



Sprostredkovateľský orgán OPIS



Európska únia

TVORÍME VEDOMOSTNÚ SPOLOČNOSŤ
Európsky fond regionálneho rozvoja

Riadiaci orgán OPIS

Národný projekt Centrálne služby dátového centra pre elektronizáciu verejnej správy

(Verzia 1-02)

Štúdiá uskutočniteľnosti pre
Ministerstvo financií Slovenskej republiky

Január 2012

Arthur D. Little GmbH
organizační složka
Danube House
Karolinská 650/1
186 00 Prague 8
Czech Republic

Obsah

1	Základné informácie	4
1.1	Úvod	4
1.2	Rozsah	4
1.3	Rámec projektu	4
1.4	Dôvod vypracovania štúdie	5
1.5	Východiská	5
1.6	Použité skratky a značky	8
2	Manažérske zhrnutie	11
3	Analýza aktuálneho stavu	13
3.1	Legislatíva	13
3.2	Existujúca technická infraštruktúra	14
4	Bezpečnostná analýza	22
4.1	Legislatívne východiská	22
4.2	Požiadavky informačnej bezpečnosti	23
5	Identifikácia možností a príležitostí	24
5.1	Identifikácia možností využitia DataCentra pre projekty OPIS PO1	24
5.2	Princípy konsolidácie pre projekty OPIS PO1	50
5.3	Finančné požiadavky projektov OPIS PO1	52
6	Návrh cieľového stavu zámeru	54
6.1	Princípy	54
6.2	Služby dátového centra	56
6.3	Procesná analýza	62
6.4	Základná koncepcia	67
6.5	Technická architektúra	79
6.6	Procesy riadenia služieb a podpory prevádzky	92
6.7	Riadenie informačnej bezpečnosti	94
6.8	Organizácia	95
7	Finančný plán	104
7.1	Predpoklady	104
7.2	Rozpočet	108
7.3	Analýza nákladov	110
7.4	Ekonomický model	114
7.5	Analýza prínosov	120
7.6	CBA analýza	122
8	Plán implementácie	128
8.1	Metodika projektového riadenia	128
8.2	Projektová organizácia	129

8.3	Aktivity a dodávky	130
8.4	Časový harmonogram implementácie	133
9	Riadenie rizík	134
9.1	Použitá metodika.....	134
9.2	Analýza rizík	135

1 Základné informácie

1.1 Úvod

Predložený dokument bol spracovaný na základe požiadavky Ministerstva financií SR. Cieľom štúdie uskutočniteľnosti je posúdiť technickú, organizačnú a finančnú rovinu implementácie a prevádzky nadrezortného Dátového centra ako poskytovateľa centrálnych služieb dátového centra pre elektronizáciu verejnej správy.

Financovanie budovania Dátového centra sa predpokladá zo zdrojov Operačného programu informatizácie spoločnosti, z hľadiska ktorého predstavuje projekt až do odovzdania do rutinej prevádzky oprávnený náklad.

1.2 Rozsah

Táto štúdia uskutočniteľnosti popisuje súčasný stav a rámcovo navrhuje budúce riešenie centrálnych služieb nadrezortného dátového centra pre elektronizáciu verejnej správy.

Koncept centrálného dátového centra (ďalej iba Dátové centrum) poskytuje konsolidované, efektívne riadené a finančne optimálne prostredie pre prevádzku informačných systémov verejnej správy čím priamo znižuje náklady na poskytovanie eGov služieb. Dátové centrum vďaka svojej robustnosti zároveň zabezpečuje požadovanú dostupnosť a bezpečnosť eGov služieb.

Úvodnú časť štúdie tvorí analýza súčasného stavu zameraná primárne na prostredie DataCentra, ktoré už v súčasnosti poskytuje služby dátového centra mimo rezortu Ministerstva financií SR.

Jadrom štúdie je návrh riešenia, ktorý pozostáva z procesnej, technickej a organizačnej časti. Výstupom procesnej analýzy je návrh základného procesného modelu riadenia prevádzky dátového centra a identifikácia kľúčových služieb poskytovaných Dátovým centrom. V časti technického návrhu riešenia sú definované komponenty vysoko úrovňovej architektúry riešenia, ktoré sú následne bližšie rozpracované. Pre všetky komponenty je analyzovaná relevantná legislatíva, štandardy a najlepšie praktiky, je definovaný referenčný model a jeho aplikácii pre potreby Dátového centra. V záverečnej časti návrhu riešenia sú definované systémy riadenia služieb a informačnej bezpečnosti vrátane vyžadovaného organizačného zabezpečenia.

Štúdia obsahuje odhad nákladov na realizáciu projektu a finančnú analýzu navrhovaného riešenia. V časti projektového plánu je definovaná základná projektová organizácia, projektové aktivity a míľniky. Záver štúdie je venovaný analýze rizík.

1.3 Rámec projektu

Táto čiastková štúdia uskutočniteľnosti sa opiera o nasledujúce dokumenty a literatúru:

- Operačný program informatizácia spoločnosti
- Stratégia informatizácie verejnej správy,
- Národná koncepcia informatizácie verejnej správy,
- Revízia budovania eGovernmentu (strednodobý plán implementácie priorít), prerokované a schválené Vládou SR dňa 2.2.2011
- Zákon č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov
- Zákon č. 275/2006 Z.z. o informačných systémoch verejnej správy
- Výnos Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy, uverejnené v Z.z. č. 312/2010

- Konceptia rozvoja informačných systémov (KRIS) MH SR,
- Ďalšie dokumenty a legislatívne predpisy popisované v rámci tohto dokumentu

1.4 Dôvod vypracovania štúdie

Primárnym dôvodom spracovania štúdie je vyhodnotenie uskutočniteľnosti projektu vytvorenia centrálného nadrezortného poskytovateľa služieb dátového centra v rámci elektronizácie verejnej správy, ktorý má byť realizovaný ako národný projekt v zmysle prioritnej osi č. 1.

Požiadavka na elektronizáciu služieb verejnej správy bola schválená uznesením vlády SR č. 131/2008 v rámci dokumentu „Stratégia informatizácie verejnej správy“, ktorého víziou je dosahovať neustály rast spokojnosti občanov s verejnou správou prostredníctvom poskytovania služieb atraktívnym a jednoduchým spôsobom za súčasného zvyšovania svojej efektívnosti, kompetentnosti a znižovania nákladov na verejnú správu.

Konceptia nadrezortného poskytovateľa služieb dátového centra adresuje primárne požiadavku na znižovanie nákladov na verejnú správu nakoľko zabezpečuje unifikáciu prostredia pre prevádzku eGov služieb, optimalizuje využitie zdrojov, znižuje obstarávacie a prevádzkové náklady a zvyšuje efektívnosť manažmentu na všetkých úrovniach od prevádzky infraštruktúry až po manažment vzťahov. Dôležitou oblasťou, ktorú priamo rieši predložený koncept, sú služby pre zabezpečenie požadovanej miery dostupnosti a bezpečnosti pre eGov služby čo priamo prispieva k pozitívnej skúsenosti a vnímaniu služieb verejnej správy z pohľadu občana.

Hlavným cieľom štúdie je analyzovať a vyhodnotiť udržateľnosť nadrezortného Dátového centra ako alternatívu k decentralizovanému a individuálnemu prístupu k poskytovaniu služieb dátových centier. Z tohto pohľadu je celková efektívnosť navrhovaného riešenia primárne závislá na miere využitia jeho služieb v rámci projektov PO1 OPIS, resp. eliminácii budovania duplicitných poskytovateľov služieb dátových centier.

1.5 Východiská

1.5.1 Konsolidácia IKT pre organizácie štátnej správy

Správa IKT pre verejnú správu je riadená v rámci kompetencií jednotlivých rezortov, resp. subjektov verejnej správy. Na národnej úrovni momentálne neprebíha reálna aktivita (projekt), ktorej cieľom by bola konsolidácia IKT, čo spôsobuje, že väčšina subjektov štátnej správy rozvíja väčšie alebo menšie výpočtové strediská.

Na úrovni rezortu MF SR je zrejmá snaha o vybudovanie zdieľaného dátového centra, ktorá už priniesla prvé výsledky. DataCentrum ako rozpočtová organizácia MF SR už v súčasnosti poskytuje služby aj pre iné rezorty a niektoré inštitúcie samosprávy.

DataCentrum má v rámci svojho rozvoja ambíciu poskytovať IT služby na vyžiadanie orgánom štátnej správy v takom rozsahu, ktorá ich odbremení od starostlivosti o ich IT zdroje (nákup potrebných zariadení, pravidelný update SW a upgradu HW, SW aplikácií a pod.) a zároveň im umožní znížiť náklady na informačné a komunikačné technológie. Základom je prenesenie starostlivosti o IT prevádzku a infraštruktúru na DataCentrum ako poskytovateľa komplexných služieb, aby sa efektívne využívali verejné financie.

Štúdia vychádza z predpokladu, že DataCentrum bude zabezpečovať úlohu primárneho výpočtového strediska pre tie organizácie štátnej správy, ktoré nemajú vybudované vlastné výpočtové strediská, resp. z hľadiska efektivity nebude výhodné rozšírenie ich existujúcich výpočtových stredísk tak, aby boli splnené všetky požiadavky na prevádzku a bezpečnosť ISVS implementovaných v rámci OPIS PO1. DataCentrum bude zároveň zabezpečovať úlohu záložného výpočtového strediska pre organizácie štátnej správy, ktoré z hľadiska efektivity nebudú budovať vlastné záložné lokality.

1.5.2 Projekty PO1 OPIS

V súčasnosti sú ciele PO1 OPIS realizované formou samostatných projektov, pri ktorých nie sú vytvorené systémové predpoklady pre zdieľanie a konsolidáciu HW a SW infraštruktúry. Jednotliví žiadatelia majú vybudovanú rôznu úroveň IKT infraštruktúry od komplexných dátových centier so zabezpečením disaster recovery (napr. MVSRR) až po jednoduché data room spĺňajúce požiadavky podľa štandardu TIA-942 na úrovni Tier I, resp. Tier II.

V zmysle koncepcie budovania ISVS podľa NKIVS a aj charakteru poskytovaných eGov služieb sa požaduje dostupnosťou systémov v rozsahu 24x7. Zabezpečenie takejto dostupnosti vyžaduje dátové centrá na úrovni Tier 3 vrátane záložných (disaster recovery) lokalít.

PO1 OPIS projekty primárne implementujú komplexné a jedinečné informačné systémy, ktoré vyžadujú integráciu na ostatné systémy ISVS.

1.5.3 Dátové centrá žiadateľov

Štúdia vychádza z predpokladu, že existujúce dátové centrá žiadateľov (s výnimkou DataCentra) ostávajú prevádzkované v existujúcom móde, t.j. štúdiu navrhované riešenie neovplyvňuje chod týchto dátových centier.

