| PLÁNOVANÉ ZÁMĚRY PRO IROP 2021+ KE SCHVÁLENÍ RVIS_DUBEN 2025 | | | | | |
|---|---|---|---|---|---|
| **Název záměru** | **Popis záměru** | **Předběžná doba realizace** | **Vazba na hlavní cíl IK ČR** | **Gesční úřad** | **Celk. výdaje [mil. Kč]** |
| Sušická nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 1 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>e) nástroj pro ochranu před škodlivým kódem<br>f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů<br>h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>l) bezpečnost průmyslových a řídicích systémů<br><br>Výstupem projektu budou následující technická opatření:<br>Hardeningové politiky<br>Nástroj pro řízení rizik<br>Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech<br>Systém pro správu a monitoring administrátorských přístupů<br>Systém pro ochranu klinické přístrojové techniky<br>Pokročilá AntiSpam ochrana<br>Systém pro vzdálený privilegovaný přístup<br>Interní firewall pro segmentaci | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 42,85 |

| | | | | | |
|---|---|---|---|---|---|
| Sušická nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 2 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace agregačních síťových zařízení<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 14,06 |

| | | | | | |
|---|---|---|---|---|---|
| Domažlická nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 1 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>e) nástroj pro ochranu před škodlivým kódem<br>f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů<br>h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>l) bezpečnost průmyslových a řídicích systémů<br><br>Výstupem projektu budou následující technická opatření:<br>Hardeningové politiky<br>Nástroj pro řízení rizik<br>Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech<br>Systém pro správu a monitoring administrátorských přístupů<br>Systém pro ochranu před moderním malwarem a Zero-day útoky<br>Systém pro ochranu klinické přístrojové techniky<br>Pokročilá AntiSpam ochrana<br>Systém pro vzdálený privilegovaný přístup<br>Interní firewall pro segmentaci | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 28,42 |

| | | | | | |
|---|---|---|---|---|---|
| Domažlická nemocnice- Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti- Projekt 2 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace na úrovni páteřních prvků<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Bezpečné úložiště pro PACS a NIS<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 37,75 |
| Horažďovická nemocnice- Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Zabezpečení komunikace agregačních síťových zařízení<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 13,51 |

| | | | | | |
|---|---|---|---|---|---|
| Klatovská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 1 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>e) nástroj pro ochranu před škodlivým kódem<br>f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br>l) bezpečnost průmyslových a řídicích systémů<br><br>Bezpečnostní politiky a další dokumentace, analýza rizik<br>Externí audit kybernetické bezpečnosti<br>Hardeningové politiky<br>Nástroj pro řízení aktiv<br>Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech<br>Systém pro správu a monitoring administrátorských přístupů<br>Systém pro ochranu klinické přístrojové techniky<br>Systém pro správu identit<br>Pokročilá AntiSpam ochrana<br>PKI<br>Systém pro vzdálený privilegovaný přístup | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 48,15 |

| | | | | | |
|---|---|---|---|---|---|
| Klatovská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti organizace-Projekt 2 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace na úrovni páteřních prvků<br>Zabezpečení komunikace agregačních síťových zařízení<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Řízení přístupu k datové síti<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Bezpečné úložiště pro PACS a NIS<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 46,77 |

| | | | | | |
|---|---|---|---|---|---|
| Rokycanská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 1 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>e) nástroj pro ochranu před škodlivým kódem<br>f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů<br>i) aplikační bezpečnost<br>l) bezpečnost průmyslových a řídicích systémů<br><br>Výstupem projektu budou následující technická opatření:<br>Hardeningové politiky<br>Nástroj pro řízení aktiv<br>Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech<br>Systém pro správu a monitoring administrátorských přístupů<br>Systém pro ochranu klinické přístrojové techniky<br>Pokročilá AntiSpam ochrana<br>Systém pro vzdálený privilegovaný přístup | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 15,6 |
| Rokycanská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 2 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace na úrovni páteřních prvků<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Bezpečné úložiště pro PACS a NIS<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 35,17 |

