



# OBJEDNÁVKA č. 0195/2017/KH/O

**Odběratel**

IČ: 70890692 DIČ: CZ70890692

**Moravskoslezský kraj**

28. října 2771/117

70218 Ostrava

Vyřizuje: Zuber Tomáš Ing.

Telefon: 595 622 367

Odbor: KH-2

**Dodavatel**

IČ: 03589277 DIČ: [REDACTED]

**BeePartner a.s.**

nám. Svobody 527

73961 Třinec

Vyřizuje:

Telefon:

**Objednáváme u Vás:**

zajištění zpracování návrhu technického řešení projektu "Rozvoj ICT v prostředí IZS", včetně architektonických výstupů dle požadavků výzvy IROP č. 28 - Specifické informační a komunikační systémy a infrastruktura II. v souladu s přílohou č. 1 a přílohou č. 2 k objednávce č. 0195/2017/KH/O. Termín plnění finálního návrhu dodat do 11 týdnů ode dne akceptace objednávky, předat 2x na CD-ROMu a prostřednictvím úložiště definovaného zadavatelem. Přílohy č. 1 a č. 2 k objednávce budou zaslány pouze elektronicky, ostatní podklady budou zaslány také pouze elektronicky. Maximální cena nepřesáhne částku ve výši 70.000,- Kč bez DPH, tj. 84.700,- Kč vč. DPH.

Datum požadovaného splnění: 05.05.2017

Přílohy:

**UPOZORNĚNÍ:** Odběratel uplatní institut zvláštního způsobu zajištění daně dle § 109a zákona o DPH a hodnotu plnění odpovídající dani z přidané hodnoty uvedené na faktuře uhradí v termínu splatnosti této faktury stanoveném dle objednávky přímo na osobní depozitní účet dodavatele vedený u místně příslušného správce daně v případě, že:

- a) dodavatel bude ke dni uskutečnění zdanitelného plnění zveřejněn v aplikaci „Registr plátců DPH“ jako nespolehlivý plátcce, nebo
- b) dodavatel bude ke dni uskutečnění zdanitelného plnění v insolvenčním řízení.

Odběratel nenese odpovědnost za případné penále a jiné postihy vyměřené či stanovené správcem daně dodavateli v souvislosti s potenciálně pozdní úhradou DPH, tj. po datu splatnosti této daně.

Úhrada faktury se provádí 14. kalendářní den od data doručení faktury.

Povinnost zaplatit cenu je splněna dnem odepsání příslušné částky z účtu objednatele.

**MAX. CENA CELKEM (vč. DPH)****84 700,00 Kč****Podrobnosti platby:**

Na účet

Číslo výdajového účtu MSK : 27-1650676349/0800

Datum: 16. 02. 2017

MORAVSKOSLEZSKÝ KRAJ  
Krajský úřad  
28. října 117  
18 OSTRAVA  
-25-

Ing. Tomáš Kotyza  
ředitel krajského úřadu

Po dobu nepřítomnosti zastoupen  
Ing. Annou Klímšovou  
zástupkyní ředitele  
vedoucí odboru financí

**Příloha č. 1 objednávky****Požadavky na zpracování Návrhu technického řešení****1. Úvodní informace**

Moravskoslezský kraj připravuje projekt „Rozvoj ICT v prostředí IZS“ k předložení do Integrovaného regionálního operačního programu, výzvy č. 28 - Specifické informační a komunikační systémy a infrastruktura II, pro specifický cíl 3.2 "Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT" (dále jen „IROP“). Podrobné informace k výzvě jsou na odkazu <http://www.dotaceeu.cz/cs/Microsites/IROP/Vyzvy/Vyzva-c-28-Specificke-informacni-a-komunikacni-systemy-a-infrastrukturu>.

Jedná se o projekt, jehož předpokládané náklady jsou 95 mil. Kč vč. DPH, bude realizován v Integrovaném bezpečnostním centru Moravskoslezského kraje v Ostravě (dále jen „IBC“). Informace o IBC je možné získat na adrese: <http://www.hzsmk.cz/index.php?ID=2501>. Bližší specifikace projektu tvoří přílohu objednávky.

