Karta projektového okruhu

Číslo a název projektového okruhu: 6.2 Bezpečnost a krizové řízení

Garant karty projektového okruhu: Ministerstvo vnitra

Spolupracující subjekty: Ústřední orgány státní správy ve spolupráci s územními samosprávnými celky

Výčet strategií a cílů, na jejichž plnění se projektový okruh podílí:

Strategický dokument	Strategický/Specifický cíl
Strategický rámec rozvoje veřejné správy České republiky pro období 2014–2020	Strategický cíl 3 – Zvýšení dostupnosti a transparentnosti veřejné správy prostřednictvím nástrojů eGovernmentu Specifický cíl 3.1 - Dobudování funkčního rámce eGovernmentu
Strategie rozvoje informačních a komunikačních technologií (ICT) regionů ČR v letech 2013 – 2020	Rozvoj technologické infrastruktury veřejné správy - jednotná komunikační platforma, technický rozvoj IZS.
Digitální strategie rozvoje měst a obcí	ICT na podporu samosprávných činností v obcích a krajích: • Podpora činnosti policie • Podpora činnosti složek integrovaného záchranného systému

Zdůvodnění potřebnosti projektového okruhu včetně popisu výchozího stavu:

Výchozí stav:

Integrovaný záchranný systém (dále IZS) je systém spolupráce a koordinace složek, orgánů státní správy a samosprávy, fyzických a právnických osob při společném provádění záchranných a likvidačních prací. IZS se u nás buduje od roku 1993. Základním právním předpisem pro IZS je nyní zákon č. 239/2000 Sb., o integrovaném záchranném systému a změně některých zákonů.

MV pro IZS a bezpečnostní sbory provozuje radiokomunikační síť Pegas pro hlasové a datové komunikace s funkcemi, které neposkytují komerční operátoři. S vývojem ICT a výstavbou nových informačních a operačních středisek IZS uživatelé požadují nové funkcionality a kapacity. V roce 2015 dokončovaný projekt zavedl některé nové funkcionality, prvky bezpečnosti a softwarově zvýšil kapacitu systému pro skupinové hovory až na hranici jeho hardwarových možností.

Zdůvodnění potřebnosti projektového okruhu:

Do budoucna zbývá maximalizovat dosud neúplné pokrytí území ČR signálem sítě Pegas, odstranit nedostatky kyberbezpečnosti a důkladně tento kritický systém zabezpečit proti výpadkům napájení. Dále je třeba zajistit efektivní komunikační nástroje u HZS ČR v oblasti krizového řízení a zvýšit informační podporu velitele zásahu a jednotek HZS ČR prostřednictvím mobilních zařízení.

Zvyšování efektivity činnosti výše uvedených systémů je tedy možné jen pod podmínkou jejich vyšší integrálnosti, a to ve smyslu sdílení dat a informací a jejich vyhodnocování. To tedy dále znamená zajištění dostatečných přenosových kapacit a rychlostí, kapacit pro ukládání a zálohování dat, vytvoření interface pro předávání a sdílení dat, sjednocení datových formátů tak, aby vyhovovaly všem pro specifické potřeby subjektů veřejné správy a složek IZS, bezpečnostních systémů v oblasti justice a vězeňství. Při integračních krocích je

v dané oblasti nezbytně nutné zachovat (lépe zvyšovat) „bezpečnostní triádu CIA“ (anglicky CIA = confidentiality, integrity, and availability = důvěryhodnost, integrita a dostupnost) posílenou o auditovatelnost pro data jednotlivých systémů.

Legislativní změny:

Možná potřeba úprav legislativy vyplývající z nových technologií, a tím i změněných postupů, jako je např. použití elektronických identit atd. Dotčená legislativa je např. zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů. Uchovávání a zpracování dat a obrazových záznamů dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a dále pak legislativa upravující použití kamerových systémů (např. zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 553/1991 Sb., o obecní policii, a zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti) dle metodiky ÚOOÚ.

Ke schválení byl předložen nový zákon o HZS ČR, který vytváří předpoklady pro realizaci specifického tísňového volání zdravotně postižených občanů.

Cíle projektového okruhu:

1) Maximalizace pokrytí území signálem radiokomunikační sítě Pegas, přechod sítě Pegas na současné, kyberneticky zabezpečené protokoly (částečně i karta PO 7) a zajištění energetické bezpečnosti sítě Pegas.

2) Rozvoj infrastruktury bezpečnostních složek a IZS.

3) Zvyšování informační podpory HZS ČR a složek IZS při činnostech spojených s řešením mimořádných událostí a krizových stavů.

