SEZNAM PLÁNOVANÝCH ZÁMĚRŮ PRO IROP 2021-2027 - AKTUALIZACE LISTOPAD 2024					
Název záměru	**Popis záměru**	**Předběžná doba realizace**	**Vazba na hlavní cíl IK ČR**	**Gesční úřad**	**Celk. výdaje [mil. Kč]**
Budování kapacit kybernetické bezpečnosti	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.	01.07.2021 - 31.12.2023	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	Ministerstvo spravedlnosti	33,88
Digitalizace pohřebnictví	V první etapě digitalizace všech důležitých dat z kremačních pecí, které mají wifi připojení na základě potřeby nouzového stavu vyhlášeného vládou ČR. V druhé etapě jde o digitalizaci agendy sociálních pohřbů, kterou zajišťují obce v přenesené působnosti v souladu s § 5 zákona č. 256/2001 Sb., o pohřebnictví a o změně některých zákonů ve znění pozdějších předpisů.	18.03.2021 - 31.12.2024	Cíl č. 1 – UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	Ministerstvo pro místní rozvoj	20
Elektronická matrika - IS eMatrika	Ministerstvo vnitra v 1. čtvrtletí 2019 zpracovalo Analytický materiál k přípravě projektu elektronické matriky, který zmapoval stávající výkon procesu matrik dle zákona č. 301/2006 Sb. a souběžně vedené elektronické verze záznamů odpovídající požadavkům směrnice MV ze dne 2. června 2005 č.j. VS-95/60/2-2005. Výkon agendy matrik v jednotlivých procesech byl na základě analýzy zhodnocen z pohledu možnosti elektronizace, při současném zvážení možných dopadů týkajících se ochrany a bezpečnosti osobních údajů, resp. kybernetické bezpečnosti. Analýza dále obsahuje doporučení směřující k možné optimalizaci výkonu agendy matrik, jelikož cílem není současný stav pouze překlopit do elektronických komunikačních kanálů. V návaznosti na zpracovaný analytický materiál byl ustaven Řídicí výbor pro přípravu projektu eMatrika, do něhož byli nominováni zástupci zainteresovaných odborů Ministerstva vnitra. Účelem zřízení řídicího výboru je koordinace přípravných prací a zkoumání možných řešení jednotlivých věcných a procesních problémů spojených s elektronizací agendy matriky a zavedením centrálního informačního systému eMatrika. V závěru roku 2019 byl zpracován materiál Věcný záměr projektu elektronické matriky, který shrnuje předpoklady pro nastavení IS eMatrika a vymezuje očekávané přínosy pro jednotlivé zainteresované strany. V návaznosti na Věcný záměr projektu byl v roce 2020 zpracován základní návrh architektonicko-technického řešení IS eMatrika. V roce 2021 byl zpracován návrh technického řešení IS eMatrika, jehož nedílnou součástí je i základní cenová kalkulace vybudování IS eMatrika a jeho uvedení do provozu.	01.01.2023 - 31.12.2027	Cíl č. 5 - EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo vnitra	365

Elektronická spisová služba resortu, komunikace s ISDS, ověřování elektronických prvků	- Původní elektronická spisová služba byla implementována jako podatelna a výpravna datových schránek. Funkcionalita byla rozšířena, nicméně dostatečně nenaplňuje požadavky eGovernmentu směřující ke zlepšení výkonu veřejné správy. Spisová služba je klíčovým prvkem pro zvýšení a sjednocení kvality, efektivity, dostupnosti a transparentnosti veřejné správy jak z pohledu její organizace a řízení, tak z pohledu jejich uživatelů. - Zavedení jmenného rejstříku - Realizace jediného místa pro ověřování el. podpisů, podpisů, pečetí a časových razítek (pro spis. službu a další napojené IS) - Řešit implementaci, migraci stávajících dat a následně rozvoj a údržbu.	01.01.2022 - 31.12.2026	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Český úřad zeměměřický a katastrální	80
Elektronizace úřadu práce	V rámci tohoto projektu chceme nastavit procesy vedoucí k zavedení HW i SW podpory digitalizace všech stávajících listinných dokumentů. Jedná se o dokumenty jak na vstupu do ÚP, tak na výstupu procesu ÚP, vedoucí k zefektivnění práce úředníků ÚP. Digitalizované a úředně ověřené dokumenty budou provázány se stávajícími agendovými systémy, spisovou službou, Jednotným portálovým řešením s možností aktivního vyhledávání v dokumentech dle stanovených kritérií.	18.03.2021 - 29.03.2024	Cíl č. 1 – UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	Úřad práce ČR	neuvedeno
Formulářový agendový informační systém (FAIS) ČÚZK	- Vybudování aplikačního rozhraní pro FAIS - Napojení rozhraní na systém elektronické identifikace (NIA) - Napojení na systém elektronické spisovny - Integrace cca 40 typů formulářů pro realizaci podání na zápis záznamu, poznámky nebo upozornění do katastru nemovitostí	01.01.2022 - 31.12.2025	Cíl č. 1 – UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	Český úřad zeměměřický a katastrální	20
Implementace Strategie rozvoje infrastruktury pro prostorové informace po roce 2020	Implementace Strategie rozvoje infrastruktury pro prostorové informace po roce 2020 (dále jen „GeoInfoStrategie+“) v letech 2022 - 2027, přispívající k naplňování cílů Digitálního Česka, zejména Informační koncepce ČR, v oblasti prostorových informací, a řešení specifických témat na podporu koordinovaného a efektivního rozvoje národní infrastruktury pro prostorové informace, zejména – nezbytné úpravy regulačního rámce, – definování garance prostorových dat a stanovení struktury garantovaných prostorových dat národního významu jako součásti propojeného datového fondu (PPDF), integrace prostorových dat do PPDF, – vybudování, správa a rozvoj potřebného prostředí (IS NIPI, NIPPI, IPMVP) pro vytvoření uživatelsky přívětivých služeb nad prostorovými daty ve vazbě na Katalog služeb VS včetně národního geoportálu, – vybudování uceleného systému vzdělávání pracovníků VS a podpora aplikovaného VaVaI v oblasti prostorových informací, podpora osvěty a propagace.	01.02.2022 - 31.12.2027	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo vnitra	570
Informační systém státních zastupitelství ELVIZ	Projekt „Elektronické vedení informací státního zastupitelství“ (ELVIZ) se zabývá vytvořením nového informačního systému pro elektronizaci dozorové činnosti a spisů státního zastupitelství.	1.1. 2022 - 31.12.2026	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo spravedlnosti	85

Modernizace informačních systémů pro podporu operačního řízení HZS ČR a příjmu tísňové komunikace	Dále je nutné v systému pro příjem tísňové komunikace reagovat na nové požadavky v souladu s legislativou ČR i EU. Proto byla v roce 2020 umožněna tísňová elektronická komunikace formou SMS osobám registrovaným u HZS. Po implementaci Kodexu o elektronických komunikacích bude umožněna komunikace formou SMS všem občanům ČR (realizováno ze státního rozp.). V souladu s tímto kodexem musí být v budoucnu umožněna také komunikace formou textu v reálném čase. V souvislosti s očekávaným nárůstem počtu tísňových volání a implementací technologií umožňujících textovou komunikaci lze očekávat i nárůst řešených událostí v operačním řízení u HZS ČR. V rámci programu budou realizovány následující projekty: 1. Vybudování aplikační části pro příjem tísňové komunikace: zajistit realizaci systému pro příjem tísňové komunikace v souvislosti s legislativními požadavky ČR i EU, implementovat do systému moderní technologie vícekanálové tísňové komunikace a využití umělé inteligence při příjmu tísňové komunikace, a dále zajistit dostatečnou průchodnost systému. 2. Modernizace informačního systému operačního řízení HZS ČR: zajistit zvýšenou průchodnost systému v souvislosti se zvýšeným počtem řešených mimořádných událostí, zajistit využití dat z médií s možností analýzy těchto dat s využitím moderních technologií umělé inteligence. 3. Modernizace Národního informačního systému integrovaného záchranného systému (NIS IZS): zajistit zvýšenou průchodnost a výkon, aby byl systém schopen přenést zvýšené množství informací, vytvořit rozhraní pro komunikaci s aplikacemi třetích stran, vybudovat testovací prostředí pro dostatečné testování jednotlivých informačních systémů i interoperability mezi nimi. 4. Modernizace systému Statistické sledování událostí: realizovat úpravy, aby byl systém schopen v souladu s požadavky HZS ČR zpracovávat a vyhodnocovat požadované informace o mimořádných událostech. 5. Vybudování systému cloudu pro HZS ČR: realizace cloudového řešení ve 3 lokalitách vč. stavebních úprav, pořízení HW vybavení pro realizaci cloudové platformy (síťové prvky, servery, diskové pole, technologie zálohování), migrace jednotlivých systémů, případné zvýšení kapacity a propustnosti sítě v lokalitách datových center, kontrola dostatečné síťové kapacity a propustnosti nutné pro využití technologie cloudu.	neuvedeno	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Hasičský záchranný sbor	750

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.	11.03.2021 - 31.12.2026	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	Národní archiv	262
Projekt Technická opatření kybernetické bezpečnosti resortu	Posílení fyzické bezpečnosti katastrálních úřadů a katastrálních pracovišť - Ochrana integrity komunikačních sítí (segmentace, firewall) - Dvojfázová autentifikace uživatelů - Monitorovací systém, SIEM - Implementace kryptografické ochrany - Implementace ochrany serverů před škodlivým kódem - Ochrana koncových zařízení před škodlivým kódem - Penetrační testy	01.04.2021 - 31.12.2024	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	Český úřad zeměměřický a katastrální	20
Přivětivé ISVS rezortu ŽP	Konsolidace elektronických služeb rezortu s legislativou e-governmentu.	01.07.2022 - 31.12.2026	Cíl č. 1 – UŽIVATELSKY PŘÍVĚTIVÉ A EFEKTIVNÍ „ON-LINE“ SLUŽBY PRO OBČANY A FIRMY	Ministerstvo životního prostředí	200