**2. Rozsah a požadavky na zpracování**

Předmětem zpracování je vytvoření a zpracování **Návrhu technického řešení projektu** (dále jen „Návrh“) pro výše uvedený projekt. Při zpracování musí být dodrženo následující:

- a) Návrh technického řešení musí být v souladu s požadavky 28. výzvy IROP
- b) Návrh technického řešení musí být v rozsahu a souladu s požadavky dokumentu *Pravidla pro vydání stanoviska odboru hlavního architekta eGovernmentu (Příloha č. 4 Specifických pravidel pro žadatele a příjemce výzvy IROP č. 28)*
- c) Architektonické výstupy budou zpracovatelem doplněny také do korporátního modelu Moravskoslezského kraje, který je ve formátu Archi Model (.archimate) a bude předán zhotoviteli na počátku plnění, tyto výstupy budou současně v souladu s Manuálem jednotného vizuálního stylu kraje.
- d) Pro modelování v jazyce Archimate MV OHA využívá bezplatný nástroj Archi, dostupný z adresy <http://www.archimatetool.com>.
- e) Zpracovatel v rámci plnění vytvoří postup implementace návrh časového harmonogramu realizace.
- f) Při modelování a grafické vyjádření korporátní architektury je nutné vycházet z architektonické metodiky MSK, která vychází z metodického rámce TOGAF a využívá modelovací jazyk ArchiMate. KÚ MSK využívá pro modelování v jazyce Archimate bezplatný nástroj Archi. Metodika je dostupná na webových stránkách Moravskoslezského kraje [http://www.msk.cz/cz/verejna\\_sprava/korporatni-architektura-moravskoslezskeho-kraje-83244/](http://www.msk.cz/cz/verejna_sprava/korporatni-architektura-moravskoslezskeho-kraje-83244/).
- g) Návrh – Architektura (řešení) projektu bude dále obsahovat:

Výstupem bude shrnutí veškerých podstatných procesních, aplikačních, technických a technologických aspektů projektu přes všechny čtyři vrstvy architektonické vize eGovernmentu, jako jsou procesní změny, změny aplikačních služeb, zvolená technologie, technické parametry případných jednotlivých zařízení, výhody a nevýhody těchto předpokládaných řešení, vyplývající technická rizika pro realizaci a podmínky následného provozu a údržby:

- Enterprise architektura projektu – prokázání dodržení metodik, standardů a vzorů Národního architektonického plánu veřejné správy ČR.
- Přehled prvků navrhovaného řešení a jejich pozice v kontextu enterprise a aplikační architektury úřadu a navazujících subjektů veřejné správy.
- Způsob využití sdílených prvků architektur úřadu a eGovernmentu.
- Přehled nahrazovaných procesů a technologických prvků a začlenění navrhovaného řešení do stávajícího prostředí úřadu a eGovernmentu.
- Podrobnější architektura řešení projektu, jeho funkční a ne-funkční specifikace.
- Stanovení úrovně dodávky služeb realizovaných projektem s dodržením minimálních požadovaných standardů.

- Popis následné technické a technologické podpory realizovaného řešení a způsobu jejího zajištění.
- Podrobný popis nových funkcionalit – tato část bude zpracována dle pokynů výzvy č. 28 Integrovaného regionálního operačního programu.

Součástí musí být vždy i odpovídající architektonické výstupy spojené s projektem. Je požadováno, aby byly vypracovány architektonické diagramy (pohledy) doprovázené vysvětlením. Architektonický obsah je nezbytný zejména pro prokázání, že při návrhu projektu byl uplatněn celostní architektonický přístup, byly uplatněny stanovené architektonické principy eGovernmentu a jim odpovídající návrhové vzory. Povinné architektonické vzory jsou vypracovány na různých úrovních detailu, architektury úřadu i architektury řešení. Architektonické vzory jsou uvedeny na stránkách Ministerstva vnitra ČR, v agendě odboru hlavního architekta eGovernmentu: (<http://www.mvcr.cz/clanek/agenda-odboru-hlavniho-architekta-egovernmentu.aspx?q=Y2hudW09Nw%3d%3d>) .

