a strategických dokumentoch EÚ a Organizácie Severoatlantickej zmluvy (ďalej len „NATO“), ako aj v dokumentoch ďalších významných organizácií po celom svete, kde sa narušenie kybernetického priestoru chápe ako jedna z kľúčových hrozieb súčasnosti. EÚ v rámci svojho kybernetického priestoru zadefinovala východiská a ciele kybernetickej bezpečnosti v podobe **Stratégie kybernetickej bezpečnosti EÚ**, z ktorej vychádzajú aj princípy, ciele, priority a postupy budovania kybernetickej bezpečnosti v Slovenskej republike.

17. júna 2015 vláda Slovenskej republiky schválila uznesením č. 328/2015 **Koncepciu kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020**, ktorej cieľom bolo navrhnúť nový inštitucionálny rámec riadenia kybernetickej bezpečnosti v Slovenskej republike. Reagovala tak na prioritu návrhu smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sieťových a informačných systémov v Únii a na určenie vnútroštátneho príslušného orgánu pre bezpečnosť sieťových a informačných systémov.

Návrh **Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020** schválila vláda SR dňa 2. marca 2016 uznesením č. 93/2016. Akčný plán obsahuje návrh úloh, ktorých cieľom je zabezpečiť primeranú ochranu kybernetického priestoru štátu pred potenciálnymi hrozbami, ktorých uplatnením by mohli vzniknúť Slovenskej republike nenahraditeľné škody, a tak by mohla byť narušená dôveryhodnosť štátu, či organizácie. Akčný plán ku Koncepcii je jeden zo základných dokumentov definujúcich zoznam úloh na obdobie rokov 2016 až 2020 zameraných na tvorbu právnych predpisov, štandardov, metodických pokynov, pravidiel, bezpečnostných politík, medzinárodnej spolupráce, zvyšovania povedomia a spôsobilostí, ako aj iných aktivít potrebných k zaisteniu ochrany a obrany národného kybernetického priestoru.

NBÚ zriadil a prevádzkuje Bezpečnostné a prevádzkové monitorovacie centrum SK CSIRC. Vláda SR uložila Národnému bezpečnostnému úradu zriadiť uvedené centrum SK CSIRC uznesením vlády SR č. 771 z 9. januára 2008, ktorým schválila „**Koncepciu šifrovej ochrany informácií v SR na roky 2009 – 2013“ a neutajovanú prílohu „Návrh opatrení na realizáciu Koncepcie ŠOI“** s úlohami v oblasti realizácie kybernetickej obrany v SR. Jednou z úloh bolo konštituovať národný CSIRC v rámci NBÚ ako ústredné koordinačné a technické centrum pre riešenie problematiky kybernetickej ochrany zabezpečujúce najmä koordináciu činností podriadených orgánov v rámci ochrany kybernetického priestoru. NBÚ prostredníctvom svojho pracoviska SK CSIRC spracováva informácie o kybernetických incidentoch prevažne v utajovaných komunikačných a informačných sieťach. Uskutočňuje tak predovšetkým v spolupráci s NCIRC (NATO CIRC) aj EU NSIAM (European Union Network Security Incident Alert Mechanism)ako aj ďalšími pracoviskami. Tieto informácie spolu s navrhovanými protiopatreniami sú ďalej distribuované formou bulletinov aj ďalším rezortom utajovaným informačným systémom (KIS Apeiron) a zároveň informácie o hrozbách a incidentoch sú zdieľané s ďalšími rezortmi aj prostredníctvom Národného bezpečnostného analytického centra (NBAC). Úrad prostredníctvom nadrezortného komunikačného a informačného systému Apeiron postupuje taktiež varovania vydané EÚ v rámci SR. EÚ vytvorila pre svoje utajované systémy zaradené do kritickej infraštruktúry jednotný varovný systém EU NSIAM, prostredníctvom ktorého distribuuje členským krajinám varovné správy. Kontaktným bodom v SR pre systém NSIAM je SK CSIRC pri Národnom bezpečnostnom úrade. V súčasnosti je aktuálna **Koncepcia šifrovej ochrany informácií Slovenskej republiky na roky 2017 – 2020**, ktorej cieľom je vytýčiť smerovanie ďalšieho vývoja ŠOI v Slovenskej republike s ohľadom na pokrok v informačných technológiách a v informatizácii spoločnosti. Úlohou šifrovej ochrany informácií je predovšetkým zabezpečiť dôvernosť informácií v kybernetickom priestore počas celého ich životného cyklu a prípadne aj možnosť chrániť ich integritu, autenticitu a nepopierateľnosť. Požiadavka na zabezpečenie ochrany informácií šifrovaním vyplýva priamo zo zákona č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých

zákonov v znení neskorších predpisov, podľa ktorého informácie, ktoré sú utajovanými skutočnosťami, musia byť pri prenose chránené prostriedkami šifrovej ochrany informácií.

Aktuálne prebiehajú práce na návrhu **zákona o kybernetickej bezpečnosti**, ktorý komplexne upraví oblasť kybernetickej a informačnej bezpečnosti, zavedie základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Zároveň sa do slovenského právneho poriadku transponuje európska Smernica o sieťovej a informačnej bezpečnosti (NIS). Dňa 9. novembra 2017 bol vládny návrh zákona o kybernetickej bezpečnosti predložený na rokovanie Národnej rady Slovenskej republiky, druhé čítanie prebehne v januári 2018.

Slovenská republika ako členská krajina NATO a EÚ sa podieľa aj na tvorbe medzinárodných strategických a koncepčných dokumentov, medzinárodných politík a štandardov. V rokoch 2013 – 2014 Národný bezpečnostný úrad plnohodnotne prevzal úlohu budovania kybernetickej obrany a informačnej bezpečnosti NATO v podmienkach Slovenskej republiky v rámci obranného plánovania Ciele síl 2013. NBÚ má gesciu nad plnením cieľa „Informačná bezpečnosť a kybernetická obrana“ (E5308: Information Assurance and Cyber Defence), ktoré je Slovenská republika povinná plniť v rámci procesu obranného plánovania (NATO Defence Planning Capabilities). Spôsob plnenia tohto cieľa spôsobilostí bol na národnej úrovni rozpracovaný v materiáli „**Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky“.** Cieľom materiálu je zabezpečiť plnenie záväzku Slovenskej republiky voči NATO vyplývajúceho z dokumentu pre riešenie kolektívnych obranných spôsobilostí, ktorý rieši budovanie kolektívnych obranných spôsobilostí v jednotlivých, pravidelných plánovacích cykloch. Prijatím materiálu má NBÚ pozíciu zabezpečovať a koordinovať vybudovanie spôsobilostí SR v oblasti kybernetickej obrany vyplývajúcich z tohto materiálu. NBÚ zároveň každoročne predkladá vláde SR na schválenie správu o plnení úloh vyplývajúcich z tohto materiálu.

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

NA

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)

Národný bezpečnostný úrad v spolupráci so Slovenskou technickou univerzitou v Bratislave

Od roku 2004 do roku 2009 zadal NBÚ viacero úloh v oblasti výskumu a vývoja v oblasti NEV, ktoré riešil v spolupráci so Slovenskou technickou univerzitou v Bratislave. Národný bezpečnostný úrad disponuje vlastným interným laboratórnym prostredím, v rámci ktorého vykonáva výskumné aktivity zamerané na oblasť NEV. Základný zoznam úloh riešených formou výskumu a vývoja v spolupráci so Slovenskou technickou univerzitou v Bratislava, fakulta elektrotechniky a informatiky:

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

- Vývoj meracej aparatúry na zónové merania priestorov a programového vybavenia pre aparatúru na zónové merania priestorov a merania útlmu tienených komôr (rok 2004-2006)

  Riešenými oblasťami boli predovšetkým vývoj všesmerovej vysielacej anténny, vývoj a výroba špeciálnych prevodníkov, vývoj programového vybavenia pre predmetnú aparatúru a vývoj a realizácia zástavby aparatúry do špeciálnych ochranných obalov. Vyvinutá aparatúra bola využívaná ako primárny systém na vykonávanie zónových meraní priestorov v súlade s platnými predpismi na ochranu pred nežiaducim elektromagnetickým vyžarovaním až do decembra 2016.

- Vytvorenie databázy konštrukčných materiálov z hľadiska hodnôt ich elektromagnetického útlmu (rok 2007)

  Bola vypracovaná štúdia „Databáza konštrukčných materiálov z hľadiska hodnôt ich elektromagnetického útlmu“. Obsahom štúdie bolo:
  1. Teoretické základy mechanizmov elektromagnetického tienenia
  2. Spôsoby merania tieniacich vlastností konštrukčných materiálov.
  3. Posúdenie možností budúceho riešenia (možnosti získania databázy tieniacich vlastností konštrukčných materiálov a možnosti realizácie meraní tieniacich vlastností).
  4. Bola spracovaná Základná štúdia č. ŠFEI/2007/3576 k projektu vytvorenia databázy konštrukčných materiálov z hľadiska hodnôt ich elektromagnetického útlmu a „Zásady pre návrh priestorov s nízkym vyžarovaním elektromagnetických vĺn do okolia.

- Simulácia elektromagnetických polí, na základe údajov získaných z dostupných zdrojov vytvoriť databázu materiálov za účelom ich využitia pri simuláciách šírenia elektromagnetických polí a realizovať simulácie šírenia elektromagnetických polí z definovaného zdroja v reálnom prostredí (rok 2008-2009)

  Bola vypracovaná základná štúdia pre vytvorenie univerzálneho matematického modelu pre počítačovú simuláciu priestorového šírenia elektromagnetických signálov z užívateľom definovaného zdroja.

  V januári 2010 bola vydaná správa k riešeniu zmluvy o dielo č. 3198/2009/IBEP-001 „Simulácia a meranie elektromagnetického tlmenia stavebných materiálov. Teoretické a praktické aspekty návrhu priestorov s nízkym elektromagnetickým vyžarovaním“. Veľká časť výsledkov prác bola prezentovaná na podujatí SK NSA TEMPEST MEETING 2009 v Brunovciach. Bola navrhnutá nová metodika merania vlastností stavebných materiálov a vykonané merania.

  Praktické využitie simulácií šírenia elektromagnetických polí a ich nahradenie zónovými meraniami pri skúmaní útlmových vlastností priestorov za účelom zabezpečenia ochrany utajovaných skutočností pred ich únikom prostredníctvom nežiaduceho elektromagnetického vyžarovania sa ukázalo ako neefektívne, berúc do úvahy špecifickosť jednotlivých priestorov a z toho vyplývajúce nároky na zložitosť programu/modelov, výpočtový čas, výkon, atď.

Žilinská univerzita v Žiline
V oblasti vedy a výskumu sú pracoviská ŽU zapojené do riešenia viac ako 150 vedeckých a výskumných projektov finančne podporovaných z verejných zdrojov prostredníctvom celoštátnych grantových schém v objeme 2,1 mil. EUR. Súčasne riešia kolektívy 35 projektov podporovaných zo zahraničia, predovšetkým v rámci 6. a 7. rámcového programu EÚ. Riešiteľské kolektívy úzko spolupracujú s partnermi z hospodárskej sféry v aplikovanom výskume. V rámci štrukturálnych fondov prostredníctvom operačného programu výskum a vývoj je podporovaných 6 centier excelentnosti.

Na pôde ŽU bol realizovaný projekt Univerzitný vedecký park ŽU a nosné témy projektu sú zamerané aj na oblasť informačných a komunikačných technológií. Žilinská univerzita v Žiline sa historicky od svojho vzniku zaoberala výskumom so zameraním na oblasť dopravy a technickej praxe. V súčasnosti sa medzi nosné vedecké aktivity radia aj vývoj nových materiálov a technológií využiteľných v oblasti ochrany proti NEV a aktivity v oblasti informačných a komunikačných technológií.