Varování a informování, komunikační podpora HZS ČR	1. Jednotný systém varování a informování: 1.1 Zavádění nových technických a technologických možností informování obyvatelstva. 2. Komunikační podpora HZS ČR: Pro řešení jsou navrhována následující opatření: 2.1 Modernizace a další rozvoj videokonferenčního systému HZS ČR. Cílem je zkvalitnit a zrychlit činnost HZS ČR tím, že umožní příslušníkům HZS ČR vytvářet potřebné virtuální konferenční teamy s možností využívat relevantní obrazové podklady, a to v místnostech i v terénu včetně možnosti komunikace s externími subjekty, to vše s možností záznamu i zpětného rozboru pro účely výcviku a ověřování reakcí na situace. 2.1.1 Vytvořit jednotné komplexní komunikační řešení v oblasti videokonference. 2.1.2 Obměnit zastaralé součásti videokonferenčního systému. 3. Modernizace analogové rádiové sítě HZS ČR: Rádiová síť HZS ČR je v současné době provozována na nejednotných technologiích značně rozdílného stáří, a u jednotlivých organizačních složek také HZS ČR ve vzájemně odlišných konfiguracích. Pro řešení je navrhováno následující opatření: 3.1 Modernizace analogové rádiové sítě HZS ČR: Budou pořízena a instalována zařízení pro obměnu, modernizaci a doplnění infrastrukturních prvků rádiové sítě, včetně prostředků a nástrojů pro jejich vzdálenou správu, dohled a propojování. Dále budou pořízena, z části instalována a zavedena do užívání koncová zařízení různých druhů vč. příslušenství (např. přenosné, mobilní a pevné radiostanice), která umožní budoucí přechod na digitální rádiový provoz. Řešena bude i nezbytná úprava souvisejících technologií.	neuvedeno	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo vnitra - Hasičský záchranný sbor	500
Vytvoření Geoportál 2 CENIA MŽP	Vytvoření centrálního informačního systému zajišťujícího jednotnou prezentaci prostorových dat ČR a informací veřejné správy včetně nástrojů pro jejich popis, vyhledání, validaci a poskytování dle aktuálních standardů v souladu s legislativními požadavky na prostorová data v ČR i EU.	01.11.2019 - 30.06.2025	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo životního prostředí	61,4
Program kybernetické bezpečnosti Správy železnic	Předmětem programu je naplnění zákonných požadavků kybernetické bezpečnosti prostřednictvím implementace pokročilých systémů pro ochranu sítě, jejího perimetru a uživatelů. Zejména se jedná o segmentaci sítě, revitalizaci a rozšíření ochrany perimetru, řízení přístupů, pořízení log managementu a nástrojů pro detekci událostí a ochrany před nimi. Síť správy železnic zajišťuje řízení a management provozování železniční dopravní cesty (provoz dráhy) a komplexí procesní fungování Správy železnic jakožto státního manažera železnic.	1. 2023 - 12. 2027	IKČR 3.08 Kybernetická bezpečnost	Správa železnic	543.4
Rozšíření LTP pro ostatní typy/formáty dokumentů vč. elektronického povinného výtisku	Cílem je rozšířit dlouhodobé úložiště digitálních dat LTP pro další typy dokumentů zejm. pro elektronický povinný výtisk k zajištění výkonu závazků plynoucích pro Národní knihovnu ČR z připravovaných novelizací zákona č. 257/2001 Sb., o knihovnách a podmínkách provozování veřejných knihovnických a informačních služeb (knihovní zákon), zákona č. 37/1995 Sb., o neperiodických publikacích, a zákona č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon) – tzv. Trojnovely.	2. 2022 - 12. 2025	IKČR 1.04 Digitální služby rezortů	Ministerstvo kultury	173.5

eLustrace II / Elektronická lustrace v evidenci vězněných osob pro oprávněné žadatele	Předmětem projektu je vývoj a implementace nového informačního systému Elektronické lustrace v evidenci vězněných osob pro oprávněné žadatele (dále jen eLustrace II) Nový IS má zajistit zautomatizování a zefektivnění vyřizování požadavků na výpisy údajů z evidence vězněných osob a nahradit již značně zastaralý systém eLustrace. Dodáním nového IS dojde k naplnění následujících cílů: • automatizování poskytování údajů prostřednictvím elektronizace procesů • efektivnění vyřizování žádostí o poskytnutí údajů z evidence vězněných osob • zkrácení lhůt pro vyřízení žádostí oprávněných subjektů • využití jednoznačné identifikace dotazujícího subjektu (OVM, PFO, PO, FO) • odbourání telefonických lustrací • umožnit FO získat pro jejich potřebu potvrzení o době omezení osobní svobody • umožnit FO získat pro jejich potřebu potvrzení o zaměstnání. • umožnit FO získat potvrzení plátce zdravotního a sociálního pojištění • umožnit FO získat potvrzení o zpracování osobních údajů správcem • rozšíření skupiny oprávněných žadatelů o FO a PO • rozšíření spektra poskytovaných údajů z evidencí Vězeňské služby oprávněným subjektům	1. 2023 - 12. 2025	IKČR 5.13	Vězeňská služba České republiky	5.0
Opatření pro kybernetickou bezpečnost v IPVZ	Vyřešení problémů v oblasti informační a kybernetické bezpečnosti, informačního systému IPVZ v oblasti fyzické, aplikační a systémové bezpečnosti. Mezi hlavní aktivity projektu patří činnosti spadající do kategorií: fyzická bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí a aplikační bezpečnost. Zvýšení bezpečnosti dat a informačních systémů, zvýšení spolehlivosti a dostupností dat a informačních systémů, automatizace a digitalizace vybraných procesů a zrychlení procesu řízení. • Architektura a integrace: řešení, které zajišťuje spolupráci jednotlivých prvků v rámci IPVZ ale i vazby na informační systémy partnerských organizací v rámci ekosystému IPVZ. Identifikace kybernetických bezpečnostních incidentů, včetně včasného varování všech bezpečnostních rolí. Nástroj pro ověřování identity uživatelů a řízení přístupových oprávnění .	1. 2021 - 12. 2022	IKČR 3.08	Institut postgraduálního vzdělávání ve zdravotnictví	19.0

Optimalizace agendových a provozních IS, zvýšení podpory výkonu agend včetně zavedení úplného elektronického oběhu dokumentů	Efektivní využití IS zajišťujících provoz agend úřadu a vnitřní chod úřadu, jejich optimalizaci a integraci tam, kde je to účelné – např. agendy akreditací, open data, administrace dotačních programů, řízení projektů, ale i např. personálních procesů či procesů finančních. Zvýšení podpory výkonu agend IT prostředky - zlepšování informační podpory interních procesů a provozních činností (tzv. back-office). Zavedení úplného elektronického oběhu dokumentů (digitalizace, bezpečné zálohování, archivace, snadný přístup k elektronickým dokumentům a jejich zveřejnění vč. metadat na centralizovaných úložištích) – naplnění povinností dle legislativy, úspora nákladů i efektivnější využití lidských zdrojů.	1 .2023 - 12. 2025	IKČR 6.02 Vnitřní digitalizace úřadů	Ministerstvo zdravotnictví	160.0
Inovace kritické infrastruktury ČHMÚ	Projekt zacílený na kybernetickou bezpečnost ČHMÚ (složeného ze 6 subprojektů) s předpokládaným spolufinancováním z Integrovaného regionálního operačního programu 2021-27 (IROP 21-27), v rámci Priority 1 – Zlepšení výkonu veřejné správy, Specifického cíle 1.1: Využívání přínosů digitalizace pro občany, podniky, výzkumné organizace a veřejné orgány v oblasti kybernetické bezpečnosti. Hlavním cílem projektu je zvýšit odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům.	9. 2022 - 12. 2025	IKČR 3.08 Kybernetická bezpečnost	Český hydrometeorologický ústav	328.0
Digitalizace konzulárních agend	Účelem tohoto projektového záměru je přispět k naplnění cílů MZV stanovených v Informační koncepci MZV a potřeb Konzulárního odboru. Tato koncepce ideově vychází z cílů a principů obsažených v Informační koncepci České republiky, která je součástí „Strategie koordinované a komplexní digitalizace České republiky – Digitální Česko“, současně vychází nejenom z cílů eGovernmentu, vedení MZV, ale i požadavků uživatelů služeb ICT. Cílem záměru je vytvoření systému uživatelsky přívětivých on-line služeb pro péči o občany v zahraničí založeného na principech, které umožní efektivně řídit a koordinovat tuto péči. Jedná se o portálové řešení v souladu s metodikou Odboru hlavního architekta eGovernmentu MV ČR. Součástí záměru je též vytvoření nástrojů pro manažerské a metodické řízení poskytování této péče, poskytování personalizovaných digitálních služeb občanům i cizincům s elektronickou identitou (NIA), a to v oblastech úkonových i informačních, vytvoření informačního systému na podporu zefektivnění poskytování konzulárních služeb a naplnění povinností MZV dle zákona o právu na digitální službu a DEPO v oblasti správních agend.	1. 2022 - 12. 2027	IKČR 1.04 Digitální služby rezortů	Ministerstvo zahraničních věcí	216.0

Provozní podpora a rozvoj IDM včetně úprav souvisejících systémů a procesů	Cílem projektu je zajištění provozní podpory a rozvoje stávajícího systému IAM MV (Identity & Access Management resortu Ministerstva vnitra České Republiky) pro správu uživatelských účtů resortu MV a jejich oprávnění v systémech resortu MV, cestou pořízení vývojových a technických služeb systému IAM resortu MVČR skládajícího se z následujících komponent: • Microsoft Synchronization Service 2016 SP2 • Uživatelského a administrátorského portálu EasyIDM 4.2 • SQL Server Reporting Services 2016 Systém zajišťuje správu více jak 72 tisíc uživatelských účtů z 49 organizací resortu MV a v současnosti podporuje provoz 20 aplikací resortu MV a je provozován v dvou prostředích resortu MV (testovacím a produkčním. Systém je informačně a funkčně propojen s dalšími součástmi informatické infrastruktury MV ČR, zejména se systémy EKIS (zdroj dat pro IAM MV) a adresářovými službami (IAM MV je zdrojem dat). Součástí projektu jsou proto nezbytné integrační práce na úrovni spolupracujících systémů, konfigurace datových objektů, nastavení atributů apod. za účelem dosažení konzistence informačního obsahu v rámci celého systémového řetězce. Současně s finalizací těchto prací se předpokládá i naplnění požadavků zásad kybernetické bezpečnosti v rámci provozního prostředí resortu MV, úprava souvisejících systémů ERP (EKIS/SAP), nástrojů pro segmentaci sítě a zejména zpracování provozní a procesní dokumentace k zajištění workflow pro využití předmětných nástrojů v rámci MV. Provozní podpora systému IAM MV spočívá v zajištění: • Řešení incidentů v požadované kvalitě (viz tabulka požadovaných SLA) • Podpora provozu a správy systému IAM druhé úrovně • Podpora při řešení požadavků koncových uživatelů systému IAM • Udržování aktuální provozní, administrátorské, uživatelské dokumentace a vytváření aktuálních školících prezentací a návodů v rozsahu 10 MD/ročně • Řešení odstraňování následků případné havárie HW, SW a systému IAM • Zajištění patchování a upgrade provozovaného HW, operačního SW a všech komponent systému IAM • Zajišťování školení administrátorů a uživatelů minimálně 4 x ročně v rozsahu:	11.2022 - 6. 2025	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	Ministerstvo vnitra	85.00

