digitální ; ČESKO

Vládní program digitalizace
České republiky 2018+

INFORMAČNÍ KONCEPCE ČR

Implementační plán hlavního cíle č. 3 - IK ČR
Rozvoj celkového prostředí podporujícího digitální technologie a budování/provoz klíčových systémů eGovernmentu

Verze dokumentu: **1.1**

Datum poslední změny dokumentu: **26. 8. 2021**

Poznámka k verzi:

_____

Úřad vlády České republiky, Nábřeží Edvarda Beneše 4, 118 01 Malá Strana
info@digitalnicesko.cz digitalnicesko.cz

Obsah

1 Základní informace

1.1 Rekapitulace cílů

Cíl – Dílčí cíl – Popis
IK ČR 3 Rozvoj celkového prostředí podporujícího digitální technologie
IK ČR 3.01 Aktivně prosazovat alokaci prostředků z ESIF na podporu prostředí digitálních technologií
Při tvorbě nového programovacího období bude ČR aktivně prosazovat alokaci prostředků z ESIF na podporu prostředí digitálních technologií, v rámci IK ČR pro rozvoj rozsahu a dostupnosti služeb elektronické veřejné správy.
IK ČR 3.02 Digitalizace dosud nedigitalizovaného obsahu
Digitalizace dosud nedigitalizovaného obsahu důležitého pro podporu konkurence-schopnosti a rozvoj eGovernment služeb pro veřejnost. Jedná se například o fondy duševního vlastnictví, knihovní fondy a fond kulturního dědictví, dokončení digitalizace katastru nemovitostí, digitalizace výstupů územního plánování zejména územních plánů, projektových dokumentací, digitalizace historických úředních dokumentů, agend pro podporu stavebnictví atd.
IK ČR 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu
Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu, jako předpokladu pro plně digitální, bezpapírové procesy veřejné správy.
IK ČR 3.04 Rozvoj a provoz základních registrů
Zkvalitnění, aktualizace a validace obsahu Registru práv a povinností. Jedná se zejména o zlepšení popisu dekompozice činností agend, agendových rolí a správné registrace agendových, provozních i dalších systémů (ISVS) do příslušných agend, ve vazbě na informace o řízení přístupu k datovým položkám, včetně prostorových. Dále o správu číselníků všech údajů důležitých pro řízení služeb eGovernmentu (životní události a situace, komponenty IS a jejich služby, datové sady apod.). Obecně jde o řídící (meta) informace eGovernmentu a tzv. META-informační systém (Meta-IS). V této souvislosti je nutné pro stále častější užívání těchto nástrojů při vývoji a správě služeb zjednodušit jejich obsluhu a provázat ji přirozeně s životním cyklem agend a informačních systémů veřejné správy.
IK ČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy
Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy. Komunikační infrastruktura veřejné správy včetně Centrálního místa služeb (CMS) se musí stát sdíleným, bezpečným a řízeným komunikačním prostředím zejména pro všechny správce agendových systémů v přenesené působnosti. Musí umožnit bezpečné propojování poskytovaných online služeb s jejich uživateli, a to jak uvnitř veřejné správy, tak i pro klienty na internetu. Celá komunikační infrastruktura musí být nákladově efektivní, bez zbytečných duplicit v komunikačních kanálech, robustní a bezpečná s definovanými a měřitelnými parametry jednotlivých služeb formou SLA. Budována bude i nadále vícezdrojově, s využitím vlastní infrastruktury veřejné správy i s využitím komerčních služeb. Komunikační prostředí veřejné správy je nástrojem umožňujícím dostupnou, spolehlivou a bezpečnou komunikaci mezi jednotlivými IT systémy a uživateli těchto systémů. Komunikačního prostředí veřejné správy je mimo jiné nutné pro využití při zajišťování vnitřního pořádku a bezpečnosti, bezpečnosti státu a řešení krizových situací. Bezpečná a dostatečně odolná cesta přenosu informací mezi dotčenými složkami veřejné správy, jejichž informační a rozhodovací potenciál je klíčový pro případ rychlé reakce, je nezbytným technickým předpokladem odolnosti státu vůči všem hrozbám bez rozdílu. Existence funkční infrastruktury parametricky odpovídající poskytovaným službám, s případnou rezervou pro další rozvoj těchto služeb, je také podmínkou dalšího rozvoje eGovernmentu a naplňování mnoha vládních strategií (např. Strategie digitálního vzdělávání do roku 2020, Strategie digitální gramotnosti). Aby se předešlo spontánním zásahům do tohoto prostředí, je potřeba rozvoj komunikačního prostředí veřejné správy korigovat. Koncepce rozvoje komunikačního prostředí veřejné správy bude sledovat dlouhodobé cíle a zajistí efektivní vynakládání prostředků v této oblasti.
IK ČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe

Cíl – Dílčí cíl – Popis
Zavedení systému důvěryhodné elektronické identifikace do praxe. Do cíle spadá jak elektronická identifikace občanů a zástupců právnických osob (NIA, nové občanské průkazy, komerční poskytovatelé identifikace, …) a cizinců, tak společná centrální fyzická i elektronická identifikace úředníků prostřednictvím jednotného autentizačního systému (SSO). Součástí cíle jsou i prostředky pro elektronický podpis a pečeť pro úředníky a úřady, a jejich poskytování jako sdílené služby státu. Součástí cíle je i zajištění elektronizace oprávnění k úkonům na základě zákonných zmocnění, plných mocí, profesních způsobilostí (lékaři apod.) a dalších oprávnění (řidičská, zbrojní apod.).
IK ČR 3.07 Rozvoj a provoz základních služeb
Implementace strategie sdílení dat mezi veřejnou správou a privátním sektorem formou Digitální mapy veřejné správy, zejména Digitální technické mapy ČR a dalších autoritativních široce využitelných datových zdrojů (vzniklých např. na základě použití metod jako je BIM – Informační modelování staveb apod.) jako nedílných součástí Národní infrastruktury pro prostorové informace.
IK ČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu
Podpora opatření kybernetické bezpečnosti pro veřejnou správu. Obsahem cíle je zajišťování důvěry a bezpečnosti interních i externích digitálních služeb veřejné správy plněním „Akčního plánu k Národní strategii kybernetické bezpečnosti ČR“, a to pro příslušné období, a dalšími opatřeními, nezahrnutými do jiných cílů IK ČR. Opatření tohoto cíle pro veřejnou správu souvisí s opatřeními cílů DES HC5 pro celou společnost, zejména pak s dílčími cíli 5.4 a 5.5. Cíl byl přesunut z DES 5.1, protože je zaměřen výhradně na veřejnou správu a patří tak do IK ČR.

1.2 Klasifikace záměrů A, B a C

A. Záměr je dlouhodobě připravený, schválený v gesčním úřadu, je „v běhu“, má zajištěné financování (např. projekty již schválené OHA). V rámci metodiky to odpovídá stavu „závazku“, popř. dalších stavů. Záměry „A“ jsou uvedeny v příloze implementačních plánů.
B. Záměr je definovaný gesčním úřadem, tj. má prioritu a podporu v gesčním úřadu, ale nemá finanční nebo personální krytí. Tyto záměry tvoří těžiště implementačního plánu.
C. Potřebný záměr, existuje koncept záměru (tj. prakticky všechna políčka jsou vyplněná), ale není dojednána podpora gestora, gesční úřad, ani zdroje (typicky průřezové záměry, multiresortní a sdílené).

V katalogu záměrů se nachází ještě další záměry ve stavu „**D**“, tj. náměty na záměr. Tyto náměty vznikly z různých inspirací, například z potřeby pomoci úřadů dostát požadavkům architektonickým principů a zásad řízení ICT ze schválené Informační koncepce. Mnohé náměty mohou být ještě nedostatečně popsané, duplicitní nebo příliš detailní, proto je pro jejich převod do stavu „C“ při příštím implementačním plánování nutná jejich konsolidace.

1.3 Shrnutí problematiky, celkové přínosy

Cílem opatření v rámci hlavního cíle 3 je ve spolupráci se sociálními partnery a s dalšími subjekty vytvořit prostředí, podporující českou společnost v digitální transformaci. Plnění tohoto cíle je spolu s legislativními úpravami klíčovým předpokladem významného posunu v celé oblasti vzdělávání, výzkumu a vývoje, ICT infrastruktury, legislativy, trhu práce, standardizace a kybernetické bezpečnosti. Je třeba se zaměřit na vytvoření příznivých podmínek pro oblast eGovernmentu, například cestou rozvoje Národního identitního prostoru České republiky, v rámci něhož by každý občan, potenciálně schopný digitální komunikace, měl disponovat alespoň jedním elektronickým identitním prostředkem na vzdálené prokázání své totožnosti. Podporovat firmy a občany v přijímání digitálních technologií. Vytvořit prostředí příznivé pro vznik, vývoj a testování digitálních a mobilních služeb a s tím související nastavení očekávání občanů. Součástí tohoto cíle jsou i digitální služby v oblasti elektronických podpisů, například realizace sdílené služby pro vytváření úředně ověřeného elektronického podpisu, podle zákona o právu na digitální služby.

