SEZNAM PLÁNOVANÝCH ZÁMĚRŮ PRO IROP 2021+ V RÁMCI AKTUALIZACE PROVÁDĚCÍHO DOKUMENTU (LISTOPAD 2022)					
Název záměru	**Popis záměru**	**Předběžná doba realizace**	**Vazba na hlavní cíl IK ČR**	**Gesční úřad**	**Celk. výdaje [mil. Kč]**
Modernizace a zvýšení dostupnosti datových center PČR	Cílem projektu je: • realizace zázemí a připravenosti prostor datových center odpovídajících v co nejvýší míře standardu TIER 3 a požadavkům na provozní a kybernetickou bezpečnost provozovaných systémů, zejména systémů kritické infrastruktury ČR a PČR • zvýšení míry redundance a odolnosti datových center • zvýšení míry operability provozu IS v případě výpadku některé z vybudovaných lokalit nebo v případě krizových nebo bezpečnostních opatření • posílení konektivity připojení datových center.	neuvedeno - 31.12.2024	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	250
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

Modernizace síťových prvků s cílem zajištění zvýšení dostupnosti komunikační infrastruktury a podpory přechodu na IP telefonii	Cílem projektu je zajištění a zefektivnění komunikace PČR prostřednictvím nové technologie umožňující snadné a bezpečné využití telekomunikační a videokomunikační technologie pro vzdálenou práci. Předmětem projektu je modernizace infrastruktury komunikačních a datových sítí, vybudování IP telefonní ústředny včetně pořízení potřebného SW a HW vybavení. Realizací projektu dojde ke zrychlení a zefektivnění komunikačních a datových sítí.	neuvedeno - 31.12.2024	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	MV ČR - Policie ČR	500
Pořízení systému správy a řízení přidělování SW licencí za účelem optimalizace SW licencí a produktů využívaných PČR	Cílem projektu je pořízení systému správy a řízení přidělování SW licencí za účelem optimalizace SW licencí a produktů využívaných PČR.	neuvedeno - 31.12.2026	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	60
Varování a informování, komunikační podpora HZS ČR	1. Jednotný systém varování a informování: V současné době existující jednotný systém varování a vyrozumění je technicky i morálně zastaralý a k varování jsou využívány elektrické koncové prvky varování, které nejsou schopny přenést verbální informaci. Pro řešení jsou navrhována následující opatření: 1.1 Zavádění nových technických a technologických možností informování obyvatelstva a celková modernizace jednotného systému varování a vyrozumění (řídící infrastruktura). Náhrada elektrických koncových prvků varování (rotačních sirén) sirénami elektronickými bude realizována v další fázi rozvoje systému, v návaznosti na disponibilní finanční zdroje. 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
Zajištění zvýšení bezpečnosti informačních systémů a dat PČR prostřednictvím efektivní správy identit a dynamického přidělování oprávnění	Systém pro řízení a správu životního cyklu identit včetně dynamického řízení přidělování oprávnění, pořízení nástroje IDM (identity management) a PAM (správa privilegovaných účtů), zahrnuje proces analýzy, implementace a integrace do prostředí PČR, bude řešena metodika související s životním cyklem identit.	neuvedeno - 31.12.2026	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	MV ČR - Policie ČR	60