Komplexní ochrana informačních systémů VLS vůči kybernetickým hrozbám	Současný stav zabezpečení ICT infrastruktury je ne zcela vyhovující, což lze dokumentovat neshodou s některými požadavky zákona o kybernetické bezpečnosti 181/2014 Sb. SIS oddělení VLS si tuto situaci uvědomuje a identifikovalo následující rizikové oblasti, které zároveň popisují výchozí stav projektu: 1. Při přístupu zařízení do sítě LAN VLS ČR není ověřena jeho identita, neexistuje jistota, že komunikace probíhá opravdu s tím, za co se připojované zařízení vydává. 2. V současné době nejsou všechny objekty, kde jsou uložena aktivita ICT monitorovány kamerovým systémem. 3. Přihlašování uživatelů do informačních systémů VLS ČR probíhá ve většině případů ověřením vůči centrálnímu adresáři uživatelů MS Active Directory. Existují v provozu jednotky aplikací, které nemají implementované ověřování vůči externí DB. Tyto aplikace jsou postupně nahrazovány novými, které disponují integračním rozhraním pro účely jak ověřování uživatelů, tak i výměnu dat přes ESB. V současné době probíhá vyhodnocení VZ na implementaci systému na řízení identit (IDM). 4. V síti VLS ČR není žádný nástroj na monitorování datových toků. V současně době VLS ČR nemá možnost dohledat informace o aplikacích, které nejvíce vytěžují síť, o bezpečnostních anomáliích v síti, o komunikaci uživatelů vůči různým zdrojům a chybí i možnost uchovávat historii této komunikace. 5. Není implementována technologie DLP pro ochranu citlivých dat, a to jak na koncových stanicích, serverech nebo perimetru. 6. VLS ČR nedisponuje nástrojem pro klasifikaci nestrukturovaných dat a centrální řízení přístupu k těmto datům. 7. V rámci jednotlivých lokalit není vybudována strukturovaná kabeláž, nebo není v dostatečném objemu pro připojení zařízení, které nelze připojit bezdrátově (tiskárny, IP telefony, IP kamery, atd). 8. V rámci jednotlivých lokalit VLS ČR není vybudovaná technologie pro bezdrátový přístup (Wi- Fi) k informačním systémům.	28.02.2025	IKČR 3.08 Kybernetická bezpečnost	Vojenské lesy a statky, s.p.	38,17

FN Plzen- Nástroj pro identifikaci a hodnocení zdravotnických prostředků a dalších informačních aktiv nemocnice a nástroj pro řízení rizik	Zajištění technických bezpečnostních opatření § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti (§5 odst. 3 písm. a až l zákona č. 181/2014 Sb., o kybernetické bezpečnosti). Hlavním cílem projektu je zvýšení kybernetické bezpečnosti fakultní nemocnice Plzeň za pomoci vhodných nástrojů tvořených softwarem, hardwarem, bezpečnostní a provozní dokumentací a zefektivněním a automatizací současných procesů. Prostřednictvím projektu dojde ke zvýšení důvěrnosti, dostupnosti a integrity jak informací o pacientech a zaměstnancích, tak i k ochraně procesů nemocnice. Účelem je zajistit kompletní visibilitu a dynamický přehled nad všemi technickými aktivy v rozsahu ISMS, řídit jejich zranitelnosti a rizika. Cílem je získat přehled o nastavení a konkrétním umístění zdravotnických prostředků nemocnice, aktivních síťových prvků, serverů, koncových stanic a dalších OT a jiných technických aktiv. Dále zefektivnit a významně zrychlit proces sběru a vyhodnocování kybernetických bezpečnostních událostí a incidentů, kdy je požadován přístup externí služby SOC ktěmto nástrojům pro snížení zátěže a dotazů na zaměstnance FNP a současně kompletní informovanosti o prostřední FNP. Kromě toho je účelem projektu mitigace nálezu NUKIB zjištěné v auditní zprávě č. j. 2498/2021-NÚKIB-E/360 a implementace doporučení NUKIB na zvýšení zabezpečení prostředí, vhodnému řízení změn, aktiv, rizik, zranitelností a dalších oblastí požadovaných VyKB. Tyto nálezy nelze jiným ekonomicky a efektivně výhodným způsobem snížit na akceptovatelnou úroveň. Konkrétně se jedná o nálezy (blíže viz příloha č. 1 obsahující doslovné znění auditních nálezů): - ID 18 oblasti Řízení změn (Vysoká závažnost), - ID 32 oblasti Sběr a vyhodnocování KBU (Střední závažnost) - ID 36 oblasti Zdravotnická zařízení (Střední závažnost) - ID 37 oblasti Zdravotnická zařízení (Vysoká závažnost). Dále je cílem se přiblížit souladu s novou legislativou NIS 2.	31.12.2027	IKČR 3.08 Kybernetická bezpečnost	Ministerstvo zdravotnictví	43,53

FN Plzen - Zabezpečení přístupu do objektů a prostor FNP	Hlavním cílem projektu je zvýšení kybernetické bezpečnosti fakultní nemocnice Plzeň za pomoci vhodných nástrojů tvořených softwarem, hardwarem, bezpečnostní a provozní dokumentací. Prostřednictvím implementace projektu dojde ke zvýšení zabezpečení jednotlivých prostor žadatele, kdy prostřednictvím řízení vstupů bude zamezeno neoprávněnému přístupu k aktivům žadatele. Účelem je nahrazení stávajícího nevyhovujícího systému, který umožňuje velmi jednoduché kopírování přístupových karet novým systémem s vyšší bezpečností a připraveným na následný rozvoj minimálně po dobu udržitelnosti. Cílem tak je maximální eliminace hrozeb a zranitelností: Zranitelnosti: - nedostatečná úroveň šifrování, - Softwarové a hardwarové limity stávajícího systému Hrozby: - poškození nebo selhání technického anebo programového vybavení, - zneužití identity, - narušení fyzické bezpečnosti, - ztráta, odcizení nebo poškození aktiva, NÚKIB v rámci své auditní kontroly č.j.: 2498/2021-NÚKIB-EP360 identifikoval tyto nedostatky: - ID 25: oblast Fyzická bezpečnost - vysoká závažnost o VrámciprohlídkyserverovenDRS, která je umístěna v budově onkologie a RD3, která je umístěna v objektu komplement most auditní tým zjistil, že ani jedna serverovna nedisponuje protipožárním systémem a v obou je uloženo množství hořlavého materiálu (kartony, krabice, dřevěný a polstrovaný nábytek). Přístup do serveroven není zabezpečen kamerovým systémem a FNP nedisponuje evidencí přístupů, není tedy možné jednoznačně identifikovat, kdo do serveroven přistupuje a z jakého důvodu. Dále je cílem se přiblížit souladu s novou legislativou NIS 2.	31.12.2027	IKČR 3.08 Kybernetická bezpečnost	Ministerstvo zdravotnictví	52,46
Kybernetická bezpečnost IS ÚOOÚ	V rámci digitalizace agend uvnitř Úřadu pro ochranu osobních údajů bude nutné zajistit dostatečnou ochranu informačních systémů, zejména současného i do budoucna plánovaného IS ÚOOÚ. Projekt by měl zahrnovat jak ochranu samotnou (firewall, antivir) tak analytiku s kybernetickou bezpečností spojenou (SIEM, Logování). Jednotlivé komponenty zároveň musí běžet na novém HW.	01.12.2024	IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	Úřad pro ochranu osobních údajů	15
Technologická obnova a rozvoj analytických nástrojů ORG	IS ORG je jedním ze základních registrů a po více než 10 letech provozu vyžaduje zásadní technologickou obnovu. Primární je potřebou je nahradit HW, kterému v dohledné době skončí období podpory od výrobce. Sekundárním cílem je vytvořit v ORG modul, který bude schopen rozpoznat podezřelé jednání ve vztahu k ochraně osobních údajů, tedy například podezřelé nebo příliš časté požadavky na generování AIF ze strany OVM nebo SPUÚ.	01.12.2024	IKČR 5.09 Propojený datový fond (PPDF).	Úřad pro ochranu osobních údajů	40
Digitalizace agend ÚOOÚ	Digitalizace agend dle zákona o právu na digitální služby a dle plánu digitalizace. V případě ÚOOÚ se bude jednat primárně o agendu nevyžádaných obchodních sdělení, agendu ochrany osobních údajů ve smyslu kontrol a zpracování podnětů veřejnosti. Dále vytvoření nového interního IS ÚOOÚ, který bude obsahovat formuláře napojené na PPDF a možnost jejich vyplnění za využití elektronické identity.	31.12.2025	IKČR 1.04 Rozvoj on-line „front-office“ služeb jednotlivých rezortů.	Úřad pro ochranu osobních údajů	35

Jednotná datová základna	Jednotná datová základna představuje novou integrovanou datovou platformu v rámci resortu MPSV. Jejím cílem je agregovat data z primárních systémů a tato data transformovat do podoby konceptuálního datového modelu. Komponenta datové základny tak slouží k vzájemné datové integraci různých zdrojů dat a zabezpečení jejich jednotné interpretace v rámci celého resortu. Tato data jsou pak k dispozici odběratelům ve třech základních módech	30.06.2027	IKČR 1.04 Digitální služby rezortů	Ministerstvo práce a sociálních věcí	450
Transformace a centralizace klientského přístupu v AIS zaměstnanost	Současná aplikace pro Zaměstnanost je z historických důvodů decentralizovaná a provozovaná na nevyhovujících platformách. Nejdříve proběhne centralizace dat a následně nad těmito daty vývoj nových aplikací poskládaných do logických celků oblastí dle zákona o zaměstnanosti.	30.06.2027	IKČR 1.04 Digitální služby rezortů	Ministerstvo práce a sociálních věcí	400
Modernizace a rozšíření bezpečnostní infrastruktury Kanceláře veřejného ochránce práv	Předmětem realizace projektu je zajištění komplexní bezpečnosti všech služeb ICT, které využívají uživatelé Kanceláře veřejného ochránce práv (dále jen „KVOP“). V rámci projektu KVOP provede modifikaci architektury bezpečnostních řešení. Tam, kde to jde, chce KVOP opustit koncept řešení ve formě HW appliance (včetně dedikovaných fyzických serverů). Bezpečnostní aplikace chce převést na infrastrukturu virtuálních serverů, což umožní lepší řízení kapacit bezpečnostních služeb. Dalšími aktivitami jsou náhrady systémů, které jsou na konci své životnosti a rozšíření bezpečnostního řešení o nové systémy. Všechny změny umožní naplnit cíle projektu (zvýšit kybernetickou bezpečnost KVOP, zajistit bezpečné doručení IT služeb uživatelům KVOP a zvýšit úroveň zajištění kontinuity chodu úřadu) komplexním bezpečnostním monitoringem ICT prostředků, kontrolou činností registrovaných uživatelů, sledováním datového provozu informační infrastruktury, registrováním útoků na prostředky ICT a průběžným odhalováním případných interních a externích útočníků, atd. V cílovém stavu bude zajištěno pořízení a implementace dvou Netflow sond a HW kolektoru Netflow služby, hardware a standardní software pro nové virtuální servery (Servery, Diskové pole, Operační systémy, RDBMS). Jde o infrastrukturu nezbytnou pro modernizaci, respektive náhrad či pořízení nových bezpečnostních aplikací. Farma nových virtuálních serverů a „jejich mateřských serverů“ bude oddělena od ostatní provozní IT infrastruktury segmentací sítě. Dále bude zajištěno pořízení a implementace nových bezpečnostních aplikací, které nahradí stávající aplikace na konci své životnosti. Novými nebo nahrazenými aplikacemi bude Log Management, End point protection systém, Nástroj pro automatizaci incidenčních a Nástroj pro řízení kybernetické bezpečnosti. Stávající aplikace / systémy, budou virtualizovány (HW appliance budou migrovány na virtuální servery).	31.12.2025	IKČR 3.08 Kybernetická bezpečnost	Kancelář veřejného ochránce práv	22,76