Za „digitalizaci“ se přirozeně považuje transformace dosud nedigitalizovaného obsahu na plně digitální, nicméně spadá sem i posun ve významné a komplikované oblasti zavedení průkazné elektronické identity všech subjektů a rovněž i zkvalitnění dosud nekvalitního, již existujícího digitálního obsahu (např. obsah Registru práv a povinností).

V návaznosti na masivní nástup jednotné elektronické identifikace fyzických osob i díky bankovní elektronické identifikaci je potřebné vytvořit podmínky a centrální sdílené služby pro možnost využití této identifikace jednotně při zastupování právnických osob a organizací i jiných fyzických osob v digitálním prostoru veřejné správy ČR. Jako reakci na velký zájem klientů o využívání elektronické identifikace je potřebné tuto službu významně výkonnostně posílit.

Z hlediska předpokladů efektivního využití eGovernmentu a zlepšení mezinárodní konkurenceschopnosti ČR tvoří zásadní oblast rovněž rozvoj vysokorychlostních sítí, zejména dostupnosti vysokorychlostního internetu. Do tohoto cíle rovněž spadá rozvoj komunikační infrastruktury veřejné správy.

K tomu, aby digitalizovaná veřejná správa dobře fungovala a aby v ni organizace i občané měli důvěru, je klíčové zajistit bezpečnost digitálních služeb. Jedná se, jak o obranu proti kybernetickým útokům a zajištění efektivní a kvalitní kybernetické infrastruktury, tak o ochranu soukromí a osobních i obchodních údajů uživatelů.

Jedním ze základních předpokladů pro efektivní fungování jednotlivých centrálních i lokálních agendových i neagendových informačních systémů je jejich napojení na robustní základní registry jako centrální autoritativní zdroje základních informací. Stávající systémy základních registrů mj. i z důvodu implementace Zákona č.12/2020 o právu na digitální služby musí projít výraznými úpravami. Na tuto aktuální situaci reaguje **dílčí cíl – 3.04 Rozvoj a provoz základních registrů.** Tento cíl vychází z původního dílčího cíl 3.04 – Zkvalitnění, aktualizace a validace obsahu Registru práv a povinností a dále jej rozšiřuje v návaznosti na aktuální požadavky.

V současnosti řešená problematika GIS si vyžádala úpravu dílčího cíle 3.7, kdy jeho původní zaměření spočívalo v úzké specializaci na Digitální technické mapy ČR a Informační systém technické infrastruktury veřejné správy. Toto zaměření je stále validní a je i dále akcelerováno především v souvislosti s novým stavebním zákonem a digitalizací stavebního řízení. Nově formulovaný **dílčí cíl 3.07 Rozvoj a provoz základních služeb** v sobě nově zahrnuje i veškeré záměry z oblasti Národní infrastruktury pro prostorové informace.

1.4 Počty záměrů a odhad finanční alokace dle gesce

Stav – Gestor	Počet	Výdaje 2022 [mil. Kč]	Výdaje 2023 [mil. Kč]	Výdaje 2024+ [mil. Kč]
A	**41**	**405,07**	**167,2**	**16,94**
Česká správa sociálního zabezpečení	17	171,17	130	
FN u sv. Anny v Brně	1			
Ministerstvo dopravy	1			
Ministerstvo kultury	1	48,4	24,2	16,94
Ministerstvo práce a sociálních věcí	1	5	5	
Ministerstvo spravedlnosti	2	7	8	
Ministerstvo vnitra	7			
Ministerstvo zahraničních věcí	1	169,5	0	
Ministerstvo zemědělství	1	4		
Národní úřad pro kybernetickou a informační bezpečnost	7			
Správa základních registrů	1			
ÚV – Úřad vlády	1	0		
B	**31**	**923,87**	**374,01**	**163,24**
Česká správa sociálního zabezpečení	13	149,3	93,3	28,15
Český statistický úřad	3	40,13	7,5	
Ministerstvo kultury	2			
Ministerstvo práce a sociálních věcí	1	100		
Ministerstvo spravedlnosti	1	0	34,06	0
Ministerstvo vnitra	4	360,5	136,3	130,25
MV ČR – Policie ČR	1	60,5		
NAKIT	1	4,84	6,05	4,84
Národní úřad pro kybernetickou a informační bezpečnost	1	15		
Správa základních registrů	4	193,6	96,8	
C	**5**	**925**	**3,5**	**258,5**
Ministerstvo vnitra	3	925		
MV ČR – Policie ČR	1			
Národní archiv	1	0	3,5	258,5
Celkový součet	**77**	**2253,94**	**544,71**	**438,68**

1.5 Počty záměrů a odhad finanční alokace dle cílů

Stav – Cíl	Počet	Výdaje 2022 [mil. Kč]	Výdaje 2023 [mil. Kč]	Výdaje 2024+ [mil. Kč]
A	**41**	**405,07**	**167,2**	**16,94**
IK ČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.	5	55,4	32,2	16,94
IK ČR 3.04 Rozvoj a provoz základních registrů	6	0		
IK ČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	17	171,17	130	
IK ČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.	5	9	5	
IK ČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	8	169,5	0	
B	**31**	**923,87**	**374,01**	**163,24**
IK ČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.	1			
IK ČR 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu.	1	12,1	24,2	18,15
IK ČR 3.04 Rozvoj a provoz základních registrů	5	218	68	
IK ČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	12	476	157	100
IK ČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.	4	64,83	24,2	
IK ČR 3.07 Rozvoj a provoz základních služeb	1			
IK ČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	7	152,94	100,61	45,09
C	**5**	**925**	**3,5**	**258,5**
IK ČR 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu.	1	0	3,5	258,5
IK ČR 3.04 Rozvoj a provoz základních registrů	1	25		
IK ČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.	1	900		
IK ČR 3.07 Rozvoj a provoz základních služeb	1			
IK ČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	1			
Celkový součet	**77**	**2253,94**	**544,71**	**438,68**

1.6 Výsledky za rok 2020 - stav záměrů v realizaci

Gesční úřad – Záměr	Hotovo %	Výdaje 2022 [mil. Kč]	Výdaje 2023 [mil. Kč]	Výdaje 2024+ [mil. Kč]
Česká správa sociálního zabezpečení				
Implementace nařízení eIDAS, ČSSZ	100			
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021	50			
Ministerstvo dopravy				
Zpřístupnění informací o řidiči prostřednictvím Portálu občana	100			
Ministerstvo kultury				
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK	100			
Ministerstvo práce a sociálních věcí		**5**	**5**	
Poskytování služeb při vydávání kvalifikovaných a komerčních certifikátů v resortu MPSV	100	5	5	
Ministerstvo spravedlnosti				
Justiční autentizační a autorizační služba (JAAS)	80			
Ministerstvo vnitra		**36,3**	**12,1**	
Koordinace rozšiřování počtu Service Providerů (SeP), připojených do NIA	20			
Metodická podpora zavedení DTM ČR	10			
Právní úprava rozšíření funkcionalit RPP o údaje vedené doposud v IS o ISVS a IS DP	90			
Rozvoj ROB a souvisejících AIS	5	36,3	12,1	
RPP, rozvoj registru a jeho agendového informačního systému	80			
RPP, rozvoj, analýza datového modelu, analýza procesu plnění a užívání údajů	10			
RPP, začlenění ISoISVS do RPP a další rozvoj	20			
Ministerstvo zahraničních věcí		**169,5**	**0**	
Digitální transformace úřadu za účelem zvýšení kybernetické bezpečnosti a zlepšení poskytování služeb občanovi	7	169,5	0	
Ministerstvo zemědělství		**4**		
Vybudování přístupového bodu ke službám elektronické identifikace, MZe	10	4		
Správa základních registrů		**169,4**	**72,6**	
[P] Program – Základní registry 2.0	20			
Národní certifikační autorita (NCA)	70			
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci	85	24,2	24,2	
SZR – ISZR, ISSS	18	145,2	48,4	
ÚV – Úřad vlády		**0**		
Revize agend dle RPP	100	0		
Celkový součet		**384,2**	**89,7**	

1.7 Prioritní záměry pro období 2021-2022

Hlavními prioritami v roce 2022 a následujících jsou v rámci hlavního cíle 3 oblasti kybernetické bezpečnosti služeb veřejné správy a projekty v oblasti základních registrů, především investice do jejich posílení a rozvoje v souvislosti s přijetím Zákona o právu na digitální služby a dalšími souvisejícími zákony. Tyto záměry jsou dominantně financovány prostřednictvím Národního plánu obnovy.