- h) Součástí předmětu plnění je porovnání stávající struktury / architektury IBC s novým řešením. Pro porovnání stávající struktury / architektury IBC s novým řešením zhotovitel využije Strukturu IBC zpracovanou v rámci Návrhu technického řešení pro projekt „Vybudování komunikační platformy krizového řízení“.
- i) Navržené technické řešení musí odpovídat podporovaným aktivitám výzvy č. 28 a musí být splněna podmínka financování navrženého technického řešení (navržené řešení musí být v souladu s podporovanými aktivitami výzvy č. 28). V případě, že dojde k aktualizaci výzvy č. 28 je zhotovitel povinen dílo předat v souladu s aktuální verzí výzvy.
- j) Seznam podkladů, které předá objednatel zhotoviteli:
  - Návrh technické specifikace projektu „Rozvoj ICT v prostředí IZS“.
  - Základní Enterprise architektura IBC z doby před výstavbou budovy (2010)  
K dispozici budou části procesního modelu IBC týkající se dané problematiky, procesní model byl zpracován v prostředí programu Enterprise Architect verze 7.1. Zpracován je mimo jiné např. BPM procesu proces příjmu TIV, procesu krizového řízení, komponentový model HW a SW, deployment model. K dispozici je sada grafických výstupů v el. podobě.

### 3. Termíny plnění a způsob předání

Koncept Návrhu – Zhotovitel zpracuje **koncept** Návrhu technického řešení. Koncept bude obsahovat již zpracované veškeré jednotlivé požadované kapitoly (tj. naplnění obsahu). Předaný koncept bude sloužit objednateli k posouzení a **připomínkování**. Zhotovitel je povinen předané připomínky zcela zpracovat do finálního Návrhu. Objednatel je oprávněn vznášet připomínky a zhotovitel je povinen je zpracovat, a to i opakovaně. Objednatel postoupí Návrh technického řešení k posouzení také Ministerstvu vnitra ČR - Odbor Hlavního architekta eGovernmentu (dále jen „hlavní architekt“) k posouzení před převzetím. Připomínky, které event. vzejdou z tohoto posouzení, je rovněž zpracovatel povinen zpracovat do finálního návrhu.

Finální Návrh – Návrh technického řešení bude obsahovat požadovaný rozsah v požadované kvalitě plnění, nezbytný pro zpracování následné studie proveditelnosti.

Zhotovitel je povinen poskytnout objednateli součinnost při následném užití poskytnutých výstupů plnění (např. při hodnocení žádosti o finanční podporu, atp.).

## Termín plnění

- a) Zhotovitel předá do **6 týdnů** od akceptace objednávky **koncept Návrhu** k posouzení. Předání proběhne elektronicky na uvedené e-mailly objednatele.
- b) Objednatel provede **posouzení konceptu Návrhu** včetně zprostředkování posouzení konceptu hlavním architektem do **2 týdnů** od předání konceptu k posouzení.
- c) Zhotovitel provede **zpracování připomínek** objednatele (vč. připomínek hlavního architekta) a odevzdá doplněný **Finální Návrh do 3 týdnů** od předání těchto připomínek objednatelem.

Finální Návrh bude předán do **11 týdnů** ode dne akceptace objednávky.

## Způsob předání

Finální Návrh bude zhotovitelem předán objednateli na 2x CD-ROM a prostřednictvím úložiště definovaného zadavatelem. Přístup bude zhotoviteli poskytnut. O předání a převzetí vyhotoví zhotovitel předávací protokol dle pokynů objednatele. Na předávacím protokolu bude uveden přesný rozsah plnění v souladu s objednávkou, termín počátku a konce plnění. Kopie potvrzeného předávacího protokolu bude přílohou faktury.

## 4. Komunikace a Kontaktní údaje

V průběhu plnění je zhotovitel povinen se na základě pozvánek objednatele účastnit jednání k předmětu plnění v sídle objednatele, a to i opakovaně.