Fakultní nemocnice Brno- Modernizace bezdrátové síťové infrastruktury	Z provedené analýzy rizik byly také identifikovány nejzávažnější zranitelnosti týkající se bezdrátové komunikační sítě: •Zranitelnost vnesená konstrukční vadou nebo úmyslnou slabinou v hardware •Zastaralost technických prostředků Ve schváleném Plánu zvládání rizik byla na tyto zranitelnosti reagování opatřením „Modernizace technických prostředků“ součástí kterého jsou a)Zastaralá infrastruktura poskytuje díky svým zranitelnostem zbytečný prostor pro možný útok či závadu, které mohou způsobit nedostupnost, kompromitaci nebo i ztrátu dat b)Realizace modernizace Wi-Fi sítí c)Pořízení serverovny pro CI – řešení v kontejneru Popis cílového stavu Hlavní cílem je zvýšení kybernetické bezpečnosti infrastruktury pro provoz informačních systémů nemocnice. Toho bude dosaženo realizací několika dílčích projektů zaměřených na řešení uvedených problémů. Tento konkrétní projekt zvyšuje bezpečnost bezdrátové přístupové sítě, jejíž prvky jsou užívány pro propojení medicínských přístrojů, pro personál nemocnice při výkonu práce a pro pacienty a návštěvníky. Každá z těchto skupin komunikací musí být vzájemně bezpečně izolovaná od ostatních a chráněna před případným únikem informací a napadením. K tomu bude sloužit modernizovaná síť bezdrátových přístupových bodů s centrálním řízením přístupu a provozu. Pro zvýšení bezpečnosti a správné fungování bezdrátové infrastruktury (WiFi) FN Brno bude provedena její modernizace náhradou, které bude podporovat segmentaci WiFi pomocí oddělených sítích (ESSID), dále bude využívat nejaktuálnějších bezpečných protokolů a bude podporovat ověřování uživatelů pomocí 802.1x. WiFi řešení umožní dále použití „sítě pro hosty“, kde bude možné izolovat jednotlivé připojené klienty, omezit přístupy do vnitřních sítí a omezit i rychlost spojení. Sítě pro hosty se uvažují i pro využití v rámci výzkumných projektů a spolupráce s Masarykovou universitou, tak aby externí subjekty nemohly ohrozit interní infrastrukturu nemocnice. Všechny přístupové body WiFi sítě budou připojeny na centrální správu řízené pomocí centrálních kontrolerů umožňujících se zastupovat a pracovat v bez výpadkovém režimu (HA).	31.12.2027	IKČR 3.08 Kybernetická bezpečnost	Ministerstvo zdravotnictví	49,19

Kybernetická bezpečnost ve Státním zdravotním ústavu Usti nad Labem	V rámci projektu budou realizovány následující součásti: - Nástroj NAC (Network Access Control), jedná se o nástroj pro ochranu přístupu do sítě, kdy dochází k identifikaci připojených zařízení před přístupem do sítě, jedná se o protokol a standard IEEE 802.1x, v rámci této části projektu budou dále pořízeny další aktivní prvky s cílem zajištění propustnosti vnitřní sítě na páteři 10Gbps - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. - Nástroj EDR pro ochranu koncových stanic. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného "se učení", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Zajištění nákupu dvou datových trezorů o celkovém objemu 90TB dat s cílem zajistit ochranu proti ransomware dlouhodobým uložením realizovaných záloh.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	37,35
Kybernetická bezpečnost PN Kosmonosy	V rámci projektu bude provedeno: - Fyzické zabezpečení serverů v rozsahu uzamykatelných racků, doplnění klimatizační jednotky, samostatná stojící UPS, propojení zařízení optickými spoji s dostatečnou kapacitou. - Provedení segmentace LAN. - Nákup páteřních aktivních prvků a distribučních aktivních prvků včetně nasazení NAC (Network Access Control), jedná se o nástroj pro ochranu přístupu do sítě, kdy dochází k identifikaci připojených zařízení před přístupem do sítě, jedná se o protokol a standard IEEE 802.1x. - Nástroj EDR pro ochranu koncových stanic. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného "se učení", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Provedení segmentace sítě, zavedení monitoringu sítě. - Vybudování záložní serverovny v rámci zvýšení dostupnosti provozovaných aktiv.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	24,97

Kybernetická bezpečnost ve Státním zdravotním ústavu	V rámci projektu je předpokládána realizace: - Kamerového systému, EZS, čteček a trezoru, dále je plánována rekonstrukce serverovny (chlazení, monitoring prostředí, stavba, nové rozvaděče (230 V) a UPS, hasicí systém). - Čtečky k tiskárnám v rácmi ochrany tištěných dokumentů. - Nákup firewallu, core switchů a switchů (celkem 25ks). - Rozšíření antiviru ESET o sandbox a modul šifrování, webu s https, nových PC a notebooků. - Provedení penetračních testů. - SW a monitoring sítě vč. implementace. - Druhé hvězdy optiky a offline zálohy včetně projektu."	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	37,35
FN Plzen -Zvýšení segmentace, dostupnosti a odolnosti počítačové sítě nemocnice	V rámci projektu je předpokládáno: - Komplexní zabezpečení sítě, které zahrne nákup nových páteřních aktivních prvků, doplnění přepínacích prvků na vybraná místě sítě, posílení konektivity v datovém centru na 10Gb, doplnění nezávislých přívodů elektrické energie k vybraným kritickým prvkům, doplnění licence monitoringu a správy prvků, doplnění licence pro ověřování přístupu do sítě v rámci IEEE 802.1x.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	46,65
FN Plzeň - Nástroj pro řízení technických zranitelností a privilegovaných přístupů FN Plzen -	Projekt zahrne následující součásti: - Technologie pro správu privilegovaných účtů Privileged Identity Management (PIM), nebo Privileged Access Management (PAM) v rozsahu kontroly nad účty externích dodavatelů, zajištění vysoké úrovně informační bezpečnosti, oddělení dohledu nad účty externích dodavatelů od provozu. - Vulnerability management nástroj pro zajištění monitoringu stavu jednotlivých prvků, činnnosti správců, reportingu, zhodnocení naplnění doporučené konfigurace výrobce aj.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	34,94
FN Pzeň -Zálohování a ochrana datové základy	V rámci projektu bude realizováno: - Řešení pro zajištění zálohování a ochranu datové základny. - Dvě provozované serverovny budou vybaveny automatickým zhášecím systémem.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	49,75
FN Ostrava - Zajištění bezpečného centrálního úložiště	V rámci projektu je požadována dodávka instalace celkem 3 diskových polí s následujícími rozdílnými funkcemi: - Tier 1 velikost 400 TB, bez SPOF, min 500 NAS, min 100 klonů LUN aj. - Tier 2 velikost 2PB, bez SPOF. - Rozšíření současného záohovacího pole o 900TB. - Pásková jednotka pro 400 slotů LTO9. - Nezbytné SW vybavení a související služby.	24.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	49,79

Fakultní nemocnice Hradec Králové- Zvýšení kybernetické bezpečnosti ve FN HK II.	V rámci projektu je předpokládána realizace: - Dodávka 2 ks firewallu v rámci soudobých funkcí včetně integrace VPN koncentrátoru, součástí řešení bude dále WAF včetně vícefktorové autentizace pro uživatele přistupující na webové portály. Součástí řešení je dále provedení vnitřní segmentace sítě. - Nástroj EDR pro ochranu koncových stanic i serverů. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic i serverů, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného ""se učení"", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Rozšíření SIEM Qradar.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50
Kybernetická bezpečnost Fakultní nemocnice Olomouc	- Pořízení a implementace centrálních routerů včetně firewallů pro zabezpečení, kontrolu a routign vnitřní sítě včetně kontroly provozu mezi segmenty. Řešení je realizováno v HA ve dvou různých lokalitách. - Zabezpečení analýzy komunikačního provozu v rozsahu IPS. - Technologie pro správu privilegovaných účtů Privileged User Management (PUM), nebo Privileged Access Management (PAM) v rozsahu kontroly nad účty externích dodavatelů, zajištění vysoké úrovně informační bezpečnosti, oddělení dohledu nad účty externích dodavatelů od provozu. - Nástroj EDR pro ochranu koncových stanic. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného ""se učení"", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Licence OS a virtualizace pro zajištění vysoké dostupnosti infrastruktury.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50

Zvýšení kybernetické bezpečnosti ve Fakultní nemocnici u sv. Anny v Brně	V rámci projektu budou realizována následující opatření: - Zvýšení fyzické bezpečnosti o 40 kamer rozmístěných na kritických místech pro přístup k provozované infrastruktura a dále monitoringu racku v serverovně a to jak z hleeiska bezpečnostního, tak provozních hodnot. - Implementace bezagentkého PAM řešení pro monitoring činnsoti správců pro všechny provozované platformy včetně konzole pro správu atp. - Vulnerability management nástroj pro zajištění monitoringu stavu jednotlivých prvků, činnnosti správců. - Pořízení a implementaci nástroje SIEM pro zajištění bezpečnostního dohledu. Rozsah požadovaných funkcí lze popsat jako event Management, agregace a pokročilá korelace, tj. korelace z více zdrojů, příjem a sběr logů a flow, centrální správu a reporting, a to včetně vlastních logů. - Pořízení datového úložiště pro více funkcí,příkladně uchování záloh, dále pro testování. - SASE portál pro řízení a konfiguraci provozovaných firewallových řešení.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50
Fakultní nemocnice Hradec Králové- Zvýšení kybernetické bezpečnosti ve FN HK III.	Projekt zahrnuje následující bezpečnostní opatření: - Mikrosegmentace virtuální serverů farmy. - VMware NSX Data Center Advanced per Processor a VMware vRealize Network Insight 6 Advanced. - Antivirový systém Carbon Black pro VMWARE a Linux. - Vytvoření odděleného testovacího prostředí. - Obměna core přepínačů pro zajištění fungování asi 500 VLAN. - Bezpečné úložiště pro zálohování obsahující HW a SW komponenty.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50
Fakultní nemocnice Hradec Králové-Zvýšení kybernetické bezpečnosti ve FN HK IV.	V rámci projektu je realizováno: - Opatření řeší doplnění stávajícího systému EZS a EPS o plynové stabilní hasicí zařízení (dále jen plynové GHZ) v místnostech serverů. - Nástroj NAC (Network Access Control), jedná se o nástroj pro ochranu přístupu do sítě, kdy dochází k identifikaci připojených zařízení před přístupem do sítě, jedná se o protokol a standard IEEE 802.1x a to pro nejuméně 10 000 zařízení. - V rámci výměny distribučních prvků bude povýšena rychlost připojení na 30 důležitých datových rozvaděčích (každý bude připojen 2 páry optiky) z 2x 1Gbps na 2x 10Gbps.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50