Univerzitný vedecký park sa orientuje na vedecký prístup k riešeniu problémov aplikovaných v praxi, pričom využíva a integruje znalosti a skúsenosti vedcov a odborníkov z praxe. Jednou z hlavných oblastí záujmu je ochrana kritickej infraštruktúry kde jednotlivé výskumné tímy prinášajú riešenia problémov a inovatívne prvky v monitorovaní tejto infraštruktúry. Dôležitou časťou výskumných aktivít je vývoj systémov, ktoré zmierňujú alebo úplne potláčajú negatívne pôsobenia ľudského faktora. Výskumné aktivity so špecifickým zameraním sú zamerané na oblasť vývoja nových materiálov a technológií. Ide o výskum a vývoj systémových aplikácií na báza optických vlákien a fotonických prvkov, výskum metód a aplikácií v biomedicínskom inžinierstve a výskum nekonvenčných pohonov a ich komponentov. Posledná oblasť výskumu sa okrem vlastného výskumu zameriava na podporu hlavných výskumných zámerov Univerzitného vedeckého parku ŽU v Žiline. Ide o aplikovaný výskum v oblasti informačných a komunikačných technológií. Predmetom výskumu sú oblasti výskumu senzorových sietí a spracovania neurčitej informácie, spracovania audiovizuálnej informácie, a výskum v oblasti znalostných technológií a podpory rozhodovania.

Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Okrem napĺňania svojho poslania ako vzdelávacej inštitúcie v rezorte obrany plní AOS aj vedecké úlohy. Prioritne rieši projekty výskumu a vývoja najmä na podporu bezpečnosti a obrany SR, pričom rieši celý rad projektov zameraných na oblasť bezpečnosti komunikačných a informačných systémov. Medzi partnerov, s ktorými AOS spolupracuje patria okrem slovenských organizácií napr.: THALES COMMUNICATIONS S.A.(TCF), Francúzsko, Military University of Technology (MUT), Poľsko,, Royal Military Academy (RMA), Belgicko, JOANNEUM RESEARCH (JR), Rakúsko, Netherlands Organization for Applied Scientific Research (TNO), Holandsko, Fraunhofer Institut für Kommunikation Informationsverarbeitung und Ergonomie (FKIE), Germany.

Akadémia ozbrojených síl je členom AFCEA Slovak Chapter ("Slovenská asociácia dodávateľov a užívateľov vojenských komunikačných a informačných systémov AFCEA"), ktorá sa zaoberá najmä problematikou riadiacich systémov a informačných technológií pre použitie v štátnej správe s dôrazom na ozbrojené sily.
Partnerstvá sú rozvíjané na základe zmlúv o spolupráci v oblasti vedy a techniky. Jedná sa najmä o vytváranie spoločných vedeckovýskumných pracovísk excelentnosti, predkladanie ponúk na spoločné riešenie vedeckých projektov, spolupráca pri ich riešení, spoločné uverejňovanie výsledkov dosiahnutých pri ich riešení, vzájomné poskytovanie vedeckých informácií, vzájomná personálna, materiálovo-technická a technologická podpora, spolupráca pri organizovaní vedeckých podujatí a sprostredkovanie prístupu k poznatkom súčasného stavu vedy, materiálového výskumu, technológie a vývoja špeciálnej techniky. Jednou z takýchto zmlúv je aj Zmluva s NBU.

Univerzita P. J. Šafárika Košice
UPJŠ sa v minulosti podieľala na viacerých výskumných a vývojových projektoch, ktoré súviseli s infraštruktúrou PKI a EP, kde v rámci spolupráce s komerčným sektorom prispela k úspešnému návrhu, vývoju, implementácii a spusteniu pilotného riešenia elektronických volieb, v rámci ktorých bola využitá infraštruktúra PKI ako hlavná technologická platforma.

Univerzita disponuje skúseným odborným personálom, ktorý sa zaoberá návrhom a analýzou kryptografických algoritmov a protokolov a ich implementáciou na softvérovej a hardvérovej úrovni. Výskumní pracovníci univerzity v minulosti v oblasti kryptológie publikovali viacero odborných článkov a výsledky svojej výskumnej činnosti prezentovali na významných medzinárodných konferenciách.

Technická univerzita v Košiciach
Trvalý rozvoj vedy v súčasnosti významne podporuje sedem centier excelentného výskumu, ktoré garantujú výskumné a vývojové aktivity a projekty na relevantnej medzinárodnej kvalitatívnej úrovni v oblastiach ich pôsobenia a viaceré sú relevantné aj z pohľadu predkladaného národného projektu:

• Centrum informačných a komunikačných technológií pre znalostné systémy,
• Centrum excelentnosti výkonových elektronických systémov a materiálov pre ich komponenty,
• Centrum excelentného výskumu získavania a spracovania zemských zdrojov,
• Centrum excelentného výskumu progresívnych stavebných konštrukcií, materiálov a technológií,
• Centrum výskumu riadenia technických, environmentálnych a humánnych rizík pre trvalý rozvoj produkcie a výrobkov v strojárstve,
• Centrum excelentnosti integrovaného výskumu a využitia progresívnych materiálov a technológií v oblasti automobilovej elektroniky,
• Centrum výskumu účinnosti integrácie kombinovaných systémov obnoviteľných zdrojov energií.

Národný bezpečnostný úrad
Od roku 2004 do roku 2009 zadal NBÚ viacero úloh v oblasti výskumu a vývoja v oblasti NEV. Žiadateľ disponuje vlastným interným laboratórnym prostredím, v rámci

ktorého vykonáva výskumné aktivity zamerané na oblasť NEV. Základný zoznam úloh riešených formou výskumu a vývoja v spolupráci so Slovenskou technickou univerzitou v Bratislava, fakulta elektrotechniky a informatiky:
• Vývoj meracej aparatúry na zónové merania priestorov a programového vybavenia pre aparatúru na zónové merania priestorov a merania útlmu tienených komôr (rok 2004-2006).
• Vytvorenie databázy konštrukčných materiálov z hľadiska hodnôt ich elektromagnetického útlmu (rok 2007).
• Simulácia elektromagnetických polí, na základe údajov získaných z dostupných zdrojov vytvoriť databázu materiálov za účelom ich využitia pri simuláciách šírenia elektromagnetických polí a realizovať simulácie šírenia elektromagnetických polí z definovaného zdroja v reálnom prostredí (rok 2008-2009).

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

Národné PKI

Na Slovensku sa téma výskumu národnej infraštruktúry PKI prakticky nerieši. Napriek tomu, že samotná podstata a princípy fungovania PKI infraštruktúry má viaceré, už pomerne dlho známe výhody, na národnej úrovni nie je PKI infraštruktúra, až na svetlé výnimky poslednej doby – kedy sa PKI infraštruktúra využila pri budovaní certifikačnej autority poskytujúcej pre nové občianske preukazy (eID) sadu privátnych/verejných kľúčov/certifikátov, vrátane kvalifikovaného certifikátu určeného na vytváranie zaručeného elektronického podpisu – príliš často spomínaná a využívaná. V rámci Slovenska je možné s infraštruktúrou PKI stretnúť skôr len príležitostne, aj to viac menej len pre jednoúčelové prípady, ako napr. bezpečný prostriedok autentizácie pri využívaní elektronických služieb (čipové karty, kľúčové páry, elektronické podpisovanie dávok/výkazov) komerčných, finančných inštitúcií. (napr. Všeobecná zdravotná poisťovňa, ČSOB banka).

Z pohľadu samotného výskumu je však infraštruktúra PKI, vrátane tej národnej, bez akéhokoľvek významnejšieho záujmu/projektu. Väčšina všetkých aktivít súvisiacich s výskumom/vývojom v oblasti PKI súvisí skôr s návrhom/úpravami/modifikáciami softvérového vybavenia, zjednodušením procesov a implementáciou bezpečnejších formátov/algoritmov.

V medzinárodnom kontexte je výskum v rámci PKI infraštruktúry doménou významných inštitúcií a organizácií, ako napr. NATO alebo The National Institute of Standards and Technology (NIST). NATO využíva PKI infraštruktúru ako súčasť kontrolovaného prostredia, ktorým riadi prístup používateľov k zdrojom IS. Neustály technologický rast a nezadržateľný nárast výpočtových kapacít však núti rozvíjať oblasť PKI o nové a bezpečnejšie algoritmy, rýchlejšie a výkonnejšie kryptografické zariadenia a bezpečnejšie aplikačné programové vybavenie. Konkrétne technické špecifikácie nových výskumných činností však zostávajú prakticky bez väčších výnimiek súčasťou utajených informácií jednotlivých štátov/organizácií, pričom ich nedostupnosť býva v takýchto prípadoch dlhoročná**.**

Inovatívne riešenia ochrany utajovaných skutočností (OUS) – zodolnenie a vyladenie systémov

Doposiaľ boli publikovať bezpečnostné nastavenia len na najpoužívanejšie platformy OS pre počítače. Otázkam bezpečnosti operačných systémov mobilných zariadení sa prakticky nevenovala žiadna, alebo len minimálna pozornosť. V súčasnosti však mobilné zariadenia predstavujú neoddeliteľnú súčasť IKT, je potrebné podrobne analyzovať jednotlivé operačné systémy, ich zraniteľnosti a navrhnúť bezpečnostné nastavenia (šablóny) ktorých aplikáciou bude možné využívať mobilné zariadenia na prenos a uchovávanie utajovaných skutočností.

Inovatívne riešenia OUS prostriedkami ŠOI

V súčasnosti neexistuje riešenie spôsobilé chrániť utajované skutočnosti stupňa utajenia „Vyhradené“ a „Dôverné“ v národných sieťach, preto má prijímateľ ambíciu, takéto riešenie v spolupráci s partnermi vyvinúť a následne poskytovať používateľom bezodplatne. V rámci interoperability s NATO bol vyvinutý protokol SCIP, ktorý v blízkej budúcnosti bude predstavovať komunikačný štandard. Preto je potrebné, aby existovalo univerzálne komunikačné riešenie prenášajúce a chrániace hlas, video aj správy s implementovanou podporou protokolu SCIP. Požiadavka prepojenia neutajovaných a utajovaných systémov zo dňa na deň rastie, preto ďalším prínosom tejto aktivity bude vyvinutie univerzálnej brány (gateway), pomocou ktorej bude možné bezpečné prepojenie komunikačných systémov spôsobilých chrániť utajované skutočnosti rôzneho stupňa utajenia.

Bezpečná mobilná pracovná stanica

Je potrebné vyvinúť modulárny flexibilný systém umožňujúci chrániť utajované skutočnosti podľa požiadaviek používateľa. Modulárny systém umožní využiť všetky prednosti jednotlivých častí a v spolupráci s ostatnými súčasťami umožní potlačiť negatíva, čo v konečnom dôsledku prinesie požadovanú úroveň bezpečnosti.

Ochrana proti NEV

Nežiaduce elektromagnetické vyžarovanie (ďalej len „NEV“) predstavuje z hľadiska fyzikálnych princípov jeden z možných spôsobov úniku utajovaných skutočností (ďalej len „US“). Vzhľadom na neustále rastúcu úroveň súčasných technických a technologických možností toto riziko taktiež neustále stúpa. Riziko úniku US prostredníctvom NEV je o to nebezpečnejšie, že je prakticky nezistiteľné, nakoľko nepovolaná osoba s príslušnou technikou vykonáva detekciu a následnú a rekonštrukciu informácií z NEV diaľkovo, t.j. bez potreby vstupu do chráneného resp. kontrolovateľného priestoru. Navyše je detekcia vykonávaná pasívne, t.j. bez generovania akéhokoľvek signálu, ktorý by bolo možné monitorovať.