V průběhu plnění poskytuje objednatel k dispozici následující kontakty:

Ing. Aleš Trnka, projektový manažer, odbor evropských projektů, KÚ MSK; e-mail: [ales.trnka@msk.cz](mailto:ales.trnka@msk.cz)

Ing. Tomáš Zuber, vedoucí oddělení pro krizové řízení, e-mail: [tomas.zuber@msk.cz](mailto:tomas.zuber@msk.cz)

Plk. Ing. Jiří Němčík, Hasičský záchranný sbor Moravskoslezského kraje; email: [jiri.nemcik@hzsmsk.cz](mailto:jiri.nemcik@hzsmsk.cz)

Kpt. Ing. Tomáš Kašpar, Hasičský záchranný sbor Moravskoslezského kraje; email: [tomas.kaspar@hzsmsk.cz](mailto:tomas.kaspar@hzsmsk.cz)

## Projekt Rozvoj ICT v prostředí IZS

### Výzva č. 28 – Specifické informační a komunikační systémy a infrastruktura II.

Prioritní osa 3: Dobrá správa území a zefektivnění veřejných institucí

Investiční priorita IP 2c: Posilování aplikací v oblasti IKT určených pro elektronickou veřejnou správu, elektronické učení, začlenění do informační společnosti, elektronickou kulturu a elektronické zdravotnictví

Specifický cíl SC 3.2: Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT

---

#### • Cíle projektu

Projekt Integrovaného bezpečnostního centra (dále IBC), na který projekt Rozvoje ICT a služeb v prostředí IZS úzce navazuje, řešil mimo jiné prostorově integrované pracoviště pro příjem všech národních čísel tísňového volání (150 HZS, 155 ZZS, 158 PČR, 156 MPO) a integraci republikového systému příjmu tísňového čísla 112. Dosavadní příjem tísňových volání (dále TiV) je řešen u jednotlivých složek IZS prostřednictvím různých dispečerských systémů, které jsou na určité úrovni komunikačně integrovány a lze na určité úrovni předávat informace o již zadané události mezi složkami.

- 1) Jedním z cílů tohoto projektu je vytvoření systému pro společný příjem tísňových volání všech základních složek Integrovaného záchranného systému (dále jen IZS) a Městské policie Ostrava (dále jen MPO) v rámci IBC MSK. Jedná se o generačně zcela nový systém pro příjem tísňových volání nejen 112 a 150, ale i ostatních národních čísel TiV 155, 158 a 156 se společnou technologií a informačním systémem pro podporu příjmu TiV s novou úrovní provázanosti do jednotlivých dispečerských systémů složek IZS s důrazem na nové vlastnosti a funkcionality v telefonní části systému příjmu TiV při zachování principu národních čísel TiV a evropského čísla TiV 112. S touto částí projektu souvisí doplnění HW centra IBC (servery, telefonní subsystém, datová úložiště).
- 2) Jedním z dalších cílů projektu je realizace zcela nového moderního systému komunikace se sluchově a řečově postiženými občany na území Moravskoslezského kraje pomocí mobilní aplikace s přenosem polohy volajícího/komunikujícího a příprava rozhraní pro budoucí projekt Pan-European Mobile Emergency App (PEMEA) – EENA.
- 3) Z důvodu poskytování kvalitnějších vizuálních informací všem dispečerům IBC o situaci na i mimo území města Ostravy (klíčové dopravní prvky – tunel, dálnice apod.) a pro jejich efektivnější rozhodování v procesu návrhu sil a prostředků při řešení mimořádných událostí je potřebná integrace stávajících kamerových systémů do aplikace GIS. Realizovatelnost tohoto cíle je vázána na pořízení dedikovaného HW (servery) a SW licence.
- 4) Dalším z cílů projektu je zvýšení kvality předávaných technologických informací z nástaveb výjezdových vozidel do Integrovaného systému výjezdu. Jedná se o zcela nové funkcionality, které umožní předávat dispečerům operačního střediska a do strojní služby (systému pro evidenci vozidel HZS MSK) nové informace o stavu vozidel

a techniky s možností jejich vizualizace do geografických informačních systémů, což umožní efektivnější způsob rozhodování při využití zásahové techniky.