| | | | | | |
|---|---|---|---|---|---|
| Nemocnice Svatá Anna-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace agregačních síťových zařízení<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 13,32 |

| | | | | | |
|---|---|---|---|---|---|
| Stodská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 1 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>e) nástroj pro ochranu před škodlivým kódem<br>f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br>l) bezpečnost průmyslových a řídicích systémů<br><br>Výstupem projektu budou následující technická opatření:<br>Hardeningové politiky<br>Nástroj pro řízení aktiv<br>Zabezpečení proti škodlivému kódu a analýza aktivit na koncových stanicích a serverech<br>Systém pro správu a monitoring administrátorských přístupů<br>Systém pro ochranu před moderním malwarem a Zero-day útoky<br>Systém pro ochranu klinické přístrojové techniky<br>Pokročilá AntiSpam ochrana<br>PKI<br>Systém pro vzdálený privilegovaný přístup<br>Interní firewall pro segmentaci | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 42,85 |

| | | | | | |
|---|---|---|---|---|---|
| Stodská nemocnice-Modernizace ICT pro zvýšení úrovně kybernetické bezpečnosti-Projekt 2 | Hlavní aktivitou projektu je zabezpečení IS a KS v souladu se standardy kybernetické bezpečnosti podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a podle hlavy II, vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti.<br>Hlavní aktivity, které bude žadatele realizovat, jsou následující technická opatření:<br>Oblasti dle ZKB:<br>b) nástroj pro ochranu integrity komunikačních sítí<br>c) nástroj pro ověřování identity uživatelů<br>d) nástroj pro řízení přístupových oprávnění<br>g) nástroj pro detekci kybernetických bezpečnostních událostí<br>i) aplikační bezpečnost<br>j) kryptografické prostředky<br>k) nástroj pro zajišťování úrovně dostupnosti informací<br><br>Výstupem projektu budou následující technická opatření:<br>Zabezpečení komunikace na úrovni páteřních prvků<br>Zabezpečení komunikace agregačních síťových zařízení<br>Zabezpečení a monitoring přístupu koncových zařízení na úrovni datové sítě<br>Řízení a zabezpečení provozu bezdrátové sítě<br>Řízení přístupu k datové síti<br>Zvýšení dostupnosti a bezpečnosti výpočetního prostředí běhu informačních aktiv- zabezpečená výpočetní farma<br>Prostředí pro virtualizaci a ochranu informačních aktiv na koncových stanicích<br>Bezpečné úložiště pro PACS a NIS<br>Zajištění kontinuity systémů a služeb – zálohování dat | 30.04.2024-02.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo zdravotnictví | 46,93 |