V Slovenskej republike ani vo väčšine krajín EÚ a NATO v súčasnosti neexistuje komplexný systém ochrany pred NEV, ktorý by bol schopný dostatočne rýchlo reagovať na nové hrozby NEV súvisiace s neustále sa zvyšujúcou úrovňou súčasných technických a technologických možností a ktorý by efektívne pokrýval všetky riziká úniku US prostredníctvom NEV. Problematika skúmania a posudzovania NEV je náročná na odborný potenciál pracovníkov a taktiež aj na špecifické technické vybavenie.

Neexistujú presné metodiky ako vykonávať celý rozsah TEMPEST meraní v súlade s existujúcimi bezpečnostnými štandardami. Taktiež neexistujú ucelené riešenia meracích systémov špecializujúcich sa na TEMPEST pre celú oblasť ochrany pred NEV.

Zraniteľnosti v moderných hardvérových architektúrach

Téma zraniteľností v softvéri, ktoré je možné zneužiť na narušenie dôvernosti, integrity či dostupnosti kybernetických prostriedkov je veľmi široká, dobre definovaná a pochopená. Venujú sa jej mnohé metodiky, medzinárodné štandardy a celosvetovo sa jej venujú tisícky otvorených výskumných tém. Existuje klasifikácia zraniteľností, spôsob ich detekcie a prevencie, metodiky mitigácie.

Naproti tomu téma zraniteľnosti v hardvéri bola až donedávna výskumnou komunitou prevažne ignorovaná, s výnimkou výskumu špecifickej úzkej oblasti výskumu postranných kanálov (elektromagnetické vyžarovanie, napájacie a časovacie útoky, kreatívne využitie senzorov a podobne), i to často zúženej na konkrétny typ hardvéru či softvéru. V nedávnej dobe však bolo odhalených množstvo celých nových tried zraniteľností efektívnych naprieč širokým spektrom hardvéru, ktorých následky a plný rozsah sú v súčasnosti nepreskúmané, čím sa oblasť dostala na špičku záujmu práve prebiehajúceho celosvetového výskumu. Je to spôsobené viacerými faktormi:

• hardvérové architektúry sú čoraz komplikovanejšie, čo prináša nové triedy útokov a nové vektory útoku,
• zraniteľnosti v hardvéri je mimoriadne ťažké odstrániť,
• zraniteľnosti v hardvéri môžu mať významnejší dopad na narušenie bezpečnosti systému ako zraniteľnosti v softvéri,
• prakticky všetky nedávno odhalené triedy útokov sú univerzálne a zraniteľný hardvér je všadeprítomný - zraniteľné sú servery, pracovné stanice, mobilné telefóny, tablety, tlačiarne a iné zariadenia od všetkých významných svetových výrobcov,
• úspešné využitie zraniteľnosti v hardvéri je často zo softvéru (operačného systému) ťažké alebo nemožné odhaliť,
• kybernetická bezpečnosť ako oblasť zažíva veľký rozmach, na verejnosť prenikajú informácie o dobre organizovaných, v určitých prípadoch údajne štátmi podporovaných skupinách útočníkov. Stáva sa otázkou národného záujmu byť schopný odolávať novým typom hrozieb.

Využitie umelej inteligencie v oblasti pokročilých kybernetických hrozieb

Približne od roku 2013 sa dramaticky zlepšujú algoritmy umelej inteligencie a nachádzajú svoje miesto v najrôznejších aplikáciách, vrátane oblasti kybernetickej bezpečnosti. Rozvíjajú sa tiež oblasti ako supervised / unsupervised learning, reinforcement learning a podobne. Samostatnou kategóriou výskumu je adversarial machine learning - výskum techník, ako na umelú inteligenciu zaútočiť a spôsobiť misklasifikáciu alebo zlé naučenie modelu.
Umelá inteligencia v oblasti pokročilých kybernetických hrozieb má množstvo uplatnení, od detekcie neželanej sieťovej aktivity (kybernetické útoky, skenovanie, odhaľovanie sieťových anomálií), cez podporu pri analýze potenciálne škodlivého kódu, až po odstraňovanie chýb a akceleráciu vývoja.

Otvorenými výskumnými témami sú rôzne možnosti aplikácie umelej inteligencie na oblasť kybernetickej bezpečnosti, výskum a vývoj rôznych detekčných techník a zvyšovanie efektivity práce bezpečnostných analytikov nad veľkou množinou dát.

Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach

V minulosti bolo typicky ťažisko vývoja softvéru na jednom autorovi (typicky softvérovej spoločnosti), ktorý do svojho produktu voliteľne zahrnul limitovaný počet knižníc tretích strán, zakúpených a zaintegrovaných počas vývoja softvéru, ku ktorým mal autor softvéru často zakúpenú podporu od autorov knižníc. Takýto produkt bol distribuovaný ako jeden softvérový balík a vzťah s používateľom bol založený na implicitnej dôvere v konkrétneho autora tohto softvéru. Distribučná cesta bola často fyzická (dátové nosiče). Bezpečnosť softvéru a distribučnej cesty bolo možné do značnej miery overiť a riadiť.

Zmena paradigmy vývoja softvéru, súvisiaca s masívnym rozvojom Internetu, spôsobila, že tento jednoduchý model dôvery už neplatí:

- Súčasný softvér sa skladá z tisícov malých komponentov od rôznych autorov. Tieto komponenty majú rozdielne licencie, distribučné cesty, odlišný životný cyklus vrátane vydávania bezpečnostných záplat, podporu, mnohé z nich sú vyvíjané rôznymi typmi komunít alebo dokonca vôbec nevyvíjané. Nielenže už v tomto stave nie je bezpečnosť softvéru manažovateľná, ale tieto komponenty majú svoje ďalšie závislosti, čo problém ďalej znásobuje významne nad možnosti zbežnej kontroly a overenia.
- Spôsob zostavovania aplikácií a ich distribučný model je výrazne komplexnejší, ako v minulosti. Aplikácie už nemusia byť distribuované a udržiavané ako celok, ale napríklad v prípade webových aplikácií so závislosťami z obsahových distribučných sietí (CDN) sa výsledná jedinečná verzia aplikácie zostaví pre každé jedno zobrazenie webovej stránky úplne nanovo. Množstvo softvéru je distribuovaného v zdrojovom tvare, s aktualizáciami vo forme releasov alebo nepretržitým tokom nových funkcií a opráv zapisovaných priamo do online repozitára. Tú istú funkcionalitu a API poskytuje viacero konkurenčných knižníc (napr. v prípade kryptografických knižníc). Aj pri "klasickom" modeli dopredu vytvorenej zostavy aplikácie (build) je teda týchto buildov obrovské množstvo podľa toho, kto, v ktorom čase, s akou kombináciou komponentov a v akých verziách zostavu robil.
- Funkcionalita, ktorú používateľ vníma ako ucelenú aplikáciu, sa často poskytuje cez široký rozsah rôzneho softvéru a hardvéru s odlišnými vlastnosťami, verziami a zostavami softvéru, napríklad kombinácia webovej či mobilnej aplikácie bežiacej na rôznych zariadeniach používateľa (zostavených v reálnom čase a potenciálne odlišne pre každého klienta), zároveň na serveroch prevádzkovateľov jednotlivých služieb, z ktorých niektorí môžu prichádzajúce požiadavky spracovávať v rôznych dátových centrách, pomocou vstupného prvku (semi)náhodne distribuované na viaceré backend servery, ktoré môžu rôzne jednotlivé požiadavky spracúvať na rôznej verzii a zostave softvéru.
- Oblasť kybernetickej bezpečnosti zažíva veľký rozmach a aj pri tom softvéri, ktorý je ešte stále vyvíjaný "klasickým" modelom, je pre autorov obtiažne udržať zabezpečenie vývoja a distribúcie softvéru na dostatočnej kvalitatívnej úrovni, čo ústi do tzv. supply chain útokov.

Toto prináša rozsiahle riziká pre koncových používateľov, prevádzkovateľov serverovej infraštruktúry a bezpečnosť spracúvaných dát. Príkladov z nedávnej minulosti, kedy došlo k ohrozeniu bezpečnosti z dôvodu nedostatočnej kontroly nad životným cyklom a distribučnou cestou softvéru, je viacero. Za všetky spomeňme tieto:

- Malvér NotPetya, distribuovaný v roku 2017 pomocou "supply chain" útoku na autora firemného daňového softvéru MeDoc, spôsobil ďalekosiahle škody v národnom hospodárstve Ukrajiny, postihol viaceré sektory a organizácie vrátane bánk, ministerstiev, energetických firiem, s presahom cca. 20% infekcií do ďalších krajín, vrátane Francúzska, Nemecka, Talianska, Poľska, Ruska, Veľkej Británie, Spojených štátov Amerických a Austrálie.
- limitovaný výskum Národného Bezpečnostného Úradu v septembri 2017 odhalil malvér v balíkových repozitároch Python. Desať populárnych softvérových balíkov sa stalo obeťou "typosquatting" útoku, kedy útočník podsunul falošné verzie populárnych knižníc urllib, bzip, crypt a ďalších. Tieto knižnice boli dostupné medzi júnom a septembrom 2017, preukázateľne viac krát stiahnuté a zahrnuté do ďalšieho softvéru. Výskum sa stretol s veľkým medzinárodným ohlasom a na základe jeho výsledkov sa okrem PyPi (Python) repozitára začali bezpečnosťou svojich repozitárov zaoberať aj komunity okolo iných programovacích jazykov, vrátane NPM (JavaScript) a ďalších.
- v septembri 2017 bol stiahnutý plugin DisplayWidgets pre WordPress s vyše 200 tisíc inštaláciami, do ktorého jeho autor vložil škodlivý kód. Až dodatočne bolo zistené, že plugin aj s používateľmi jeho pôvodný autor pred niekoľkými mesiacmi predal.

Medzi miestami, kde je možné vložiť škodlivý kód, sú teda softvérové repozitáre (github, …), repozitáre knižníc (pypi, npm, …), aplikačne repozitáre (docker hub, …) distribučné obsahové siete a ďalšie miesta. Útočníkom môže byť priamo autor aplikácie (DisplayWidgets), alebo externý útočník (NotPetya). Objem týchto repozitárov je obrovský (napr. pypi - cca. 125 tisíc balíkov, github - cca. 10 miliónov repozitárov) a neustála fluktuácia robí bezpečnostnú inšpekciu veľmi obtiažnou. Predmetom výskumu je teda skúmanie koreňových príčin bezpečnostných problémov, analýza modelov dôvery a závislostí v online repozitároch, následná identifikácia tých repozitárov a distribučných sietí, ktorých zneužitie by potenciálnemu útočníkovi umožnilo ľahkým spôsobom veľký dosah a následne výskum metód a techník na efektívnu identifikáciu škodlivého kódu, napríklad prehľadávaním repozitárov knižníc alebo počas zostavovania či distribúcie finálneho softvéru.