V oblasti kybernetické bezpečnosti se jedná především o záměry Ministerstva zahraničních věcí, ČSSZ, Policie ČR a program Zajištění kybernetické bezpečnosti poskytovatelů zdravotnických služeb v Praze, Další potřeby v oblasti kybernetické bezpečnosti, a to jak z oblasti poskytovatelů zdravotnických služeb, tak i veřejné správy budou realizovány z prostředků IROP 2021+. a to jak v oblasti ale i v obecném kontextu v rámci záměru s názvem: Digitální transformace úřadu za účelem zvýšení kybernetické bezpečnosti a zlepšení poskytování služeb občanovi.

V rámci Nadpožadavků státního rozpočtu je pak prioritou financování záměrů pro budování a obměnu komunikační infrastruktury.

2 Sestava plánovaných záměrů dle data ukončení realizace (klasifikace B, C)

Rok – Měsíc dokončení realizace – Název záměru	Počet	Hotovo %	Výdaje 2022 [mil. Kč]	Výdaje 2023 [mil. Kč]	Výdaje 2024+ [mil. Kč]
2019	**2**				
12	**2**				
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK	1	100			
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK	1				
2021	**3**		**0**		
12	**3**		**0**		
ČSSZ – obměna HW pro Archiv nárokových podkladů	1		0		
ČSSZ – Pořízení SAN volume controler (SVC) pro centrální datové úložiště	1		0		
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021	1	50			
2022	**14**		**341,33**	**24,2**	
1	**1**				
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu	1				
12	**13**		**341,33**	**24,2**	
ČSSZ – Aplikace KOC	1		8		
ČSSZ – Aplikace NEM 2. část	1		8		
ČSSZ – GDPR	1		37		
ČSSZ – licence ORACLE	1		15		
ČSSZ – licence VMware – VSAN	1		10		
ČSSZ – Rozvoj stávajících APV (INS, MKV, SRP) - 2. část	1		20		
ČSSZ – Úpravy aplikace POJ 2.část	1		15		
Pořízení softwarově definovaného DC a obnova systémových prostředků DC	1		100		
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci	1	85	24,2	24,2	
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí	1		25		
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence	1		15		
Zajištění zvýšení kybernetické bezpečnosti Policie ČR	1		60,5		
SIS_0 Centrální autentizační bod	1		3,63		
2023	12		1207,54	215,75	63,24

Rok – Měsíc dokončení realizace – Název záměru	Počet	Hotovo %	Výdaje 2022 [mil. Kč]	Výdaje 2023 [mil. Kč]	Výdaje 2024+ [mil. Kč]
5	**1**	**70**			
Národní certifikační autorita (NCA)	1	70			
12	**11**		**1207,54**	**215,75**	**63,24**
Digitální spisovna	1		12,1	24,2	18,15
Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, kybernetická bezpečnost Správy základních registrů (SZR)	1		24,2	24,2	
Infrastruktura	1			57	
Kybernetická bezpečnost IIS ČSSZ	1		24,2	12,1	10
ROS - 2020+	1		26	6	
ROS – IAIS - 2020+	1		10,5	1,5	
Rozvoj ROB a souvisejících AIS	1	5	36,3	12,1	
SZR – ISZR, ISSS	1	18	145,2	48,4	
Vysokorychlostní datová síť krajů a technologická centra krajů	1		900		
Dohledové centrum eGovernmentu	1		24,2	24,2	30,25
Zajištění kompetence bezpečného vývoje pro digitální systém státní správy	1		4,84	6,05	4,84
2024	**1**		**0**	**34,06**	**0**
2	**1**		**0**	**34,06**	**0**
Budování kapacit kybernetické bezpečnosti	1		0	34,06	0
2026	**2**		**0**	**3,5**	**258,5**
12	**2**		**0**	**3,5**	**258,5**
Národní digitální archiv III (NDA III)	1		0	3,5	258,5
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění	1				
2027	**1**		**300**	**100**	**100**
12	**1**		**300**	**100**	**100**
Rozvoj nových digitálních služeb Centrálního místa služeb	1		300	100	100
(prázdné)	**1**				
(prázdné)	**1**				
Metodická podpora zavedení DTM ČR	1	10			
Celkový součet	**36**		**1848,87**	**377,51**	**421,74**

3 Plánované náklady a pracnosti záměrů (klasifikace B, C)

Název záměru	Výdaje 2022 [mil. Kč]	Celk. výdaje [mil. Kč]	TCO [mil. Kč]	Odhad pracnosti	Pracnost udržitelnosti
Budování kapacit kybernetické bezpečnosti	0	34,06			
ČSSZ – Aplikace KOC	8	13			
ČSSZ – Aplikace NEM 2. část	8	18			
ČSSZ – GDPR	37	37			
ČSSZ – licence ORACLE	15	40			
ČSSZ – licence VMware – VSAN	10	10			
ČSSZ – obměna HW pro Archiv nárokových podkladů	0	3			
ČSSZ – Pořízení SAN volume controler (SVC) pro centrální datové úložiště	0	12,4			
ČSSZ – Rozvoj stávajících APV (INS, MKV, SRP) - 2. část	20	29,5			
ČSSZ – Úpravy aplikace POJ 2.část	15	34,25			
Digitální spisovna	12,1	54,45			
Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, kybernetická bezpečnost Správy základních registrů (SZR)	24,2	72,6			
Infrastruktura		57			
Kybernetická bezpečnost IIS ČSSZ	24,2	48,4			
Metodická podpora zavedení DTM ČR		2			
Národní certifikační autorita (NCA)		48,4		3200	1506
Národní digitální archiv III (NDA III)	0	262			
Pořízení softwarově definovaného DC a obnova systémových prostředků DC	100	100			
ROS - 2020+	26	47		100	
ROS – IAIS - 2020+	10,5	13		100	
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK		4,23		200	0
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci	24,2	72,6		13000	3500
Rozvoj nových digitálních služeb Centrálního místa služeb	300	500			
Rozvoj ROB a souvisejících AIS	36,3	72,6			
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí	25				
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu					

Název záměru	Výdaje 2022 [mil. Kč]	Celk. výdaje [mil. Kč]	TCO [mil. Kč]	Odhad pracnosti	Pracnost udržitelnosti
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021		287,5		6900	4400
SZR – ISZR, ISSS	145,2	221,43		2510	753
Vysokorychlostní datová síť krajů a technologická centra krajů	900	2750		5000	9000
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK		3,72		200	1600
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence	15	30			
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění		60			
Zajištění zvýšení kybernetické bezpečnosti Policie ČR	60,5	60,5			
Dohledové centrum eGovernmentu	24,2	96,8			
Zajištění kompetence bezpečného vývoje pro digitální systém státní správy	4,84	19,36			
SIS_0 Centrální autentizační bod	3,63	4,84		150	290
Celkový součet	**1848,87**	**5119,64**		**31360**	**21049**

4 Přehled pokrytí cílů – plánované záměry (klasifikace B, C)

Cíl – Záměr
IK ČR 3.02 Digitalizace dosud nedigitalizovaného obsahu.
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK
IK ČR 3.03 Vytvoření prostředí pro dlouhodobé ukládání a archivaci digitálního (úředního) obsahu.
Digitální spisovna
Národní digitální archiv III (NDA III)
IK ČR 3.04 Rozvoj a provoz základních registrů
ROS - 2020+
ROS – IAIS - 2020+
Rozvoj ROB a souvisejících AIS
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
SZR – ISZR, ISSS
IK ČR 3.05 Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy.
ČSSZ – Aplikace KOC
ČSSZ – Aplikace NEM 2. část
ČSSZ – licence ORACLE
ČSSZ – licence VMware – VSAN
ČSSZ – obměna HW pro Archiv nárokových podkladů
ČSSZ – Pořízení SAN volume controler (SVC) pro centrální datové úložiště
ČSSZ – Rozvoj stávajících APV (INS, MKV, SRP) - 2. část
ČSSZ – Úpravy aplikace POJ 2.část
Infrastruktura
Pořízení softwarově definovaného DC a obnova systémových prostředků DC
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK
Rozvoj nových digitálních služeb Centrálního místa služeb
Vysokorychlostní datová síť krajů a technologická centra krajů
IK ČR 3.06 Zavedení systému důvěryhodné elektronické identifikace do praxe.
ČSSZ – GDPR
Národní certifikační autorita (NCA)
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci
SIS_0 Centrální autentizační bod
IK ČR 3.07 Rozvoj a provoz základních služeb
Metodická podpora zavedení DTM ČR
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021
IK ČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.