Psychiatrická nemocnice Horní Beřkovice-Zvýšení kybernetické bezpečnosti v Psychiatrické nemocnici Horní Beřkovice	V rámci projektu budo realizovány následující součásti: - Zajištěné výměny dveří do serverovny za protipožární, nákup a instalace kamerového a přístupového systému. - Dobudování single mode sítě mezi 5 budovami nemocnice. - Zajištění nástroje pro ověřování identit AD včetně jeho napojení na provozované IS (SSO). - Nástroj EDR pro ochranu koncových stanic i serverů. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic i serverů, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného ""se učení"", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. - Netflow sonda je dalším z opatření, které má zajistit bezpečnost v rámci komunikace uvnitř organizace. - Zajištěním vysoké dostupnosti využitím stávající výpočetní infrastruktury jako záložního pracoviště a nákupm primární infrastruktury (servery a pár L3 přepínačů). - Penetrační testování pro ověření stavu prostředí a provozovaných komponent.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	16,57
Psychiatrická léčebna Šternberk-Zvýšení zabezpečení informačního systému a síťové komunikace	V rámci projektu budo realizovány následující součásti: - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. Organizace se zaměřuje na uchovánílogů zejména o činnosti administrátorů. - Pořízení a implementace centrálního řešení IDM pro organizaci včetně dvoufaktorové autentizace, které bude použito v rácmi externích přístupů (VPN). - Zajištěním bezpečnosti sítě nákupem dvojice firewallů provozovaných v HA, dále provedením segmentace sítě a zajištěním implememntace IEEE 802.1x včetně netbytných SW a HW komponent. - Netflow sonda je dalším z opatření, které má zajistit bezpečnost v rámci komunikace uvnitř organizace. - Penetrační testování pro ověření stavu prostředí a provozovaných komponent. - V rámci zajištění dostupnosti bude dobudována záložní serverovna včetně nezbytného vybavení, nově zakoupené vybavení bude použito pro primární provoz a současné vybavení pro záložní site.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	34,45

Centrum kardiovaskulární a transplantační chirurgie Brno-Zvýšení kybernetické bezpečnosti CKTCH	V rámci projektu bude realizováno: - Vytvoření 2. datového centra pro vytvoření vysoké dostupnosti provozovaných systémů v georgeficky oddělené lokalitě. - Zálohovací systém a úložiště pro ukládání online záloh. - Rozšíření počtu serverů a navýšení kapacity úložiště formou hyper-konvergované infrastruktury za účelem umožnění rozdělení testovacího a produkčního prostředí informačních systémů. - Dokončení nasazení EDR řešení od společnosti BitDefender na koncových stanicích. - Dokončení nasazení systému pro správu privilegovaných účtů CyberArk. - Dokončení implementace systému SIEM QRadar. - Dokončeno nasazení VMware Horizon – řešení pro zabezpečení pracovních dat uživatelů.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50
Centrum kardiovaskulární a transplantační chirurgie Brno-Rozšíření kybernetické bezpečnosti CKTCH	V rámci projektu bude realizováno: - Vytvoření 3. datového centra pro ukládání OffLine záloh (vybavení datového centra vystrojeným rozvaděčem se zabezpečeným přístupem, zajištění licence pro zajištění offline záloh, pořízení serveru pro zajištění offline záloh, pořízení úložiště pro zajištění offline záloh). - Správa mobilních zařízení a aplikací na mobilních zařízeních (zajištění oddělení kontejnerů pracovních a osobních dat na mobilních zařízeních, zajištění správy mobilních zařízení a řízení aplikací na mobilních zařízeních). - Zabezpečení odloženého tisku - Mikrosegmentace sítě (zajištění oddělení zranitelných zařízení a MiddleWare od produkčních systémů na úrovni mikrosegmentace sítí a aplikací pořízením patřičných síťových prvků). - Ochrana dat a dokumentů pomocí technologie DLP (zajištění kategorizace dokumentů, monitoringu a restrikcí manipulace s dokumenty, zabránění úniku osobních dat zvláštní povahy, pořízení 2 ks loadbalancerů pro zajištění vysoké dostupnosti a balancování zátěže pro přístup k ISZS, pořízení 3 ks fyzických serverů pro virtualizaci hypervisorem VMware ESXi, zajištění systému pro řízení odloženého zabezpečeného tisku). - Operativní monitoring provozu (zajištění operativního monitoringu provozu informačních systémů včetně performance monitoringu informačních systémů a databází a bezpečnostního monitoringu). - Zajištění vysoké dostupnosti pro přístup k ISZS.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50

Zdravotní ústav se sídlem v Ostravě-Zvýšení kybernetické bezpečnosti Zdravotního ústavu se sídlem v Ostravě	V rámci projektu budou realizována následující opatření: - Nástroj EDR pro ochranu koncových stanic. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného "se učení", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Nástroj NAC (Network Access Control), jedná se o nástroj pro ochranu přístupu do sítě, kdy dochází k identifikaci připojených zařízení před přístupem do sítě, jedná se o protokol a standard IEEE 802.1x - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	14,74
Fakultní nemocnice Brno-Zvýšení kybernetické bezpečnosti FN Brno II	V rámci projektu se předpokládá realizovat: - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. - Technologie pro správu privilegovaných účtů Privileged Identity Management (PIM), nebo Privileged Access Management (PAM) v rozsahu kontroly nad účty externích dodavatelů, zajištění vysoké úrovně informační bezpečnosti, oddělení dohledu nad účty externích dodavatelů od provozu. - GRID vrstvená storage technologie pro 500TB, druhé zařízení pro deduplikaci do druhé lokality, řešení bude určeno pro zabezpečení zálohování.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	50
Fakultní nemocnice Brno-Zvýšení fyzické kybernetické bezpečnosti FN Brno	Zajištění dodání a instalace kontejnerové serverovny v rámci TIER III., 12 rackových stojanů při 5kW na rack, nepřímý freecooling, zhášení plynem, EZS, CCTV, všechny technologie uvnitř kontejneru.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	38,58
Rehabilitační ústav Hrabyně-Zvýšení úrovně bezpečnosti informačních aktiv Rehabilitačního ústavu Hrabyně	V rámci projektu budou realizována následující opatření: - Nákup 2 ks centrálních firewallů, firewall bude umístěn v po jednom kuse na každou z provozovaných lokalit (Hrabyně, Chuchelná) a v rámci firewallů bude rovněž vytvořen SSL tunel mezi lokalitami, funkce firewallu budou v rozsahu Sandboxing, IPS, Antimalware, Antibot, AV, SSL inspekce. - Nástroj NAC (Network Access Control), jedná se o nástroj pro ochranu přístupu do sítě, kdy dochází k identifikaci připojených zařízení před přístupem do sítě, jedná se o protokol a standard IEEE 802.1x - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. - Zajištění vysoké dostupnosti druhým diskovým polem zajištujícím deduplikaci dat, zajištěním serverové infrastruktury v rámci vysoké dostupnosti provozovaných aplikací. - Zajištění vysoké dostupnosti nákupem úložiště pro nestrukturovaná data (PACS).	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	49,61

Národní centrum ošetřovatelství a nelékařských zdravotnických oborů-NCO NZO Brno – Kybernetická bezpečnost	V rámci projektu budo realizovány následující součásti: - Zajištění rekonstrukce serverovny zajištěním systémů EKV a PTZS včetně připojení na PCO. - Nasazení EDR/XRD pokročilých technololgií na stanice, technologie zahrnuje nejen lokální monitoring koncového bodu, ale sdílení dat o případném útoku, automatizované a řízené reakce ve spolupráci aj. - Na perimetru bude nasazen IDS nástroj. - Budou rovněž obnoveny vybrané aktivní prvky.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	16
Státní léčebné lázně Janské Lázně, státní podnik- Rozšíření vysoké dostupnosti a zabezpečení integrity dat v SLL	V rámci projektu bude realizováno: - Nákup a instalace nových core switchů Aruba 6300. - Zakoupení a zafouknutí celkem 12 singlemode optických vláken do již připravených chrániček. - Zakoupeí nové výkonné klimatizační jednotky do servervony. - Zakoupení a instalace nových záložních zdrojů pro rozvaděče. - Nové SSD dskové pole včetně instalace. - Placená verze produktu Veeam Backup Essentials zakoupená pro všechny virtuální servery a počítače. - Vybavení serverovny PTZ kamerou, dálkovým ovládáním osvětlení a přístupovým systémem. - Nákup a instalace databázového serveru včetně licencí infarstrtukturních SW.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	5,46
Psychiatrická nemocnice Jihlava-Zvýšení kyberbezpečnosti a posílení ochrany dat v Psychiatrické nemocnici Jihlava	V rámci projektu budou realizovány následující součásti: - Obměna vybraných switchů z důvodů jejich zastaralosti a nedostupnosti patchů a podpory výrobce. - Pořízení 1 ks firewallu pro ochranu proti malware a využití funkcí Sandboxu.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	18,5
Psychiatrická nemocnice Havlíčkův Brod-Zvýšení úrovně kybernetické bezpečnosti v PNHB	V rámci projektu budou realizována následující opatření: - Nákup 2 ks centrálních firewallů, firewall bude umístěn v HA na jednu lokalitu funkce firewallu budou v rozsahu IPS, Antimalware, AV, SSL inspekce. - Log Management včetně implementace a nastavení tvoří základ pro centrální uchovávání a ochranu logů v rámci organizace. Kromě centralizace nástroj zajistí podporu při analýze logů a vybrané prvky pro jejich třídění a řazení. - Pro zajištění dostupnosti je plánován nákup druhého diskového pole pro zajištění deduplikace ve druhé lokalitě a dále nákup nové páskové knihovny. - Netflow sonda je dalším z opatření, které má zajistit bezpečnost v rámci komunikace uvnitř organizace. - Nákup core switchů a edge switchů v rámci obměny současných nevyhovujících prvků.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	10

Masarykův onkologický ústav-Posílení kybernetické bezpečnosti v Masarykově onkologickém ústavu	V rámci projektu budo realizovány následující součásti: - Nástroj EDR pro ochranu koncových stanic. Nástroje Endpoint Detection & Response posilují bezpečnost koncových stanic, jelikož kromě antivirové ochrany dále zajišťuje další formy ochrany na základě průběžného "se učení", zajišťuje rovněž možnosti aktivní ochrany stanice před útokem, či její izolace v případě, že útok probíhá na stanici, dynamicky ověřuje skryté hrozby, soubory před spuštěním atp. - Nákup 1 ks centrálního firewallu, funkce firewallu budou zřejmě v rozsahu IPS, Antimalware, AV, SSL inspekce.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	20
Státní zdravotní ústav-Kybernetická bezpečnost ve Státním zdravotním ústavu	V rámci projektu je předpokládána realizace: - Kamerového systému, EZS, čteček a trezoru, dále je plánována rekonstrukce serverovny (chlazení, monitoring prostředí, stavba, nové rozvaděče (230 V) a UPS, hasicí systém). - Čtečky k tiskárnám v rámci ochrany tištěných dokumentů. - Nákup firewallu, core switchů a switchů (celkem 25ks). - Rozšíření antiviru ESET o sandbox a modul šifrování, webu s https, nových PC a notebooků. - Provedení penetračních testů. - SW a monitoring sítě vč. implementace. - Druhé hvězdy optiky a offline zálohy včetně projektu.	31.12.2027	IK ČR 3.8 Podpora opatření kybernetické bezpečnosti	Ministerstvo zdravotnictví	37,35
Open data v resortu ŽP	Přínosy/cíle projektu: - posílení transparentnosti a zlepšení komunikace uvnitř rezortu ŽP i komunikace ve vztahu k cílovým skupinám (PO, FO podnikající, FO nepodnikající, odborná veřejnost, vysoké školství, apod.) - zlepšení vnímání rezortu ŽP díky zkvalitnění datových služeb - popularizace témat a tematických datových sad zpracovávaných rezortem ŽP, jejich následná jednotná metodická a technické publikace pro různé cílové skupiny za účelem podpory a rozvoje digitální ekonomiky založené na Open Data (datové sady umožní tvorbu nových aplikací a služeb vytvořených třetími stranami) - zvýšení odbornosti pracovníků rezortu ŽP - úspora nákladů cílových skupin na získání dat/informací - podpora opětovného použití dat Vytvoření technického řešení pro vytváření, plnění a publikaci rezortního lokálního katalogu otevřených dat. Řešení zajistí plnění národních zákonných povinností pro zveřejňování dat a publikaci HVDS pro oblast Životního prostředí. Řešení integruje různé datové zdroje a umožní zvýšení automatizace při přístupu k veřejným informacím. Řešení umožní automatizaci mezinárodního reportingu.	31.12.2025	IK ČR 3.2 Digitalizace dosud nedigitalizovaného obsahu	Ministerstvo životního prostředí	45