- 5) S předchozím cílem úzce souvisí zvýšení spolehlivosti internetové konektivity Integrovaného bezpečnostního centra, kdy účel této konektivity se z úrovně informační podpory dostal na úroveň velmi zásadního prvku pro komunikaci s mobilními jednotkami napříč složkami IZS. Zvýšení spolehlivosti lze dosáhnout transparentním zdvojením konektivity s automatickým dynamickým routováním (bezvýpadkovým provozem při nedostupnosti jedné z konektivit). Dopady na řešení této části projektu jsou do potřebné infrastruktury, zajištění nezávislosti konektivit na ISP (internet service providera), oblasti HW, konfigurací a monitoringu.
- 6) S částí projektu řešení spolehlivosti internetové konektivity souvisí bezpečnostní problematika ochrany perimetru internetové konektivity a samotné vnitřní sítě IBC, nutnost zajištění nových moderních prostředků pro ochranu před kybernetickým útokem s ohledem na komplexní řešení celého systému kybernetické bezpečnosti sloužícího pro plánování, detekci, vyhodnocení, protipatření a reportování kybernetických incidentů (sondy, systém vyhodnocení incidentů s aktivní ochranou - HW, SW, následné periodické aktualizace), zároveň tento projekt zajistí harmonizaci prostředí IBC MSK v souladu s podmínkami danými zákonem o kybernetické bezpečnosti, včetně zpracování projektu kybernetické bezpečnosti.
- 7) Na řešení předchozí části navazuje problematika zálohování dat a projekt obnovy po havárii s realizací záloh mimo budovu IBC (tzv. geografická záloha dat) a s tím spojeným vybudováním infrastruktury (konektivita, datové úložiště, SW prostředky pro zálohování, návrh a zpracování podrobného plánu zálohování a archivací klíčových technologických částí IBC).
- 8) Posledním cílem (ne významem) je zajištění vyšší kvality a dostupnosti poskytovaných služeb jak provoznímu personálu, tak potažmo a hlavně občanům v nouzi. Neodmyslitelnou součástí systémů, které jsou toto schopny zabezpečit, je moderní, stabilní a spolehlivý systém monitoringu technologií dispečerských systémů a inteligentního systému řízení a dohledu budov. Stávající systémy (CA Spectrum a Service Desk, EBI) je nutno modernizovat a rozšířit, aby bylo možno zaintegrovat nové výše uvedené systémy. Jedná se o modernizaci jak HW tak SW části systémů.

#### • Výsledky projektu

Ad 1)

V zásadě jde o zkvalitnění a zrychlení převzetí informací od volajících na TIV, rychlejší identifikaci místa události případně volajícího, a to se společným rychlejším sdílením jak hlasové tak datové části informací a s jednotnou technologickou úrovní zajištění příjmu TIV. Toto vše umožní rychlejší a kvalitnější zpracování nezbytných údajů pro rozhodovací proces v operačním řízení, návrh sil a prostředků a vyslání na místo mimořádné události.

Ad 2)

Nový systém komunikace se sluchově a řečově postiženými občany na území Moravskoslezského kraje pomocí mobilní aplikace umožní zcela nový způsob intuitivní komunikace s dispečery všech složek na IBC s dokonalejší identifikací místa komunikujícího postiženého občana s jednoduchým a snadným způsobem komunikace pro upřesnění dané situace. *Výsledkem by měla být efektivní a rychlá výměna informací s dopadem na rychlejší odezvu a pomoc ze strany složek IZS.*

Ad 3)

Výsledkem této části projektu je rychlý přístup k vizuálním informacím kamerových systémů v prostředí rutinně využívaném všemi dispečery složek IZS napříč IBC s vazbou na řešenou událost (vše v jednom společném prostředí GIS aplikace IBC)

Ad 4)

Výstupem této části projektu jsou nové funkcionality a informace v dispečerských systémech, které umožní nový pohled při rozhodovacím procesu v operačním řízení - detailní přehled o aktuálním stavu výjezdové techniky v daném konkrétním čase a o použitelnosti techniky v aktuální čas případně u další mimořádné události.

Ad 5)

Výsledkem této části projektu je zvýšení spolehlivosti dostupnosti internetové konektivity a zajištění datového spojení s výjezdovou technikou. Při potenciální výpadku jedné konektivity dojde automaticky bez výpadku a bez jakéhokoliv zásahu síťových administrátorů k přesměrování datového toku na záložní konektivitu.