Cíl – Záměr
Budování kapacit kybernetické bezpečnosti
Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, kybernetická bezpečnost Správy základních registrů (SZR)
Kybernetická bezpečnost IIS ČSSZ
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění
Zajištění zvýšení kybernetické bezpečnosti Policie ČR
Dohledové centrum eGovernmentu
Zajištění kompetence bezpečného vývoje pro digitální systém státní správy

5 Kontaktní osoby – plánované záměry (klasifikace B, C)

Gestor – Kontaktní osoba – Název záměru
Česká správa sociálního zabezpečení
Nováková Jana
ČSSZ – Aplikace KOC
ČSSZ – Aplikace NEM 2. část
ČSSZ – GDPR
ČSSZ – licence ORACLE
ČSSZ – licence VMware – VSAN
ČSSZ – obměna HW pro Archiv nárokových podkladů
ČSSZ – Pořízení SAN volume controler (SVC) pro centrální datové úložiště
ČSSZ – Rozvoj stávajících APV (INS, MKV, SRP) - 2. část
ČSSZ – Úpravy aplikace POJ 2.část
Digitální spisovna
Infrastruktura
Kybernetická bezpečnost IIS ČSSZ
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021
Český statistický úřad
Böhm Petr
ROS - 2020+
ROS – IAIS - 2020+
SIS_0 Centrální autentizační bod
Ministerstvo kultury
Zmij Jan
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK
Ministerstvo práce a sociálních věcí
Nováková Jana
Pořízení softwarově definovaného DC a obnova systémových prostředků DC
Ministerstvo spravedlnosti
Pohludka Vojtěch
Budování kapacit kybernetické bezpečnosti
Ministerstvo vnitra
Kuchař Petr
Vysokorychlostní datová síť krajů a technologická centra krajů
Knotek František
Rozvoj ROB a souvisejících AIS

Gestor – Kontaktní osoba – Název záměru
Hrabě Pavel
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
Urban Bohdan
Rozvoj nových digitálních služeb Centrálního místa služeb
Zůbek Bohuslav
Dohledové centrum eGovernmentu
Kubátová Eva
Metodická podpora zavedení DTM ČR
Tretera Jan
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
MV ČR – Policie ČR
Kraus Martin
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění
Zajištění zvýšení kybernetické bezpečnosti Policie ČR
NAKIT
Pur Marek
Zajištění kompetence bezpečného vývoje pro digitální systém státní správy
Národní archiv
Vojáček Milan
Národní digitální archiv III (NDA III)
Národní úřad pro kybernetickou a informační bezpečnost
Paggio Viktor
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
Správa základních registrů
Kalenský Libor
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci
Knotek František
Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, kybernetická bezpečnost Správy základních registrů (SZR)
Národní certifikační autorita (NCA)
SZR – ISZR, ISSS

6 Popisy záměrů (klasifikace A, B, C)

Gestor – Stav – Název záměru – Popis záměru
Česká správa sociálního zabezpečení
A
ČSSZ – Agregace (Digi Česko)
Agregace.
ČSSZ – Další rozvoj IKR
Nové služby a další rozvoj APV IKR.
ČSSZ – Dohledový systém datových center
Realizace dohledového centra.
ČSSZ – HW vybavení nově vybudovaného datového centra ČSSZ
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – licence MS, Oracle, IBM (Digi Česko)
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – licence Oracle (Digi Česko)
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – Navýšení výpočetního výkonu centrálního datového úložiště (Digi Česko)
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.
ČSSZ – Obměna a rozšíření aktivních prvků ČSSZ (Digi Česko)
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.
ČSSZ – Obměna Blade serverů
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – obměna diskových polí (Digi Česko)
ČSSZ – Obměna infrastrukturních serverů v oblasti DMZ a NAS
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – Obměna síťových prvků datové sítě
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – obnova HW (Digi Česko)
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – Pořízení a obnova HW a SW
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – Rozšíření centrálního datového úložiště
Záměr registrován v rámci investičních akcí ČSSZ.
ČSSZ – SLBD 2020+
Záměr registrován v rámci investičních akcí ČSSZ.
Implementace nařízení eIDAS, ČSSZ
B
ČSSZ – Aplikace KOC
Implementace aplikace pro kontrolní činnosti.
ČSSZ – Aplikace NEM 2. část
Další rozvoj APV pro výkon nemocenského pojištění.
ČSSZ – GDPR
Implementace GDPR do IIS ČSSZ.
ČSSZ – licence ORACLE
Nákup licencí ORACLE v rámci posilování infrastruktury IIS ČSSZ.
ČSSZ – licence VMware – VSAN
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.
ČSSZ – obměna HW pro Archiv nárokových podkladů
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.

Gestor – Stav – Název záměru – Popis záměru
ČSSZ – Pořízení SAN volume controler (SVC) pro centrální datové úložiště
Pořízení SAN volume controler (SVC) pro centrální datové úložiště.
ČSSZ – Rozvoj stávajících APV (INS, MKV, SRP) - 2. část
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.
ČSSZ – Úpravy aplikace POJ 2.část
Záměr registrován v rámci investičních akcí ČSSZ – finančně nezajištěná akce.
Digitální spisovna
Dlouhodobé a důvěryhodné ukládání a správa všech elektronických dokumentů o jednotlivých klientech přicházejících do integrovaného informačního systému ČSSZ a elektronických dokumentů vytvářených či zpracovávaných v různých agendových aplikacích ČSSZ při vyřizování podání klientů. Zajištění dlouhodobého uchovávání těchto informací po dobu životního cyklu klienta. Automatická skartace a předávání dat Státnímu archivu. S rozborem a návrhem řešení obsahující návrh variant řešení, jejich vyhodnocení, predikce vývoje a trendů v oblasti potřebnosti řešení ukládání, správy a skartace dat v návaznosti na jejich životní cyklus. Studie obsahuje dále návrh rozhraní na vstupní, agendové a výstupní subsystémy IIS ČSSZ a návrh na rozhraní a způsob předávání informací do státního archivu.
Infrastruktura
Kybernetická bezpečnost IIS ČSSZ
Projekt řeší požadavky kybernetické bezpečnosti, které ČSSZ jako správce kritické informační infrastruktury Integrovaného informačního systému ČSSZ naplňuje v souladu se zákonem č. 181/2014 Sb., zákon o kybernetické bezpečnosti a vyhláškou š. 82/2018 Sb., vyhláška o kybernetické bezpečnosti. Týká se zajištění monitoringu a řízení používání výměnných zařízení a datových nosičů a dále zavádění bezpečnostních opatření pro bezpečné využívání mobilních zařízení a jiných technických zařízení, nástrojů pro sběr a vyhodnocování kybernetických bezpečnostních událostí, jejich vyhodnocování a včasné varování.
Smlouva o nákupu HW komponent a poskytnutí služby pro zajištění provozu CVS na roky 2018–2021
Centrální výpočetní systém (CVS) slouží k provozování aplikačního programového vybavení a správě dat používaných při provádění důchodového pojištění zaměstnanců (s výjimkou příslušníků), osob samostatně výdělečně činných a osob dobrovolně účastných důchodového pojištění. Protože se jedná o systém, který je prvkem kritické informační infrastruktury, je potřeba zajistit jeho nepřetržitý provoz a rozvoj. Předmětem projektu je nákup HW, služeb service HW a podpory systémového SW. Rozvoj programového vybavení se provádí vlastními zaměstnanci i dodavatelsky.
Český statistický úřad
B
ROS - 2020+
Cílem projektu bude implementovat vybrané požadavky cílového konceptu ZR 2.0, zákona č. 12/2020 o právu na digitální služby a novely zákona o základních registrech. Konkrétně půjde o tyto aktivity: a) zařazení nových referenčních údajů do ROS – realizace požadavku vyplývajícího z §10 zákona o právu na digitální služby (zařazení kontaktních údajů do ROS). V této souvislosti se předpokládá vytvoření nové editační služby ROS a úprava dosavadních publikačních služeb ROS. Předpokládané náklady na tuto akci jsou 103 MDs tj. 1 500 000 KČ (vč. DPH). b) aplikace analytického modulu – aplikace analytického modulu umožní kontrolu integritních vazeb v rámci editorů registrů, kontrolu integritních vazeb mezi základními registry, vytváření vlastních a předpřipravených reportů na základě provozních a infrastrukturních dat (reporty budou využity k optimalizaci služeb ROS) a poskytování údajů ve formě open dat (buď ve formě statistik o počtech osob dle vybraných charakteristik (region, právní forma apod.) nebo ve formě poskytování informací o jednotlivých osobách). Předpokládané náklady na tuto akci jsou 1000 MDs tj. 13 800 000 KČ (vč. DPH). c) implementace APP cache – APP cache bude sloužit na podporu analytického modulu, bezodstávkového provozu ROS a k převzetí určité části publikačních služeb při velkém zatížení vlastní databáze ROS. Předpokládané náklady na tuto akci jsou 860 MDs tj. 12 500 000 KČ (vč. DPH) d) zlepšování kvality dat vedených v ROS – realizace širokého spektra aktivit vedoucích ke zvýšení kvality dat v ROS, větší kontrole správce nad údaji vedenými v ROS a rozšíření možností poskytování exportů z ROS. Konkrétně se bude jednat o doplnění možnosti zápisu speciálního PSČ k adresnímu kódu, filtrování změn na registrované IČO pro poskytování notifikací uživatelům ZR, zobrazování historických změn k IČO ve správcovské aplikaci, rozšíření exportů správcovské aplikace, výmaz a oprava záznamu v externím číselníku ROS, zpřístupnění výdeje údajů správci nebo úpravu testovacích dat na platné agendy a OVM. Předpokládané náklady na tuto akci jsou 200 MDs tj. 3 000 000 KČ (vč. DPH).
ROS – IAIS - 2020+