Integrovaný systém na podporu činnosti jednotiek typu CSIRT

Existuje veľa čiastkových technológií, ktoré pokrývajú niektoré z potrieb jednotiek CSIRT. Výskum v tejto oblasti je ohraničený na parciálne témy:

- SIEM softvér
- tiketovacie systémy, databázy konštituencie, databázy aktív a spôsoby ich budovania
- softvér na agregáciu a distribúciu informácií (na úrovni indikátorov alebo dokumentov)
- klasifikáciu
- senzory, skenery zraniteľností a miskonfigurácie

V súčasnosti neexistuje komplexná analýza potrieb jednotiek typu CSIRT na podporný softvér. Vzájomná prepojenosť jednotlivých systémov, šírka ponuky ich funkcií a ich zladenie s procesmi jednotiek typu CSIRT sú pritom kľúčové pre efektívne poskytovanie služieb a úspešné zvládanie neustále rastúceho počtu bezpečnostných incidentov, ktoré musia jednotky CSIRT riešiť alebo koordinovať.

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

V rámci aktivít národného projektu bude uplatňovaný **systém partnerstva**, v ktorom každá z participujúcich inštitúcií v projekte bude mať pridelené konkrétne úlohy aj finančné prostriedky. Princíp partnerstva bude založený na základe uzavretia partnerských zmlúv s partnermi projektu, v ktorých bude mať každý partner a tiež prijímateľ pridelené výskumné úlohy a k nim pridelenú časť nenávratného finančného príspevku. Partneri boli vyberaní s ohľadom na ich skúsenosti, kvalitu a relevantnosť pre oblasť národného projektu tak, aby skladba konzorcia bola reprezentatívna a zahŕňala subjekty z štátnych a verejných výskumných inštitúcií.

Podnikateľské subjekty, ktoré v projekte plnia dôležitú úlohu, budú v národnom projekte vystupovať v pozícii spolupracujúcich subjektov, pričom budú vyberaní v súlade so zákonom o verejnom obstarávaní.

Vzhľadom na špecifickú povahu a rozsah výskumných činností sa predpokladá zriadenie **vedeckej rady projektu**, ktorá bude pozostávať zo zástupcov/vedeckých kapacít žiadateľa a vybraných partnerov a ktorá bude riadiť a koordinovať rámcové aktivity národného projektu. Pre jednotlivé výskumné témy sa predpokladá zriadenie vedeckých projektových výborov, ktoré budú zodpovedné za operatívne riadenie jednotlivých výskumných činností v rámci konkrétnych výskumných tém, pričom členovia vedeckých projektových výborov budú zástupcov/vedeckých kapacít partnerov zúčastnených na konkrétnej výskumnej téme. Samotné výskumné tímy budú koncipované spôsobom, že na čele tímu bude definovaný garant (senior-výskumník), ktorý bude nositeľom výskumnej témy, bude mať svojho definovaného zástupcu a bude koordinovať všetky aktivity v rámci jednotlivých výskumných etáp. Garant bude poskytovať súčinnosť vedeckému projektovému výboru.

Cieľom predkladaného národného projektu je okrem dosiahnutia samotných obsahových výstupov aj snaha o podstatné zvýšenie kvalitatívnej úrovne výskumu a vývoja v oblastiach, na ktorý je zameraný. V tomto zmysle je snahou zintenzívniť medzinárodnú vedecko-technickú spoluprácu v rámci Európskeho výskumného priestoru, ako aj ostatných relevantných medzinárodných organizácií/iniciatív a platforiem. NBÚ v rámci národného projektu bude spolupracovať so **zahraničnými partnermi**, a to najmä s NBÚ ČR, ktorý je gestorom problematiky kybernetickej bezpečnosti a zároveň národnou autoritou pre túto oblasť. Na zabezpečenie tejto činnosti bolo vybudované Národné centrum kybernetickej bezpečnosti so sídlom v Brne. Úlohou centra je koordinácia spolupráce na národnej a medzinárodnej úrovni pri predchádzaní kybernetickým útokom a pri návrhu a prijímaní opatrení pri riešení incidentov aj proti prebiehajúcim útokom. Ďalšími zahraničnými partnermi budú Nemecký spolkový úrad pre bezpečnosť v informačných technológiách a šifrovej ochrane informácií a Francúzska národná agentúra pre bezpečnosť informačných

systémov. Obe inštitúcie majú dlhoročnú tradíciu, vysoký medzinárodný kredit vďaka špičkovému personálu, ktorým disponujú vo všetkých oblastiach ich činnosti. Taktiež sa plánuje spolupráca aj s inými výskumnými pracoviskami a vedeckými pracovníkmi v Slovenskej republike a tiež aj v zahraničí. Jedná sa najmä o spoluprácu so Slovenskou akadémiou vied a holandskými odborníkmi pre oblasť NEV. Tieto zahraničné subjekty budú v projekte zapojené ako podporovatelia, teda nebudú mať štatút partnerov projektu.

Stav výskumno-vývojovej infraštruktúry relevantnej pre realizáciu výskumných aktivít jednotlivých partnerov:

NBÚ
Laboratórne prostredie žiadateľa využívané **pre oblasť NEV** bude možné vzhľadom na vek materiálno-technologického vybavenia (viac ako 8 rokov) využiť len ako doplnkovú výskumno-vývojovú infraštruktúru a pre potreby národného projektu sa predpokladá dobudovanie laboratórneho prostredia mimo sídla úradu (Brunovce). Toto je v súčasnosti bez chráneného priestoru a bez vybudovanej základnej infraštruktúry (klimatizácia, sieťová kabeláž, atď.).

Materiálno-technologické vybavenie laboratórneho prostredia **pre oblasť ŠOI** vzhľadom na jeho vek (viac ako 5 rokov) bude potrebné upgradovať tak, aby výkonnostne umožnilo plánované výskumno-vývojové činnosti.

Laboratórne prostredie pre oblasť **kybernetickej bezpečnosti** (vek 4 roky) je využiteľné pre plánovaný národný projekt po jeho doplnení ďalším materiálno-technologickým vybavením. Úrad zriadil a prevádzkuje Bezpečnostné a prevádzkové monitorovacie centrum SK CSIRC. Vláda SR uložila Národnému bezpečnostnému úradu zriadiť uvedené centrum SK CSIRC uznesením vlády SR č. 771 z 9. januára 2008, ktorým schválila „Koncepciu šifrovej ochrany informácií v SR na roky 2009 – 2013“ a neutajovanú prílohu „Návrh opatrení na realizáciu Koncepcie ŠOI“ s úlohami v oblasti realizácie kybernetickej obrany v SR. Jednou z úloh bolo konštituovať národný CSIRC v rámci NBÚ ako ústredné koordinačné a technické centrum pre riešenie problematiky kybernetickej ochrany zabezpečujúce najmä koordináciu činností podriadených orgánov v rámci ochrany kybernetického priestoru. Úrad prostredníctvom svojho pracoviska SK CSIRC spracováva informácie o kybernetických incidentoch prevažne v utajovaných komunikačných a informačných sieťach.

ÚPJŠ Košice
Partner má v súčasnosti k dispozícii dve výpočtové zariadenia, ktoré sú konfigurované ako HPC (High Performance Computing) a slúžia pre potreby Prírodovedeckej fakulty. Obe výpočtové zariadenia sú vybudované z menších výpočtových jednotiek, pričom tvoria architektúru master-slaves (nodes). Tieto zariadenia boli zakúpené v rámci rôznych európskych projektov a preto sú využívané viacerými výskumnými tímami. Požiadavka na permanentnú alokáciu týchto výpočtových prostriedkov preto nepripadá do úvahy. Rovnako ide o zariadenia, ktoré boli zaobstarané pred viac ako štyrmi rokmi, a sú preto, vzhľadom na súčasný trend a štandardy zastaralé. Pre riešenie nových výskumných projektov je nevyhnutné zaobstaranie nových výpočtových prostriedkov, pre dosiahnutie efektívneho výskumného procesu a optimálnych výsledkov. Preferuje sa

vybudovanie nového laboratórneho prostredia dedikovaného špeciálne pre potreby kryptografie a elektronického podpisu.

ŽU Žilina
Na pôde ŽU bol realizovaný projekt Univerzitný vedecký park ŽU. Nosné témy projektu sú zamerané aj na oblasť informačných a komunikačných technológií.

AOS Liptovský Mikuláš
Akadémia disponuje laboratórnou technikou, špeciálnymi softvérovými produktmi a dlhodobo sa venuje výskumno-vývojovej činnosti do ktorej zapája aj vlastných študentov a doktorandov.
AOS LM má vybudované laboratórium elektromagnetického vyžarovania a susceptibility ktoré je komplexne vybavené zariadením a prístrojmi slúžiacimi na experimentálne meranie a testovanie elektronických zariadení.
AOS LM má tiež laboratórium informačnej bezpečnosti ktoré je komplexne vybavené zariadeniami slúžiacimi na testovanie a prípravu siete a technických prostriedkov na rôznych operačných systémoch.

STU Bratislava
STU bola projekt výstavby Univerzitného vedeckého parku STU Bratislava a Univerzitného vedeckého parku MTF STU. V rokoch 2009-2011 STU realizovala viaceré projekty financované zo štrukturálnych fondov EÚ napr. „Zlepšenie a modernizácia vzdelávacej technickej a informačno-komunikačnej infraštruktúry pracovísk STU. Medzi univerzitné pracoviská patria centrá excelentnosti – Centrum excelentnosti SMART technológií, systémov a služieb, Centrum excelentnosti sídelnej infraštruktúry znalostnej ekonomiky, Národné centrum pre výskum a aplikácie obnoviteľných zdrojov energie, Centrum excelentnosti pre diagnostiku materiálov a ďalšie.

TUKE Košice
Disponuje laboratóriami, ktoré sú vybavené špeciálnymi zariadeniami, modernými osobnými počítačmi, pracovnými stanicami, databázovými a internetovými severmi, najmodernejšími technologickými automatmi pre riadenie technologických procesov, takmer celým záberom technologických sietí, modelmi reálnych technologických procesov a ďalšou potrebnou laboratórnou technikou, špeciálnymi softvérovými produktmi, meracími stanicami a pod. – relevantné unikátne laboratóriá:
• Laboratórium rečových technológií v telekomunikáciách
• Laboratórium. počítačových sietí
• Laboratórium kybernetiky
• Vysokonapäťová hala
• Centrum pre Inteligentné technológie
• Laboratórium automobilovej elektroniky
• Centrum pokročilých metód spracovania číslicových signálov
• Laboratórium technológií v elektronike
• Laboratórium nukleárnej magnetickej rezonancie
• Laboratórium bezpečnosti informačných a komunikačných technológií
• Laboratórium senzorových a bezdrôtových technológií

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)

Prínos k plneniu stratégie RIS3 SK

Predkladaný projektový zámer národného projektu bol koncipovaný tak, aby zohľadňoval v plnej miere prepojenie oblasti výskumu a vývoja, ktoré patri medzi špecializácie RIS3 SK z pohľadu dostupných vedeckých a výskumných kapacít (oblasť výskumu informačno-komunikačných technológií a sekundárne oblasť nových materiálov/nanotechnológií prostredníctvom výskumných aktivít akademických partnerov) a kľúčových oblastí hospodárskej špecializácie a to primárne nasledovných oblastí:

- Automobilový priemysel a strojárstvo,
- Spotrebná elektronika a elektrické prístroje,
- Informačné a komunikačné produkty a služby.

To znamená, že predkladaný národný projekt má potenciál prispieť k rozvoju troch zo štyroch základných oblastí hospodárskej špecializácie RIS3 SK. Predkladaný národný projekt sa venuje pomerne špecifickej problematike v rámci kybernetickej bezpečnosti, ale samotné výsledky výskumu a vývoja budú relevantné v širšom zmysle pre oblasť bezpečnosti informačných systémov, ktoré majú čoraz väčší význam v automobilovom priemysle. Výsledky výskumu a vývoja predkladaného zámeru národného projektu budú mať veľký potenciál tak v oblasti moderných automobilových informačných systémov, ako aj pre rýchlo sa rozvíjajúcu oblasť autonómnych dopravných prostriedkov.

