Riadok	Názov projektu	Gescia	Celková investícia [€ s DPH]	2027				2028				2029				2030				2031				Popis
				Spolu [€ s DPH]	zo ŠR [€ s DPH]	z NRPP [€ s DPH]	iné zdroje [€ s DPH]	Spolu [€ s DPH]	zo ŠR [€ s DPH]	z NRPP [€ s DPH]	iné zdroje [€ s DPH]	Spolu [€ s DPH]	zo ŠR [€ s DPH]	z NRPP [€ s DPH]	iné zdroje [€ s DPH]	Spolu [€ s DPH]	zo ŠR [€ s DPH]	z NRPP [€ s DPH]	iné zdroje [€ s DPH]	Spolu [€ s DPH]	zo ŠR [€ s DPH]	z NRPP [€ s DPH]	iné zdroje [€ s DPH]	
1	Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe.	MIRRI / SKB	966 117,18	322 039,06	79 566,19		242 472,87	322 039,06	79 566,19		242 472,87	322 039,06	79 566,19		242 472,87									Obsahuje náklady spojené s obnovou softvérovej a hardvérovej podpory.
2	Posilnenie preventívnych opatrení, zvýšenie rýchlosti detekcie a riešenia incidentov (ITVS).	MIRRI / SKB	930 000,00	310 000,00	310 000,00			310 000,00	310 000,00			310 000,00	310 000,00											Zahŕňa výdavky od roku 2026 na zabezpečenie prevádzky a udržateľnosti projektu. Výdavok je potrebný na pokrytie prevádzky bezpečnostného dohľadového centra (V| CSIRT, NASES), proaktívnych služieb a reaktívnych služieb, ktoré poskytuje centrálne pre verejnú správu vrátane systému včasného varovania. Obsahuje náklady na licenčný SW a rozšírenie/obnovu HW po jeho životnosti.
3	Rozvoj a úprava informačného systému (IS CPDI) - dátové integrácie)	MIRRI / ŠT2 - SITVS	1 377 000,00	500 000,00	500 000,00			500 000,00	500 000,00			377 000,00	377 000,00											Dátové integrácie (DI). Vzhľadom na skutočnosť, že realizácia dátových integrácii bude kontinuálne nevyhnutná na strane MIRRI SR ako správcu CPDI, preto je nevyhnutné alokovať nevyhnutné kapitálové zdroje na tieto aktivity. Zároveň máme zato, že aj dobadovanie CIP
4	Národný projekt vytvorenia, resp. zvýšenia spôsobilosti distribuovaných dátových centier.	MIRRI / SKB	10 000 000,00	10 000 000,00	10 000 000,00			0,00				0,00												DR2: Využitie distribuovaných dátových centier, Automatizované zálohovanie a replikácia
5	Zálohovacie centrum - HW, SW (KaVP).	MIRRI / NASES	2 000 000,00	2 000 000,00	2 000 000,00			0,00				0,00												
6	Govnet - obnova HW core infraštruktúry.	MIRRI / NASES	1 600 000,00	1 600 000,00	1 600 000,00			0,00				0,00												
7	KaVP rozsírenie HW - Planovane rozsirovanie HW	MIRRI /	1 500 000,00	500 000,00	500 000,00			500 000,00	500 000,00			500 000,00	500 000,00											
8	Projekt vzdelávania osôb od 65 rokov v digitálnych zručnostiach.	MIRRI	40 150 000	150 000	150 000			8 000 000,00		8 000 000		10 000 000,00		10 000 000		10 000 000		10 000 000		12 000 000		12 000 000		Vzdelávanie v oblasti digitálnych zručností je do veľkej miery závislé na vzdelávaní v zamestnaní, resp. na zamestnávateľom hradených programoch. Zvlášť problematické je to pre ľudí v post-produktívnom veku, ktorí tak majú veľmi limitovaný prístup k rozvoju digitálnych zručností. Podľa indexu digitálnej ekonomiky a spoločnosti (DESI) za rok 2024 má v SR aspoň základné digitálne zručnosti 18,77% obyvateľov vo veku 65 - 77 rokov, pričom európsky priemer je na úrovni 28,19%. Podľa štúdie Inštitútu pre verejné otázky - "Zaostrené na seniorov" majú seniori pretrvávajúci problém riešen so sofistikovanými, ale aj s mnohými bežnými značnosťami ako napr. používanie bežných periférnych zariadení, download a uploud súborov/údajov, nastavenie internetového pripojenia či využívanie elektronických služieb na internete. Pre niektorých predstavuje problém aj používanie bežných aplikácií – programov, a viac ako tretina ankiet problémy s ovládaním stolného počítača, notebooku či ovládaním smartfónu alebo tabletu. " Zámerom aktivity je pokračovať v kontinuite programov v rámci POO SR, K17 Investícia č. 7: Zlepšovanie digitálnych znalostí seniorov a distribúcia Senior-tabletov, ktorý mal za cieľ zlepšiť digitálne znalosti celkovo 100 440 osobám od 65 rokov.