Gestor – Stav – Název záměru – Popis záměru
ROS-IAIS je ISVS, definovaný zákonem č. 111/2009 Sb. o základních registrech. Jde o centrální webové řešení, které poskytuje nástroj pro přidělení IČO, zápis osob i změn referenčních údajů do ROS u těch editorů ROS, kteří nemají vlastní informační systém pro vedení a zápis osob do ROS. Kromě toho přináší možnost získávat aktuální údaje ze základních registrů a další výhody, jako je například tištěných výstupů referenčních údajů osoby. Správcem ROS-IAIS je Český statistický úřad. Okruh uživatelů ROS-IAIS je poměrně rozsáhlý. Používají jej pracovníci profesních komor, vybraných ministerstev, ústředních, krajských a obecních úřadů a dalších orgánů veřejné moci. ROS-IAIS tak v současnosti využívá více než 2.000 orgánů veřejné moci. Technické řešení ROS-IAIS bylo připravováno v letech 2010–2012. V této době nebylo dostatek praktických informací o potřebách jednotlivých orgánů veřejné moci. Využívání ROS-IAIS je tak zejména u méně zdatných uživatelů vnímáno jako zbytečně komplikované a těžkopádné. V některých případech také uživatelé využívají funkcionalitu nesprávně nebo proces zápisu nedokončí, což může vést k problémům s aktuálností osob v ROS a vyšší kapacitní nároky na zajištění podpory ze strany správce. Také chybí větší kontrola kvality údajů zasílaných do ROS. Výše uvedené skutečnosti mají za následek, že uživatelé ROS-IAIS využívají pro svoji činnost data ze základních registrů jen velmi omezeně a spíše je získávají tradičními způsoby tedy přímo od subjektu údajů. Cílem projektu bude změna uživatelského rozhraní a rozšíření funkcionalit pro administraci a podporu aplikace tak, aby se zjednodušily a sjednotily postupy vedoucí k zápisu, opravě, odstranění nebo aktualizaci vedených osob, omezila variabilita stávající funkcionality, zajistilo automatické provedení aktualizací RUIAN na základě plánované úlohy a vytvořil průvodce na podporu práce méně zkušených uživatelů. Dále se předpokládá doplnění údajů ROS-IAIS o nově vedené referenční údaje ROS, úprava uživatelských manuálů ROS-IAIS a větší kontrola textových zápisů do ROS (mělo by se jednat výlučně o zahraniční adresy). Očekáváme, že výše uvedené úpravy zvýší motivaci uživatelů aktualizovat a využívat referenční údaje základních registrů a zároveň zvýší kvalitu dat vedených v ROS. Společně s tím budou uvolněny nemalé kapacity správce ROS-IAIS, které se v současnosti věnují podpoře uživatelů ROS-IAIS. Realizované změny budou zároveň představovat první krok pro zajištění budoucího využití ROS-IAIS při získávání nezbytných údajů ze základních registrů a z propojeného datového fondu pro činnost decentralizovaných agend veřejné správy zaměřených na evidenci vybraných fyzických a právnických osob.
SIS_0 Centrální autentizační bod
Vybudování centrálního autentizačního bodu pro externí uživatele aplikací ČSÚ zjednoduší situaci především respondentům se statistickou povinností. Tito uživatelé aplikací ČSÚ si budou moci zvolit způsob autentizace k aplikaci, který jim nejlépe vyhovuje. Odpadne nutnost lokální registrace do dané aplikace. Vedle zachování možnosti autentizace lokálním účtem aplikace (registr externích uživatelů ČSÚ) bude možné zvolit autentizaci prostřednictvím systému Datových schránek. Toto bude vhodná a pravděpodobně preferovaná metoda autentizace právnických osob, které byly obeslány zprávou o své statistické povinnosti prostřednictvím zprávy do Datové schránky. Výhodou tohoto způsobu autentizace je především odpadnutí procesu registrace uživatele. Další možností autentizace k aplikacím ČSÚ bude autentizace prostřednictvím Národní identitní autoritou (NIA). Toto může být vhodná alternativa pro přihlášení fyzické osoby, která vystupuje vůči právnické osobě se statistickou povinností jako zpracovatel zajišťující plnění této povinnosti. Nemusí se nutně jednat o pracovníka dané právnické osoby, může jít o smluvního dodavatele služeb. V případě tohoto druhu autentizace je nutné zajistit propojení takové fyzické osoby s příslušnou právnickou osobou. Pro autentizaci osob z jiných OVM pak lze použít služby JIP/KAAS.
FN u sv. Anny v Brně
A
Elektronizace zdr. dokumentace, FN u svaté Anny v Brně
Projekt schválený OHA v rámci výzev z ESIF.
Ministerstvo dopravy
A
Zpřístupnění informací o řidiči prostřednictvím Portálu občana
Zajištění dostupnosti dat z registru řidičů veřejnosti on-line formou. V první fázi publikace základního kontextu údajů o řidiči prostřednictvím portálu veřejné správy (Portál občana) v rozsahu identifikace osoby, řidičského průkazu a skupin řidičského oprávnění, stavu konta bodového hodnocení řidiče a informace o platnosti dokladů agendy řidičů. Ve druhé fázi publikace rozšířeného kontextu údajů, doplnění o výpis přestupků, podrobnosti bodového hodnocení či omezení řidičského oprávnění.
Ministerstvo kultury
A
Správa a evidence muzejních sbírek