Súčasne vzhľadom na výskumné témy bude mať predkladaný projekt priamo pozitívny vplyv na podniky pôsobiace v oblasti elektrotechnického priemyslu a informačných a komunikačných produktov a službách – výsledky výskumu a vývoja v rámci národného projektu budú mať potenciál generovať nové a inovované produkty a služby v týchto priemyselných odvetviach.

Hlavné ciele predkladaného národného programu

- **Vybudovanie Národnej PKI**
  Cieľom je vybudovanie PKI infraštruktúry - národnej technologickej platformy , ako súčasti kontrolovaného prostredia, ktorým riadi prístup používateľov k zdrojom IS. PKI bude obohatená o nové a bezpečnejšie algoritmy, rýchlejšie a výkonnejšie kryptografické zariadenia a bezpečnejšie aplikačné programové vybavenie, pričom bude spôsobilá na ochranu utajovaných skutočností/informácií.

- **Zodolnenie a vyladenie systémov ochrany utajovaných skutočností**
  Cieľom je navrhnúť bezpečnostné nastavenia (šablóny), ktorých aplikáciou bude možné využívať mobilné zariadenia na prenos a uchovávanie utajovaných skutočností.

- **Ochrana utajovaných skutočností prostriedkami šifrovej ochrany informácií**
  Cieľom je vyvinúť univerzálne VPN riešenie spôsobilé chrániť utajované skutočnosti stupňa utajenia „Vyhradené“ a „Dôverné“ v národných sieťach vrátane bezpečného prepojenia neutajovaných a utajovaných komunikačných systémov spôsobilých chrániť utajované skutočnosti rôzneho stupňa utajenia.

- **Ochrana proti NEV**
  Cieľom je zabrániť úniku utajovaných skutočností prostredníctvom nežiaduceho elektromagnetického vyžarovania.

- **Implementácia bezpečnej mobilnej pracovnej stanice**
  Cieľom je vyvinúť modulárny flexibilný systém bezpečnej mobilnej pracovnej stanice v režimoch tenký klient (thin client), tučný klient (fat client) a pracovná stanica na usb kľúči (WS on USB stick),umožňujúci chrániť utajované skutočnosti podľa požiadaviek používateľa.

- **Odhalenie zraniteľnosti v moderných HW architektúrach**
  Cieľom je odhaliť zraniteľnosti v moderných HW architektúrach a tým prispieť k ich vyššej bezpečnosti. Zistiť ktoré architektúry sú napadnuteľné a či existujú bezpečné moderné architektúry; aké ďalšie varianty útokov existujú; kde sú hranice týchto techník; aké sú rôzne vektory útoku a z nich prameniace hrozby; aké sú možnosti mitigácie; aké sú dopady tejto techniky na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb.

- **Eliminácia pokročilých kybernetických hrozieb prostredníctvom využitia umelej inteligencie**
  Cieľom je zvýšiť kybernetickú bezpečnosť s využitím možností umelej inteligencie.

- **Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach**
  Cieľom je zvýšiť kybernetickú bezpečnosť prostredníctvom identifikácie škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach. Cieľom je zároveň odhalenie príčin bezpečnostných problémov, analýza modelov dôvery a závislostí v online repozitároch, následná identifikácia tých repozitárov a distribučných sietí, ktorých zneužitie by potenciálnemu útočníkovi umožnilo ľahkým spôsobom veľký dosah a následne výskum metód a techník na efektívnu identifikáciu škodlivého kódu, napríklad prehľadávaním repozitárov knižníc alebo počas zostavovania či distribúcie finálneho softvéru.

- **Podpora činnosti jednotiek typu CSIRT**
  Cieľom je efektívne poskytovanie služieb a úspešné zvládanie neustále rastúceho počtu bezpečnostných incidentov, ktoré musia jednotky CSIRT riešiť alebo koordinovať.

9. Očakávaný stav a merateľné ciele

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

Vybudovaním Národnej PKI sa rozšíri možnosť využívať princípy asymetrickej kryptografie pre ochranu utajovaných skutočností stupňa utajenia Vyhradené. Používanie potrebných certifikátov v bezpečnom QSCD nosiči (napr. zamestnanecká karta s čipom) zjednoduší a výrazne cenovo zníži používanie technických prostriedkov ktoré sú spôsobilé chrániť utajované skutočnosti stupňa utajenia Vyhradené. Merateľným cieľom sú výsledky

testov jednotlivých funkcionalít kľúčového páru vygenerovaného pomocou eliptických kriviek.

Aplikáciou **bezpečnostných šablón** na mobilné zariadenia s rôznymi operačnými systémami sa zvýši bezpečnosť uvedených zariadení a rozšíri možnosť využívať ich na ochranu utajovaných skutočností. Merateľným cieľom je prevedenie vybraných typov útokov na zariadenia v ktorých sú aplikované bezpečnostné nastavenia.

Očakávaných stavom v rámci riešenia problematiky **ochrany utajovaných skutočností prostriedkami ŠOI** je univerzálne VPN riešenie spôsobilé chrániť utajované skutočnosti stupňa utajenia „Vyhradené“ a „Dôverné“ v národných sieťach vrátane bezpečného prepojenia neutajovaných a utajovaných komunikačných systémov spôsobilých chrániť utajované skutočnosti rôzneho stupňa utajenia. Merateľným cieľom je analýza zdrojového kódu navrhnutého VPN riešenia.

Skúmaním jednotlivých parciálnych oblastí **ochrany proti nežiadúcemu elektromagnetickému žiareniu** je možné zabrániť úniku utajovaných skutočností prostredníctvom nežiaduceho elektromagnetického vyžarovania. Merateľným cieľom sú príspevky do databáz Web of Science Core Collection a SCOPUS.

Očakávaným stavom je **bezpečná mobilná pracovná stanica pracujúca** v režimoch tenký klient, tučný klient a pracovná stanica na usb kľúči, umožňujúci chrániť utajované skutočnosti podľa požiadaviek používateľa. Merateľným cieľom sú výsledky testov požadovaných funkcionalít v jednotlivých režimoch činnosti.

Odhalenie zraniteľnosti v moderných HW architektúrach umožní úspešnú mitigáciu a tým zvýši bezpečnosť zariadení. Merateľným cieľom sú výsledky penetračných testov a testov zraniteľností.

Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach prispeje k odhaleniu príčin bezpečnostných problémov. Merateľným cieľom je množina identifikovaného škodlivého kódu.

Podporou činnosti jednotiek typu CSIRT sa zabezpečí efektívne poskytovanie služieb a úspešné zvládanie neustále rastúceho počtu bezpečnostných incidentov. Merateľným cieľom sú výsledky testovania vyvinutého komplexného systému.

10. Bližší popis merateľných ukazovateľov.[6]

[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.

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.[7]

Cieľ národného projektu	Merateľný ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	Súvisiaci programový ukazovateľ[8]
Vybudovanie národnej PKI	% implementácie národnej technologickej platformy PKI spôsobilej na ochranu utajovaných skutočností	100 % (plnohodnotne implementovaná technologická platforma PKI spôsobilá na ochranu utajovaných skutočností stupňa utajenia a/ Vyhradené b/ EU-Restricted c/ NATO-Restricted	Výskum, vývoj, návrh a implementácia národnej technologickej platformy PKI spôsobilej na ochranu utajovaných skutočností/informácií stupňa utajenia a) Vyhradené b) EU-Restricted c) NATO-Restricted	
	% implementácie národnej technologickej platformy PKI pre potreby interoperability s PKI platformami EU/NATO	100 % (plnohodnotne implementovaná národná technologická platforma PKI pre potreby interoperability s PKI platformami EU/NATO	Výskum, vývoj, návrh a implementácia národnej technologickej platformy PKI pre potreby interoperability s PKI platformami EU/NATO	
	% implementácie národnej technologickej platformy spôsobilej na ochranu utajovaných skutočností vyšších stupňov utajenia	100 % (plnohodnotne implementovaná technologická platforma spôsobilá na ochranu utajovaných skutočností stupňa utajenia a/ Dôverné b/ Tajné	Výskum, vývoj, návrh a implementácia národnej technologickej platformy spôsobilej chrániť utajované skutočnosti/informácie stupňa utajenia Dôverné/Tajné s využitím klienta platformy PKI na stupeň utajenia Vyhradené pre autentifikáciu	

[7] 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.

[8] Národný projekt by mal obsahovať minimálne jeden relevantný projektový ukazovateľ, ktorý sa agreguje do programového ukazovateľa. Pri ostatných projektových ukazovateľoch sa uvedie N/A.

	% rozpracovania	100 %	Návrh teoretického modelu národnej technologickej platformy PKI spôsobilej chrániť utajované skutočnosti pre potreby zabezpečenia ich dôveryhodnosti, autentickosti a integrity počas ich celého životného cyklu	
Inovatívne riešenia OUS – zodolnenie a vyladenie systémov	% implementácie šablóny platformy MS Windows % implementácie šablóny platformy Unix % implementácie šablóny platformy Linux % implementácie šablóny platformy OS X % implementácie šablóny platformy iOS % implementácie šablóny platformy Android	100 % 100 % 100 % 100 % 100 % 100%	Výskum, vývoj, návrh a implementácia spoločných bezpečnostných šablón a nastavení pre technické prostriedky založené na platformách Microsoft Windows, Unix, Linux, OS X, iOS a Android	

	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia upravenej distribúcie OS Linux pre použitie v technických prostriedkoch	
	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia upravenej distribúcie OS Android pre použitie v technických prostriedkoch	
Inovatívne riešenia OUS prostriedkami ŠOI	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia univerzálneho VPN riešenia spôsobilého chrániť US stupňa utajenia „VYHRADENÉ“ v národných KIS	
	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia univerzálneho VPN riešenia spôsobilého chrániť US stupňa utajenia „DÔVERNÉ“ v národných KIS	
	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia univerzálneho komunikačného (hlas, video, správy) riešenia spôsobilého chrániť US stupňa utajenia „VYHRADENÉ“ s implementovanou podporou protokolu SCIP	

	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia univerzálneho komunikačného (hlas, video, správy) riešenia spôsobilého chrániť US stupňa utajenia „DÔVERNÉ“ s implementovanou podporou protokolu SCIP	
	% vývoja % implementácie	100% 100%	Výskum, vývoj, návrh a implementácia univerzálnej brány (gateway) pre prepojenie komunikačných systémov spôsobilých chrániť US rôzneho stupňa utajenia (Neutajované, Vyhradené, Dôverné, resp. EÚ/NATO) s implementovanou podporou protokolu SCIP	
	% návrhu	100 %	Návrh emulátora vybraných bezdrôtových sietí v Národnom TEMPEST laboratóriu NBÚ za účelom vykonávania meraní NEV vysokofrekvenčných vysielačov (mobilné telefóny, rádiové stanice, atď.) s využitím vlastnej základňovej stanice (BTS), vrátane vytvorenia metodiky vykonávania uvedených meraní	O0071 Počet zrekonštruovaných zariadení výskumnej infraštruktúry

Ochrana proti NEV	% návrhu	100 %	Vývoj a návrh metodiky a meracích prípravkov pre overovanie útlmových vlastností opticko-metalických prevodníkov a tienených skriniek (t. j. technologické racky určené pre umiestnenie zariadení spracovávajúcich utajované skutočnosti)	Počet publikácií subjektov zo SR v databázach Web of Science Core Collection a SCOPUS
			Skúmanie vlastností signálov z rôznych hardvérových komponentov počítača a zo vstupno-výstupných periférnych zariadení a vytvorenie databázy signálov za účelom ich využitia pri analýze signálov v Národnom laboratóriu TEMPEST NBÚ	
	Počet skúmaných typov tlačiarní		Skúmanie rôznych typov tlačiarní s rôznou technológiou tlače a pri rôznych nastaveniach parametrov tlače (prevádzkový mód, veľkosť rozlíšenia tlače, atď.) v TEMPEST laboratóriu a ich vplyvy na výsledky meraní ich NEV	