Zajištění zvýšení dostupnosti, bezpečnosti a efektivní správy dokumentů zpracovávaných v rámci agend PČR	Cílem projektu je: • zvýšení udržitelnosti klíčových informačních systémů PČR v souvislosti s trestním řízením • zvýšení dostupnosti a bezpečnosti dokumentů zpracovávaných v rámci všech agend PČR • zvýšení výtěžnosti z dat zpracovávaných a získávaných v rámci trestního řízení • zvýšení efektivity práce a zkrácení času potřebného k rutinním činnostem v rámci analytických a operativních činností SKPV • zajištění bezpečného uchování a archivování dokumentů • zajištění eliminace následků v případě bezpečnostích a provozních incidentů (např. havárie úložiště, napadení ransomware) a zefektivnění a podpoření procesů předcházení a obnovení po havárii (Disaster Recovery - DR).	neuvedeno - 31.12.2024	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	400
Zajištění zvýšení dostupnosti, zodolnění a bezpečnosti provozní infrastruktury MBP s umožněním realizace dalších agend digitalizace organizace	Cílem projektu je zajištění bezproblémového provozu Mobilní bezpečné platformy Policie ČR (dále jen „MBP“) a některých souvisejících systémů a aplikací na další období prostřednictvím obměny technologické provozní infrastruktury MPB za účelem zvýšení její bezpečnosti a automatizované reakce na případné bezpečnostní nebo provozní incidenty.	neuvedeno - 31.12.2023	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	65
Zajištění zvýšení dostupnosti a bezpečnosti provozních dat informačních systémů PČR prostřednictvím jejich řízeného ukládání a zálohování	Cílem projektu je zajištění zvýšení úrovně dostupnosti, provozní a kybernetické bezpečnosti dat a informačních systémů PČR včetně systémů KII a VIS dle zákona o kybernetické bezpečnosti. Realizací projektu dojde k pořízení a implementaci diskových úložišť a technologie podpory zálohování a DR (disaster recovery) umožňující bezpečné a výkonné uchovávání záloh dat a informačních systémů PČR s podporou ochrany proti kybernetickým útokům typu ransomware a automatizovaných procesů obnovy a DR.	neuvedeno - 31.12.2023	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	MV ČR - Policie ČR	165
Zvýšení dostupnosti, bezpečnosti a modularity aplikační architektury MBP za účelem jejího dalšího rozvoje a realizace dalších agend digitalizace organizace	Cílem projektu je: • zvýšení bezpečnosti komunikačních a informačních systémů PČR využívaných v rámci mobilních zařízení • zvýšení a zefektivnění udžitelnosti a dostupnosti infrastruktury mobilních koncových zařízení pro policisty v přímém výkonu služby • zvýšení efektivity práce s mobilními koncovými zařízeními a využíváním platformy MBP • modernizace aplikační architektury umožňující další efektivní rozvoj a udržitelnost MBP • navýšení dostupnosti MBP.	neuvedeno - 31.12.2024	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	150
Zvýšení odolnosti organizace a připravenost na závažné situace vytvořením bezpečné platformy pro podporu vzdálené práce uživatelů a správu mobilních zařízení	Cílem projektu je zajištění zvýšení bezpečnosti a ochrany sítě a systémů PČR v případě vzdáleného přístupu uživatelů. V rámci projektu dojde k pořízení infrastruktury, technologie a vybavení umožňující zabezpečeným způsobem vzdálenou práci uživatelů a vzdálenou správu koncových zařízení. Ve svém důsledku dojde realizací projektu ke zvýšení akceschopnosti pracovníků PČR prostřednictvím umožnění plnohodnotné vzdálené práce nejen v době pandemie, bezpečnostních nebo nepředvídatelných situacích, ale i pro práci z domova za normální situace. Dále dojde k rozšíření platformy o poskytování specifických výkonných pracovních stanic pro analytické využití.	neuvedeno - 31.12.2023	Cíl č. 5 – EFEKTIVNÍ A CENTRÁLNĚ KOORDINOVANÉ ICT VEŘEJNÉ SPRÁVY	MV ČR - Policie ČR	200