Gestor – Stav – Název záměru – Popis záměru
Zprovoznění IS Správy a evidence muzejních sbírek zajišťující správu a evidenci sbírkových předmětů a podporující výkon agend veřejné správy
B
Rozšíření bezpečnostních produktů Checkpoint, infrastrukturní projekt MK
Projekt "Rozšíření bezpečnostních systémů checkpoint" je plánován v souvislosti se zvýšením bezpečnosti Ministerstva kultury, čímž reaguje na zjištění a doporučení ze strany NBÚ a metodických pokynů NÚKIB.
Zabezpečení digitalizace sbírek Technického Muzea Brno, MK
Pořízení skeneru pro digitalizaci výkresů, map a pozůstalostí a zpřístupnění tohoto kulturního dědictví badatelům a veřejnosti. Ochrana a zachování sbírkových předmětů.
Ministerstvo práce a sociálních věcí
A
Poskytování služeb při vydávání kvalifikovaných a komerčních certifikátů v resortu MPSV
Jednotlivým úředníkům vydávající správní rozhodnutí je zajišťován výdej a generování kvalifikovaných certifikátů dle nařízení eIDAS. Pro vzájemné budování důvěry na elektronickém trhu jsou a budou vydávány kvalifikované serverové certifikáty dle nařízení eIDAS (tzv. elektronické pečetě).
B
Pořízení softwarově definovaného DC a obnova systémových prostředků DC
Na konci roku 2022 bude plně funkční, operabilní softwarově definované datové centrum s nově zavedenými technologiemi, které umožní rychlou reakci na aktuální stav a dynamické přidělování datových zdrojů dle aktuální potřeby. Bude využita technologie aplikačních a datových kontejnerů, která umožní operativní škálovatelnost výkonu všech vrstev tak, aby nedocházelo k častému jevu z nasazování nových řešení v rámci eGovermentu České republiky a to přetížení informačních systémů a jejich infrastruktury při zahájení provozu.
Ministerstvo spravedlnosti
A
Hardware složek justice (skenery)
Nákup OCR zařízení pro převádění podání do digitální podoby se strojově čitelnou vrstvou. Součást projektu eISIR.
Justiční autentizační a autorizační služba (JAAS)
Cílem projektu je vybudovat univerzální centrální komponentu justiční autentizační a autorizační služby (dále jen „JAAS“), která bude zajišťovat jednotné místo pro autentizaci uživatelů pomocí všech relevantních metod (LDAP, JIP/KAAS, ISDS, NIA). Rezort ministerstva nyní využívá v rámci provozu svých interních informačních systémů proprietární způsoby autentizace. Jedná o generovaná přístupová hesla, napojení na LDAP, JIP/KAAS, využití ISDS či další způsoby. To způsobuje duplicity a nejednotné typy implementací v provozovaných systémech. Po vybudování řešení JAAS pak budou jednotlivé provozované systémy (aplikace) využívat standardizovaný způsob komunikace pouze s JAAS, čímž se zjednoduší architektura úřadu i jednotlivých aplikací, zároveň bude možné přidávat další relevantní autentizační metody jednotně pro celý resort bez nutnosti je separátně implementovat do jednotlivých aplikací. JAAS bude integrován s externími či interními poskytovateli identitních služeb. Typicky bude mezi JAAS a externím či interním poskytovatelem identitních služeb vytvořen tzv. vztah důvěry, který umožňuje akceptovat výsledek autentizace u zvoleného poskytovatele identitních služeb pro přístup do poskytovatelů služeb/aplikací v resortu justice. Systém je založen na krabicovém řešení postaveném na open source platformě Identity Server doplněné o registr subjektů a digitálních mandátů, který bude obsahovat informace o zmocnění či mandátech, které opravňují jeden subjekt jednat jménem jiného subjektu. Nově dodávaná komponenta tak zjednoduší autentizaci a autorizaci interních a externích uživatelů informačních systémů resortu justice do jednoho centrálního bodu, který umožní odstranit duplicity implementované v současných systémech a předejít jejich tvorbě v nových systémech. To přinese úspory v implementaci a údržbě IT systémů.
B
Budování kapacit kybernetické bezpečnosti

Gestor – Stav – Název záměru – Popis záměru
Předmětem projektu je zvýšení úrovně zabezpečení informačních systémů využívaných v rámci rezortu justice, které bude realizováno prostřednictvím systému detekce síťového provozu, IPS systému a Sandboxu. Implementací systému detekce síťového provozu dojde ke zkvalitnění pravidelného monitorování potenciálních hrozeb z vnější sítě internetu. Z důvodu plánovaného navýšení přenosové kapacity sítě je zároveň nezbytné rozšíření IPS systému tak, aby pokrýval celou kapacitu datové sítě rezortu. Nasazení Sandboxu povede ke zkvalitnění práce všech zaměstnanců rezortu, a to tím, že Sandbox sníží propustnost malware a nevyžádané pošty.
Ministerstvo vnitra
A
Evidence Národního archivního dědictví na Portálu Národního archivu ČR
Evidence NAD bude prostřednictvím IS PEvA II navázána na evidenci původců, evidenci archivů a dalších subjektů, které vedou základní evidenci NAD podle § 16 archivního zákona. Rovněž bude vytvořena vazba NAD na další funkce Národního portálu, a to zvláště v oblasti elektronického výběru archiválií a zveřejňovaných archivních pomůcek.
Kontinuální rozvoj DCeGOV, OKB MV
Tento projekt navazuje na předchozí projektové aktivity jednotlivých projektů „Dohledového centra eGovernmentu“. Vybudováním „DCeGOV“ bylo v oblasti centralizace bezpečnostního a provozního dohledu k implementaci převážné části zásad a požadavků vyplývajících ze zákona č. 181/2014 Sb. a pokrytí první části resortu MV službami centralizovaného monitoringu vybraných provozovaných informačních systémů. Realizací projektu dojde k vytvoření „IS DCeGOV“ a napojení dalšího portfolia informačních systémů v souladu s implementačním plánem projektu na Dohledové centrum se souběžnou implementací nových částí ICT infrastruktury provozovaného DCeGOV. Vytvoření „IS DCeGOV“ pro zajištění provozně-bezpečnostního dohledu a řízení bezpečnosti systémů v aktivním i pasivním módu s ohledem na požadavky zákona o kybernetické bezpečnosti. Napojení dalších IS rezortu MV na aktivní dohled. Nová verze systému Ambiente HoneyNet – nová verze systému reagující na nové kybernetické hrozby.
Koordinace rozšiřování počtu Service Providerů (SeP), připojených do NIA
Rozšiřování SeP v Národním identitním prostoru. Navazuje na podobný bod kontrolní pořadí=2306008 s textem: Plně implementovat služby kvalifikovaného systému dle zákona 250/2017 Sb. A to jak vnějších systémů, tak do vnitřních systémů
Právní úprava rozšíření funkcionalit RPP o údaje vedené doposud v IS o ISVS a IS DP
Jak informační systém o informačních systémech veřejné správy (IS o ISVS), tak informační systém o datových prvcích (IS DP) byly až doposud vedeny jako samostatné informační systémy veřejné správy. Z důvodů duplicity s architekturou základních registrů je dlouhodobým záměrem NAP převedení jejich funkcionalit pod univerzální referenční rozhraní, které je nyní reprezentováno Informačním systémem základních registrů ISZR a obecným referenčním rozhraním pro komunikaci tzv. eGSB/ISSS v rámci Centrálního místa služeb. Z výše uvedených důvodů je v obou případech třeba provést úpravu technické povahy a tyto samostatné ISVS převést do RPP.
RPP, rozvoj registru a jeho agendového informačního systému
Nové funkcionality: katalog životních událostí, úkonů na žádost, evidence adres výkonu agend, evidence veřejnoprávních smluv, Realizace Opendat RPP.
RPP, rozvoj, analýza datového modelu, analýza procesu plnění a užívání údajů
Je potřeba naplnit údaji nový ISoISVS, pokrývající ale všechny IS úřadů v jejich celém životním cyklu a v integraci nejenom na agendy a služby, ale i na všechny klíčové ekonomické a projektové centrální služby veřejné správy a jejich IS. Nutné přizpůsobit stávající údaje v RPP dle zákona 12/2020 Sb. tak aby byly datovou základnou k poskytovaným službám OVM
RPP, začlenění ISoISVS do RPP a další rozvoj
Je potřeba vybudovat nový ISoISVS, pokrývající ale všechny IS úřadů v jejich celém životním cyklu a v integraci nejenom na agendy a služby, ale i na všechny klíčové ekonomické a centrální služby veřejné správy a jejich IS.
B
Rozvoj nových digitálních služeb Centrálního místa služeb
Rozvoj nových digitálních služeb Centrálního místa služeb. Aplikační rozvoj nových digitálních služeb CMS. IROP 2021-27
Rozvoj ROB a souvisejících AIS