	% rozpracovania metodiky	100 %	Vývoj a návrh metodiky vykonávania meraní NEV zariadení na mieste inštalácie (tzv. „on-site testing“) a návrh technického riešenia merania NEV zariadení v mieste ich inštalácie	Počet publikácií subjektov zo SR v databázach Web of Science Core Collection a SCOPUS
Bezpečná mobilná pracovná stanica	% vývoja % implementácie	100 % 100 %	Výskum, vývoj, návrh a implementácia bezpečnej mobilnej pracovnej stanice využívajúci výstupy ostatných výskumných tém a aktivít v režimoch tenký klient (thin client), tučný klient (fat client) a pracovná stanica na usb kľúči (WS on USB stick)	
Zraniteľnosti v moderných hardvérových architektúrach	A/N	A/N	Výskum útokov na pamäťové moduly vrátane techník typu rowhammer: identifikácia ohrozených platforiem, techník útoku, spôsobov ich detekcie a mitigácie	
	A/N	A/N	Výskum bezpečnosti nedokumentovaných komponentov chipsetov a procesorov	
	A/N	A/N	Výskum útokov na implementáciu cache	

Zraniteľnosti v moderných hardvérových architektúrach	A/N	A/N	Výskum útokov na implementáciu vnútorných jednotiek procesora vrátane špekulatívneho vykonania kódu, vrátane techník Meltdown a Spectre	
	A/N	A/N	Analýza a klasifikácia existujúcich tried zraniteľností, výskum iných nových typov hardvérových zraniteľností so zameraním na moderné hardvérové architektúry, používané v osobných počítačoch, serveroch, mobilných zariadeniach a IoT, určenia dopadu na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb, spôsobu ich detekcie a mitigácie	

Využitie umelej inteligencie v oblasti pokročilých kybernetických hrozieb	A/N	A/N	Identifikácia scenárov použitia umelej inteligencie v oblasti pokročilých kybernetických hrozieb	
	% návrhu % implementácie	100 % 100 %	Návrh a implementácia prototypu klasifikátora sieťovej komunikácie, schopného identifikovať na základe metadát kybernetické útoky aj v šifrovanej komunikácii	
	% návrhu % implementácie	100 % 100 %	Návrh a implementácia prototypu klasifikátora software na nezhubný a rôzne typy malvéru	
	% návrhu % implementácie	100 % 100 %	Návrh a implementácia prototypu využitia UI na vyhľadávanie zraniteľností v kóde	
	% návrhu % implementácie	100 % 100 %	Návrh a implementácia prototypu využitia UI na koreláciu bezpečnostných udalostí, hodnotenie kritickosti a klasifikáciu incidentov	

Využitie umelej inteligencie v oblasti pokročilých kybernetických hrozieb	% návrhu % implementácie	100 % 100 %	Výskum zraniteľnosti strojového učenia voči technikám adversarial machine learning a ak je to možné, návrh spôsobu identifikácie prípadov škodlivého učenia	
Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach	A/N	A/N	Analýza modelov dôvery a závislostí v online repozitároch, identifikácia repozitárov a distribučných sietí, ktorých využívaním dochádza k implicitnej dôvere	
	A/N	A/N	Výskum techník na identifikáciu škodlivého kódu	
	% rozpracovanosti	100 %	Vytvorenie metodiky a nástrojov na identifikáciu škodlivého kódu vo vybraných prípadoch	
Integrovaný systém na podporu činnosti jednotiek typu CSIRT	% rozpracovanosti	100 %	Analýza aktivít CSIRT tímov a ich požiadaviek na funkcionalitu podporných technológií pre tieto aktivity	
	% rozpracovanosti	100 %	Analýza existujúcich riešení na podporu činnosti CSIRTov, identifikácia chýbajúcich komponentov či prepojení	

	% rozpracovanosti	100 %	Návrh, vývoj a kvalitatívne testovanie komplexného systému, pokrývajúceho potreby jednotiek typu CSIRT	

Iné údaje, ktorými je možné sledovať napĺňanie cieľov národného projektu (ak relevantné)				
Cieľ národného projektu	Ukazovateľ	Indikatívna cieľová hodnota	Aktivita projektu	

Predmetná časť sa týka projektových ukazovateľov	
Názov merateľného ukazovateľa[9]	% návrhu
Akým spôsobom sa budú získavať dáta?	Testovanie požadovaných funkcionalít
Názov merateľného ukazovateľa[10]	% implementácie
Akým spôsobom sa budú získavať dáta?	Testovanie požadovaných funkcionalít v implementovanom prostredí
Názov merateľného ukazovateľa[11]	% rozpracovanosti
Akým spôsobom sa budú získavať dáta?	Čiastkové výstupy z analýz
Názov merateľného ukazovateľa[12]	A/N
Akým spôsobom sa budú získavať dáta?	A – podarilo sa dokázať existenciu napr. zraniteľnosti systému N – nepodarilo dokázať existenciu napr. zraniteľnosti systému

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	Počet[13]

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

	relevantné)	
Možnosť využívať princípy PKI na ochranu utajovaných skutočností, t. j. možnosť využívať certifikáty uložené napr. v čipe preukazu zamestnanca orgánu verejnej moci	Zamestnanci orgánov verejnej moci	Cca 200 000
Zvýšenie bezpečnosti používaných technických prostriedkov, zvýšenie počtu platforiem ktoré môžu technické prostriedky využívať	Zamestnanci orgánov verejnej moci + podnikatelia spracúvajúci utajované skutočnosti	Cca 300 000
Zníženie ceny a zvýšenie dostupnosti prostriedkov šifrovej ochrany informácií	Zamestnanci orgánov verejnej moci + podnikatelia spracúvajúci utajované skutočnosti	Cca 300 000
Rozšírenie portfólia používaných zariadení vyhovujúcich z hľadiska ochrany pred NEV	Zamestnanci orgánov verejnej moci	Cca 200 000
Štandardizácia meracích postupov, ktoré doteraz nie sú štandardizované	Orgány verejnej moci a zahraničné inštitúcie, ktoré vykonávajú nerania NEV	Cca 70 organizácií
Schopnosť rýchlej reakcie na kybernetické hrozby	FO, PO, OVM	Ide o širokú cieľovú skupinu prijímateľov, ktorí budú benefitovať zo schopnosti rýchlej reakcie na kybernetické hrozby.

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

12. Aktivity

a) Uveďte detailnejší popis aktivít.

V rámci cieľa **„Vybudovanie Národnej PKI“** sa predpokladá realizácia nasledovných aktivít:

1. Výskum, vývoj, návrh a implementácia národnej technologickej platformy PKI spôsobilej na ochranu utajovaných skutočností/informácií stupňa utajenia
   a. Vyhradené
   b. EU-Restricted

c. NATO-Restricted
2. Výskum, vývoj, návrh a implementácia národnej technologickej platformy PKI pre potreby interoperability s PKI platformami EU/NATO
3. Výskum, vývoj, návrh a implementácia národnej technologickej platformy spôsobilej chrániť utajované skutočnosti/informácie stupňa utajenia Dôverné/Tajné s využitím klienta platformy PKI na stupeň utajenia Vyhradené pre autentifikáciu
4. Návrh teoretického modelu národnej technologickej platformy PKI spôsobilej chrániť utajované skutočnosti pre potreby zabezpečenia ich dôveryhodnosti, autentickosti a integrity počas ich celého životného cyklu

Cieľom je využívanie PKI infraštruktúry ako súčasti kontrolovaného prostredia, ktorým riadi prístup používateľov k zdrojom IS. Neustály technologický rast a nezadržateľný nárast výpočtových kapacít však núti rozvíjať oblasť PKI o nové a bezpečnejšie algoritmy, rýchlejšie a výkonnejšie kryptografické zariadenia a bezpečnejšie aplikačné programové vybavenie. Konkrétne technické špecifikácie nových výskumných činností však zostávajú prakticky bez väčších výnimiek súčasťou utajených informácií jednotlivých štátov/organizácií, pričom ich nedostupnosť býva v takýchto prípadoch dlhoročná.

Informačné a komunikačné technológie (ďalej aj ako „IKT“) dnes predstavujú neoddeliteľnú súčasť každodenného života a prenikajú prakticky do všetkých oblastí činnosti globálnej spoločnosti. Výsledkom toho je enormný nárast objemu elektronických dát, ktoré sa v rámci IKT elektronicky spracovávajú. Veľké množstvo elektronických dát v súčasnej dobe plnohodnotne nahradilo predchádzajúcu papierovú formu, avšak jeden dôležitý aspekt predstavuje pre elektronické dáta stále ťažko prekonateľné obmedzenie – bezpečná, spoľahlivá, efektívna, dôveryhodná a dlhodobá archivácia s rovnakou možnosťou overenia vo vzdialenej budúcnosti. Základným súčasným predpokladom je nevyhnutnosť disponovať:

- fyzickým nosičom, ktorý je schopný dlhodobého uchovávania elektronických dát
- komplexným aplikačným programovým vybavením (software), ktorý by bol schopný elektronické dáta uchovávať v čitateľnej a prezentovateľnej podobe, vrátane všetkých ostatných vyššie menovaných podmienok.

Zatiaľ čo v prípade výskumu fyzických nosičov prebieha výskum a inovácie prakticky nepretržite, v oblasti aplikačného programového vybavenia, ktoré by riešilo komplexnú problematiku uchovávania, čitateľnosti a prezentovateľnosti dát vrátane zabezpečenia ich dlhodobej dôveryhodnosti dochádza k výskumným aktivitám iba v ojedinelých prípadoch, aj to prakticky len v niektorých vybraných charakteristikách bez komplexnejšieho rozsahu.

Výsledkom aktivít bude ucelený postup, metodika, štandard alebo univerzálny formát pre elektronické dáta, ktorý by bol medzinárodne uznávaný/štandardizovaný a prostredníctvom ktorého by bolo možné odvodiť konkrétnejšie princípy, mechanizmy a modely pre vývoj univerzálnych softvérových nástrojov slúžiacich na zabezpečenia dlhodobej dôveryhodnosti elektronických dát.

V rámci cieľa **„Inovatívne riešenia OUS – zodolnenie a vyladenie systémov“** sa predpokladá realizácia nasledovných aktivít:

1. Výskum, vývoj, návrh a implementácia spoločných bezpečnostných šablón a nastavení pre technické prostriedky založené na platformách Microsoft Windows, Unix, Linux, OS X, iOS a Android
2. Výskum, vývoj, návrh a implementácia upravenej distribúcie OS Linux pre použitie v technických prostriedkoch

3. Výskum, vývoj, návrh a implementácia upravenej distribúcie OS Android pre použitie v technických prostriedkoch

Cieľom je vytvorenie bezpečnostných nastavení pre väčšinu v súčasnosti používaných platforiem. Vzhľadom na komplexnosť témy, bolo možné doposiaľ publikovať bezpečnostné nastavenia len na najpoužívanejšie platformy OS pre počítače. Otázkam bezpečnosti operačných systémov mobilných zariadení sa prakticky nevenovala žiadna, alebo len minimálna pozornosť. V súčasnosti však mobilné zariadenia predstavujú neoddeliteľnú súčasť IKT, je potrebné podrobne analyzovať jednotlivé operačné systémy, ich zraniteľnosti a navrhnúť bezpečnostné nastavenia (šablóny) ktorých aplikáciou bude možné využívať mobilné zariadenia na prenos a uchovávanie utajovaných skutočností.