Na druhej strane však žiadateľ môže využiť služby DataCentra a tak doplniť služby, ktoré poskytuje jeho interné dátové centrum. Typickým príkladom môžu byť služby typu IaaS / PaaS pre testovacie a vývojové prostredie, služby pre podporu dostupnosti a kontinuity prevádzkovaných systémov a pod..

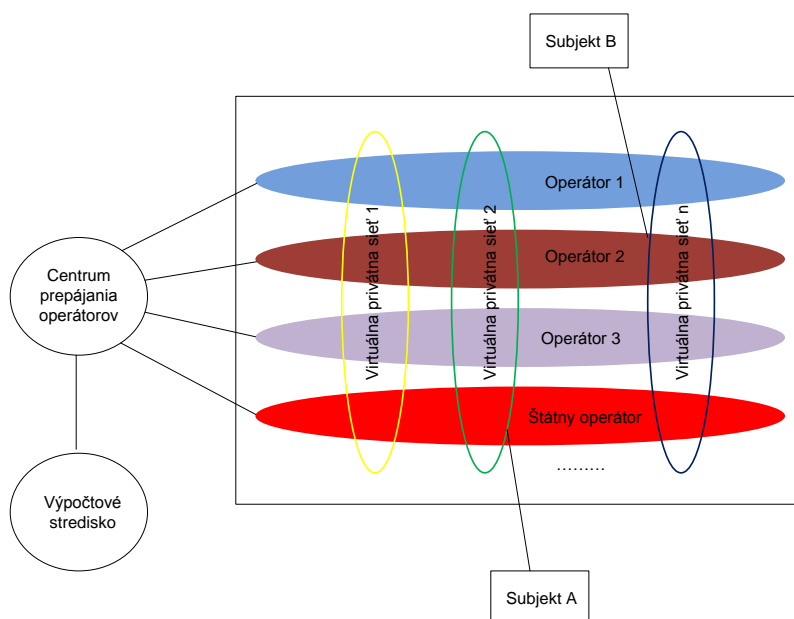
1.5.4 Rozvoj komunikačno-technologickej infraštruktúry ISVS na centrálnej úrovni

V rámci PO1 OPIS bola v roku 2009 vypracovaná „Štúdia uskutočniteľnosti prioritnej osi č. 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS zameraných na rozvoj komunikačno-technologickej infraštruktúry IS verejnej správy na centrálnej úrovni“ (ďalej aj Štúdia RKTÍ). Primárnym cieľom Štúdie bolo navrhnutie efektívneho a účinného postupu implementácie projektov pre zabezpečenie komunikačno-technologickej infraštruktúry informačných systémov verejnej správy v súlade s celkovou architektúrou integrovaného informačného systému verejnej správy.

Štúdia RKTÍ ako cieľové riešenie rozpracovala alternatívu, ktorej charakteristika je z pohľadu komunikačnej a technologickej infraštruktúry popísaná v nasledujúcich bodoch:

Komunikačná infraštruktúra :

- Použije sa obmedzený počet operátorov. S operátormi bude uzavretá rámcová zmluva na dobu určitú. Po jej uplynutí bude opätovne vyhodnocovaná kvalifikácia.
- Zodpovednosť za vzájomné prepojenie operátorov, tak aby bolo možné prepojenie jednotlivých VPN štátnej správy je na strane operátorov.
- Samospráva sa bude pripájať do VPN štátnej správy pre oblasť prenesených kompetencií.
- Ministerstvo financií bude držiteľom Kontrolnej a koordinačnej kompetencie s praktickým dosahom na kvalifikáciu operátorov, podmienky poskytovania služieb (SLA)

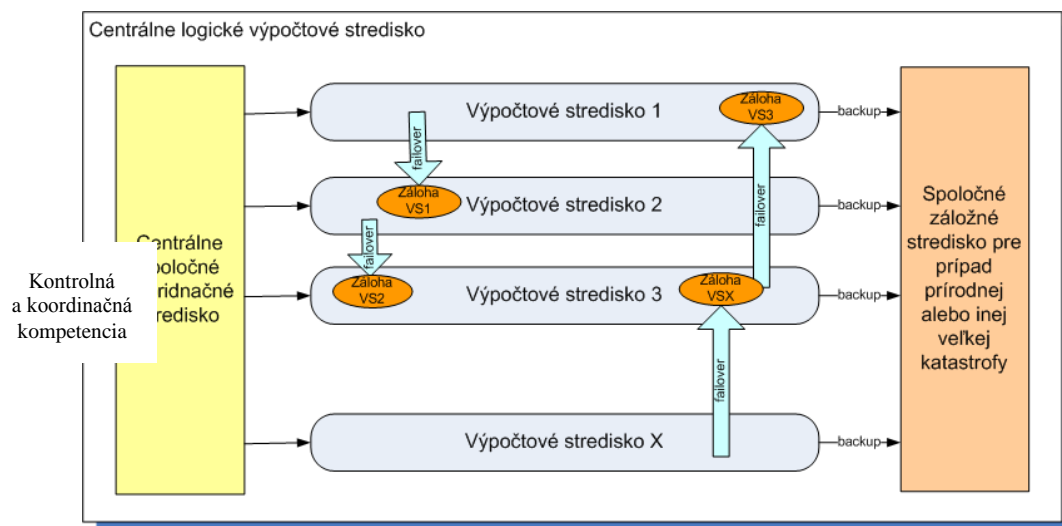


Z pohľadu technologickej infraštruktúry Štúdia RKTÍ navrhla vybudovanie centrálneho logického výpočtového strediska, ktoré predstavuje logickú úroveň fyzických dátových centier. Skladá sa zo samostatných fyzických dátových a spoločného záložného strediska pre prípad prírodnej alebo inej veľkej katastrofy. Štúdia predpokladala kvalifikáciu 7 dátových centier, ktoré prináležia nasledovným povinným osobám: Ministerstvo financií, Úrad vlády, Ministerstvo vnútra, Sociálna poisťovňa, Úrad geodézie, kartografie a katastra, Ministerstvo zdravotníctva (NCZI), Štatistika.

Koordináciu činnosti jednotlivých fyzických dátových centier je zabezpečená Kontrolnou a koordinačnou kompetenciou, ktorá:

- Koordinuje a metodicky usmerňuje chod samostatných výpočtových stredísk
- Obsahuje centrálny monitoring chodu služieb jednotlivých výpočtových stredísk
- Nezasahuje priamo do chodu jednotlivých výpočtových stredísk

Ostatné výpočtové centrá sú hostované kvalifikovanými dátovými centrami. Časť dátových centier (nekvalifikovaných) bude „prežívať“ naďalej. Od programu OPIS sa očakávala finančná motivácia tých, ktorí podporia implementáciou navrhovaný model, reprezentovaný kvalifikovanými dátovými centrami. Tak bude dochádzať k tesnejšej forme navrhovanej centralizácie.



Štúdia RKTÍ zároveň identifikovala nasledovné kľúčové riziká spojené s budovaním centralizovanej IKT infraštruktúry:

- Organizačné riziká a problémy:
 - neochota poskytovať služby DC iným rezortom
 - neochota umiestniť spravované zdroje do kvalifikovaných dátových centier
 - nebudú vytvorené organizačné a personálne predpoklady na fungovanie kvalifikovaných dátových centier
- Technologické riziká a problémy
 - technologické obmedzenia migrácie aplikácií do kvalifikovaných dátových centier
 - nekompatibilita systémov z dôvodu veľkej diverzifikácie platforiem
 - nemožnosť virtualizácie
 - nedostatočné kapacity kvalifikovaných dátových centier
- Legislatívne riziká a problémy
 - nebudú vytvorené legislatívne predpoklady na vytvorenie Centrálného logického dátového centra štátu
 - legislatívny proces vytvorenia podmienok na centralizáciu bude trvať dlho

Predkladaná štúdia v súlade so závery štúdie RKTÍ adresuje rozvoj DataCentra ako centrálného poskytovateľa služieb dátového centra tak, aby toto spĺňalo požiadavky na kvalifikované dátové centrum.

1.6 Použité skratky a značky

Tabuľka 1 – Prehľad použitých skratiek

APV	Aplikačno-programové vybavenie
BC	Business Continuity
CA	Certifikačná autorita
DC	Dátové centrum

DRP	Disaster Recovery Plan
EPS	Elektronická požiarňa signalizácia
FC	Fibre Channel
FOB	Fyzická objektová bezpečnosť
HA	High Available
HACS	Hot-Aisle Containment System
HW	Hardvér
IaaS	Infraštruktúra ako služba
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IKT	Informačné a komunikačné technológie
IS	Informačný systém
ISVS	Informačný systém verejnej správy
IT	Informačné technológie
ITIL	IT Infrastructure Library
ITSM	IT Service Management
KRIS	Koncepcia rozvoja informačných systémov
LAN	Local Area Network
NAS	Network Attached Storage
NBÚ	Národný bezpečnostný úrad
NKIVS	Národná koncepcia informatizácie verejnej správy
OPIS	Operačný program informatizácia spoločnosti
PaaS	Platforma ako služba
PKI	Public Key Infrastructure
SaaS	Softvér ako služba
SAN	Storage Area Network
SDP	Skorá detekcia požiaru
SHZ	Stabilné hasiace zariadenie
SLA	Service Level Agreement
SLM	Service Level Management
SMIB	Systém manažérskej informačnej bezpečnosti
SOA	Service Oriented Architecture
SPOF	Single Point Of Failure
SW	Softvér
TI	Technická infraštruktúra

UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
ZEP	Zaručený elektronický podpis
WAN	Wide Area Network

2 Manažérske zhrnutie

Súčasný stav prostredia projektov OPIS PO1 sa vyznačuje zvláštnym paradoxom. Pokiaľ na základnej konceptuálnej úrovni v oblasti poskytovania eGov služieb existuje úzka integrácia medzi jednotlivými projektmi, ktorá je podporená aj na úrovni technologickej prostredníctvom zadefinovaných princípov a štandardov pre potrebu integrácie jednotlivých komponentov, v oblasti zabezpečenia eGov služieb potrebnou IKT infraštruktúrou je stav úplne opačný. Jednotlivé projekty žijú svojím úplne samostatným životom, bez akýchkoľvek integračných alebo konsolidačných aktivít.

Pre prostredie projektov je preto charakteristická neprítomnosť konsolidácie IKT prostriedkov a služieb na medzi projektovej alebo z pohľadu žiadateľa na nadrezortnej úrovni. To spôsobuje, že je predpokladaný rozvoj väčších alebo menších výpočtových stredísk ktoré má dnes zriadené a prevádzkuje väčšina subjektov štátnej správy. Tieto zdroje sú už z historického hľadiska budované samostatne či už z pohľadu technologickeho alebo z pohľadu riadenia IKT, pričom tento stav viac menej pretrváva a aktuálne riešenia projektov OPIS tento stav konzervuje. Na druhej strane je ale potrebné povedať, že v súčasnosti badať tendencie smerujúce ku konsolidácii prostriedkov IKT na nadrezortnej úrovni. Ako príklad je možné spomenúť DataCentrum Ministerstva financií alebo koncepciu inteligentného regiónu Košice, v rámci ktorej je cieľom konsolidovať nie len zdroje IKT, ale aj technologicke znalosti. DataCentrum sa stáva určitým konsolidačným prvkom aj z pohľadu prebiehajúcich projektov OPIS, na úrovni rezortnej – kde je plánovaná prevádzka systémov CEP v jeho priestoroch a aj na úrovni nadrezortnej, kde sa predpokladá hostovanie systému eHealth, Ministerstva zdravotníctva.