9	Posilnenie spôsobilosti a operačnej kapacity centrálneho bezpečnostného operačného centra pre verejnú správu.	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Centrálny SOC bol vybudovaný v rámci predchádzajúcich projektov, avšak jeho operačná spôsobilosť pokrýva iba obmedzený počet subjektov verejnej správy. Prevádzka nie je zabezpečená v režime 24/7/365 s plným personálnym obsadením pre všetky kritické ISVS. Chýbajú personálne a technologické kapacity pre pokročilé analytické nástroje a automatizácie reakcie (SOAR), kapacity threat intelligence a forenznej analýzy a analýzy škodlivého kódu sú obmedzené. Napojenie sektorových SOC a subjektov na centrálny monitoring je nedostatočné. Sektorové SOC existujú len v obmedzenej miere a nie sú systematicky budované. Významná časť kritických ISVS nie je napojená na žiadny bezpečnostný operačný dohľad. Pre dosiahnutie plného pokrytia je potrebné podporiť vznik nových a posilnenie existujúcich sektorových SOC a zabezpečiť onboarding vybraných kritických ISVS pod systém centrálneho alebo sektorového SOC. Podľa požiadaviek NIS2 (smernica 2022/2555) a zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti je potrebné zabezpečiť centrálny dohľad nad kybernetickou bezpečnosťou pre prevádzkovateľov základných služieb a kritickú infraštruktúru. V porovnaní s krajinami V4 (ČR prevádzkuje NÚKIB SOC s plným 24/7 pokrytím od roku 2022, Poľsko má CSIRT GOV s obdobnými kapacitami) zaostáva SR v rozsahu pokrytia aj v úrovni automatizácie detekcie a reakcie.
10	Modernizácia nástrojov a kapacít pre pokročilé testovanie bezpečnosti ISVS.	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Centrálne skenovanie zraniteľností je zavedené a funguje v základnom rozsahu. Prevažuje neinvazívne skenovanie, ktoré identifikuje iba povrchové zraniteľnosti. Kapacity pre invazívne (autorizované) skenovanie, pokročilé penetračné testovanie a red-teaming operácie sú obmedzené personálne aj technologicky. Chýbajú nástroje pre kontinuálne automatizované hodnotenie zraniteľností (CAVA), riadenie zraniteľností (angl. vulnerability management), riadenie záplat (angl. patch management) simulácie útokov a narušení (BAS/adversary simulation), pokročilé forenzné nástroje a platformy pre aktívne vyhľadávanie hrozieb (angl. threat hunting). Subjekty verejnej správy sa postupne zapájajú do centrálneho hodnotenia zraniteľností (angl. vulnerability assessment), avšak hĺbka a kvalita testovania nezodpovedá aktuálnemu hrozbovému prostrediu, potrebné riadenie zraniteľností (vulnerability management) a penetračné testovanie a red-teaming. Podľa vyhlášky NBÚ č. 227/2025 Z. z. sú prevádzkovatelia povinní vykonávať pravidelné hodnotenia zraniteľností a penetračné testy. V porovnaní s ČR (NÚKIB prevádzkuje pokročilé kapacity pre technickú kontrolu od roku 2023) a Estónskom (RIA disponuje red-team kapacitami) zaostáva SR v pokročilom testovaní.
11	Vytvorenie certifikačného a špecializačného rámca pre odborníkov na kybernetickú a informačnú bezpečnosť vo verejnej správe.	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Centrálne skenovanie zraniteľností je zavedené a funguje v základnom rozsahu. Prevažuje neinvazívne skenovanie, ktoré identifikuje iba povrchové zraniteľnosti. Kapacity pre invazívne (autorizované) skenovanie, pokročilé penetračné testovanie a red-teaming operácie sú obmedzené personálne aj technologicky. Chýbajú nástroje pre kontinuálne automatizované hodnotenie zraniteľností (CAVA), riadenie zraniteľností (angl. vulnerability management), riadenie záplat (angl. patch management) simulácie útokov a narušení (BAS/adversary simulation), pokročilé forenzné nástroje a platformy pre aktívne vyhľadávanie hrozieb (angl. threat hunting). Subjekty verejnej správy sa postupne zapájajú do centrálneho hodnotenia zraniteľností (angl. vulnerability assessment), avšak hĺbka a kvalita testovania nezodpovedá aktuálnemu hrozbovému prostrediu, potrebné riadenie zraniteľností (vulnerability management) a penetračné testovanie a red-teaming. Podľa vyhlášky NBÚ č. 227/2025 Z. z. sú prevádzkovatelia povinní vykonávať pravidelné hodnotenia zraniteľností a penetračné testy. V porovnaní s ČR (NÚKIB prevádzkuje pokročilé kapacity pre technickú kontrolu od roku 2023) a Estónskom (RIA disponuje red-team kapacitami) zaostáva SR v pokročilom testovaní.