Sjednocení principů zajišťování kybernetické bezpečnosti infrastruktur národních parků s principy zajišťování kybernetické bezpečnosti MŽP.	Sjednocení principů zajišťování kybernetické bezpečnosti infrastruktur národních parků s principy zajišťování kybernetické bezpečnosti MŽP. Součástí záměru je nasazení technických opatření dle ZoKB v národních parcích, např. monitoring síťového provozu, IDM, SIEM, správa a ověřování identit, log management... Předpokládá se pořízení HW i SW a dohledových služeb, přičemž MŽP bude národní parky dál metodicky řídit.	1. 2023 - 12. 2024	IKČR 3.08 Kybernetická bezpečnost	Ministerstvo životního prostředí	97
Kvalitní zabezpečení sítí a ICT a s tím související ochrana digitalizátů Muzea umění Olomouc	Předmětem projektu je zajištění bezpečnosti IT infrastruktury a digitalizátů Muzea umění Olomouc, včetně související modernizace a rozšíření zastaralého HW a SW. Projekt bude mít kladný vliv na zvýšení efektivity procesů a dostupnosti poskytovaných služeb v rámci organizace. Hlavním cílem projektu je zajištění komplexní kybernetické bezpečnosti organizace. Digitální kopie a elektronické originály sbírkových předmětů zajišťují trvalé uchování kulturního dědictví a představují unikátní možnost prezentace badatelům a zájemcům z celého světa. Digitalizáty sbírek muzejní povahy jsou součástí klíčové skupiny dat, které tvoří kulturní dědictví státu. Data uložená v lokálních informačních systémech jsou linkována do centrálních registrů a vědeckých projektů národní úrovně (eSbirky, LidDat, Národní autority…) a zajišťují tak zpřístupnění a datovou integraci v rámci resortu kultury v celé republice. Ztráta dat představuje promarnění vysokých investic a způsobí obtížně nahraditelné škody, protože dojde k poškození datových struktur národních a mezinárodních (Europeana) projektů a opakovaná digitalizace předmětů bude mít negativní vliv na technický stav vlastních sbírek. Cílem kybernetických opatření je tedy zajistit ochranu stávajících dat. Manipulace a následné dlouhodobé uložení sbírek je pečlivě plánováno a opakované vyjmutí a vrácení z předmětů ze stabilního prostředí depozitářů je vysoce nežádoucí. Výpadek digitalizační linky / ztráta digitálních dat je tedy značnou komplikací a mimo přímých finančních škod obrovského rozsahu může přímo ovlivnit technický stav dotčených předmětů a znemožnit vědeckou práci mnoha odborníků a zájemců o kulturu v celé České republice i mimo ni.	01.02.2023 - 30.09.2025	IKČR 3.08 Kybernetická bezpečnost	Ministerstvo kultury	20

IS LOSOOS (Informační systém lustrace osob omezených na osobní svobodě).	Předmětem projektu je vývoj, implementace a provozování nového informačního systému Lustrace osob omezených na osobní svobodě (dále jen IS LOSOOS). IS LOSOOS má zajistit zautomatizování a zefektivnění vyřizování požadavků na poskytnutí údajů z evidence vězněných osob vedených Vězeňskou službou České republiky („Vězeňská služba“) a nahradit již značně zastaralý technicky nedostčující dosavadní systém eLustrace. Hlavním cílem projektu je vývoj, testování, nasazení a provoz nového IS LOSOOS, který bude základem přeměny Vězeňské služby na moderní, funkční a efektivně fungující instituci. Dodáním nového IS dojde k naplnění následujících cílů: • zefektivnění stávajícího způsobu vyřizování žádostí o poskytnutí údajů z evidencí Vězeňské služby, zejména: o snížení administrativní zátěže pro Vězeňskou službu o zautomatizování poskytování údajů v co největší míře prostřednictvím maximální elektronizace procesů o rozšíření spektra poskytovaných údajů z evidencí Vězeňské služby oprávněným subjektům o odbourání telefonických lustrací o typizace formy žádostí • rozšíření skupiny oprávněných žadatelů o FO a PO • využití jednoznačné identifikace dotazujícího se (oprávněného) subjektu (OVM, PFO, PO, FO) prostřednictvím justičního autentizačního a autorizačního systému (JAAS) a • vytvoření portálu pro schvalování přístupů do IS LOSOOS pro zvláštní skupiny žadatelů • umožnit FO získat o potvrzení o době a typu omezení osobní svobody o potvrzení o zaměstnání v době omezení osobní svobody a výši výdělku o potvrzení plátce zdravotního a sociálního pojištění o potvrzení pro účely procesu rehabilitace účastníků I, II. a III. odboje o potvrzení o zpracování osobních údajů správcem (včetně souvisejících práv) • snížení administrativní zátěže na straně žadatelů o poskytnutí údajů z evidence vězněných osob • zkrácení lhůt pro vyřízení žádostí oprávněných subjektů • využití uživatelsky přívětivého a očekávatelného prostředí a formulářů včetně možnosti učinění	01.01.2023 - 31.12.2025	IKČR 1.04 Digitální služby rezortů	Ministerstvo spravedlnosti	25

EnviHELP2 - Centrální podpora služeb pro klienty MŽP	EnviHELP2 je generační obměnou stávajícího helpdeskového nástroje. Bude rozcestníkem a nástrojem pro komplexní environmentální poradenství resortu ŽP. Bude koncentrovat např. metodický výklad legislativy, návody pro práci s AIS včetně integrace s těmito systémy, odpovídání dotazů/servisdesk, znalostní bázi aj.). Cílem je centralizace různých kanálů aktivního i reaktivního poradenství v resortu ŽP formou aplikačních služeb inteligentně využívajících aktuálně budované integrační platformy MŽP (CRŽP, EnviIAM, EnviÚEP, centrální servisDESK/CMDB), dostupné služby eGovernmentu (NIA, ISSS, ISZR, AIS-RPP/Katalog služeb/gov.cz, SDG) či rozhraní externích aplikací včetně napojení callcenter anebo servisdesku/ů IT služeb. Tyto nástroje budou propojovat know-how odborníků resortu ŽP s požadavky žadatelů o informace/rady. EnviHELP2 bude vycházet ze zkušeností dosluhujícího EnviHELP1 s tím, že občanům bude umožňovat dostávat aktuální a adresné informace v oblastech agend ŽP (např. ochrany přírody, ovzduší, vod a odpadového hospodářství), a to zejména prostřednictvím znalostní báze, tematického slovníku, řešených životních situací a parametrizovaných dotazů např. podle geografické oblasti zájmu, věku či jiných individuálních proměnných, zajišťovat podporu veřejnosti v oblasti životního prostředí. Ambicí a inovací by mohla být implementace AI/ML mechanismů pro co možná nejlépe personalizované poskytování relevantních informací, distribuci dotazů, vyhodnocování zpětné vazby/poptávky a dále možnosti univerzálního, plně logovaného, a otevřeného sdílení údajů na úrovni API (např. "trasování" stavu řešení, vyřizování systémy 3. stran, odkazování na podklady aj.). V oblasti legislativy bude tento záměr podporovat zejména aplikaci zákonů č. 123/1998 Sb. a č. 106/1999 Sb. v kontextu zákona č. 12/2020 Sb. Jinými slovy cílí na to, stát se moderním prostředkem pro efektivní komunikaci mezi státem a občany - tj. na uspokojení poptávky po garantovaných informacích. Zároveň bude nástrojem ke snížení administrativní zátěže spojené s touto agendou (na straně žadatelů i úředníků). Nemalý přínos se dá spatřovat i v tom, že prostřednictvím EnviHELPu 2 bude možné objektivně vyhodnocovat spokojenost s informační podporou a poskytováním služeb, které návazně na to povedou k (tlaku na) jejich zlepšování, tedy k větší transparentnosti služeb státu občanům.	01.07.2022 - 31,12,2025	IKČR 1.04 Digitální služby rezortů	Ministerstvo životního prostředí	70
ISSV - Informační systém správy voleb	Projekt má přinést nápravu neuspokojivého stavu v oblasti správy voleb, kde chybí systematické využití výpočetní techniky a nástrojů eGovernmentu. Seznamy voličů jsou vedeny jednotlivými obcemi – rozpadají se na více než 6 000 databází. Obce do nich sice čerpají data ze základních registrů, ale ve výsledku je nezřídka vedou papírově, nebo na lokálním disku. Podávání kandidátních listin nemá jednotná pravidla, která by umožnila jednoduché vytvoření registru kandidátů. Mezi podáním kandidátních listin, vytvořením oline databáze kandidátů a výrobou hlasovacích lístků dnes nastupuje ruční práce ČSÚ a registračních úřadů, které musejí např. v komunálních volbách zadat do systému data o desetitisících kandidátů. Neexistuje databáze členů okrskových volebních komisí. Stát nemá spolehlivé informace o obsazování téměř 15 000 komisí vykonávajících státní správu na úseku voleb. Pro starosty obcí je komunikace s volebními stranami mnohdy zbytečně komplikovaná. V době, kdy každý volič má možnost prokázat svoji identitu pomocí elektronického prostředku, existuje možnost sběru podpisů na podporu kandidatury v zásadě jen v listinné podobě.	01.07.2023 - 31.12.2026	IKČR 1.04 Digitální služby rezortů	Ministerstvo vnitra	200

Informační systém veřejné dopravy (ISVD)	Informační systém veřejné dopravy bude poskytovat data o jízdních řádech, přestupních vazbách, provozních nepravidelnostech atd., v rámci veřejné osobní (hromadné) dopravy, provozované na území České republiky: 1. po železniční dráze (celostátní, regionální, místní), 2. po městské dráze, tedy zejména tramvajové, trolejbusové a speciální, 3. veřejnou linkovou dopravou (včetně městské autobusové dopravy), 4. po lanové dráze (s výjimkou drah bez převažující přepravní funkce v rámci např. lyžařských areálů či zábavních center), 5. nad rámec současných právních povinností dále vnitrozemskou vodní dopravou. ISVD nemá ambice integrovat leteckou dopravu, protože je poskytována ve zcela jiném mezinárodním měřítku než dopravní služby pozemní. Předpokládá se, že předmětem ISVD budou i výlukové jízdní řády ve smyslu § 21a dopravního řádu drah a § 4 vyhlášky o jízdních řádech veřejné linkové dopravy, včetně jízdních řádů náhradní dopravy, budou-li k dispozici. Realizace ISVD je rozdělena na čtyři vzájemně časově i funkčně navazující části, označovaných jako subsystémy, a to: I. subsystém dopravní sítě, II. subsystém dopravní informace, III. subsystém správní agenda, IV. subsystém provoz systému. ISVD vzniká především z toho důvodu, že současný CIS JŘ je morálně a technicky zastaralý, nesplňuje požadavky Nařízení 2017/1926 a přizpůsobit jej pro potřeby zadavatele by bylo z hlediska funkčních požadavků a požadavků na kybernetickou bezpečnost informačního systému veřejné správy z hlediska principů 3E neodůvodnitelné. Předpokládá se, že rutinní provoz ISVD bude zahájen k 1. 2. 2025 a provoz CIS JŘ bude ukončen ke konci roku 2025, kdy bude plně nahrazen systémem novým, obsahující nejen informace o jízdních řádech, ale i provozní situaci ve veřejné dopravě, návaznostech spojů, nástroje potřebné pro schvalování jízdních řádů veřejné linkové dopravy a městských drah, kalkulaci tarifních závazků a další funkce, které jsou spojeny se současným systémem.	01.01.2023 - 31.12.2030	IKČR 5.13 Agendové infomační systémy	Ministerstvo dopravy	290