| | | | | | |
|---|---|---|---|---|---|
| Zajištění kybernetické bezpečnosti infrastruktury ÚPV | Předmětem záměru je zvýšení kybernetické bezpečnosti informačních systémů veřejné správy (ISVS) a provozních informačních systémů (PIS) provozovaných ÚPV. ÚPV je správcem 3 významných ISVS a 6 PIS. Projekt je zaměřen na zvýšení kybernetické bezpečnosti celé infrastruktury s efektem na všechny uvedené systémy. ÚPV je držitelem certifikací dle ISO 27001, ISO 22301 a ISO 9001.<br>Záměrje rozdělen do tří projektů:<br>1.Zvýšení síťové bezpečnosti<br>V rámci projektu bude pořízen nový logmanagement server pro centrální ukládání logů ze všech dotčených systémů. Dále bude pořízena sonda pro monitorování síťového provozu pro detekci anomálií.<br>Budou pořízeny nástroje pro monitoring serverů a koncových stanic potřebných pro zřízení dohledového centra (Security operation center). Nad těmito nástroji bude zřízena služba dohledového centra pro zajištění analýzy a včasné reakce na bezpečnostní události a incidenty.<br>V rámci tohoto projektu budou dále pořízeny nové firewally včetně implementace web aplikačního firewallu.<br>2.Zajištění zálohování<br>V rámci projektu bude zajištěno pořízení dvou nových zálohovacích serverů včetně nástroje pro centrální zálohování veškerých dat zpracovávaných v dotčených systémech. Dále bude pořízeno diskové pole záložní lokality pro ukládání záloh v geograficky odlišné lokalitě.<br>3.Management identit<br>V rámci projektu bude pořízen hardware a zaveden centrální nástroj pro management identit včetně napojení na existující identitní systémy (AD, LDAP) a personální systém a zajištění podpory. Zavedením nástroje dojde k automatizaci přidělování a odebírání přístupových práv do informačních systémů na základě organizačního zařazení, zlepšení evidence přístupových oprávnění do externích systémů, centralizaci vydávání přístupových a podpisových certifikátů a zajištění pravidelné certifikace přístupových oprávnění. | 01.09.2023-30.06.2026 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Úřad průmyslového vlastnictví | 16,78 |
| Komunikační perimetr pro vnitřní služby IS MV | Předmětem projektu je bezpečný Perimetr MVČR jehož úkolem bude zprostředkovávat řízené a evidované propojení informačních systémů subjektů MV ČR a státní správy ke službám (aplikacím), které poskytují informační systémy jiných subjektů státní správy. Službou je v tomto kontextu uvažována služba určitého informačního systému (aplikace), který je připojen k Perimetru MVČR. Jedna aplikace službu poskytuje a jiné ji používají (konzumují).<br>1) Nákup příslušné technologie k vybudování bezpečnostního Perimetru MVČR<br>2) Vybudování bezpečnostního Perimetru MVČR – instalace, konfigurace, implementace a příprava pro napojení do dalších neveřejných sítí a samotné propojení<br><br>Předmětem projektu není správa (automatizace) služeb a zařízení sítě ITS | 01.09.2025-31.12.2027 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo vnitra | 100 |

| | | | | | |
|---|---|---|---|---|---|
| Národní dashboard | Identifikace problému:<br>“Co nezměříte, to neřídíte” je všeobecně známé pravidlo řízení organizace.<br><br>Informace o skutečném využívání jednotlivých Informačních systémů pro jednotlivé agendy nejsou známy. Dlouhodobě tyto informace chybí pro řízení investic, pro řízení nákladů (CAPEX, OPEX i lidských zdrojů), chybí pro řízení resortů a provozujících organizací.<br><br>Stejně tak nejsou měřeny žádné relevantní metriky samotných útvarů, které se na řízení digitalizace státu nyní i v budoucnu budou podílet.<br><br>Tento úkol popisuje kontext a základní metriky měřené v rámci jednotlivých digitálních služeb (Služba VS) a metriky popisující výkon útvarů podílejících se na řízení digitalizace státu. | 01.12.2024-30.06.2026 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Digitální a informační agentura | 38,89 |
| MPSV - Konsolidace fungování systému pro mezinárodní komunikaci | Hlavním cílem je kompletní převzetí kódů z EU a zajištění dalšího rozvoje elektronické výměny informací z oblasti sociálního pojištění na mezinárodní úrovni a další rozvoj sytému včetně legislativních změn v souladu s požadavky EU. | 01.05.2023-31.12.2025 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo práce a sociálních věcí | 66 |
| MPSV - Zajištění IT systému pro sekci rodinné politiky a sociálních služeb | Konsolidace a centralizace mapování potřeb cílových skupin, monitoring kvality poskytovaných služeb. | 01.05.2023-31.12.2025 | IKČR 6 Efektivní a pružný digitální úřad | Ministerstvo práce a sociálních věcí | 500 |
| IDM justice | Nasazení IDM na MSp, pilotní projekt eISIR, využití řešení CzechIDM dle již realizovaného projektu v rámci KS ČB. V první fázi bude řešeno pro KS, VS a NS, včetně MSp. Druhá vlna bude soustava SZ, okresní složky a NSS. | 01.07.2023-31.12.2026 | IKČR 3 Rozvoj celkového prostředí podporujícího digitální technologie | Ministerstvo spravedlnosti | 152 |
| Afinitní doména pro PK - interoperabilita zdravotnických záznamů | Cílem je vytvořit a provozovat AfD Pk včetně nezbytné HW infrastruktury pro interoperabilitu poskytovatelů zdravotních služeb na území Pardubického kraje. | -31.12.2026 | IKČR 5 Efektivní a centrálně koordinované ICT veřejné správy | Ministerstvo zdravotnictví | 90 |
| Dataset management system | Sběr a editace dat udržitelného rozvoje (UR) od příslušných gestorů datových sad přes jednotné rozhraní. Systém umožní kontrolovaně editovat, nebo zpracovávat data a metadata podle přiřazených rolí. Zveřejnění indikátorů UR jako otevřená data. Zpřístupnění dat pro mezinárodní organizace (Správcovské agentury). | 01.07.2023-31.12.2025 | IKČR 5 Efektivní a centrálně koordinované ICT veřejné správy | Ministerstvo životního prostředí | 14,52 |