12	Program prechodu kritických ISVS na postkvantovú kryptografiu (PQC).	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Kritické ISVS využívajú kryptografické mechanizmy (RSA, ECC, ECDSA) založené na matematických problémoch, ktoré budú riešiteľné kvantovými počítačmi. Inventarizácia kryptografických aktív nebola vykonaná, nie je známy rozsah závislosti na ohrozených algoritmoch. SR nemá národnú stratégiu prechodu na PQC. Európsky regulačný rámec vyžaduje prípravu na postkvantovú éru: NIS2 (smernica 2022/2555) ukladá povinnosť zabezpečiť priemyselnú kryptografickú opatrenia, CRA (nariadenie 2024/2847) požaduje kryptografickú agilitu produktov, eIDAS 2.0 (nariadenie 2024/1183) predpokladá PQC pripravenosť kvalifikovaných dôveryhodných služieb. NIST dokončil štandardizáciu prvých PQC algoritmov (ML-KEM, ML-DSA, SLH-DSA) v roku 2024, ENISA vydala odporúčania pre migráciu v roku 2025. Hrozba „harvest now, decrypt later" (HNDL) sa týka údajov s dlhodobou dôvernosťou vrátane štátnych tajomstiev, zdravotných záznamov a osobných údajov občanov. V porovnaní s krajinami EÚ: Francúzsko (ANSSI) a Nemecko (BSI) už vydali národné cestovné mapy PQC migrácie, Holandsko realizuje pilotné projekty od roku 2024. SR je v tejto oblasti na začiatku.
13	Posilnenie riadenia kontinuity prevádzky, zálohovacej infraštruktúry a disaster recovery kapacít pre kritické ISVS.	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Väčšina prevádzkovateľov kritických ISVS nemá vypracované a pravidelne testované plány kontinuity prevádzky (BCP) ani plány obnovy po havárii (DRP) v súlade s požiadavkami § 20 zákona č. 69/2018 Z. z. a vyhlášky NBÚ č. 227/2025 Z. z. Zálohovanie údajov sa vykonáva nejednotne, prevažne bez automatizácie, bez geografickej distribúcie a bez pravidelného overovania obnoviteľnosti záloh. Chýba centrálna zálohovacia infraštruktúra využívajúca distribuované dátové centrá, ktorá by umožnila automatizovanú replikáciu kritických údajov do geograficky oddelených lokalít. Testovanie disaster recovery (DR) plánov sa vykonáva sporadicky alebo vôbec. Nie sú zavedené pravidelné cvičenia obnovy, ktoré by overili reálnu schopnosť subjektov obnoviť prevádzku v stanovených časových parametroch (RTO/RPO). Podľa smernice NIS2 (2022/2555) je riadenie kontinuity prevádzky a krízové riadenie jedným z minimálnych bezpečnostných opatrení pre subjekty spadajúce do pôsobnosti smernice. V porovnaní s krajinami V4: ČR (NÚKIB) zaviedla povinné testovanie DR plánov pre prevádzkovateľov základných služieb od roku 2023. Estónsko prevádzkuje distribuovanú zálohovaciu infraštruktúru „Data Embassy" s replikáciou do zahraničných dátových centier. SR je v tejto oblasti na začiatku a nemá systémový prístup k riadeniu kontinuity prevádzky kritických ISVS.
14	Autonómna operačná bezpečnosť a kognitívne SOC (aSOC).	MIRRI / SKB	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				
15	Investície do cloudových technológií, ktorých správa je v zodpovednosti MIRRI SR	MIRRI / ŠT2 - SITVS	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Čiastkovou investíciou je budovanie moderného lokálneho cloudu, rozvoj verejného cloudu, migrácia informačných systémov do cloud a samozrejme investície do technológií (licencií, HW, služieb) s cieľom nahradiť, zjednodušiť a zlacniť aktuálnedigitálne služby. V súčasnosti je stav digitalizácie na nedostatočnej úrovni, aj v dôsledku toho že štát preferuje budovanie kľúčpových informačných systémov na úrovni lokálnych dátových centier bez prístupu k moderným technológiám.Dáta preukazujúce výhodnosť hybridného (privát/public) - cloud riešenie, ktoré preferujeme my samozrejme dokážeme zadokľad.