Digitalizace soudních agend eTrest, eSpráva a ePR	Hlavním cílem projektu je digitalizace soudního trestního řízení, v podobě vytvoření, zprovoznění a kompletního nasazení informačního systému (modulu) eTrest, digitalizace správní agendy soudní, v podobě vytvoření, zprovoznění a kompletního nasazení informačního systému (modulu) eSpráva, a modernizace agendy elektronického platebního rozkazu, v podobě vytvoření, zprovoznění a kompletního nasazení informačního systému (modulu) ePR. Všechny tyto systémy budou informačními systémy veřejné správy dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, a zároveň budou nadstavbovými agendovými moduly nad tzv. eSpisem, popsaném dále v dokumentu. Projekt je zaměřen na vytvoření 3 nových centrálních IS, které umožní kompletní digitalizaci dokumentů (s oprávněnými výjimkami), spisů a procesů v soustavě soudů v trestní agendě, správní agendě a agendě elektronického platebního rozkazu. Nové agendové IS eTrest, IS eSpráva a IS ePR budou vytvořeny na základě definovaných potřeb požadavků soudů a zaměstnanců soudů, které budou vymezeny v průběhu realizace projektu v rámci analýzy a návrhů příslušných řešení. Zejména bude požadován soulad systémů se současnými legislativními požadavky, jež jsou kladeny na ISVS, a jejich otevřenost pro možnost integrace nově požadovaných národních a evropských legislativních nároků. Nové IS budou založeny na moderních technologiích bez nutnosti zpětné komptability a nebudou tak zatíženy potřebou propojení s již existujícími moduly a aplikacemi. Všechny potřebné funkce a moduly systémů budou nově vytvořeny výhradně pro potřeby soudů a implementovány do nově vytvořených IS.	01.05.2023 - 30.06.2027	IKČR 3.03 Digitální archivy	Ministerstvo spravedlnosti	628,55

Elektronizace vězeňství a činností zaměstnanců VS ČR	Hlavní ambicí projektu je zefektivnění realizace práv a povinností vězněných osob, snížení administrativní zátěže zaměstnanců VS ČR ve vztahu k naplňování těchto práv a povinností, nahrazení a zrychlení manuálních postupů a procesů v oblasti činností VS ČR ve vztahu k povinnostem stanoveným zákony č. 555/1992 Sb., 169/1999 Sb., 293/1993 Sb., 129/2008 Sb. moderními technologiemi. Další ambicí tohoto projektu je zvýšení bezpečnosti při provádění uvedených činností. Investice v rámci projektu: 1. Informační panel pro vězněné osoby (žádosti o pohovory, plánování návštěv, hlášení k lékaři, podávání podnětů a stížností, přístup k právním předpisům a vnitřnímu řádu atp.) 2. Elektronizace evidence a identifikace (včetně biometrie) vězněných osob v prostorách věznice 3. Video hovory vězněných osob 4. E - learning 5. Bezpečnostní kamery na uniformách a oděvu zaměstnanců VS ČR 6. Elektronická písemná komunikace vězněných osob 7. Elektronizace přemísťování a umísťování vězněných osob 8. Elektronizace spisu vězněné osoby 9. Aktualizace Vězeňského informačního systému 10. Výdej stravy, nákupy ve vězeňských kantýnách Cílem projektu je snížení administrativního zatížení, výrazné zvýšení efektivnosti využívání pracovní doby a doby služby - zejména v oblasti odborných činností ve vztahu k zacházení s vězněnými osobami, eliminace selhání lidského faktoru v oblasti zajišťování práv a povinností vězněných osob, eliminace korupčních rizik, posílení bezpečnosti (např. eliminace průniku omamných a psychotropních látek do věznic).	01.04.2024 - 31.12.2030	IKČR 1.04 Digitální služby rezortů	Vězeňská služba České republiky	1500
Jednotný elektronický systém zdravotnické dokumentace Vězeňské služby České republiky	Cílem projektu je zavedení jednotné elektronické zdravotnické dokumentace ve Vězeňské službě České republiky a opuštění stávajícího vedení zdravotnické dokumentace výhradně v listinné formě, čímž dojde ke zvýšení bezpečnosti a ochrany informací zjištěných o pacientovi, snadnější kontinuita poskytování zdravotních služeb, potažmo kvality zdravotních služeb z důvodu rychlejšího získávání informací o zdravotním stavu a poskytnutých zdravotních službách, umožnění promptnější výměny informací mezi jednotlivými zdravotnickými zařízeními Vězeňské služby ČR i mimovězeňskými poskytovateli zdravotních služeb. Předmětem projektu je pořízení nového informačního systému pro vedení zdravotnické dokumentace v souladu s právními předpisy, zejména zákonem č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, a zákonem č. 325/2021 Sb., o elektronizaci zdravotnictví.	01.06.2023 - 30.06.2027	DES 4.09 Podpora budování specifické infrastruktury pro využití digitalizace, nových technologií a nových obchodních a organizačních modelů ve všech výše nevyjmenovaných (ostatních) sektorech.	Vězeňská služba České republiky	55
Systém elektronické evidence nízkoemisních plaket	Systém elektronické evidence nízkoemisních plaket pro ověřování oprávnění k povolení vjezdu vozidel do nízko emisních zón (NEZ) s vazbou na Jednotnou digitální bránu. Záměr je podmíněn vytvořením těchto zón. Předpokládané pokrytí nákladů by bylo ze státního rozpočtu - z kapitoly MŽP - 315.	01.05.2024 - 31.12.2026	IKČR 1.03 Univerzální obslužné kanály	Ministerstvo životního prostředí	12

PSIVÚ - Vývoj nejvhodnějšího softwarového řešení platformy pro sdílení a integraci veřejných údajů (PSIVÚ)	Cílem je vybudování platformy pro sdílení a integraci veřejných údajů (dále PSIVÚ) jako informačního systému veřejné správy, který je nedílnou součástí referenčního rozhraní veřejné správy a jehož prostřednictvím bude zajišťováno sdílení takových dat a služeb mezi informačními systémy veřejné správy, jejichž charakter neumožňuje sdílení pomocí současných možností informačního systému sdílené služby dle zákona č. 111/2009 Sb. Platforma bude vybudována tak, aby byla součástí globální architektury veřejného datového fondu a disponovala specifickými funkcionalitami: a) zajištění jednotlivým OVM a SPUÚ přístup ke garantovaným otevřeným datům ve VDF; b) dávkový přístup k obsahu jednoho nebo více údajů bez vazby na konkrétní subjekt práva, a to ke kompletnímu obsahu nebo k obsahu vázanému na jednu datovou položku (např. sdílení a výměna datových/informačních kontejnerů); c) sdílení prostorových informací a služeb, ale i neprostorových údajů; d) multikriteriální vyhledávání dat napříč jednotlivými zdroji dat; e) napojení na rozhraní EU dataspaců; f) umožnění zpoplatnění sdílených dat; Cílem vybudování platformy pro sdílení a integraci veřejných údajů je vytvořit prostředí, ve kterém bude možno orgánům veřejné moci na základě dostupných datových sad zprostředkovat tato data prostřednictvím definovaných služeb pro: - rozhodování v agendách veřejné správy (na základě poptávky jednotlivých agend rozborem právních předpisů) s ohledem na kompetence vymezené legislativou (v kontextu registru práv a povinností), - publikační místa pro veřejnost (národní geoportál, Czech POINT, datové schránky, webové služby). Platforma pro sdílení a integraci veřejných údajů vychází z konceptu sdílených služeb, bude součástí infrastruktury eGovernmentu České republiky a bude respektovat požadavky stanovené zákonem o kybernetické bezpečnosti.	26.09.2022 - 30.09.2025	Cíl č. 5 - Efektivní a centrálně koordinované ICT veřejné správy	DIA (Digitální informační agentura)	150

Psychiatrická nemocnice v Kroměříži - kyberbezpečnost	Projekt má za cíl vybudovat zabezpečené prostředí pro chod informačních systémů nemocnice s důrazem na ochranu integrity a důvěrnosti dat. Cílem je zavedení technických opatření, která budou zabezpečovat kybernetickou bezpečnosti základních a podpůrných informačních systémů podle požadavků ZKB a NIS2. Navazuje na cíle strategie Zdraví 2030 a její prioritní oblast 3.5 Digitalizace zdravotnictví pořízením robustní IT infrastruktury s vysokou úrovní kybernetické bezpečnosti. Projekt vybuduje bezpečné prostředí pro běh informačního systému nemocnice v prostředí se segmentovanou sítí s chráněným perimetrem. Nové aktivní prvky zajistí řízení komunikace v rámci komunikační sítě a jejího perimetru. Pomocí kryptografie zajistí důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií. Klíčovým faktorem bezpečnosti dat je ověření lékaře, či jiného zdravotnického pracovníka, a správa jeho identity, aby se k citlivým údajům o pacientovi dostal jen oprávněný personál. S tím souvisí i řízení přístupů a správa identit s nimi propojených v nemocnici tak, aby tyto informace nebo služby byly přístupné pouze povolaným osobám. Uživatelé budou moci přistupovat do systémů po dvoufaktorovém ověřování a jejich identita bude centrálně spravována. Současně však také bude sledována činnost privilegovaných účtů, kdy bude zavedena jejich centrální správa se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům včetně zajištění transparentního přihlášení. Rizikovost akcí jak u privilegovaných účtů, tak u běžných uživatelů, bude hodnocena a případné rizikové akce nebudou dovoleny. Dění ve vnitřní síti bude pečlivě monitorováno a kybernetické hrozby budou detekovány. Detekční systém zaznamenává události v rámci infrastruktury a dává je k dispozici odpovědným osobám (rolím) pro vyhodnocení dopadů činnosti a s upozorněními na události, či hrozby. Proto bude pořízen pokročilý nástroj pro analýzu síťového provozu, sledování výkonu, detekci hrozeb a rizik s hlubokou viditelností do sítě pro ochranu vnitřní sítě. Systém také zajistí blokování nežádoucí komunikace, ochranu všech aktiv v síti od koncových stanic přes mobilní zařízení až po servery. Zvláštní pozornost je věnována vhodným prvkům pro ochranu proti útoku zaměřeném na odepření služeb. Součástí jsou také	01.06.2023 - 31.05.2026	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	37,37