V rámci cieľa **„Inovatívne riešenia OUS prostriedkami ŠOI“** sa predpokladá realizácia nasledovných aktivít:

1. Výskum, vývoj, návrh a implementácia univerzálneho VPN riešenia spôsobilého chrániť US stupňa utajenia „VYHRADENÉ“ v národných KIS
2. Výskum, vývoj, návrh a implementácia univerzálneho VPN riešenia spôsobilého chrániť US stupňa utajenia „DÔVERNÉ“ v národných KIS
3. Výskum, vývoj, návrh a implementácia univerzálneho komunikačného (hlas, video, správy) riešenia spôsobilého chrániť US stupňa utajenia „VYHRADENÉ“ s implementovanou podporou protokolu SCIP
4. Výskum, vývoj, návrh a implementácia univerzálneho komunikačného (hlas, video, správy) riešenia spôsobilého chrániť US stupňa utajenia „DÔVERNÉ“ s implementovanou podporou protokolu SCIP
5. Výskum, vývoj, návrh a implementácia univerzálnej brány (gateway) pre prepojenie komunikačných systémov spôsobilých chrániť US rôzneho stupňa utajenia (Neutajované, Vyhradené, Dôverné, resp. EÚ/NATO) s implementovanou podporou protokolu SCIP

Cieľom aktivít je vyvinúť univerzálne VPN riešenie spôsobilé chrániť utajované skutočnosti stupňa utajenia „Vyhradené“ a „Dôverné“ v národných sieťach. V súčasnosti neexistuje takéto riešenie, preto má úrad ambíciu, takéto riešenie v spolupráci s partnermi vyvinúť a následne poskytovať používateľom bezodplatne. V rámci interoperability s NATO bol vyvinutý protokol SCIP, ktorý v blízkej budúcnosti bude predstavovať komunikačný štandard. Preto je potrebné, aby existovalo univerzálne komunikačné riešenie prenášajúce a chrániace hlas, video aj správy s implementovanou podporou protokolu SCIP. Požiadavka prepojenia neutajovaných a utajovaných systémov zo dňa na deň rastie, preto ďalším prínosom tejto aktivity bude vyvinutie univerzálnej brány (gateway), pomocou ktorej bude možné bezpečné prepojenie komunikačných systémov spôsobilých chrániť utajované skutočnosti rôzneho stupňa utajenia.

V rámci cieľa **„Ochrana proti NEV“** sa predpokladá realizácia nasledovných aktivít:

1. Výskum, vývoj a návrh technologickej platformy Národného TEMPEST laboratória pre vykonávanie meraní NEV zariadení. Aktivita zahŕňa aj stavebnú rekonštrukciu priestorov, vybudovanie chráneného priestoru pre spracovávanie utajovaných skutočností do stupňa utajenia „Tajné“ (najmä mechanické zábranné prostriedky a technické zabezpečovacie prostriedky), vybudovanie základnej infraštruktúry

(klimatizácia, sieťová kabeláž, atď.) a vybudovanie bezodrazovej komory. Realizácia aktivity spolu s realizáciou aktivít č. 2-5 je predpokladom pre vybudovanie Národného TEMPEST laboratória s automatizovaným, presným a rýchlym procesom merania NEV zostáv počítačov a periférnych zariadení, ako aj špecifických druhov zariadení využívaných na spracovávanie utajovaných skutočností (najmä zariadenia s bezdrôtovými rozhraniami, tienené technologické skrinky a opticko-metalické prevodníky).

2. Návrh emulátora vybraných bezdrôtových sietí v Národnom TEMPEST laboratóriu NBÚ za účelom vykonávania meraní NEV vysokofrekvenčných vysielačov (mobilné telefóny, rádiové stanice, atď.) s využitím vlastnej základňovej stanice (BTS), vrátane vytvorenia metodiky vykonávania uvedených meraní.
3. Vývoj a návrh metodiky a meracích prípravkov pre overovanie útlmových vlastností opticko-metalických prevodníkov a tienených skriniek (t. j. technologické racky určené pre umiestnenie zariadení spracovávajúcich utajované skutočnosti)
4. Skúmanie vlastností signálov z rôznych hardvérových komponentov počítača a zo vstupno-výstupných periférnych zariadení a vytvorenie databázy signálov za účelom ich využitia pri analýze signálov v Národnom laboratóriu TEMPEST NBÚ.
5. Skúmanie rôznych typov tlačiarní s rôznou technológiou tlače a pri rôznych nastaveniach parametrov tlače (prevádzkový mód, veľkosť rozlíšenia tlače, atď.) v TEMPEST laboratóriu a ich vplyvy na výsledky meraní ich NEV.
6. Vývoj a návrh metodiky vykonávania meraní NEV zariadení na mieste inštalácie (tzv. „on-site testing“) a návrh technického riešenia merania NEV zariadení v mieste ich inštalácie

Cieľom je vypracovať metodiky ako vykonávať celý rozsah TEMPEST meraní v súlade s existujúcimi bezpečnostnými štandardami. Taktiež vypracovať ucelené riešenia meracích systémov špecializujúcich sa na TEMPEST pre celú oblasť ochrany pred NEV.

Vychádzajúc z vyššie uvedeného sa predpokladá, že medzi hlavné vedecké prínosy bude patriť:

- schopnosť dostatočne rýchlo reagovať na nové hrozby NEV súvisiace s neustále sa zvyšujúcou úrovňou súčasných technických a technologických možností,
- komplexné pokrytie hrozby zneužitia informácií z NEV,
- zvýšenie efektivity ochrany pred NEV,
- zníženie celkových nákladov na realizáciu ochrany pred NEV,
- medzinárodná prestíž v oblasti ochrany pred NEV.

V rámci cieľa **„Bezpečná mobilná pracovná stanica“** za využitia výsledkov ostatných aktivít sa predpokladá realizácia nasledovných aktivít:

1. Výskum, vývoj, návrh a implementácia bezpečnej mobilnej pracovnej stanice využívajúci výstupy ostatných výskumných tém a aktivít v režimoch tenký klient (thin client), tučný klient (fat client) a pracovná stanica na usb kľúči (WS on USB stick)

Cieľom je vyvinúť modulárny flexibilný systém umožňujúci chrániť utajované skutočnosti podľa požiadaviek používateľa. Modulárny systém umožní využiť všetky prednosti jednotlivých častí a v spolupráci s ostatnými súčasťami umožní potlačiť negatíva, čo v konečnom dôsledku prinesie požadovanú úroveň bezpečnosti. Takáto flexibilný systém prinesie nemalé finančné úspory, nakoľko sa bude v plnej miera snažiť využiť existujúce

prostredie (fyzická a objektová bezpečnosť, technické prostriedky a pod), prípadne ho upraviť s minimálnymi nákladmi.

V rámci cieľa **„Zraniteľnosti v moderných hardvérových architektúrach"** sa predpokladá realizácia nasledovných aktivít:

1. Výskum útokov na pamäťové moduly vrátane techník typu rowhammer: identifikácia ohrozených platforiem, techník útoku, spôsobov ich detekcie a mitigácie
2. Výskum bezpečnosti nedokumentovaných komponentov chipsetov a procesorov
3. Výskum útokov na implementáciu cache
4. Výskum útokov na implementáciu vnútorných jednotiek procesora vrátane špekulatívneho vykonania kódu, vrátane techník Meltdown a Spectre
5. Analýza a klasifikácia existujúcich tried zraniteľností, výskum iných nových typov hardvérových zraniteľností so zameraním na moderné hardvérové architektúry, používané v osobných počítačoch, serveroch, mobilných zariadeniach a IoT, určenia dopadu na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb, spôsobu ich detekcie a mitigácie

Cieľom je zamerať sa na niektoré dôležité nové kategórie zraniteľností.

Row hammering útok. Jedná sa o novú triedu útokov na pamäťové čipy v moderných počítačových architektúrach, pri ktorých je možné opätovným zápisom na dôkladne pripravené miesta v pamäti ovplyvniť obsah inej časti pamäti a obísť tak akékoľvek hardvérové a softvérové ochrany operačného systému. Prvý výskum bol publikovaný už v Júni 2014, prvé praktické využitie v roku 2015. Útok sa pôvodne obmedzoval len na Intel architektúru a vybrané pamäťové čipy bez ECC. V roku 2016 však bola zraniteľnosť a možnosť jej zneužitia demonštrovaná aj na mobilných zariadeniach s OS Android a výrazne väčšiu množinu pamäťových čipov rôznych výrobcov. Úvodné predpoklady, že problém sa vyrieši znížením taktu pamäti RAM a plošným zavedením používania ECC pamätí, sa nepotvrdil. Naopak, až v roku 2017 bola publikovaná adaptácia útoku aj na flash pamäti a viacero vylepšení pôvodných typov útoku, ktoré ho umožňujú vykonať aj na architektúrach, kde to predtým bolo nemysliteľné. V rámci témy sú aktuálne otvorené výskumné otázky, aké sú limity techniky row hammering; ktorý hardvér je zraniteľný; ako pokusy o využitie zraniteľnosti odhaliť; či, do akej miery a na akom hardvéri je možná mitigácia; aké sú dopady tejto techniky na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb.

Zraniteľnosti využívajúce nezdokumentované komponenty chipsetov a procesorov. Veľmi nedávno, až v novembri 2017, boli publikované prvé informácie o zraniteľnostiach v Intel Management Engine (IME). Jedná sa o špecializovaný proprietárny procesor, ktorý je vnorený v moderných počítačových architektúrach všetkých dnes používaných počítačov s procesorom Intel. Podľa prvotných informácií obsahuje IME samostatný operačný systém Minix, nezávislý od hlavného operačného systému počítača, týmto operačným systémom neviditeľný, s privilegovaným prístupom do celej pamäti počítača, na jednotlivé zbernice a periférie. Chyby v tomto systéme je možné zneužiť na plnú a nepozorovateľnú kompromitáciu serverov a pracovných staníc. V rámci témy sú aktuálne otvorené výskumné otázky, akých ďalších architektúr sa problém týka; aká je správna mitigácia; či a ako je možné odhaliť pokusy o útok alebo úspešný útok; aké sú dopady tejto techniky na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb.

Útoky, využívajúce architektúrne vlastnosti moderných CPU. Jedná sa predovšetkým o zraniteľnosti Meltdown a Spectre, publikované v januári 2018. Táto úplne nová trieda útokov využíva novým spôsobom implementačné vlastnosti procesorov architektúr Intel, AMD, ARM pre prekonanie ochrán medzi procesom a jadrom, procesmi navzájom, aj sandboxov v rámci jedného procesu. Téma je absolútne nová a kompletne nepreskúmaná. Medzi otvorené výskumné otázky patrí: ktoré architektúry sú napadnuteľné a či existujú bezpečné moderné architektúry; aké ďalšie varianty prezentovaných útokov existujú; kde sú hranice týchto techník; aké sú rôzne vektory útoku a z nich prameniace hrozby; aké sú možnosti mitigácie; aké sú dopady tejto techniky na odporúčania (best practices) pre prevádzku softvéru vrátane informačných systémov, pracujúcich v rôznych stupňoch utajenia, ako aj cloudových služieb.