16	GaaP (government as a platform)	MIRRI / ŠT2 - SITVS	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Integrovaná verejná správa a inteligentná verejná správa nevyhnutne potrebuje, aby verejná správa začala realizovať digitalizáciu s ohľadom na zákazníka (občana, podnikateľa) s cieľom služby (aj elektronické služby) mali v prvom kroku integrovať, tak aby služby nepôsobili osamote ale v kontexte väzieb na iné služby a následne transformovať služby s cieľom mať proaktívne a inteligentné služby. Cieľom má by fvytvorenie GaaP (government as a platform) verejná správa ako služba. V súčasnosti sú služby, tak ako to je štandardom pre nedigitálne služby používané ako samostatné jednotky, neintegrované služby bez vzájomnej korelácie samozrejme s výnimkou služieb ktorí su akceptované na úrovni medzirezortných (CPDI, IT AM...).
17	Budovanie inštitucionálnych a technických kapacít pre dohľad nad AI a európskou dátovou reguláciou.	MIRRI / SDA	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Vybudovanie národnej infraštruktúry pre digitálnu integritu a suverénne využívanie AI. Cieľom je prechod od pasívneho dodržiavania predpisov k proaktívnemu technologickému líderstvu. Zabezpečuje budovanie personálnych kapacít (odborníci na AI, reguláciu a dátové právo s cieľom rastu na 30 FTE do roku 2030) a technickej infraštruktúry pre monitoring a audit AI systémov. Konkrétne komponenty investície: 1. Národný regulačný AI Sandbox: Vytvorenie kontrolovaného prostredia (Safe Harbor) pre MSP, priemysel a výskum na testovanie AI riešení pred vstupom na trh. 2. IT systémy pre dohľad (UDI-IS): Nástroje na audit AI, overovanie dátovej integrity a súladu s AI Act, Data Act a DGA. 3. Metodiky a štandardy: Procesy pre bezpečné zavádzanie AI do praxe. Očakávané prínosy a spätná väzba: Prínosy: Zvýšenie schopnosti štátu regulovať AI, podpora inovácií a zosúladenie s EÚ rámcom. Prepojenie na ID 57 (Občania): Reforma priamo rieši systémovú ochranu základných práv, s osobitným dôrazom na ochranu maloletých v digitálnom priestore pred rizikami spojenými s AI.
18	Zvyšovanie kybernetickej odolnosti kritickej infraštruktúry GOVNET a ÚPVS.	MIRRI / NASES	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				V oblasti security hardeningu kritickej infraštruktúry GOVNET a ÚPVS chýba jednotný a systematicky uplatňovaný rámec. Existujú síce čiastkové bezpečnostné opatrenia a smernice, avšak ich uplatňovanie je nejednotné a limitované personálnymi aj odbornými kapacitami správcov infraštruktúry. Absencia centralizovaného riadenia hardeningových štandardov a kontinuálneho vyhodnocovania bezpečnostnej odolnosti zvyšuje riziká pre dostupnosť a bezpečnosť služieb e-Governmentu.
19	Povinné pripojenie štátnych inštitúcií na infraštruktúru GOVNET.	MIRRI / NASES	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				Pripojenie štátnych inštitúcií na infraštruktúru GOVNET je v súčasnosti neúplné a nejednotné, pričom časť orgánov verejnej moci využíva alternatívne alebo historicky vzniknuté riešenia. To zvyšuje náklady na prevádzku, komplikuje bezpečnostný dohľad a oslabuje celkovú kybernetickú odolnosť štátu. Bez systematického a povinného prístupu k GOVNET bude fragmentácia infraštruktúry pretrvávať a zvyšovať bezpečnostné riziká.
20	Rozvoj funkčných a technických kapacít ÚPVS pre poskytovanie mobilných služieb.	MIRRI / NASES	TBD po skončení zberu pre potreby IFS					0,00				0,00				0				0				ÚPVS v súčasnosti poskytuje služby primárne prostredníctvom webového rozhrania, pričom plnohodnotná podpora mobilných služieb je obmedzená. To znižuje používateľský komfort a dostupnosť elektronických služieb verejnej správy, najmä v porovnaní s trendmi v iných krajinách EÚ. Ak nedôjde k cielenému rozvoju mobilných kapacít, využívanie digitálnych služieb štátu bude zaostávať za očakávaniami občanov.