| | | | | | |
|---|---|---|---|---|---|
| Nástroj na monitorování relevantních výsledků a výstupů VaV | Na to aby státní rezorty (včetně NÚKIB) mohli být účinnou autoritou v oblasti své působnosti, je nezbytné, aby měli přehled o veškerém aktuálním vývoji, který je v daných oblastech zaznamenán. To jim umožňuje poskytovat relevantní stanoviska a přijímat vhodná rozhodnutí, která následně formují celý národní ekosystém a všechny zainteresované aktéry. V dynamicky se rozvíjejících oblastech, jako jsou digitální technologie a kybernetická bezpečnost, však stát nemá dostatečné kapacity na to, aby měl přehled o všem co je (přinejmenším) z hlediska výzkumu a vývoje dosaženo a kam daná oblast směřuje. V tomto ohledu by byl pro potřeby OVVI užitečný nástroj s umělou inteligencí, který by byl schopen sledovat informace dostupné na internetu (v relevantních zdrojích) v reálném čase a informovat o nejaktuálnějších (a nejzásadnějších) výsledcích a trendech dosažených ve VaV KIB. Kromě krátké informace o odhalení významného objevu, trendu nebo výsledku výzkumu by nástroj mohl vytvořit také krátké shrnutí jeho podstaty (včetně nastavitelné úrovně technologického detailu v závislosti na preferencích čtenáře). Nástroj by OVVI umožnil mít aktuální přehled o tom jakých výsledků bylo ve VaV dosaženo (ja na národní tak mezinárodní úrovni) i jaké oblasti VaV považuje výzkumná komunita za nejproblémovější. Právě přehled o dění a potřebách výzkumné komunity je jedným z klíčových předpokladů pro úspěšné plnění role Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti, které na NÚKIB vzniklo na základě nařízení Evropského parlamentu a Rady EU 2021/887. Nástroj by byl ovšem využitelný nejen na OVVI ale multidisciplinárně a mezirezortně, v závislosti na přednastaveném typu informací, které by měl nástroj vyhledávat a zpracovávat. | 01.01.2025-31.12.2026 | IKČR 6 Efektivní a pružný digitální úřad | Národní úřad pro kybernetickou a informační bezpečnost | 5 |
| Automatizovaný koordinátor online meetingů | Univerzální nástroj využitelný napříč státní správou určený ke zjednodušení a zefektivnění online schůzek, jejichž počet neustále roste. Nástroj by se primárně zaměřil na přepis řeči do textu s detekcí klíčových informací (např. podle zadaného tématu schůzky) a automatické generování zápisu. Nástroj by ukládal a evidoval zápisy ve složkách podle jejich obsahu a zároveň by je automaticky nabízel k nahlédnutí před dalšími schůzkami na stejné téma (propojení s kalendářem). Současně by nástroj mohl obsah schůzek redukovat na bullet pointy, zvýrazňovat otázky nebo v případě delších schůzek formulovat manažerská shrnutí. Doplnkově by nástroj mohl zachytávat také obraz a zvuk, či automaticky překládat zápisy do jiných jazyků. Další úrovní by mohlo být automatické plánování navazujících schůzek v případě, že se na tom zástupci jednajících stran usnesli. | 01.01.2025-31.12.2026 | IKČR 6 Efektivní a pružný digitální úřad | Národní úřad pro kybernetickou a informační bezpečnost | 2 |
| "Grammarly" pro spisovou službu | Jazykový model zaměřený na gramatickou korekci textů v českém jazyce (a úřadovém žargonu). Z hlediska využití AI by mohl kromě kontroly gramatiky (primární účel) samostatně generovat některé typy dokumentů (např. Letter of Support, Letter of Intent apod.), dle předloženého vzoru (obsah by se měnil na základě požadavku např. vložením zadávací dokumentace k výzkumnému projektu, jenž žádá NÚKIB o podporu skrze Letter of Support). Nástroj by ideálně měl představovat modul pro spisovou službu, aby byl využitelný přímo v ní. | 01.01.2025-31.12.2026 | IKČR 6 Efektivní a pružný digitální úřad | Národní úřad pro kybernetickou a informační bezpečnost | 0,7 |