Ad 6)

Změna v požadavku na úroveň dostupnosti internetové konektivity a problematiku s tím spojenou, požadavky na zabezpečení interních sítí a provozu IBC a požadavky dané zákonem o kybernetické bezpečnosti vyvolává potřebu realizace potřebných opatření v komunikační infrastruktuře. Výsledkem bude ochrana perimetru internetové konektivity a samotné vnitřní sítě IBC, zajištění nových moderních prostředků pro ochranu před kybernetickým útokem s ohledem na komplexní řešení celého systému kybernetické bezpečnosti sloužícího pro plánování, detekci, vyhodnocení, protipatření a reportování kybernetických incidentů (sondy, systém vyhodnocení incidentů s aktivní ochranou - HW, SW, následné periodické aktualizace), zároveň výsledkem tohoto projektu je zajištění harmonizace prostředí IBC MSK v souladu s podmínkami danými zákonem o kybernetické bezpečnosti, včetně zpracování projektu kybernetické bezpečnosti.

Ad 7)

Výsledkem této části projektu je vybudování systému zálohování dat a konfigurací zařízení, která budou uložena mimo budovu IBC (geografická záloha), a která budou sloužit v případě obnovy systémů po havárii. Součástí realizace bude komplexní zpracování materiálů a postupů potřebných pro obnovení provozu po případné havárii.

Ad 8)

Výsledkem je realizace modernějších systémů dohledu a monitoringu jak informačních systémů, tak dohledu technologií budov s integrací a konfigurací nových funkcionalit řešených v rámci tohoto projektu.

- **Místo realizace projektu**

Projekt bude realizován částečně v zázemí IBC, na dispečerských pracovištích i mimo objekt IBC - ad 4), ad 7). Působnost projektu je v rámci celého MSK, v případě ad 1) s přesahem do celé ČR (částečně se dotkne celorepublikového systému příjmu TiV 112)

- **Popis cílových skupin projektu**

Cílovou skupinou projektu jsou v první řadě občané MSK, potažmo podnikatelé a všechny cílové skupiny, pro které poskytuje IZS služby, jak při příjmu mimořádných událostí, tak při

jejich řešení. Další cílovou skupinou jsou samotní provozovatelé těchto systémů – základní složky IZS a MPO včetně provozního personálu zajišťujícího provoz těchto systémů.

- **Popis synergických nebo komplementárních vazeb na realizované / zrealizované či plánované projekty / investiční akce**

Název projektu: Integrované bezpečnostní centrum Moravskoslezského kraje (IBC MSK)

Dotační zdroj (např. ROP, název prioritní osy): ROP NUTS II Moravskoslezsko, prioritní osa 1. Regionální infrastruktura a dostupnost

Termín realizace (měsíc a rok zahájení, měsíc a rok ukončení): 10/2008 – 05/2011

Celkový rozpočet projektu: 679.113.750 Kč

Popis projektu (stručně, 1-2 věty): Cílem projektu bylo vybudování Integrovaného bezpečnostního centra, ve kterém je integrován příjem všech tísňových volání z území Moravskoslezského kraje a současně je vytvořeno prostorově sdružené operační pracoviště složek I integrovaného záchranného systému (IZS) v kraji, konkrétně pak Hasičského záchranného sboru Moravskoslezského kraje, Zdravotnické záchranné služby moravskoslezského kraje, Policie ČR Moravskoslezského kraje a Městské policie Ostrava.

#### Podrobný popis projektu

- **Výchozí stav**

Ad 1)

Systém příjmu TiV probíhá ve společném prostoru dispečerského sálu IBC každou složkou zvlášť nad společnou telefonní ústřednou, ale v rozdílném dispečerském systému (dále DS). Po převzetí události a jejích zapsání v daném DS je událost při nutné součinnosti další složky předána datově a v případě nutnosti i hlasově dispečerům dalších složek. Zpracování události je napříč složkami řešeno sekvenčně.

Ad 2)

V současné době probíhá komunikace s dispečery prostřednictvím předávání a zpracovávání SMS zpráv s postizenými bez možnosti technologické a SW podpory komunikace, identifikace a předání místa volajícího/komunikujícího. Stávající systém je do systému IBC SW integrován, je již na úrovni doby vzniku před 10-15ti lety.

Ad 3)

Dnes existuje proprietární a neintegrováný SW pro sledování výstupů kamerových systémů, který slouží především pro kamerový dohled MPO a existují licence pouze pro určitý počet pracovišť (ne pro každé pracoviště). Výstupy lze tedy využívat, nikoliv však na každém dispečerském pracovišti.