Všeobecne je možné konštatovať že prostredie OPIS disponuje značným množstvom zdrojov na IKT infraštruktúru avšak v rámci súčasne plánovaného priebehu projektov ich nedokáže spoločne využiť. Každý projekt predpokladá vlastnú, redundantnú a vysoko dostupnú infraštruktúru v mnohých prípadoch s umiestnením v dvoch a niekedy až v troch geograficky oddelených lokalitách. Na túto infraštruktúru sú v rámci projektov dedikované nie malé finančné zdroje, pričom je potrebné zabezpečiť finančné zdroje aj na následnú prevádzku a podporu tejto infraštruktúry a v neposlednom rade aj na podporu používateľov eGov služieb. Súčasný stav zabezpečenia IKT infraštruktúry, jej prevádzky a podpory v prostredí projektov OPIS sa preto javí minimálne ako nevýhodný z hľadiska využitia plánovaných technických prostriedkov IKT, ak nie vyslovene neekonomický pre optimálne naplnenie zámeru informatizácie verejnej správy.

Koncepcia IISVS popísaná v NKIVS, ktorá je základným rámcom pre projekty OPIS, kladie vysoké požiadavky na zabezpečenie dostupnosti, interoperability a bezpečnosti informačných systémov. Jednotlivé komponenty IISVS preto kladú nemalé nároky na vytvorenie zodpovedajúcej technologickej infraštruktúry spolu so zabezpečením jej prevádzky a podpory. Potrebné je preto koncepčným spôsobom riešiť jednak oblasť zabezpečenia budovaných eGov služieb nevyhnutnou IKT infraštruktúrou, tak aj zabezpečenie prevádzky a podpory tejto infraštruktúry.

Základnou myšlienkou tejto koncepcie je zabezpečenie centrálnych služieb dátového centra pre elektronizáciu verejnej správy, ktoré konsolidovaným spôsobom pokryjú požiadavky projektov OPIS PO1. Zo strategického hľadiska umožní takáto koncepcia vytvoriť prostredie pre budúci rozvoj eGov služieb tak, aby IKT pri rozvoji neboli obmedzujúcim faktorom ale vedeli pružne reagovať na budúce požiadavky a zmeny.

Vývoj v oblasti poskytovania IT služieb, vo forme “Cloud Computing”, otvára nové pole možností tým, že umožňuje jednoduchý prístup k dynamicky konfigurovateľným službám. Cloud predstavuje nový spôsob šetrenia IT nákladov formami, ktoré propagujú štandardné formy optimalizácie a zdieľania infraštruktúry, ako aj poskytovania unifikovaných služieb. Pre súčasný stav prevádzky a podpory v prostredí projektov OPIS je poskytovanie služieb formou Government Private Cloud-u spôsobom, ktorý sa eliminujú hlavné problémové faktory často uvádzané pre Verejné Cloud-y (často iba Cloud-y) akými sú: bezpečnosť, neznáma spoľahlivosť infraštruktúry a vlastníctvo dát.

Cieľovým stavom je stratégia formovania a správy infraštruktúry, ktorá nielen zabezpečí optimalizáciu kvality a nákladov z pohľadu krátkodobého, ale zároveň bude aj garantom jej udržateľnosti z hľadiska dlhodobého.

3 Analýza aktuálneho stavu

3.1 Legislatíva

Legislatívny rámec je daný kompetenciami MF SR. Základné kompetencie ministerstva definuje zákon č. 575/2001 Z.z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov.

Ďalšie zákony, ktoré sú relevantné pre definované služby dátového centra sú v nasledovnej tabuľke:

Tabuľka 2 – Kľúčové právne predpisy

Hlavné právne predpisy	
Číslo	Názov
Zákon č. 275/2006 Z.z.	o informačných systémoch verejnej správy v znení neskorších predpisov
Zákon č. 610/2003 Z.z.	o elektronických komunikáciách v znení neskorších predpisov
Zákon č. 215/2002 Z.z.	o elektronickej podpise v znení neskorších predpisov a prislúchajúce vyhlášky NBÚ
Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z.z.	o štandardoch pre informačné systémy verejnej správy
Zákon č. 428/2002 Z.z.	o ochrane osobných údajov v znení neskorších predpisov
Zákon č. 215/2004 Z.z.	o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
Štandard STN ISO/IEC 27001	Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti
Štandard STN ISO/IEC 20000	Informačné technológie. Manažment služieb.
Zákon č. 45/2011 Z. z.	o kritickej infraštruktúre
Zákon 215/2004 Z.z.	o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov
Vyhláška NBÚ č. 336/2004	o fyzickej bezpečnosti a objektovej bezpečnosti v znení neskorších predpisov

DataCentrum v rámci existujúceho legislatívneho prostredia už v súčasnosti pôsobí ako nadrezortný poskytovateľ IT služieb pre organizácie verejnej správy. V zmysle cieľov štúdie sa adresuje interný rozvoj (kvantitatívny a kvalitatívny) DataCentra s cieľom poskytovať IT služby s vyššou pridanou hodnotou pre subjekty verejnej správy. Vychádzajúc z predpokladu, že existujúce pôsobenie DataCentra je v súlade s platnou legislatívou, je možné konštatovať, že neexistujú zásadné právne bariéry pre realizáciu daného projektového zámeru.

3.2 Existujúca technická infraštruktúra

3.2.1 DataCentrum

DataCentrum, ako samostatná rozpočtová organizácia MF SR, sídli v administratívnej budove na Cintorínskej 5, v Bratislave (t.j. v užšom centre mesta). V niekoľko poschodovej budove sú administratívne priestory pre jednotlivé organizačné zložky DataCentra a dátová sála, ktorá predstavuje primárne dátové centrum (PDC) organizácie.

3.2.1.1 Technická infraštruktúra

Technická infraštruktúra DataCentra je zameraná na zabezpečenie služieb informačných systémov pre inštitúcie verejnej správy a služieb podpory prevádzky pre tieto IS. Primárna orientácia je na informačné systémy ministerstva financií SR, ale prevádzkované sú aj informačné systémy iných ministerstiev a niektorých inštitúcií samosprávy. Druhou oblasťou sú informačné systémy samotného DataCentra, slúžiace napr. na podporu používateľov prevádzkovaných IS, testovanie ako aj ďalšie menšie informačné systémy. Ako jedny z významných je možné uviesť nasledovné informačné systémy:

- Rozpočtový informačný systém (RIS)
- Informačný systém Štátnej pokladnice (IS ŠP)
- Informačný systém jednotného účtovníctva štátu (JÚŠ), v pilotnej prevádzke
- Záložný systém ARDAL (Agentúra pre riadenie dlhu a likvidity)
- Informačné systémy ministerstva financií Slovenskej republiky, ministerstva životného prostredia Slovenskej republiky (MŽP); ministerstva dopravy pôšt a telekomunikácií Slovenskej republiky (MDPT)
- Rozpočtový IS pre samosprávu (RIS.SAM)
- Informačný systém Nitrianskeho a Banskobystrického samosprávneho kraja (NSK)
- Informačný systém štrukturálnych fondov (ITMS)
- Informačný systém účtovníctva fondov (ISUF)
- Systémy pre integračné a automatizované testovacie centrum (IATC)
- Skupina podporných systémov, medzi ktoré patrí napr. systém Call Centra a Service Desk
- Portál www.informatizacia.sk

Systémová infraštruktúra

Systémovú infraštruktúru potrebnú na zabezpečenie prevádzky jednotlivých informačných systémov je možné rozdeliť z dvoch hlavných pohľadov:

- hľadisko platformy informačných systémov,
- hľadisko sieťového rozdelenia systémov.

Z pohľadu platformy sú kľúčovou časťou infraštruktúry DataCentra systémy radu HP 9000 s operačným prostredím Unix (HP-UX) a databázovým prostredím Oracle. Pre tieto systémy sú aplikované možnosti virtualizácie na úrovni hardvérových partícií (nPar).

Využívaný je jeden systém typu HP Integrity Superdom (HP Superdome SD 64), ktorý predstavuje najvyššiu triedu serverov daného radu a ktorý je osadený procesormi Intel Itanium. Na danom systéme sú prevádzkované produkčné a testovacie informačné systémy na platforme SAP – Jednotné účtovníctvu štátu (JÚŠ), informačné systémy MDPT, MŽP a NSK, IS ESO ako aj modul zabezpečujúci funkcionality IS ŠP pre platobný styk (ŠP Pay) a systém VPS.

Ďalšie zo serverov radu HP 9000 reprezentujú servery strednej triedy. Využívaný je 1 server typu HP Integrity – HP rx8640, ktorý je osadený procesormi Intel Itanium a 1 starší typ servera - HP rp8420, ktorý je osadený procesormi na platforme PA-RISC. Na serveri typu HP rx8640 je prevádzkovaná časť informačného systému štátnej pokladnice, ktorá je vytvorená na platforme SAP a na serveri typu HP rp8420 sú prevádzkované moduly IS ŠP - MANEX a PI a infraštruktúrne systémy LDAP a PKI.

Platforma OS Unix je tiež využívaná pre časť informačných systémov určených na používateľskú a technickú podporu. Na dvojici starších serverov HP rp3440, je napr. prevádzkovaná databáza Oracle pre aplikáciu Service Desk a na serveri HP rx3600 tzv. Konzola 2 – dohľadový systém infraštruktúry (Systém pre podporu prevádzky informačných technológií - SPPIT), založený na produktoch HP OVO. Okrem uvedených systémov je platforma Unix využívaná ešte pre viacero menších systémov a aplikácií.

Špecifickou oblasťou aplikácie platformy Unix je primárny aj záložný uzol prepojenia na EÚ (národný uzol TAXUD), vytvorený na systémoch IBM RISC P5. HW a SW vybavenie tohto uzla je zabezpečované priamo z Bruselu a zamestnanci Datacentra dané systémy len manažujú.

Ďalšou platformou infraštruktúry DataCentra sú systémy s operačným prostredím MS Windows a Linux, ktoré prevažne využívajú HW komponenty HP.

V rámci tejto platformy sú dedikované samostatné serverové systémy (skupiny serverov) pre prevádzku určených informačných systémov (skupín IS). Aplikované je aj virtuálne prostredie VMware a Citrix. Z platformy Windows / Linux je možné ako najdôležitejšie uviesť nasledovné systémy.