Zvýšení kybernetické bezpečnosti Městské nemocnice Čáslav	V rámci projetu bude realizováno: -zavedení systému řízení bezpečnosti informací a báze znalostí v oblasti kybernetické bezpečnosti včetně souvisejících procesů a dokumentace -pořízení de-duplikační jednotky pro zvýšení dostupnosti a celkové retence záloh -pořízení zálohovací páskové knihovny (předpoklad LTO09, WORM) -pořízení fyzického zálohovací serveru -pořízení zavedení dynamické segmentace (NAC, 802.11), pro bezpečný přístup k podnikové síti, zajistí bezpečný a oddělený přístup zaměstnanců a pacientů -pořízení a implementace nástroje pro řízení přístupů a identit, správa přístupu na kritické systémy infrastruktury (PIM/PAM) -pořízení a implementace NGFW (Next Generation FireWall), včetně WAF (Web Application Firewall) -pořízení a implementace systému RSD (bezpečný vzdálený přístup k aplikacím), zabezpečení přístupu ke koncovým zařízením pomocí dvou-faktorové autentizace uživatelů -pořízení a nasazení antivirového systému včetně EDR (Endpoint Detection and Response) -pořízení a implementace NDR (Network Detection & Response), SW nástroj pro síťovou detekci bezpečnostních hrozeb , vizualizace síťové komunikace, analýza síťového provozu, detekce škodlivých aktivit -pořízení a vybudování DR prostředí, HW+SW infrastruktura nezbytná pro běh pořízených bezpečnostních technologií a pro zajištění business continuity (servery, storage, síťové prvky, licence)	01.06.2024 - 31.05.2026	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	24,6

Zvýšení kybernetické bezpečnosti KHS Plzeň	KHS si klade za cíl zvýšit kybernetickou bezpečnost IT systémů, které používá ke své činnosti. KHS při své běžné činnosti zpracovává citlivá data obyvatel ČR a dále zaměstnanců KHS. Z uvedených důvodů by KHS v případě možné alokace finančních prostředků zakoupila a vyměnila za stávající switche za nové. Primárním cílem je inovace části počítačové sítě KHS Plzeňského kraje formou náhrady zastaralých a výrobcem již nepodporovaných přepínačů HP 1910-48G,1910-24G a 1810-8G a Mikrotik tak, aby byla zajištěna požadovaná dostupnost souvisejících služeb. Zastaralá a výrobcem nepodporovaná zařízení je nutno průběžně nahrazovat novými jednak proto, aby bylo možno zachovávat požadovanou dostupnost služeb počítačové sítě KHS Plzeňského kraje formou záruky výměny porouchaného zařízení novým v požadované době, a jednak i z bezpečnostních a provozních důvodů, neboť výrobcem nepodporovaná zařízení již nezaručují bezchybnou funkčnost, zejména protože neumožňují nezbytnou průběžnou aktualizaci svého programového vybavení odstraňujícího nalezené chyby. Potenciální alternativní možnost navýšení vlastních skladových zásob pro nahrazování porouchaných zařízení s uplynulou záruční lhůtou nepřipadá v tomto případě v úvahu, protože se jedná vesměs o výrobcem již nepodporovaná zařízení, pro která tedy neexistuje žádná možnost oprav možných chyb programového vybavení, tedy ani zajištění jejich správné funkčnosti. Předpoklad ceny cca 140.000,- Kč. Můžeme doložit podrobnosti. KHS by dále v rámci zvýšení kybernetické bezpečnosti chtěla zvýšit zabezpečení e-mailové komunikace. Nákup a nasazení Fortine FortiMail 200F. Zvýšení bezpečnosti e-mailové komunikace dle doporučení NÚKIBu. Jedná se o zařízení, které chrání emailový server proti spamu, malwaru a dalším e-mailovým hrozbám. S FortiMail lze zabránit tomu, aby byl náš systém i lidské zdroje zahlceni nevyžádanou poštou. V příchozím směru FortiMail efektivně blokuje spam a malware. Jeho filtr příchozí pošty zlikviduje spam a malware dříve, než dojde k odeslání zprávy, na úrovni TCP spojení. V odchozím směru kontroluje jednotlivé zprávy tak, aby nedošlo k zařazení našeho systému do blacklistu. FortiMail umožňuje dynamicky i staticky kontrolovat jednotlivé uživatele, vlivem čehož získáme kompletní kontrolu nad bezpečnostními politikami a uživateli. FortiMail poskytuje Identity – Based Encryption (IBE), kterou lze použít pro bezpečné doručení zpráv (metoda push nebo pull). Předpoklad ceny cca 110.000,- Kč. Můžeme doložit podrobnosti. Dále KHS předpokládá výdaje s nastavením systémů a potřebné dokumentace KHS tak, aby splňovala	01.08.2023 - 31.12.2023	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	1,25
Navýšení kybernetické bezpečnosti - Nemocnice Letovice	Nemocnice Letovice poskytuje občanům preventivní, léčebnou, diagnostickou, léčebně rehabilitační, ošetřovatelskou a paliativní péči. Aby bylo možné provozovat výše zmíněné činnosti, je potřeba zajistit konzistentní technologický systém s vysokou dostupností, zajištěním integrity a důvěrnosti. V příloze je k dispozici dokument "Studie proveditelnosti", která řeší celkově neuspokojivou situaci v oblasti ochrany IS/KS a sítě Nemocnice Letovice, příspěvkové organizace z pohledu standardů zákona o kybernetické bezpečnosti.	01.07.2023 - 30.06.2025	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	15,06

Kybernetická bezpečnost IS Nemocnice Kyjov, příspěvková organizace	Cílem tohoto projektu je zajistit soulad Nemocnice Kyjov jakožto provozovatele informačních a komunikačních systémů, jenž zpracovává, zprostředkuje a ukládá citlivé údaje, s požadavky Zákona o kybernetické bezpečnosti a s prováděcí vyhláškou. Technická opatření navrhovaná tímto projektem směřují právě k zajištění souladu s požadavky zákona, čímž přispějí k předcházení hrozbě kybernetických a bezpečnostních incidentů. Výsledkem projektu tedy bude posílení ochrany informačních a komunikačních systémů žadatele před kybernetickými útoky. V rámci projektu budou technická opatření zabezpečena v rámci 6 aktivit: Realizace nástroje pro řízení přístupu na síti, Implementace nástroje pro risk asset management, Skenner zranitelností a hardeningové politiky, Nástroj pro správu privilegovaných účtů, Nástroj pro sběr a korelaci událostí a logů – log management, Zajištění fyzické bezpečnosti datového centra. Podporovanou aktivitou této výzvy je kybernetická bezpečnost. Cíle projektu tuto aktivitu naplňují.	01.04.2022 - 30.06.2025	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Ministerstvo zdravotnictví	18,46
Centrála NÚKIB pro zajištění kybernetické bezpečnosti ČR - Černá Pole	Cíl projektu: Zajistit a zvýšit úroveň kybernetické bezpečnosti kritické informační infrastruktury NÚKIB v nově vybudované centrální lokalitě NÚKIB včetně vybudování a zabezpečení nového multifunkčního kybernetického polygonu NÚKIB. Kybernetickou bezpečnost KII NÚKIB je v plánu zajistit skrze nové nebo modernizované prvky kybernetické bezpečnosti zejména v oblasti fyzické bezpečnosti, bezpečnosti komunikačních sítí, správy a ověřování identit, řízení přístupových oprávnění, ochrany před škodlivým kódem, sběru a vyhodnocování kybernetických bezpečnostních událostí, kryptografických prostředků a zajišťování úrovně dostupnosti informací. Cíle bude dosaženo v rámci aktuálně připravované stavby nové centrální administrativní budovy NÚKIB v Brně "Černá Pole", která se stane novou hlavní lokalitou NÚKIB a tedy i centrálním místem zajištění kybernetické bezpečnosti v ČR. Potřebná úroveň doplnění a rozšíření zabezpečení KII v kontextu nové budovy a budoucích stavů zaměstnanců i infrastruktury efektivně navazuje na již realizované projekty a nákupy do dosavadních lokalit a infrastruktury NÚKIB. V případě dramatického prodloužení výstavby centrální budovy existuje náhradní varianta s omezeným rozsahem.	01.01.2021 - 31.12.2028	Cíl č. 3 - Rozvoj celkového prostředí podporujícího digitální technologie	Národní úřad pro kybernetickou a informační bezpečnost	439,72

Informační systém pro správu rezidenčních míst	Vznik nového informačního systému IPVZ pro správu a administraci rezidenčních míst s propojením na externí systémy Ministerstva financí (RIS ZED) a Ministerstva zdravotnictví (GINIS). Cílem je také budoucí propojení s resortním informačním systémem Administrátor. Informační systém pro správu rezidenčních míst (IS RM IPVZ) bude sloužit k efektivnímu řízení rezidenčních míst ve zdravotnictví, včetně všech nezbytných administrativních úkonů a integrace s dalšími relevantními systémy. Tento systém bude navržen tak, aby umožnil snadnou a bezpečnou správu dat, komunikaci s externími systémy a poskytoval uživatelům přehledné a aktuální informace. Realizace projektu Informačního systému pro správu rezidenčních míst přinese efektivní nástroj pro správu a administraci rezidenčních míst ve zdravotnictví, zlepší komunikaci a spolupráci mezi různými institucemi a zajistí bezpečné (NIS2) a transparentní prostředí pro příjemce dotací. Hlavní cíle nového informačního systému na správu RM - Evidence zájemců o dotace: Systémově odladěný nový proces schvalování a administrace jednotlivých žádostí o dotace. - Kompletní přenos dat a jejich administrace: Zajištění přenosu dat o financování akcí z IPVZ do ZED, včetně historických dat. - Aktualizace a dokumentace: Aktualizace stavů akcí a vkládání relevantních dokumentů do ZED. - Vyhotovování rozhodnutí: Příprava automatických šablon potřebných rozhodnutí. - Zvýšení informovanosti: Poskytnutí harmonogramů a automatizovaných e-mailových notifikací příjemcům dotací. - Konzultace a spolupráce: Zajištění konzultací a spolupráce mezi IPVZ a externími dodavateli systémů.	1.9.2024 - 31.12. 2025	IKČR 1.04 Digitální služby rezortů	Ministerstvo zdravotnictví	8,6
Položková banka s řízeným využitím AI	Položkové banky (nebo též "banky testových úloh") jsou software pro tvorbu, recenzi, ukládání a správu testových položek a testů. Zahrnují databázi a objektové úložiště. V položkové bance se spolu s testy a úlohami uchovávají i popisné informace – metadata včetně psychometrických charakteristik položek vypočtených z předchozích běhů testů, jichž lze využít jako zpětné vazby pro zlepšování při dalších běžích testů. Systém udržuje nejen informace o autorovi položky, o recenzentech, o výsledku recenze, o zařazení k tématu, ale i o chování položek v předchozích běžích testů, což umožňuje průběžné zkvalitňování testových položek a testů. AI funkcionality zahrnují automatizaci tvorby testových položek a prediktivní analýzu, což urychlí tvorbu testů a zajistí jejich vyšší kvalitu a relevanci. Dále umožňují personalizaci a adaptivní testování, zlepšují bezpečnost a efektivněji řídí lidské a technické zdroje při přípravě a administraci testů. Součástí projektu bude vytvoření zázemí IS a pro trénování AI.	1.8.2024 - 31.12.2026	IKČR 5.13 Agendové infomační systémy	Ministerstvo zdravotnictví	38