V rámci cieľa **"Využitie umelej inteligencie na identifikáciu a elimináciu pokročilých kybernetických hrozieb"** sa predpokladá realizácia nasledovných aktivít:

1. Identifikácia scenárov použitia umelej inteligencie v oblasti pokročilých kybernetických hrozieb
2. Návrh a implementácia prototypu klasifikátora sieťovej komunikácie, schopného identifikovať na základe metadát kybernetické útoky aj v šifrovanej komunikácii
3. Návrh a implementácia prototypu klasifikátora software na nezhubný a rôzne typy malvéru
4. Návrh a implementácia prototypu využitia UI na analýzu a deobfuskáciu malvéru, hľadanie korelácií medzi jednotlivými vzorkami a identifikácia trendov a skupín malvéru
5. Návrh a implementácia prototypu využitia UI na vyhľadávanie zraniteľností v kóde
6. Návrh a implementácia prototypu využitia UI na koreláciu bezpečnostných udalostí, hodnotenie kritickosti a klasifikáciu incidentov
7. Výskum zraniteľnosti strojového učenia voči technikám adversarial machine learning a ak je to možné, návrh spôsobu identifikácie prípadov škodlivého učenia.

Umelá inteligencia v oblasti pokročilých kybernetických hrozieb má množstvo uplatnení, od detekcie neželanej sieťovej aktivity (kybernetické útoky, skenovanie, odhaľovanie sieťových anomálií), cez podporu pri analýze potenciálne škodlivého kódu, až po odstraňovanie chýb a akceleráciu vývoja. Cieľom aktivity je využiť poskytované možnosti umelej inteligencie v oblasti kybernetickej bezpečnosti. Otvorenými výskumnými témami sú rôzne možnosti aplikácie umelej inteligencie na oblasť kybernetickej bezpečnosti, výskum a vývoj rôznych detekčných techník a zvyšovanie efektivity práce bezpečnostných analytikov nad veľkou množinou dát.

V rámci cieľa **"Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach"** sa predpokladá realizácia nasledovných aktivít:

1. Analýza modelov dôvery a závislostí v online repozitároch, identifikácia repozitárov a distribučných sietí, ktorých využívaním dochádza k implicitnej dôvere
2. Výskum techník na identifikáciu škodlivého kódu
3. Vytvorenie metodiky a nástrojov na identifikáciu škodlivého kódu vo vybraných prípadoch

Medzi miestami, kde je možné vložiť škodlivý kód, sú softvérové repozitáre (github, …), repozitáre knižníc (pypi, npm, …), aplikačne repozitáre (docker hub, …) distribučné obsahové siete a ďalšie miesta. Útočníkom môže byť priamo autor aplikácie (DisplayWidgets), alebo externý útočník (NotPetya). Objem týchto repozitárov je obrovský (napr. pypi - cca. 125 tisíc balíkov, github - cca. 10 miliónov repozitárov) a neustála fluktuácia robí bezpečnostnú inšpekciu veľmi obtiažnou. Predmetom výskumu je teda skúmanie koreňových príčin bezpečnostných problémov, analýza modelov dôvery a závislostí v online repozitároch, následná identifikácia tých repozitárov a distribučných sietí, ktorých zneužitie by potenciálnemu útočníkovi umožnilo ľahkým spôsobom veľký dosah a následne výskum metód a techník na efektívnu identifikáciu škodlivého kódu, napríklad prehľadávaním repozitárov knižníc alebo počas zostavovania či distribúcie finálneho softvéru.

V rámci cieľa **“Integrovaný systém na podporu činnosti jednotiek typu CSIRT”** sa predpokladá realizácia nasledovných aktivít:

1. Analýza aktivít CSIRT tímov a ich požiadaviek na funkcionalitu podporných technológií pre tieto aktivity
2. Analýza existujúcich riešení na podporu činnosti CSIRTov, identifikácia chýbajúcich komponentov či prepojení
3. Návrh, vývoj a kvalitatívne testovanie komplexného systému, pokrývajúceho potreby jednotiek typu CSIRT

Cieľom aktivity je výskum ohraničený na parciálne témy:

- SIEM softvér
- tiketovacie systémy, databázy konštituencie, databázy aktív a spôsoby ich budovania
- softvér na agregáciu a distribúciu informácií (na úrovni indikátorov alebo dokumentov)
- klasifikáciu
- senzory, skenery zraniteľností a miskonfigurácie

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
• integrácia národných algoritmov do prostredia národnej technologickej platformy PKI, • integrácia schválených EU-Restricted a NATO-Restricted algoritmov do prostredia národnej technologickej platformy PKI, • integrácia národnej	Vybudovanie Národnej PKI	Žiadateľ a partner	40

technologickej platformy PKI s PKI platformami EU/NATO • vývoj bezpečnostného mechanizmu využívajúceho klienta s využitím PKI-V pre autentifikáciu a jeho integrácia do prostredia s vyšším klasifikačným stupňom.			
možnosť využívať platformy Microsoft Windows, Unix, Linux, OS X, iOS a Android	Zodolnenie a vyladenie systémov ochrany utajovaných skutočností	Žiadateľ a partner	12
• vytvorenie univerzálneho VPN riešenia • vytvorenie univerzálneho komunikačného riešenia • Výskum, vývoj, návrh a implementácia univerzálnej brány	Ochrana utajovaných skutočností prostriedkami šifrovej ochrany informácií	Žiadateľ a partner	40
• Výskum, vývoj a návrh technologickej platformy Národného TEMPEST laboratória pre vykonávanie meraní NEV zariadení. Aktivita zahŕňa aj stavebnú rekonštrukciu priestorov, vybudovanie chráneného priestoru pre spracovávanie utajovaných skutočností • Návrh emulátora vybraných bezdrôtových sietí • Vývoj a návrh metodiky a meracích prípravkov pre overovanie útlmových vlastností opticko-metalických prevodníkov a tienených skriniek • Skúmanie vlastností signálov • Skúmanie rôznych typov tlačiarní • on-site testing“) a návrh technického riešenia merania NEV zariadení	Ochrana proti NEV	Žiadateľ a partner	40
Výskum, vývoj, návrh a implementácia bezpečnej mobilnej pracovnej stanice	Implementácia bezpečnej mobilnej pracovnej stanice	Žiadateľ a partner	12
• Výskum útokov na pamäťové moduly	Odhalenie zraniteľnosti v moderných HW architektúrach	Žiadateľ a partner	24

• Výskum bezpečnosti nedokumentovaných komponentov chipsetov a procesorov • Výskum útokov na implementáciu cache • Výskum útokov na implementáciu vnútorných jednotiek procesora • Analýza a klasifikácia existujúcich tried zraniteľností			
• aplikácia umelej inteligencie na oblasť kybernetickej bezpečnosti • nové detekčné techniky • zvýšenie efektivity práce bezpečnostných analytikov nad veľkou množinou dát	Eliminácia pokročilých kybernetických hrozieb prostredníctvom využitia umelej inteligencie	Žiadateľ a partner	24
• identifikácia tých repozitárov a distribučných sietí, ktorých zneužitie by potenciálnemu útočníkovi umožnilo ľahkým spôsobom veľký dosah • vypracovanie metód a techník na efektívnu identifikáciu škodlivého kódu	Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach	Žiadateľ a partner	36
• Analýza aktivít CSIRT tímov a ich požiadaviek na funkcionalitu podporných technológií pre tieto aktivity • Analýza existujúcich riešení na podporu činnosti CSIRTov, identifikácia chýbajúcich komponentov či prepojení • Návrh, vývoj a kvalitatívne testovanie komplexného systému, pokrývajúceho potreby jednotiek typu CSIRT • Výskum ohraničený na témy SIEM SW, tiketovacie systémy, databázy konštituencie, databázy aktív, SW na agregáciu a distribúciu informácií, senzory, skenery zraniteľností a miskonfigurácie	Podpora činnosti jednotiek typu CSIRT	Žiadateľ a partner	40

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 Vybudovanie národnej PKI		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 2 Inovatívne riešenia OUS – zodolnenie a vyladenie systémov		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov

903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 3 Inovatívne riešenia OUS prostriedkami ŠOI		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 4 Ochrana proti NEV		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie

Nevyhnutné stavebné úpravy– laboratórium Brunovce		Nevyhnutné stavebné úpravy spojené s investíciami do výskumného a vývojového a laboratórneho vybavenia
Vypracovanie stavebnej dokumentácie, stavebný dozor		Výdavky vynaložené v súvislosti so spracovaním projektovej dokumentácie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 5 Bezpečná mobilná pracovná stanica		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 6 Zraniteľnosti v moderných hardvérových architektúrach		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov

903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 7 Využitie umelej inteligencie v oblasti pokročilých kybernetických hrozieb		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 8 Identifikácia škodlivého kódu v rozsiahlych online repozitároch a obsahových distribučných sieťach		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov

903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Aktivita 9 Integrovaný systém na podporu činnosti jednotiek typu CSIRT		
521 - Mzdové výdavky		Personálne výdavky pre: odborného garanta, hlavného koordinátora, regionálnych koordinátorov, garantov výskumných tímov, výskumných pracovníkov, technikov
903 - Paušálna sadzba na ostatné výdavky projektu (nariadenie 1304/2013, čl. 14 ods. 2)		Ostatné výdavky spojené s realizáciou NP, napr. cestovné náhrady, nájomné, operatívny leasing, kancelárske potreby a materiálno-technické zabezpečenie
Vybavenie, laboratórne zariadenia, zariadenia IKT - SW, HW, licencie, sieťová infraštruktúra		Návrh, obstaranie a dodanie materiálno-technického (MT) vybavenia (predovšetkým HW, SW, SW licencie, sieťová infraštruktúra, podporná infraštruktúra, špeciálne technologické zariadenia) nevyhnutného pre realizovanie výskumných činností
Hlavné aktivity SPOLU		
Predpokladané finančné prostriedky na podporné aktivity		
Publicita projektu, informovanosť a propagácia projektu	150 000 eur	Publicita projektu bude obsahovať prezentácie projektu verejnosti a odbornej verejnosti prostredníctvom správ, seminárov a článkov. Propagácia projektu (letáky, bulletiny, brožúry, perá, označenie zariadení, informačné plagáty)

Projektové riadenie	300 000 eur	Personálne výdavky priamo súvisiace s riadením projektu – manažér projektu, manažér pre publicitu a monitorovanie, pracovník pre verejné obstarávanie, finančný manažér, asistent projektového manažéra. Tieto výdavky sú vrátane účtovníctva projektu, programovania web stránok a portálov v súvislosti s projektom. Projektový manažment bude zabezpečený metodikou agilného prístupu a PRINCE II
Podporné aktivity SPOLU		
CELKOM	39 000 000 eur	

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

NP bude realizovať Dlhodobý strategický výskum v oblasti šifrovej ochrany a IT bezpečnosti, pričom 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?

Navrhujeme použitie paušálnej sadzby na ostatné výdavky vo výške 15% z priamych personálnych výdavkov, v súlade s čl. 14 ods. 2, Nariadenia 1304/2013. V prípade identifikácie potreby v procese prípravy, vítame aj použitie štandardnej stupnice jednotkových nákladov na vybrané mzdové výdavky.

16. Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov

Informácie sa vypĺňajú iba pre investičné[14] typy projektov.

Štúdia uskutočniteľnosti vrátane analýzy nákladov a prínosov	
Existuje relevantná štúdia uskutočniteľnosti[15] ? (áno/nie)	*NA*
Ak je štúdia uskutočniteľnosti dostupná na internete , uveďte jej	

[14] 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.

[15] 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)

názov a internetovú adresu, kde je štúdia zverejnená	
V prípade, že štúdia uskutočniteľnosti nie je dostupná na internete, uveďte webové sídlo a termín, v ktorom predpokladáte jej zverejnenie (mesiac/rok)	