| | | | | | |
|---|---|---|---|---|---|
| Vybudování jádra sítě státního virtuálního operátora pro kritickou komunikaci (SVOP-Jádro) | Předmětem projektu “SVOP-Jádro” je vybudování klíčové infrastruktury jádra sítě LTE/5G umožňujícího realizaci dlouhodobě udržitelného řešení poskytujícího bezpečné mobilní vysokorychlostní datové a hlasové služby umožňující přístup ke kritickým aplikacím pro složky IZS a subjekty krizového řízení.<br>Řešení bude mít cílovou podobu Státního virtuálního operátora (SVOP) poskytujícího komunikační služby dostupné i v krizových stavech dle definovaných parametrů SLA.<br>SVOP bude specializovaný neveřejný konvergovaný virtuální operátor, plně pod kontrolou státu poskytující služby složkám IZS a dalším subjektům působícím na základě zákona č. 240/2000 Sb. Základem SVOP je kombinace vyhrazené telekomunikační infrastruktury jádra sítě a sdílené přístupové infrastruktury komerčních subjektů, zejm. pak rádiových přístupových sítí LTE/5G mobilních operátorů. Využití těchto sítí vychází ze závazku pro PPDR ukotveného v podmínkách aukce pásem 700/3700 MHz1. V budoucnu bude infrastruktura rozšiřitelná o fixní a satelitní přístupové sítě.<br>Pro dosažení cílové podoby SVOPu budou v rámci širšího SVOP programu realizovány další dílčí aktivity a projekty (např. SVOP-RAN), které rozšíří / doplní výše uvedenou technickou infrastrukturu jádra sítě a připraví organizačně-provozní zajištění. | 1.10.2024-31.12.2027 | IKČR 6 Efektivní a pružný digitální úřad | Ministerstvo vnitra | 468 |
| Konektivita 100GE pro krajské konektory | Předmětem projektu je zajistit dostatečnou propustnost krajských konektorů, které jsou přípojnými místy pro služby Centrálního místa služeb (dále jen CMS), s rychlostí 100Gbps. | 1.6.2025-31.12.2026 | IKČR 6 Efektivní a pružný digitální úřad | Ministerstvo vnitra | 306 |