- Testovací a produkčný Rozpočtový informačný systém (RIS), v prostredí OS Windows 2003 / Oracle, pričom časť systému (WEB servery systému RIS) je prevádzkovaná vo virtuálnom prostredí VMware. Pre sprístupnenie využíva RIS terminálové servery Citrix XEN. Systém je umiestnený na infraštruktúre postavenej zo serverov typu blade (šasi HP c7000).
- Informačný systém účtovníctva fondov (ISUF), v prostredí OS Windows 2003 / Oracle vytvorený na platforme SAP. Umiestnený je na samostatnom serveri typu HP DL 380. V budúcnosti sa predpokladá migrácia do virtuálneho prostredia Citrix.
- Manažérsky IS (MIS) MF SR, prevádzkovaný vo virtuálnom prostredí VMware. Zatiaľ je umiestnený na samostatnom serveri typu HP DL380, v budúcnosti sa predpokladá premiestnenie na infraštruktúru serverov typu blade.
- Informačný systém štrukturálnych fondov (ITMS), v prostredí OS Linux / Oracle - časť systému je umiestnená na dvojici virtualizačných serverov VMware a druhá časť systému, cca 10 serverov, je prevádzkovaná vo virtuálnom prostredí Citrix.
- Informačný systém štátneho sektora a VÚC, ktorý je v súčasnosti prevádzkovaný už v archívnom móde.
- Záložný systém ARDAL, v prostredí OS Windows, prevádzkovaný vo virtuálnom prostredí VMware. Umiestnený je na 3 serveroch typu blade (šasi c7000) a 5 serveroch typu HP DL 360G. Má dedikované diskové pole HP HSV 300. Daný systém je v priestoroch DataCentra len hostovaný a patrí agentúre ARDAL.

Virtualizačná platforma VMware je okrem vyššie uvedených prípadov aplikovaná tiež pre nasledovné systémy:

- interné systémy pre interných zamestnancov DataCentra - MS Active Directory, file server, doménové servery, komunikačná infraštruktúra pre prístup do Internetu,
- systémy pre externých zamestnancov sídlacích v DataCentre, umiestnené v demilitarizovanej zóne – napr. web mail,

- niektoré služby pre zákazníkov – web stránky (informatizacia.sk, datacentrum.sk, rozpocet.sk, ...).

Samostatnou skupinou systémov platformy MS Windows je Komunikačno-technologická infraštruktúra (KTI), ktorá predstavuje prístupovú infraštruktúru zabezpečujúcu prístup používateľov k aplikáciám umiestneným v DataCentre. Skladá sa z nasledovných komponentov:

- Servery pre MS Active Directory,
- access controll servery,
- 2x poštový server,
- farma Citrix serverov,
- prístupové komponenty (VPN koncentrátory, Firewaly, ...)

Z hľadiska sieťového sú systém v infraštruktúre rozdelené do 3 logických častí:

- Systémy ŠP a externé systémy
- KTI
- Interné systémy (interná LAN)

Úplne samostatnú a aj fyzicky oddelenú časť infraštruktúry predstavujú systémy pre útvar Computer Security Incident Response Team (CSIRT).

Infraštruktúra pre ukladanie dát

Infraštruktúra pre ukladanie dát je reprezentovaná nasledovnými systémami:

- Diskové polia SAN
 - SUN 9990V, s kapacitou cca 50TB – predstavuje hlavné produkčné diskové pole, ktoré je určené pre systémy vo všetkých 3 častiach siete,
 - HP XP1024, s kapacitou cca 6TB – určené pre systémy ŠP, testovacie systémy, SAP,
 - 1x HP MSA 1000, s kapacitou cca 3TB - primárne určené pre IS RIS ale ktoré využívajú aj niektoré ďalšie systémy platformy OS Windows (Service desk, ISUF, ...),
 - 1x HP MSA 1000, cca 6TB – určené pre interné systémy a dáta - napr. inštalačné súbory,
 - v blízkej budúcnosti sa dovezie zo záložného DC druhé diskové pole SUN 990V, tiež s kapacitou cca 50 TB.
- Páskové knižnice
 - robustná pásková knižnica HP, 64 mechaník – určená pre sieť ŠP - zálohovanie všetkých SAP systémov, IS ŠP, JÚŠ, ...,
 - 1x HP MSL6060, 2x mechanika – určená pre internú LAN - zálohuje systémy vo virtuálnej platforme VMware, súborový server, elektronickú poštu, databázu Oracle pre odbor 3 (štatistiky), ...,
 - 1x HP MSL6060, 4x mechanika – určená pre sieť KTI – zálohuje domény, vybrané Citrix systémy, RIS, Service Desk, ITMS, ISUF.

SAN infraštruktúra

SAN infraštruktúra je len lokálna (nie je prepojenie SAN do záložného DC) a skladá sa z nasledovných sietí.

- SAN pre interné systémy – fyzicky samostatná SAN využíva komponenty HP Brocade – 2x SAN switch 2Gbps a 2x SAN switch 4Gbps,
- SAN pre systémy v sieti KTI – využíva cca 8 ks SAN switch HP Brocade, 8Gbps,
- SAN sieť pre systémy ŠP a systémy SAP – využíva 2 vysokovýkonné a škálovateľné switche typu HP SAN Director.

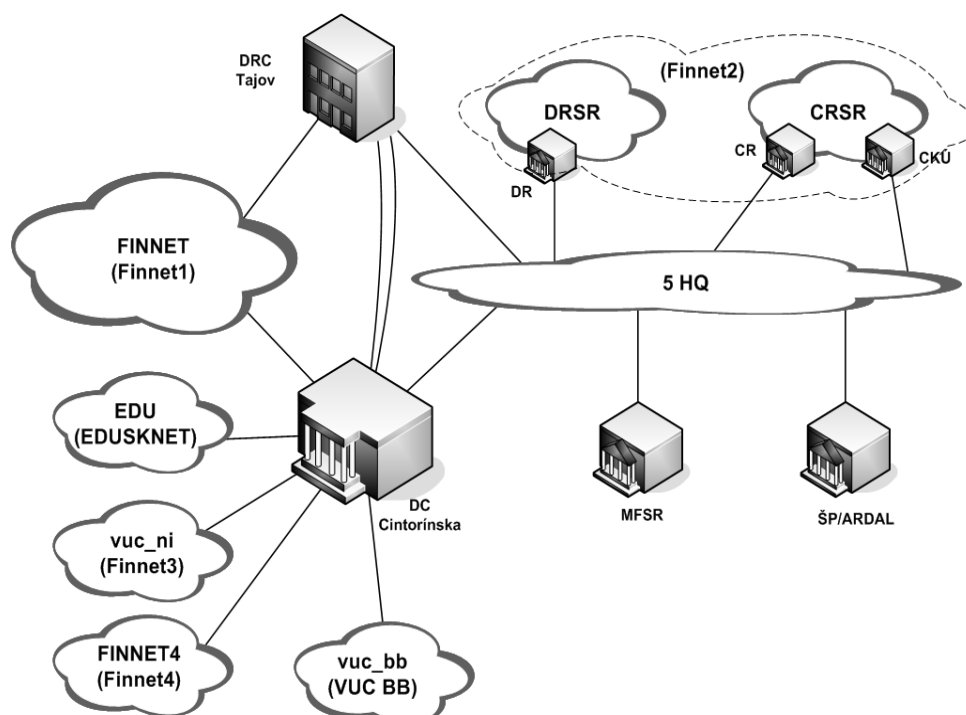
Všetky zariadenia sú do SAN siete prepojené minimálne duálnymi cestami.

Komunikačná infraštruktúra

Siete WAN

Siete WAN komunikačnej infraštruktúry zabezpečujú sprístupnenie informačných systémov prevádzkovaných v Datacentre pre klientske organizácie a používateľov, prostredníctvom sietí označovaných ako Finnet a 5HQ.

Obrázok 1 – WAN komunikačná infraštruktúra



- Finnet 1 – predstavuje VPN pre systémy KTI (komunikačno – technologická infraštruktúra), prostredníctvom ktorých Datacentrum poskytuje služby prístupu k aplikáciám pre rozsiahlu množinu organizácií štátnej správy, Štátnej pokladne a ich pobočiek,
- Finnet 2 – predstavuje VPN sieť pre Daňové riaditeľstvo (DR SR) a Colné riaditeľstvo (CR SR). Do tejto štruktúry patria aj existujúce siete Daňovej a Colnej správy, ktoré smerom na KTI využívajú existujúce prepojenie 5HQ pevnými linkami,
- Finnet 3 - vznikol po zavedení ServiceDesku pre Nitrianský samosprávny kraj. Tvori ho 114 liniek, ktoré zabezpečujú komunikáciu medzi pracoviskami,
- Finnet 4 – zabezpečuje prepojenie miest, obcí a samospráv,
- Sieť 5HQ – sieť spájajúca vrcholové orgány rezortu - MF SR, DR SR, CR SR (Colné riaditeľstvo a Colný kriminálny úrad) a Štátna Pokladňa / ARDAL.

Siete sú postavené na infraštruktúre siete ST-MPLS a ST-MEN a predstavujú navzájom oddelené VPN siete. Implementované sú QoS mechanizmy a prioritizácia prevádzky. S využitím MPLS technológie je tiež vytvorená VPN sieť VUC BB pre Banskobystrický samosprávny kraj a je zrealizované prepojenie DataCentra do dátovej siete EDUSKNET.

V DataCentre je vytvorený aj uzol prepojenia pre systémy DR SR a CR SR na sieť CCN/CSI (EÚ) - národný uzol TAXUD, s primárnym aj záložným systémom a primárnou aj záložnou konektivitou. Komunikačný uzol je vybudovaný na infraštruktúre IBM RISC serverov a zabezpečený je Firewallom Cisco.

Vytvorené je tiež priame prepojenie do záložného DRC Tajov na úrovni LAN, ktoré je šifrované. Zriadené sú 2 fyzické prepojenia – jedno sa využíva pre zrkadlenie databáz, na úrovni prostriedkov Oracle a druhé pre synchronizáciu systémov Citrix. Ďalšie fyzické prepojenie je vytvorené do primárneho dátového centra ARDAL a je dedikované len pre systém ARDAL.

Hlasový systém

DataCentrum disponuje hlasovým (telefónnym) systémom na princípe VoIP (Voice over IP) – IP CallCenter. Systém je postavený na produktoch Cisco Call Manager a poskytuje služby pokročilej hlasovej komunikácie ako napr. IVR (Interactive Voice Response).

Podporná infraštruktúra

Monitoring systémov

Monitoring systémov zabezpečujú dva systémy s logickým označením Konzola 1 a Konzola 2.

Konzola 1 predstavuje starší systém určený na monitorovanie IS ŠP a ďalších kľúčových systémov (JUŠ, SAP,...). Monitorovací systém je postavený na produkte HP OVO (Open View Opeartion) a NNM (Network Node Manager).