Ad 4)

V současnosti neexistuje žádný systém přenosu a zpracování dat ze zásahové techniky ani systém, který tato data zprostředkovává operačnímu řízení.

Ad 5)

Internetová konektivita IBC je realizována prostřednictvím jedné datové konektivity (jednoho ISP) bez zajištění jiné nezávislé konektivity.

Ad 6)



Úroveň zajištění bezpečnosti komunikací z pohledu internetové konektivity a ostatních sítí vstupujících do IBC je řešeno na úrovni v době realizace projektu IBC a v době před realizací zákona o kybernetické bezpečnosti.

Ad 7)

Doposud nebyl systém zálohování mimo budovu IBC ani systém plánování obnovy provozu po potenciální havárii řešen.

Ad 8)

Současný výchozí stav uvedených systémů odpovídá úrovni a rozsahem době realizace projektu IBC.

- **Analýza vnitřního prostředí (silné a slabé stránky)**

Silné stránky

- stávající IBC je svým řešením jedinečný a ojedinělý projekt svým rozsahem, systémem použitých technologií, prostorově integrovaným systémem příjmu TIV, společným zázemím pro všechny participující složky a realizovaným systémem úspory finančních prostředků z rozsahu. Budova a vybavení včetně správy a provozu je společně sdíleno včetně jasně stanovených pravidel podílu jednotlivých složek na provozních nákladech
- kvalitní odborný personál
- jednotná a společná infrastruktura (budova a zázemí)
- integrace informačních a komunikačních systémů
- zkušenosti ze stávajícího provozu IBC (od roku 2011)
- ...

Slabé stránky

- z důvodu rozsahu projektu stejně jako z důvodu nemožnosti technického řešení v dané době, nebyly některé nutné problematiky řešeny
- z důvodu vývoje technologií a obecně vývoje v oblasti informačních systémů, technologií a legislativy je nutno řešit nové technologie – závislost na lidských a finančních možnostech

- **Popis nulové varianty**

Nulová varianta zakonzervuje současný stav systémů bez možností dalšího vývoje a přizpůsobení se novým podmínkám a požadavkům.

- **Popis varianty rozvoje stávajícího informačního systému**

Výše popsané části projektu úzce navazují na stávající informační systémy, z části je rozvíjejí o nové funkcionality a z části nahrazují stávající funkcionality a postupy novými principy a postupy.

- **Odůvodnění varianty rozvoje stávajícího informačního systému**

Stávající systémy jsou v rutinním provozu od roku 2010/2011. Zkušenosti z provozu, vývoj v oblasti jak legislativy, technologií a možností, které nám mohou tyto technologie poskytnout

umožní realizovat novou kvalitu služeb poskytovaných občanům a dříve zmíněným cílovým skupinám. Rozvojem stávajících systémů dále uplatníme princip ochrany investic, které byly na projekt IBC vynaloženy.

- **Identifikace dopadů projektu**

Souvisí se vším výše uvedeným, realizací projektu dojde ke zkvalitnění všech projektem řešených oblastí s dopadem na rychlost a kvalitu poskytovaných služeb včetně rozšíření prostředků pro jejich poskytování a zajištění vyšší spolehlivosti daných systémů.

- **Odůvodnění potřeby projektu**

Koncem roku 2010 bylo dokončeno Integrované bezpečnostní centrum Moravskoslezského kraje (IBC). Vybudováním a zprovozněním IBC byla realizována prostorová a technologická integrace dispečerských a informačních systémů složek integrovaného záchranného systému (IZS) Moravskoslezského kraje. IZS má tak k dispozici špičkové (technologické i informační) systémy k plnění svého základního poslání – ochrany životů, zdraví a majetku občanů a návštěvníků Moravskoslezského kraje (dále jen MSK).

Cílem projektu „Rozvoj ICT a služeb v prostředí IZS“ je rozšířit a modernizovat stávající IBC o nové funkcionality a oblastech výše zmíněných. Tzn. řešení nového systému příjmu TIV napříč IBC, nového systému pro komunikaci se sluchově a řečově postiženými občany na území Moravskoslezského kraje, vybudováním nových systémů pro získávání informací z území, z výjezdových vozidel a zkvalitnění provozované infrastruktury pro podporu těchto i již provozovaných systémů tak, aby pokud možno byla zachována technologická úroveň dané doby.