Gestor – Stav – Název záměru – Popis záměru
Předmětem tohoto záměru je realizace úprav: 1. V Registru obyvatel (ROB) zejména v důsledku přijetí zákona č. 12/2020 Sb. o právu na digitální služby, mezi které patří např. rozšíření okruhu evidovaných údajů, úprava lhůty pro výmaz záznamů údajů z tohoto registru, editace osob zemřelých od 1. 7. 2010 do 30. 6. 2016, realizace úprav navazujících IS apod. 2. Souvisejících s provozem agendových informačních systémů správních evidencí (AIS EOP a AIS ECD) a výrobního systému CDBP v důsledku přijatého zákona o právu na digitální služby a souvisejících zákonů, Nařízení EU 2019/1157 a zákona o občanských průkazech. 3. Související s provozem agendového informačního systému evidence obyvatel: a) Dopady legislativy do procesů zápisu údajů a využívání údajů prostřednictvím formulářů CzechPOINT, b) Digitalizace přihlašovacích lístků k trvalému pobytu. 4. V Registru obyvatel (ROB) a navazujících agendových informačních systémech v důsledku přijetí zákona č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci.
RPP, průběžná validace ohlášených agend s výstupy legislativního procesu
Dohledové centrum eGovernmentu
"Zajištění provozu a zvýšení dohledu nad systémy KII a VIS"
C
Metodická podpora zavedení DTM ČR
Výzkumný projekt na podporu zavedení DTM ČR, který bude financován z BETA2 (bude těsně navazovat na záměr Jednotný výměnný formát Digitální technické mapy (JVF DTM).
RPP, implementace dalších číselníků nebo katalogů, služeb, událostí, rolí
Tento záměr by měl sloužit k centrální správě číselníků, které jsou použity v RPP, např. pro katalog služeb událostí, situací, rolí apod., potřebných pro řízení běhu eGovernmentu a k implementaci legislativních změn v roce 2020 (změna zákona o bankách; DEPO II), přístupy SPUU k ZR, agendám, JIP/KAAS
Vysokorychlostní datová síť krajů a technologická centra krajů
Záměr byl navržen Asociací krajů ČR a týká se výstavby a rozvoje Vysokorychlostní datové sítě krajů a technologických center krajů. Je (údajně) v souladu s Memorandem o podpoře výstavby, rozvoje a využívání telekomunikačních datových sítí veřejné správy mezi Ministerstvem vnitra, Svazem měst a obcí ČR a Asociací krajů ČR.
Ministerstvo zahraničních věcí
A
Digitální transformace úřadu za účelem zvýšení kybernetické bezpečnosti a zlepšení poskytování služeb občanovi
Záměrem je transformované ICT resortu včetně kybernetické bezpečnosti, moderní architektury a plně digitalizované návazné agendy úřadu, včetně přívětivých a moderních on-line služeb. Program Transformace má dále za cíl zavedení moderního řízení IT prostřednictvím standardů např. ITIL, eGovernment standardů, rámce TOGAF, ZoKB, NAR/NAP a další.
Ministerstvo zemědělství
A
Vybudování přístupového bodu ke službám elektronické identifikace, MZe
Předmětem záměru je vybudování jednoho centrálního autentizačního prvku resortu Ministerstva zemědělství, poskytujícího interní autentizační služby a zprostředkovávajícího přístup k externím autentizačním službám, zejména NIA a JIP/KAAS. Centrální autentizační prvek zcela odstíní agendové informační systémy a aplikace resortu MZe od detailů autentizace. Cílový agendový systém či aplikace obdrží od centrálního prvku elektronické identifikace informace o identitě, bez ohledu na to, jaký poskytovatel identitních služeb byl pro autentizaci využit. Zda byl využit interní poskytovatel identitních služeb (LDAP/AD) či externí poskytovatelé, jako jsou NIA a JIP/KAAS. Díky vybudování jednotného centrálního přístupového bodu ke službám elektronické identifikace bude v jednotlivých agendových systémech a aplikacích resortu MZe velmi jednoduché implementovat podporu autentizace prostřednictvím NIA a JIP/KASS. Agendové systémy a aplikace budou napojeny na centrální autentizační prvek resortu a tím budou automaticky akceptovat identity pocházejících z prostoru všech integrovaných identitních služeb. Napojení všech agendových systémů a aplikací rezortu MZe na centrální autentizační prvek umožní okamžitě akceptovat identity JIP/KAAS pro přihlášení ke všem těmto systémům a aplikacím pro fyzické osoby v roli úředníka. Budoucí integrace jakékoli identitní služby již nebude mít na cílové agendové systémy a aplikace žádný dopad. Veškeré změny se v takovém případě odehrají čistě na straně centrálního autentizačního prvku a pro cílové systémy a aplikace budou zcela transparentní.
MV ČR – Policie ČR
B

Gestor – Stav – Název záměru – Popis záměru
Zajištění zvýšení kybernetické bezpečnosti Policie ČR
Cílem projektu je zajištění funkční, vysoce dostupné infrastruktury řešení bezpečnostního monitoringu SIEM. Součástí je posílení, rozšíření a zvýšení schopnosti detekce, identifikace a reakce na bezpečnostní události a incidenty v ICT. V rámci projektu dojde k pořízení centrální vysoce dostupné infrastruktury pro řízení sběru logů, detekci a vyhodnocení bezpečnostních událostí, modernizaci infrastruktury řešení SIEM tak, aby plnila požadavky kladné na monitoring kritické infrastruktury, zvýšení počtu napojených a monitorovaných informačních systémů o 5 na celkových 15.
C
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění
Cílem projektu je zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění
NAKIT
B
Zajištění kompetence bezpečného vývoje pro digitální systém státní správy
NAKIT se v rámci své působnosti dlouhodobě zabývá vývojem softwarových aplikací dle požadavku veřejné správy. V současné době existují v NAKIT dva směry vývoje aplikací: klasický vývoj a dynamicky se vyvíjející agilní vývoj. S rostoucími požadavky zákazníků a celkovým zaměřením eGovernmentu zejména na front-endovou oblast aplikací pro koncové uživatele se mění i význam jednotlivých aktivit a vývoj software se stává jednou z klíčových aktivit NAKIT. Dá se tak předpokládat, že oblast vývoje software v NAKIT i nadále poroste a tím poroste i potřeba celý proces vývoje zabezpečit a zajistit bezpečnost vyvinutého kódu. Jedním z požadavků veřejné správy je sdílení vytvořeného kódu některých aplikací dalším subjektům, případně jeho zveřejnění jako open source pro využití širokou komunitou vývojářů. V tomto případě ještě více roste potřeba bezpečně vyvíjet a mít jistotu, že vzniklý kód neobsahuje skryté bezpečnostní vady vzniklé vědomě nebo nevědomě. Z těchto důvodů a při vědomí rizik souvisejících s vývojem aplikací započaly na sekci Bezpečnost a za spolupráce oddělení vývoje aplikací a týmu Portálu občana práce na tvorbě metodiky bezpečného vývoje. Je nutné přistoupit k další etapě a tou je zavádění této metodiky do praxe a zajištění praktikování bezpečného vývoje. V rámci projektu budou realizovány investice do nákupu příslušných technologií a nástrojů pro zajištění bezpečného vývoje, a to jak z pohledu vlastních analytických nástrojů, tak i nástrojů ověřujících bezpečnost programového kódu.
Národní archiv
C
Národní digitální archiv III (NDA III)
Národní digitální archiv (NDA) je infrastruktura umožňující provést výběr digitálních archiválií a jejich trvalé bezpečné uložení a zároveň zpřístupnění oprávněným osobám. Národní archiv provozuje tuto infrastrukturu na základě zákonného zmocnění pro celou síť státních archivů v ČR. Součástí IS NDA je Národní archivní portál (NArP), který poskytuje dálkově služby NDA a slouží ke komunikaci s institucemi veřejné správy na straně jedné, a s veřejností na straně druhé. V rámci projektu IS NDA II, který byl financován z IROP došlo k rozšíření kapacity a k vylepšení funkcionalit včetně napojení na Dohledové centrum eGovernmentu (DCeGOV) MV. Projekt IS NDA III na něj naváže a umožní přípravu robustního řešení integrovatelného do stávající architektury eGovernmentu (např. Portálu veřejné správy). V rámci řešení bude zpracován nejprve "Projekt technologické obměny IS NDA", kde budou aktualizovány stávající požadavky na digitální archivaci (kyberbezpečnost, archivní legislativa, požadavky e-governmentu, nové typy dokumentů, používané formáty). Následovat bude zadání veřejné zakázky na dodavatele IS NDA III. Součástí projektu je pořízení a zprovoznění digitalizační linky pro převod analogových archiválií (papír, film, audiozáznamy) do digitální podoby.
Národní úřad pro kybernetickou a informační bezpečnost
A
Navyšování integrity sítí kritické informační infrastruktury
NÚKIB poskytuje metodickou i technickou podporu všem subjektům kritické informační infrastruktury. Je určeno více než 100 prvků kritické informační infrastruktury.
Podpora vzniku dalších pracovišť typu CERT a CSIRT v ČR
Vytvoření mechanismu spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti (pracoviště typu CERT a CSIRT) a posílení jejich stávajících struktur. Popsáno v Akčním plánu a Národní strategii kybernetické bezpečnosti České republiky na období let 2015–2020.
Poskytování služeb GovCERT veřejným institucím a provozovatelům strategicky významných sítí