Konzola 2 označovaná aj ako Systém pre podporu prevádzky informačných technológií (SPPIT) je „nástupcom“ Konzoly 1. Je určená na monitorovanie serverov, sieťovej infraštruktúry (LAN sieť DC), systémov (ITSM, ISUF, ...) a aj vybraných služieb (DNS, proxy, web služby, ...). Monitorovací systém je postavený na produkte HP OVO, NNM s ďalšou rozšírenou funkčnosťou - napr. Business Availability Center (BAC) a reporting. Vybrané udalosti sa posielajú do aplikácie HP Service Desk.

V roku 2010 bol spustený projekt Centrálny Monitoring Prevádzky (CMP), v rámci ktorého vznikol útvar CMP a konsolidujú sa monitorovacie systémy v rámci DataCentra. Konsolidácia predstavuje zastrešenie funkčnosti Konzoly 1 a Konzoly 2. Fyzicky je systém realizovaný na hardvéri Konzoly 2.

Bezpečnostný monitoring

V oblasti bezpečnostného monitoringu infraštruktúry je prostredníctvom technológie Cisco MARS zabezpečovaný komplexný prehľad a vyhodnocovanie udalostí z detekčných systémov, ktoré monitorujú sieťovú (LAN) infraštruktúru ako aj z IDS a proxy systémov. Na vybraných serveroch sú nasadené sieťové sondy a agenti IDS systému IBM SiteProtector. Vybrané udalosti sa posielajú do aplikácie HP Service Desk.

Monitoring komunikačnej infraštruktúry

Súčasťou monitorovacieho systému je systém monitoringu aktívnych liniek v DataCentre, ktorý slúži na sledovanie aktuálnej činnosti liniek a ich poruchových stavov, prípadne sledovanie zaťaženia smerovačov na hlavných trasách spojení.

Dedikovaný monitorovací systém je nasadený na monitorovanie systémov národného uzla TAXAUD.

Zálohovací systém

K dispozícii sú dva samostatné zálohovacie systémy, ktoré priamo súvisia s využitím páskových knižníc.

Zálohovací systém pre internú sieť (interné systémy) – využíva jednu knižnicu MSL 6060. Riadenie zálohovania zabezpečuje aplikácia HP Data Protector.

Samostatný zálohovací systém pre systémy ŠP a ostatné systémy. Využíva ostatné dve knižnice. Zálohovanie je riadené druhou aplikáciou HP Data Protector.

Podpora používateľov - Service Desk

Pre podporu používateľov je využívaná aplikácia HP Service Desk vo verzii 4.5. Používatelia pristupujú k aplikácii prostredníctvom WEB rozhrania – Service Pages. Do systému sú prenášané aj vybrané udalosti z monitorovacích systémov (v súčasnosti sa riešenie odlaďuje). Pripravuje sa tiež prechod na novšiu verziu Service Desk systému – Service Manager.

3.2.1.2 Technologická infraštruktúra

Dátová sála

Dátová sála PDC je umiestnená na 1. poschodí budovy DataCentra a má celkovú rozlohu 246,3 m². Technické prevedenie IT systémov na dátovej sále je primárne orientované na umiestnenie v dátových skrinách (stojanoch), s výnimkami ako napr. servery pre uzol prepojenia na EÚ (TAXAD) a systémami ktoré je možné z hľadiska veľkosti považovať za samostatné dátové stojany (napr. server Superdome, diskové polia a pod.). Interné dátové rozvody sú realizované prostredníctvom metalickej kabeláže kategórie 6 a viac a optickej kabeláže, využívanej primárne pre SAN infraštruktúru.

Celkovo sa naplnenie dátovej sály v súčasnosti pohybuje na úrovni cca 55 dátových stojanov, takmer všetky v prevedení 42U. Z tohto počtu je 51 dátových stojanov využitých pre IT systémy (servery, diskové polia, ...) a 4 pre pasívne a aktívne prvky interných dátových rozvodov (LAN, SAN). Väčšina dátových stojanov pre serverové systémy je obsadená na cca 80% až 90%.

V súčasnosti, pri počte 55 dátových rozvádzačov, sú priestory dátovej sály využité na cca 64% a je možné rátať s umiestnením ešte cca 31 nových dátových stojanov pre serverové systémy. Celkové naplnenie sály predstavuje cca 86 dátových stojanov.

V blízkej budúcnosti sa v dátovej sále predpokladá umiestnenie systémov Ministerstva zdravotníctva, čo predstavuje požiadavku na priestor cca 20 nových dátových stojanov.

Plánovaná je optimalizácia IT systémov, ktorej výsledkom má byť aj redukcia počtov fyzických serverov prostredníctvom konsolidácie a virtualizácie IT systémov.

Napájanie

Napájanie všetkých dátových stojanov je realizované z dvoch nezávislých vetiev, kde každá vetva má 1 samostatný elektrický rozvádzač, 1 UPS, 1 transformátor a napájanie z elektrickej rozvodnej siete, pričom výpadok jednej vetvy neovplyvní prevádzku systémov.

Primárne napájanie je zabezpečované prostredníctvom dvojice transformátorov (hlavný a záložný), každý s výkonom 630 kVA. Priamo v dátovej sále sa nachádzajú 2 rozvádzače s redundantným výkonom 490 kW, z ktorých sú vedené 2 redundantné vetvy napájacích rozvodov pre dátové stojany. Rozvádzač každej vetvy je zálohovaný pomocou UPS s výkonom 240kW, ktorá má dobu zálohovania cca 30 minút. Celkovo je napájanie zálohované ešte dieselgenerátorom CATERPILLAR s výkonom 700 kVA.

Aktuálna záťaž od inštalovaných IT systémov na dátovej sále je 115 kW a sumárny odber, vrátane klimatizačných zariadení, je 211 kW. To predstavuje v súčasnosti výkonovú rezervu o veľkosti 125 kW.

Klimatizácia

Chladenie dátovej sály je realizované prostredníctvom 6 klimatizačných skriň UNIFLAIER UG40, s celkovým chladiacim výkonom cca 240 kW. Každá skriňa má dva chladiace okruhy s kondenzátormi umiestnenými na streche. Na zabezpečenie dostatočného chladiaceho výkonu bez ohrozenia prevádzky je akceptovaný výpadok 2 chladiacich skriň.

Protipožiarny systém

Dátová sála je vybavená požiarnou signalizáciou a automatickým hasiacim zariadením. Informácie protipožiarného systému sú vyvedené aj do monitorovacieho systému dátovej sály APC InfraStruXure.

Monitorovacie systémy

Významným prvkom zabezpečenia chodu technologických systémov dátovej sály je monitorovací systém APC (APC InfraStruXure), pomocou ktorého je možné včas identifikovať problémy v systémoch chladenia, napájania a ostatných podporných sústav. Monitorovací systém tiež umožňuje posilať varovné maily a SMS na vybrané adresy.

V nasledovnej tabuľke sú zhrnuté základné parametre PDC DataCentra.

Tabuľka 3 – Základné parametre PDC DataCentra

Parameter	Hodnota
plocha IT m ²	246
výkon kVA	240
výkonová hustota kVA/m ²	1
Redundancia UPS	2(n+1)
Redundancia G (generátor)	n
Redundancia chladenia	n+1
SHZ	áno

Fyzická bezpečnosť

Prístup do dátovej sály je na prvej úrovni chránený už pri vstupe do priestorov budovy DataCentra prostredníctvom riadeného vstupu cez turniket ovládaný bezkontaktnými kartami. Fyzický prístup na dátovú sálu je chránený ďalším turniketom a dverami s elektromagnetickým zámkom. Vstup na sálu je povolený len pre vybraný okruh osôb a zabezpečený je prostredníctvom bezkontaktných kariet. Priestor vstupu do dátovej sály, ako aj samotná sála sú monitorované kamerovým systémom so záznamom. Aktuálny obraz kamerového systému zo vstupu do sály je vyvedený na vrátnicu pre stálu službu. Obraz zo sály je k dispozícii oddeleniu bezpečnosti.

Samotná sála je rozdelená mrežami na bezpečnostné zóny, v ktorých sú podľa potreby umiestňované jednotlivé systémy.

3.2.1.3 Záložné dátové centrum

Pre časť informačných systémov prevádzkovaných v DataCentre je vytvorený aj záložný systém, ktorý je prevádzkovaný v záložnom dátovom centre formou housingu (umiestnenie vlastných systémov v priestoroch cudzieho dátového centra) - t.j. technologická infraštruktúra je zabezpečovaná formou služby. Záložné dátové centrum sa nachádza v lokalite mimo Bratislavy.

Systémová infraštruktúra

V záložnom dátovom centre je v súčasnosti umiestnená technická infraštruktúra pre IS RIS, IS ŠP, ITMS a systém Reuters, ktorá je postavená na identických platformách ako systémy v primárnom DC.

Infraštruktúra pre ukladanie dát

V záložnom DC je umiestnené jedno SAN diskové pole SUN 9990V s kapacitou cca 50TB, ktoré však bude v blízkej budúcnosti nahradené novým diskovým poľom značky HP.

Komunikačná infraštruktúra

Systémy záložného DC sú prepojené do siete Finnet 1 a 5HQ. Prostredníctvom dvoch dedikovaných liniek je realizované tiež priame prepojenie PDC a ZDC. Linky sú určené na zrkadlenie databáz (prostriedkami Oracle) a pre synchronizáciu systémov Citrix.

3.2.2 Súčasná a predpokladané využitie infraštruktúry DataCentra pre iné rezorty

Vzhľadom na to, že DataCentrum je vnímané ako rezortné integrované dátové centrum (RIDC), primárny poskytovateľ konsolidovaných IT služieb pre rezort MF SR, ostatné rezorty a samosprávu ako aj ich podriadené organizácie, dochádza už v dnešnej dobe k integrácii vybraných informačných systémov do DataCentra. V súčasnosti DataCentrum poskytuje nasledovné služby pre iné rezorty (organizácie).

- Zabezpečenie prevádzky informačných systémov SAP Ministerstva životného prostredia a Ministerstva dopravy výstavby a regionálneho rozvoja.
- Pre samosprávne kraje DataCentrum poskytuje prevádzku SAP portálu štátnej pokladnice (Košický, Nitriansky a Banskobystrický samosprávny kraj) a prevádzku účtovníctva samosprávneho kraja (Nitriansky a Banskobystrický samosprávny kraj). Zo strany MF SR je záujem postupne rozširovať služby prevádzky SAP portálu štátnej pokladnice a prevádzky účtovníctva a poskytovať ich ďalším samosprávnym krajom.
- Pre mestá a obce poskytuje DataCentrum dve základné aplikácie, ktoré vo finálnej fáze pokryjú približne 3 000 miest a obcí v SR a približne 3 000 organizácií miest a obcí v SR:
 - Rozpočtový informačný systém pre samosprávu (RIS.SAM) - v procese roll-outu na všetky mestá a obce (v súčasnosti prihlásených cca 400 obcí)
 - Jednotné účtovníctvo štátu (JÚŠ) - vo fáze pilotnej prevádzky na vybraných subjektoch samosprávy
- Hostovanie záložného systému ARDAL pre agentúru.
- Národné centrum zdravotníckych informácií (NCZI – v pôsobnosti Ministerstva zdravotníctva SR) v súčasnosti hľadá partnera pre prevádzku svojich informačných systémov pre poskytovateľov zdravotníckej starostlivosti v Slovenskej republike. Uvažuje sa s využitím DataCentra.