Indikátor:

nová funkcionalita informačního systému

počet pořízených informačních systémů

nové nebo modernizované prvky k zajištění standardů kybernetické bezpečnosti

Vazba na hlavní aktivity Implementačního plánu:

Hlavní aktivity Implementačního plánu	Vazba (ANO/NE)
1. Koncepční zajištění fungování eGovernmentu a realizace projektů ICT (včetně legislativy a řízení investic do ICT)	ANO
2. Vzdělávání v oblasti ICT a eGovernmentu včetně kybernetické bezpečnosti	ANO
3. Dobudování eGovernmentu	ANO
4. Prosazování principu Open Data	ANO
5. Rozšíření, propojení a konsolidace datového fondu veřejné správy a jeho efektivní a bezpečné využívání dle jednotlivých agend	NE
6. Dobudování infrastruktury a úložišť informačních a komunikačních systémů veřejné správy a eGovernmentu	-
7. Zvýšení kybernetické bezpečnosti IKT VS	ANO

8. Realizace systému elektronické identifikace, autentizace a autorizace a dalších služeb vytvářejících důvěru	ANO
9. Elektronizace podpůrných procesů	NE

Návaznost na předchozí projekty a výzvy:

Operační program	Výzva	V čem navazuje
Integrovaný operační program	3	Vytváření, rozvoj a údržba celostátních základních a dalších relevantních registrů veřejné správy, včetně systému bezpečného a chráněného přístupu.
Integrovaný operační program	6	Technologická centra pro obce s rozšířenou působností - Elektronizace výkonu jednotlivých agend ve veřejné správě, realizace transakcí (např. formulářů, výkazů …) elektronickou cestou a pořízení navazujících technologických řešení umožňujících zvýšení využívání eGovernmentu v podmínkách územní veřejné správy (např. vytvoření územní technologické infrastruktury nezbytné pro elektronizaci výkonu jednotlivých agend ve veřejné správě).
Integrovaný operační program	8	Rozvoj služeb eGovernmentu v krajích – technologická centra – Integrace s centrálními projekty, sdílení dat s centrálními registry ve veřejné správě, zřízení technologického centra kraje (dále jen „TCK“), včetně zajištění povinných služeb, realizace „rolloutu“ typového projektu TCK a vytváření dalších relevantních registrů pro potřeby územní veřejné správy. Budování komunikační infrastruktury územní veřejné správy: • výstavba datových sítí pro potřeby služeb veřejné správy a veřejných služeb, • projekty řešící vybudování komplexních standardizovaných informačních a komunikačních systémů, sítí a infrastruktur ve veřejné správě s důrazem na plnou interoperabilitu a vzájemné propojení s již existujícími systémy orgánů veřejné správy, • projekty na zajištění vysoké míry zabezpečení ICT (pořízení a podpora implementace bezpečnostních prvků /HW i SW/ do informačních systémů územní veřejné správy).
Integrovaný operační program	9	Zajištění přenosu dat a informací v územní samosprávě - budování komunikační infrastruktury územní veřejné správy: • výstavba datových sítí pro potřeby služeb veřejné správy a veřejných služeb, • projekty řešící vybudování komplexních standardizovaných informačních a komunikačních systémů, sítí a infrastruktur ve veřejné správě s důrazem na plnou interoperabilitu a vzájemné propojení s již existujícími systémy orgánů veřejné správy,

		• projekty na zajištění vysoké míry zabezpečení ICT (pořízení a podpora implementace bezpečnostních prvků /HW i SW/ do informačních systémů územní veřejné správy).
Integrovaný operační program	11	Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému.
Integrovaný operační program	12	Lokalizační a záznamová zařízení.
Integrovaný operační program	13	Technika pro zvýšení akceschopnosti a kvality řešení mimořádných událostí.
Integrovaný operační program	18	Pořízení moderní techniky a technologií ke zvýšení akceschopnosti složek IZS.
Integrovaný operační program	20	Zajištění akceschopnosti IZS při řešení rozsáhlých mimořádných událostí.
Integrovaný operační program	21	Zajištění efektivní hlasové a datové komunikace složek IZS při řešení mimořádných událostí.
Integrovaný operační program	23	Zajištění efektivní hlasové a datové komunikace složek IZS při řešení mimořádných událostí.

Řešené architektonické oblasti (vazba na architekturu):

V oblasti architektury je nutné nadále podporovat budování datových center a zajištění spolehlivých a bezpečných komunikací. Spolehlivost je v daném případě imperativem, protože ta ovlivňuje efektivitu činnosti složek IZS. Architektura zejména v případě IZS vyžaduje:

- jednotný systém GIS,
- jednotný standard pro hlasovou, datovou a radiovou komunikaci až na úroveň VS a SaP.

Neméně důležité pak je posílení stávajících datových úložišť a přenosových kapacit zajišťujících integraci jednotlivých systémů. Architektura systému musí být definována:

- architekturou sítě,
- definicí rozhraní,
- definicí infrastrukturní vrstvy (OS, virtualizace, databáze),
- definicí aplikační vrstvy.

Předpoklady a podmínky (max. 5 <u>obecných</u> předpokladů a podmínek realizace):

1) všechny služby a realizované projekty, musí dosahovat parametrů stanovených v Katalogu služeb, musí mít odpovídající zajištění SLA, musí být nastaveny metriky umožňující měřitelnost implementace a efektivity celého řešení,

2) dobudování a komplexní modernizace radiokomunikační sítě Pegas musí respektovat technologická specifika dosavadních a budoucích radiokomunikačních technologií, kterými se odlišují od ostatních ICT systémů.