Gestor – Stav – Název záměru – Popis záměru
Vládní CERT České republiky (GovCERT.CZ) kontinuálně poskytuje široké spektrum služeb veřejným institucím, subjektům kritické informační infrastruktury (KII), významných informačních systémů (VIS) a provozovatelům základní služby (PZS).
Splnění Akčního plánu kybernetické bezpečnosti 2015–2020
Splnění všech úkolů vyjmenovaných v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 schválila Vláda České republiky 25. května 2015, Akční plán je dlouhodobě realizován a pro vládu pravidelně jednou ročně vyhodnocován.
Školení zaměstnanců státní správy v oblasti kybernetické bezpečnosti
E-learningové kurzy kybernetické bezpečnosti pro vybrané cílové skupiny – úředníky a manažery kybernetické bezpečnosti.
Zajištění lepší a efektivnější spolupráce s GovCERT a jinými státními orgány.
Spolupráce kontinuálně prováděná a zlepšována. Zároveň je průběžně vyhodnocována v každoroční Zprávě o stavu kybernetické bezpečnosti ČR.
Zřízení nezávislého znaleckého a standardizačního centra (KII)
Centrum by umožnilo objektivně hodnotit bezpečnost jednotlivých prvků strategické informační infrastruktury.
B
Zajistit provoz národního koordinačního centra kybernetické bezpečnosti podle EU nařízení o centru kompetence
Kybernetickou bezpečnost považuje za jednu z priorit jak rámcový program EU pro výzkum a inovace Horizont Evropa, tak paralelní program Digitální Evropa zřizující síť center digitální inovace s cílem aplikovat nové technologie v praxi a uvést úspěšně na trh nové postupy nebo výrobky s důrazem na malé a střední podniky. Tyto a další programy zaměřené na kybernetickou bezpečnost by mělo podle návrhu nařízení EP a Rady [COM(2018) 630 final – 2018/0328 (COD)] nově provádět Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost („kompetenční centrum“) a jím řízená síť národních koordinačních center v jednotlivých členských státech („národní koordinační centra“). Národní koordinační centrum kybernetické bezpečnosti bude podle tohoto nařízení vykonávat NÚKIB, a mezi jeho hlavní úkoly bude patřit zejména podpora centrálního celoevropského kompetenčního centra při dosahování jeho cílů, posuzování žádostí potenciálních nových členů komunity kompetencí pro kybernetickou bezpečnost na národní úrovni, usnadňování účasti místního průmyslu a dalších hráčů na přeshraničních projektech, provádění osvěty a další. Zlepší se tak dostupnost a možnost čerpání EU prostředků především pro subjekty působící v oblasti výzkumu, vývoje a inovací kybernetické bezpečnosti.
Správa základních registrů
A
[P] Program – Základní registry 2.0

Gestor – Stav – Název záměru – Popis záměru
Program Základní registry 2.0 (ZR 2.0) vznikl na základě projednaného a schváleného Cílového konceptu ZR 2.0 a s tím související Operační strategie ZR 2.0 vládou ČR dne 10. 10. 2018 (č. usnesení 650). Program ZR 2.0 obsahuje projekty jednotlivých správců systémů ZR (tedy ROB, RPP, RÚIAN, ROS, ISZR a ORG) a dalších prioritních systémů (např. eGSB/ISSS), které reagují na 12 níže uvedených prioritních oblastí rozvoje ZR definovaných v Cílovém konceptu ZR 2.0. Jedná se o: 1) Zajištění bezodstávkového provozu ZR 2) Rozšíření množiny referenčních údajů vedených v ZR 3) Podpora interoperability v rámci EU (zohlednění role ZR ČR v rámci interoperabilní veřejné správy EU) 4) Zpřístupnění data a služeb prostřednictvím otevřených dat a služeb 5) Vedení historie údajů v ZR 6) Zavedení autoritativních údajů a rozvoj propojeného datového fondu 7) Obnova infrastruktury ZR/sdílené platformy 8) Optimalizace komunikační infrastruktury a datových center 9) Činnosti ke zlepšení spolupráce jednotlivých ZR 10) Dořešení evidence cizinců (EJFO) v ROB 11) Posílení kontroly ze strany správců registrů a vytvoření administrativních nástrojů pro správce ZR 12) Vybudování „interního testovacího“ a „vývojového“ prostředí ZR Význam a využití ZR bude v následujících letech dále růst, zejména s ohledem na: 1. Rozvoj propojeného datového fondu poskytující další zdroje údajů z klíčových oblastí výkonu VS (doprava, zdravotnictví, sociální služby apod.). 2. Rozvoj elektronické identifikace občanů, cizinců a zástupců právnických osob a dokončení portálu občana. 3. Využívání služeb ZR i ze strany soukromoprávních subjektů. Pro rozvoj digitálních služeb a růst produktivity hospodářství ČR je důležité, aby sdílené služby eGovernmentu (ZR, e-identifikace, datové schránky a další) mohly být využívány nejprve silně regulovanými podnikatelskými odvětvími (bankovnictví a pojišťovnictví, energetika, telekomunikace a vodárenství, atd.) a postupně i dalšími soukromoprávními subjekty.
B
Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti, kybernetická bezpečnost Správy základních registrů (SZR)
Cílem tohoto projektu je potřeba zvýšit odolnost a úroveň kybernetické bezpečnosti primárních a podpůrných aktiv informačních systémů SZR. Jeho realizace vychází primárně z návrhu opatření definovaných v dokumentu „Plán zvládáních rizik SZR“; interního auditu ISO 27001; recertifikačního auditu ISO 27001; provedených analýz rizik IS (případně další bezpečnostní dokumentace těchto systémů), které SZR provozuje nebo je jejich správcem a doporučeních NÚKIB týkajících se požadavků zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).
Národní certifikační autorita (NCA)

Gestor – Stav – Název záměru – Popis záměru
Předmětem projektu je vybudování Národní certifikační autority (dále taká „NCA“), zabezpečení jejího provozu a zajištění dalšího rozvoje. Vybudováním NCA vznikl systém podřízených certifikačních autorit pro vydávání: - kvalifikovaných certifikátů pro elektronický podpis, - kvalifikovaných elektronických časových razítek, - kvalifikovaných certifikátů pro elektronické pečetě. SZR splnila veškeré zákonné požadavky, které jsou na poskytovatele kvalifikovaných služeb kladeny a na základě správního rozhodnutí odboru eGovernmentu MVČR ze dne 30. 4. 2019 byla zapsána jako pátý subjekt v ČR na „Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru“. Vybudováním NCA se SZR stala kvalifikovaným poskytovatelem a správcem všech částí NCA a s tím související infrastruktury. Projekt je členěn na tyto fáze: Fáze 1 a fáze 2: 08/2018–03/2020 - Vytvoření primárně požadovaných služeb NCA a implementace s tím souvisejícího HW a SW v izolovaných sítích jednotlivých bezp. složek - Zavedení specializovaných funkcionalit pro správu NCA. - Vytvoření dokumentace systému, certifikačních politik apod. - Zajištění školení uživatelů NCA a operátorů RA - Vytvoření analýz rozvoje NCA Fáze 3: 03/2020-12/2020 - Vytvoření funkcionality pro vzdálené on-line poskytování služeb kvalifikovaných elektronických časových razítek a pečetí (fyzicky umístěné v prostředí SZR) - Pořízení dodatečného HW pro potřeby BS Fáze 4: 8/2020–7/2021 - Vydávání komerčních certifikátů Fáze 5: 2021+ - Vytvoření druhého stromu CA pro vydávání certifikátů s ECC technologií - Pořízení dodatečného HW pro potřeby BS - Vybudování CA pro vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek VS - Ověřování platnosti kvalifikovaných el. podpisů a pečetí
Rozvoj NIA – systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci
Systém plní požadavky zákona 250/2017 Sb. o elektronické identifikaci. IS se skládá ze základního federačního modulu – národního bodu – a přidružených komponent poskytujících vlastní proces elektronické identifikace a komunikaci s jednotlivými poskytovateli identit a poskytovateli služeb. Předmětem projektu je realizace změn na systému NIA, které souvisí především s – implementací změn vyplývajících ze zákona č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů a připravovaným návrhem zákona o změně zákonů souvisejících s další elektronizací postupů orgánů veřejné moci čj. MV-141013/LG-2018, sněmovní tisk 756 („DEPO“), - potřebou zajištění stabilního a bezpečného provozu tohoto systému.
SZR – ISZR, ISSS
Projekt se týká centrálně řízené a spravovaná části referenčního rozhraní propojeného datového fondu, která je tvořena těmito systémy (komponentami): - Informačním systémem základních registrů (dále jen „ISZR“), jehož součástí je i Formulářový agendový informační systém (dále jen „FAIS“), - Informačním systémem sdílené služby (dále jen „ISSS“). Jeho předmětem je implementace změn vyplývajících primárně ze zákona č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů, novelou ZoZR a novelou zákona č. 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, a připravovaným návrhem zákona o změně zákonů souvisejících s další elektronizací postupů orgánů veřejné moci čj. MV-141013/LG-2018, sněmovní tisk 756 („DEPO“).
ÚV – Úřad vlády
A
Revize agend dle RPP
Revize stávajících agend v RPP (A48, A611, A866, A868)