4 Bezpečnostná analýza

V rámci elektronizácie verejnej správy dochádza k nárastu vytvárania a spracúvania aj informácií strategického charakteru v elektronickej forme. Aktuálny stav zabezpečenia týchto informácií a s nimi spojených služieb jednotlivých IS nepokrýva všetky riziká. Treba si uvedomiť, že verejná správa sa zvyšovaním elektronizácie stále častejšie bude stávať obeťou útokov organizovaných i neorganizovaných hackerských skupín. Nedostatočné zabezpečenie IS, nedoriešené procesy riadenia a udržiavania informačnej bezpečnosti a nezáujem o problematiku tieto riziká zvyšujú. Závislosť elektronickej verejnej správy na funkčných a bezpečných službách IS bude časom narastať a bude si vyžadovať aj vyššie zabezpečenie týchto IS a údajov, ktoré sú v nich spracúvané.

Dôsledky nedostatočného riešenia informačnej bezpečnosti môžu byť veľmi široké a závažné, s celospoločenským negatívnym dopadom, napr.:

- únik citlivých finančných údajov strategického charakteru v dôsledku hackerského prieniku, alebo počítačovej infiltrácie s konečnými dôsledkami pre štát,
- oneskorenia pri strategických aktivitách inštitúcií verejnej správy v dôsledku nepripravenosti na úmyselne zapríčinené výpadky IS,
- neoprávnené zverejnenie citlivých údajov o občanoch,
- únik internej elektronickej korešpondencie zamestnancov obsahujúcej citlivé údaje a mnohé ďalšie.

Ako už bolo konštatované aj v iných štúdiách uskutočniteľnosti vo verejnej správe sú väčšinou prednostne nasadené informačné systémy pre podporu agend, ktorých výkon a spracovanie je priamo určené legislatívnymi normami, pričom využívanie IS v špecializovaných okruhoch ako aj ich centralizácia sa môže významne líšiť. Architektúra prevádzkovaných IS pritom nie vždy umožňuje komplexné riadenie informačnej bezpečnosti a v prípade kritických systémov zabezpečenie vysokej dostupnosti.

Aktuálna dekompozícia IS verejnej správy zvyšuje aj nároky a náklady na riešenie informačnej bezpečnosti. Služby súvisiace s riadením informačnej bezpečnosti ako aj samostatný výkon sa väčšinou deje pre každý IS autonómne a v rámci inštitúcie verejnej správy, ktorá za daný IS zodpovedá.

Požiadavky informačnej bezpečnosti, ktoré sa vzťahujú na projekt Centrálna služby dátového centra pre elektronizáciu verejnej správy sú v dvoch základných rovinách:

- požiadavky vyplývajúce z aplikovateľnej národnej legislatívy a medzinárodného štandardizačného rámca súvisiaceho s informačnou bezpečnosťou,
- požiadavky vyplývajúce z vecných a funkčných potrieb prípravy, vývoja a prevádzky predmetov projektov PO 1 OPIS.

4.1 Legislatívne východiská

Legislatívne a štandardizačné prvky obsahujú a agregujú široké spektrum požiadaviek informačnej bezpečnosti a pre potreby realizácie projektov PO 1 OPIS musia byť správne interpretované. Ide hlavne o nasledujúce zákony, normy a strategické dokumenty:

- Národná koncepcia informatizácie verejnej správy,
- Národná stratégia pre informačnú bezpečnosť v SR a úlohy Akčného plánu na roky 2008 až 2013,
- Zákon č.275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

- Výnos Ministerstva financií Slovenskej republiky č. 312/2010 Z. z. 9. júna 2010 o štandardoch pre informačné systémy verejnej správy,
- Oznámenie Komisie Európskemu parlamentu o „Ochrane Európy pred rozsiahlymi kybernetickými útokmi a narušeniami, zvyšovanie pripravenosti, bezpečnosti a odolnosti“ z roku 2009,
- Zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov,
- Zákon č. 215/2004 Z.z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov,
- Štandard STN ISO/IEC 27001 Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti,
- Štandard STN ISO/IEC 27002 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti,
- Štandard STN ISO/IEC 27005 Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti
- Bezpečnostná politika IS rezortu MF SR,
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.

4.2 Požiadavky informačnej bezpečnosti

Požiadavky informačnej bezpečnosti sú formálne definované legislatívnym a štandardizačným rámcom uvedeným vyššie. Jedná sa o nasledovné oblasti informačnej bezpečnosti:

- Politika bezpečnosti
- Organizácia bezpečnosti
- Klasifikácia a riadenie aktív
- Personálna bezpečnosť
- Fyzická bezpečnosť a bezpečnosť prostredia
- Riadenie komunikácií a prevádzky
- Riadenie prístupov
- Vývoj a nasadzovanie informačných systémov
- Zvládanie bezpečnostných incidentov
- Riadenie kontinuity procesov závislých od IS
- Súlad s požiadavkami

Vzhľadom na predmet štúdie sa bude potrebné venovať všetkým oblastiam, keďže predmetom štúdie je poskytovanie služieb dátového centra na centrálnej úrovni.

5 Identifikácia možností a príležitostí

5.1 Identifikácia možností využitia DataCentra pre projekty OPIS PO1

Vzhľadom na neustály a dynamický vývoj prostredia projektov OPIS PO1, bolo pri identifikácii možností a príležitostí využitia DataCentra pre projekty OPIS PO1 potrebné vytvoriť modelovú situáciu predpokladaného využitia centrálnych služieb dátového centra - t.j. umiestnenie IKT infraštruktúry vybraných projektov do centrálného dátového centra. Pri výbere projektov sa vychádzalo z posledného oficiálne schváleného rámca projektov OPIS PO1 ktorý je uvedený v dokumente Zoznam národných projektov Operačného programu Informatizácia spoločnosti na roky 2007 – 2013, (schválené 26.9.2011) a zodpovedajúcich dostupných štúdií uskutočniteľnosti a v nich uvedených informácií. Pri identifikácii projektov s potenciálom umiestnenia ich infraštruktúry do centrálného DC sa postupovalo podľa nasledovných kritérií:

Primárne boli pre začlenenie do centrálného DC uvažované projekty ktorých žiadateľom / prijímateľom je Ministerstvo financií SR, pri ktorých je najvyšší predpoklad umiestnenia ich IKT infraštruktúry v DataCentre. V ďalšom boli zahrnuté projekty s identifikovanými alebo rámcovými predpokladmi umiestnenia ich IKT infraštruktúry v priestoroch DataCentra (napr. Elektronizácia služieb zdravotníctva – zistenie z analýzy) alebo projekt Datacentrum miest a obcí (D-com), ktorý sám o sebe predstavuje umiestnenie IKT infraštruktúry v centralizovanom dátovom centre.

Ďalšími kandidátmi na prevádzku centrálnom DC boli projekty inštitúcií kde žiadateľ / prijímateľ nemá komplexne vybudovanú vhodnú infraštruktúru na zabezpečenie prevádzky (DC) z pohľadu zabezpečenie požadovanej dostupnosti a / alebo kontinuity alebo kde žiadateľ / prijímateľ realizuje málo projektov a vybudovanie zodpovedajúcej infraštruktúry by bolo výrazne ekonomicky neefektívne (napr. Elektronizácia služieb Sociálnej poisťovne – nemá k dispozícii záložné DC, NASES – dve vyťažené DC, a pod.)

Na druhej strane neboli uvažované projekty, ktorých žiadateľ má v súčasnosti vybudovanú zodpovedajúcu infraštruktúru na zabezpečenie prevádzky, prípadne sú po obsahovej a niekedy aj infraštruktúrnej stránke projekty viazané na existujúcu infraštruktúru IKT prevádzkovanú jestvujúcich dátových centrách. Z tohto dôvodu napríklad vôbec neboli zahrnuté projekty ktorých žiadateľom / prijímateľom je Ministerstvo vnútra SR. MV SR jednak disponuje vlastným primárnym aj záložným dátovým centrom pričom časť projektov predpokladá využitie existujúcej alebo spoločnej infraštruktúry, prípadne predstavuje rozšírenie prevádzkovaných systémov. Z pohľadu technického aj prevádzkového by preto boli predpoklady umiestňovania IKT infraštruktúry projektov OPIS PO1 v inom než vlastnom dátovom centre kontraproduktívne.

Obdobne je to napr. aj v prípade projektov ktorých žiadateľom / prijímateľom je Úrad geodézie, kartografie a katastra SR, ktorý disponuje novým (práve budovaným) záložným dátovým centrom a kde je z hľadiska informačného možné predpokladať úzku prepojenosť s existujúcimi systémami.

Vyššie uvedený výber jednotlivých projektov OPIS PO1, ktoré sú následne uvažované pre túto štúdiu, však nepredstavuje konečnú množinu informačných systémov u ktorých je možné predpokladať využitie služieb poskytovaných centrálnym dátovým centrom, ale predstavuje konzervatívny variant výberu, ktorý vytvára incializačné portfólio kandidátov pre poskytovanie služieb centrálnym DC. Poskytovanie týchto služieb je však možné následne rozširovať podľa aktuálnych potrieb žiadateľov / prijímateľov z oblasti projektov OPIS PO1 ale aj z iných oblastí verejnej správy - čo DataCentrum realizuje už v súčasnosti, pričom s predpokladaným rozširovaním poskytovania služieb je principiálne rátané aj pri návrhu riešenia.

Pri identifikácii technických a prevádzkových možností využitia DataCentra sa vychádzalo hlavne z očakávaných nárokov na technickú infraštruktúru projektov PO1 OPIS, u ktorých je možné predpokladať využitie služieb poskytovaných centrálnym dátovým centrom. Vzhľadom na stav rozpracovanosti jednotlivých projektov PO1 OPIS, relevantných pre túto analýzu, bolo pri identifikácii očakávaných požiadaviek na ich technickú infraštruktúru a služby dátových centier

možné primárne vychádzať len z informácií definovaných v štúdiách uskutočniteľnosti. Keďže predmetné štúdie prakticky vôbec neobsahujú informácie o technickom riešení jednotlivých projektov, ani požiadavky na ich technické zabezpečenie, bolo potrebné definovať očakávané nároky na technickú infraštruktúru projektov PO1 OPIS náhradným spôsobom a to v zmysle nižšie definovanej metodiky:

Architektúry IS v rámci týchto štúdií vychádzajú z architektúry Integrovaného informačného systému podľa NKIVS (Národná koncepcia informatizácie verejnej správy), ktorá je založená na princípoch SOA, ktoré sa aplikujú jednak pri integrácii medzi rôznymi (aj existujúcimi) ISVS ale aj pri budovaní nových systémov ISVS.