Zvýšení zabezpečení informačních systémů HZS ČR z hlediska kybernetické bezpečnosti	HZS ČR provozuje informační systémy pro podporu operačního řízení, jejichž bezchybný provoz je klíčový pro vysílání sil a prostředků k mimořádné události a které obsahují citlivé údaje. Kybernetická bezpečnost těchto systémů není v současné době na dostatečné úrovni, vzhledem ke zvyšujícímu se počtu a závažnosti kybernetických hrozeb a útoků. Pro řešení uvedeného problémového okruhu jsou navržena následující opatření: • Zvýšení zabezpečení proti novým kybernetickým hrozbám (zavedení plošného monitoringu sítí v rámci subjektu, pokročilá logovací řešení, nasazení nové generace firewallů, zavedení řešení pro kontrolu privilegovaných přístupů). • Zvýšení zabezpečení proti novým zranitelnostem (zavedení perimetrových filtrů a bezpečnostních řešení podporujících cloudovou detekci hrozeb). • Zvýšení zabezpečení prostřednictvím aktualizací zastaralých softwarů (provedení upgradů na aktuální verze a zajištění SW podpory).	neuvedeno	Cíl č. 3 – ROZVOJ CELKOVÉHO PROSTŘEDÍ PODPORUJÍCÍHO DIGITÁLNÍ TECHNOLOGIE	Hasičský záchranný sbor	270
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 •zefektivnění 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

Vybudování univerzálního prostředí pro testování, provoz aplikací a poskytování služeb (UPAAS)	Předmětem projektu Univerzální prostředí aplikací a služeb (UPAAS) je zefektivnění stávajícího provozu platformy pro již provozovaní systémy a aplikace o rozšíření druhé lokality a tím zajištění legislativní potřeby provozu. Cílem je zajistit provoz a rozvoj „nezávislého“ datového centra, resp. multitenantního prostředí, které bude sloužit pro aplikace a systémy resortu MV. Provozované prostředí UPAAS je doposud provozované v lokalitě NDC Vápenka. Vybudování druhé lokality UPAAS II je výsledkem požadavků MVCR o umístění projektů které pro svůj provoz vyžadují georedundanci a současně i vize použití moderních technologií, které jsou v dnešní době brány již jako standardy u komerčních cloudových platforem včetně zajištění bezpečnostních požadavků MV ČR.	8. 2017 - ?	IKČR 5.03 Architektura veřejné správy	Ministerstvo vnitra	303.0
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
Mobilní aplikace státu	Jednotná mobilní aplikace, která sjednotí současné roztříštěné mini mobilní aplikace a přiblíží uživatelům stávající a budoucí digitální služby státu. Odůvodnění: Od 1.1.2023 se každému uživateli, který se ke státní digitální službě přihlásí pomocí elektronické identity, automaticky vytvoří datová schránka. Datová schránka je širokou veřejností vnímána jako „email pro komunikaci se státem“. Bohužel současné UX a pravidla fungování datových schránek jsou jiná a pro běžné uživatele zcela nezvyklá. Např. je velmi nezvyklé, že zprávy z datových schránek jsou smazány po 3 měsících od doručení. Nebo že není hezká a jednoduchá aplikace na komunikace s dat. schránkami v mobilních telefonech a některé jsou dokonce placené. Min. vnitra takovou aplikaci k lednu 2019 slibovalo, ale nakonec ze záměru sešlo. Základní funčnost aplikace: Funkcionality první verze mobilní aplikace: - Mobilní „email klient“ k datovým schránkám - Portál občana - Notifikace pro komunikaci s OVM - Životní situace – vyhledání a zobrazení - Mapa s adresami veřejnosprávních institucí včetně hledání a filtrování – obecní úřady, městské a krajské, CzechPointy, pracoviště ČSSZ, ÚP atd. V dalších verzí budou integrovány agendy a aplikace dalších resortů podle jejich postupné připravenosti.	7.2022 - 7. 2026	IKČR 1.02 Centrální informační místo	Úřad vlády ČR	90.74

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 •Zjišťování 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 budo 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	- 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	V rámci projektu jsou řešeny následující bezpečnostní oblasti: - 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 nejméně 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 dvěří 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
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.	45291	IKČR 3.08 Podpora opatření kybernetické bezpečnosti pro veřejnou správu.	NAKIT	10,89
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