Na základe štandardizácie architektúry budovanej na princípoch SOA, rozsahu komplexnosti informačného systému (množstvo modulov a poskytovaná funkčnosť), požiadaviek na zabezpečenie kontinuity a prípadných ďalších predpokladov navrhovaného technického riešenia (napr. aplikácia virtualizácie, ...), je možné rámcovo špecifikovať rozsah požiadaviek informačného systému na jeho technické zabezpečenie. Špecifikácia týchto požiadaviek je založená na vzťažnej jednotke, ktorou je jeden „ dátový rozvádzač“, ktorá vyjadruje mieru požiadaviek na technické zabezpečenie IS a jej hodnota je definovaná v zmysle klasifikácie IS pre identifikáciu rámcových požiadaviek na ich technické zabezpečenie. Celkové rámcové požiadavky na technické zabezpečenie IS potom vychádzajú z celkového počtu dátových rozvádzačov špecifikovaných pre predmetný informačný systém v zmysle definovanej klasifikácie.

Klasifikácia IS pre identifikáciu rámcových požiadaviek na ich technické zabezpečenie

IS základného rozsahu – základné požiadavky

- Predpoklady
 - Komplexnosť - rozsah - 10 až 15 modulov
 - Aplikčná vrstva – umiestnenie vo virtualizovanom prostredí
 - Databázová vrstva – umiestnenie na databázovom clustri
 - Prevádzkové dáta – umiestnenie na diskovom poli triedy mid range
 - Zálohovanie dát – pásková knižnica triedy mid range
 - Všetky uvedené systémy v prevedení do dátového rozvádzača
- Nároky
 - 2 x dátový rozvádzač pre produkčné / testovacie prostredie
 - + 1 x dátový rozvádzač, v prípade že nebude aplikovaná virtualizácia

Zvýšenie základných požiadaviek – rozsah systému

- Predpoklady
 - Väčší rozsah modulov – zvýšené požiadavky na výpočtový výkon
 - Aplikácia väčšieho počtu serverov prípadne, aplikácia serverov triedy enterprise (samostatne stojace systémy)
- Nároky
 - + 2 x dátový rozvádzač – pre primárne DC
 - + 1 x dátový rozvádzač – pre záložné DC

Zvýšenie základných požiadaviek – uloženie prevádzkových dát

- Predpoklady

- Zvýšené množstvo prevádzkových dát – zvýšené požiadavky na dátový priestor / predpoklady zvyšovania požiadaviek do budúcnosti
- Aplikácia väčšieho počtu diskov (diskových políc), prípadne aplikácia diskových systémov triedy enterprise (samostatne stojace systémy)
- Nároky
 - + 2 x dátový rozvádzač / priestor pre dátový rozvádzač (samostatne stojace systémy)

Zvýšenie základných požiadaviek – uloženie zálohovaných dát / dlhodobé uloženie dát

- Predpoklady
 - Zvýšené množstvo zálohovaných dát – zvýšené požiadavky na dátový priestor / predpoklady zvyšovania požiadaviek do budúcnosti
 - Aplikácia páskových knižníc triedy enterprise prípadne, aplikácia dodatočných diskových systémov
- Nároky
 - + 1 až 2 x dátový rozvádzač / priestor pre dátový rozvádzač (samostatne stojace systémy) – podľa charakteru a predpokladaných požiadaviek informačného systému

Zabezpečenie kontinuity činností prostredníctvom záložného DC

- Predpoklady
 - Umiestnenie systémov v záložnom dátovom centre
- Nároky
 - Nároky pre umiestnenie serverových systémov v záložnom dátovom centre nemusia byť identické ako pre primárne dátové centrum (napr. nebudú obsahovať infraštruktúru pre školiace a testovacie systémy). V záložnom DC sa predpokladá umiestnenie páskového systému len v špecifických prípadoch - podľa charakteru a predpokladaných požiadaviek informačného systému.

Prevádzkové požiadavky

V zmysle koncepcie budovania ISVS podľa NKIVS a aj charakteru poskytovaných e-služieb sa ráta s dostupnosťou systémov 24 hodín denne, 7 dní v týždni.

5.1.1 Národný projekt CEP

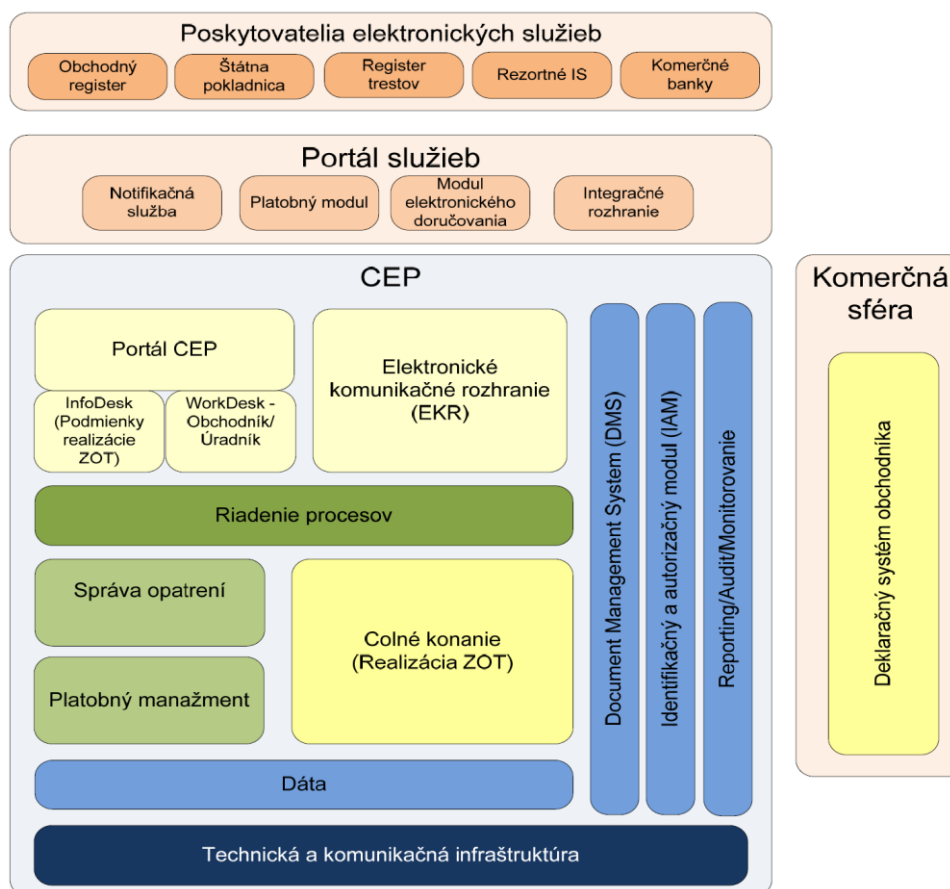
5.1.1.1 Funkcionalita

Projekt CEP má zabezpečiť elektronizáciu a automatizáciu procesov medzinárodného obchodu a zaviesť elektronické služby pre centrálnu správu a riadenie medzinárodných obchodných transakcií. Služby budú realizované prostredníctvom informačného systému ktorý umožní zaslanie unifikovaného elektronického dokumentu vývozcu/dovozcu/prepravcu na jediné miesto v štátnej správe na úplné vybavenie administratívy a povolení pre zahraničnú obchodnú transakciu (ZOT).

5.1.1.2 Architektúra

Rámcová architektúra systému CEP s jeho základnými modulmi je znázornená na nasledovnom obrázku:

Obrázok 2 – Architektúra systému CEP



Architektúra systému CEP obsahuje nasledovné hlavné moduly:

- **Portál CEP**
 - Predstavuje vstupný bod pre komunikáciu s používateľmi systému CEP
- **InfoDesk**
 - Slúži na interaktívne zadávanie ZOT
 - Pre nových používateľov umožní zadať požiadavku na registráciu nového obchodníka.
- **WorkDesk – Obchodník / Úradník**
 - Zabezpečuje komunikáciu s obchodníkom / úradníkom - priamo cez webové rozhranie alebo komunikuje s informačným systémom obchodníka (primárne pomocou technológie webových servisov cez modul Riadenie procesov).
- **Elektronické komunikačné rozhranie (EKR)**
 - Rieši výmenu elektronických dokumentov medzi systémom CEP a jeho okolím s pomocou modulu Riadenia procesov. Podľa potreby overuje platnosť zaručeného elektronického podpisu (ZEP) žiadateľa.
- **Správa opatrení**
 - Zabezpečuje správu opatrení pre systém CEP a ich pravidelný import zo systémov Colnej správy SR.
- **Riadenie procesov**

- Zabezpečuje dva typy úloh - samotné riadenie procesov a komunikačné a integračné rozhranie.
- Platobný manažment
 - Zabezpečuje manažment parametrov správnych poplatkov a zbiera a poskytuje aj informácie o úhrade správnych poplatkov.
- DMS / Dáta
 - Poskytuje úložisko pre štruktúrované dáta (databáza) a neštruktúrované dáta (elektronické dokumenty) pre moduly CEP.
- Reporting / audit / monitorovanie
 - Umožňuje vytváranie výstupných zostáv nad údajmi systému CEP.
 - Zabezpečuje jednotné zaznamenávanie všetkých dôležitých udalostí v systéme a zber dát pre ich následné vyhodnocovanie a audit.
- Identifikačný a autorizačný modul
 - Zabezpečuje jednotnú autentifikáciu a autorizáciu používateľov v rámci systému CEP a ostatných systémov (napríklad informačné systémy Colnej správy SR) a slúži na určenie prístupových práv v rámci systému CEP.
- Administračný modul
 - Slúži na nastavenie parametrov systému, audit a monitorovanie systému.

5.1.1.3 Predpokladané technické riešenie

Pre informačný systém CEP sa predpokladá vytvorenie nasledovných prostredí:

- Prevádzkové
 - Slúži na produkčnú prevádzku, umiestnené je v primárnom dátovom centre (DC).
- Záložné prevádzkové
 - Aplikačne je totožné s prevádzkovým prostredím. Zabezpečuje kontinuitu prevádzky, umiestnené je v záložnom DC.
- Stabilizačné + Školiace + Testovacie
 - Slúžia na pred produkčné testovanie, školenia používateľov a testovanie zmien a nových funkcií.

Pre implementáciu systému sa ráta s aplikáciou virtualizácie.

Predpokladá sa umiestnenie systému CEP v DataCentre.

5.1.1.4 Rámcové požiadavky na technické zabezpečenie

Informačný systém CEP je možné v zmysle definovanej klasifikácie komplexnosti špecifikovať ako systém základného rozsahu, so zabezpečením kontinuity činností prostredníctvom záložného DC.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 2 x dátový rozvážač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - 2 x dátový rozvážač – pre kompletnú infraštruktúru IKT

5.1.2 Elektronické služby Finančnej správy I. oblasť daňová (program UNITAS)

5.1.2.1 Funkcionalita

Cieľom programu UNITAS je zabezpečiť zjednotenie výberu daní, ciel a odvodov prostredníctvom budúcej Finančnej správy. Program je rozdelený na dve fázy - UNITAS I., ktorého súčasťou je reforma (zjednotenie) daňovej a colnej správy. Druhá fáza UNITAS II. sa následne venuje zjednoteniu výberu daní, cla a poistných odvodov. V rámci projektu Elektronické služby Finančnej správy I. sa predpokladá osem podprojektov v nasledovných oblastiach:

- optimalizácia HW vybavenia a optimalizácia informatickej podpory DR SR – projekt SALA,
 - účelom tohto projektu je analyzovať existujúce obmedzenia existujúceho HW vybavenia výpočtového centra DRSR, návrh a zaobstaranie nového HW vybavenia a priestorové znovu usporiadanie existujúcich HW zariadení,
- analýza súčasného stavu DO SR a návrh reštrukturalizácie k stavu podľa legislatívy účinnej k 1.1.2012 – podpora reformy organizácie a organizačnej zmeny,
- konsolidácia existujúcich informačných systémov DR SR – Projekt KONS IS,
- návrh systému zjednoteného výberu daní, cla a poistných odvodov – Projekt UNITAS Knižka,
- návrh základných princípov a harmonogramu tvorby organizačnej štruktúry FS SR – Projekt REF FS (forma TAS),
- integrovaný systém Finančnej správy – Správa daní – projekt ISFS-SD (Pilot),
- bezpečnosť projektov UNITAS – Projekt BPU,
 - realizácia a implementácia princípov a postupov informačnej bezpečnosti v rámci projektov programu UNITAS,
 - realizácia a implementácia princípov a postupov informačnej bezpečnosti do jednotlivých prevádzkovaných a novovybudovaných systémov budúcej Finančnej správy,
- elektronické služby DR SR a CR SR – Projekt Portál Finančnej správy,
 - vytvoriť funkčné a technické predpoklady pre postupné rozširovanie elektronických služieb pre klientov Finančnej správy v oblasti výberu sociálnych a zdravotných odvodov.

5.1.2.2 Architektúra

Riešenie informačného prostredia finančnej správy má byť postavené na servisne orientovanej architektúre (SOA), s dôrazom na modelovanie obchodných procesov a interoperabilitu. Z hľadiska konceptuálnej architektúry Informačného prostredia FS v daňovej oblasti sú definované nasledovné základné komponenty:

- Portál Finančnej správy – zabezpečujúci prístup k elektronickým službám v daňovej oblasti pre externé a interné subjekty. Súčasťou portálu je aj elektronická podateľňa pre spracovanie dokumentov podpísaných elektronickým podpisom,
- Integračná platforma – bude systémom pre integračné prepojenie komponentov na báze webových služieb medzi sebou navzájom, voči back-office systémom v daňovej oblasti a tiež zabezpečí integráciu s IS VS ostatných povinných osôb a modulmi eGovernmentu (keď budú vybudované),
- Štandardizovaný daňový informačný systém – je jadrom celého riešenia a základným komponentom, ktorý spája manažment vzťahov s daňovými subjektmi, register daňovníkov, správu a procesy konaní a saldokonto,
- Systém jednotného výberu daní a poplatkov – predstavuje integrované riešenie schopné spracovať procesy platieb.

5.1.2.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Zavedenie novej generácie elektronických služieb pre daňovú oblasť si však vyžiada reorganizáciu a konsolidáciu existujúcej IT infraštruktúry a prípadné sústredenie prevádzky IT infraštruktúry (servery, sieťové prvky, personálna obsluha) na jedno miesto, ktoré bude obsluhovať všetky organizácie finančnej správy. Pri konsolidácii aplikácií a serverov sa predpokladá nasadenie virtualizačných technológií. Bude tiež potrebné zabezpečiť technickú infraštruktúru testovacích prostredí s dostatočnou kapacitou, aby testovanie zmien existujúcich systémov alebo zavedenie nových informačných systémov neovplyvňovalo funkčnosť prevádzkového prostredia.

5.1.2.4 Rámcové požiadavky na technické zabezpečenie

Aj keď sú definované len základné moduly riešenia, vzhľadom na zabezpečovanú funkčnosť je možné predpokladať, že pôjde o robustný informačný systém, kde je možné definovať požiadavky pre každý modul ako pre samostatný informačný systém. Na úrovni IS ako celku sa už predpokladá optimalizácia rozmiestnenia komponentov v jednotlivých dátových rozvádzačoch.

- Portál Finančnej správy
 - rozšírený systém, bez zvýšených požiadaviek na uloženie dát
- Integračná platforma
 - systém základného rozsahu
- Štandardizovaný daňový informačný systém (ŠDIS)
 - rozšírený systém, so zvýšenými požiadavkami na uloženie dát a zálohovanie (v záložnom DC je uvažovaná pásková knižnica), diskový systém je zdieľaný s IS jednotného výberu daní a poplatkov
- Systém jednotného výberu daní a poplatkov
 - rozšírený systém, so zvýšenými požiadavkami na uloženie dát, požiadavky na zálohovanie sú rátané v rámci ŠDIS, diskový systém je zdieľaný s ŠDIS

Identifikácia rámcových požiadaviek na technické zabezpečenie - Portál Finančnej správy

- Požiadavky na primárne DC
 - 2,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - 1,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT

Identifikácia rámcových požiadaviek na technické zabezpečenie – Integračná platforma

- Požiadavky na primárne DC
 - 1,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - o 0,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT

Identifikácia rámcových požiadaviek na technické zabezpečenie - ŠDIS

- Požiadavky na primárne DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1,5 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové systémy

- Požiadavky na záložné DC
 - 2 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1,5 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové systémy

Identifikácia rámcových požiadaviek na technické zabezpečenie - Systém jednotného výberu daní a poplatkov

- Požiadavky na primárne DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1,5 x dátový rozvádzač – pre diskové úložné systémy
- Požiadavky na záložné DC
 - 2 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1,5 x dátový rozvádzač – pre diskové úložné systémy

Identifikácia rámcových požiadaviek na technické zabezpečenie - spolu

- Požiadavky na primárne DC
 - 13 x dátový rozvádzač
- Požiadavky na záložné DC
 - 10 x dátový rozvádzač

5.1.3 Datacentrum miest a obcí (DCOM)

5.1.3.1 Funkcionalita

Cieľom projektu je vytvoriť čo najlepšie podmienky na urýchlenie procesu informatizácie obecnej správy. Predmetom projektu je vytvorenie unifikovaných SW riešení potrebných pre obecnú správu, ktoré budú poskytované ako služba zo špecializovaného Datacentra obcí a miest – v skratke DCOM (prípadne Datacentrum miest a obcí – DCMO).

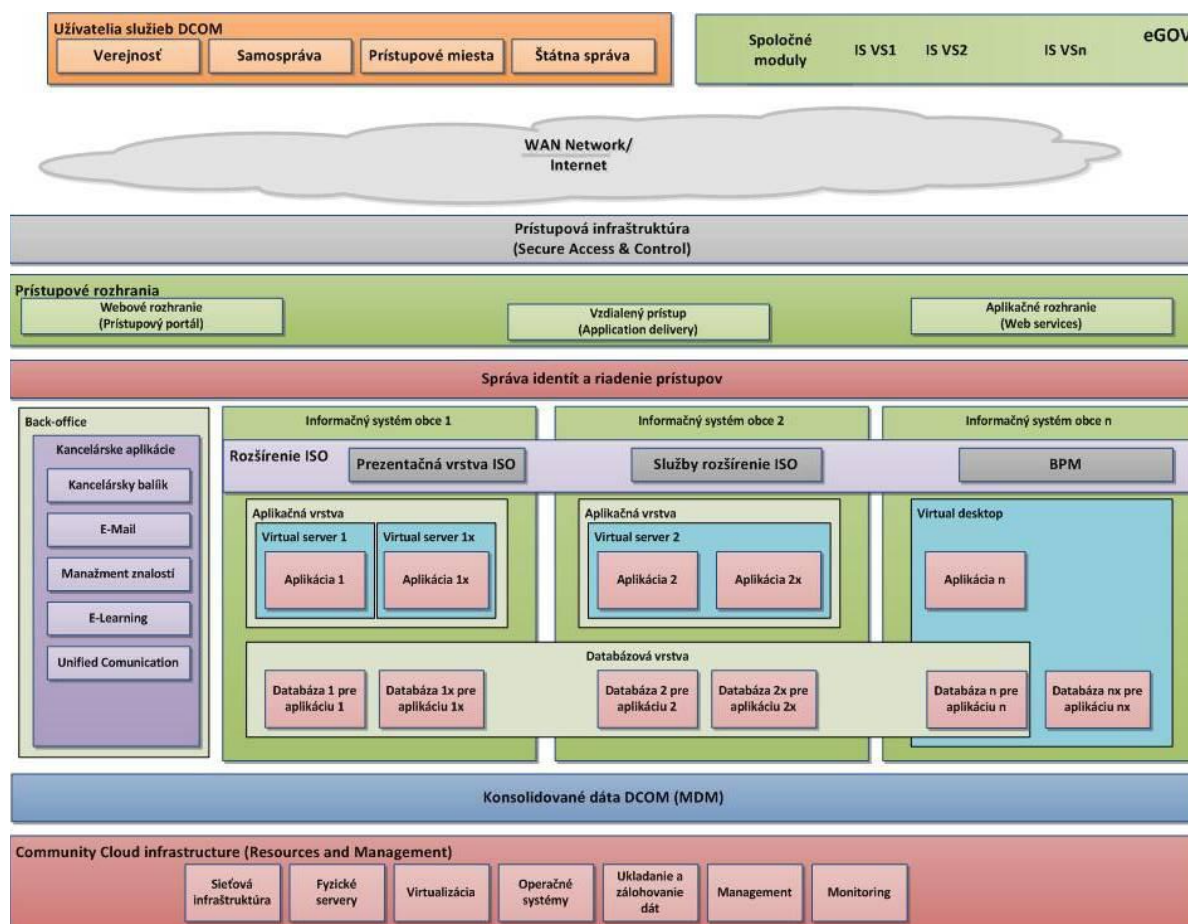
5.1.3.2 Architektúra

Celková architektúra DCOM predpokladá využitie niektorých existujúcich systémov, spolu s aplikáciou systémov nových:

- pôvodné aplikácie samospráv (ISO) so zachovaním pôvodného front-endu, prezentačnej vrstvy pre pracovníkov samospráv, vrstvy web služieb (doplnenie pôvodného ISO),
- rozšírenie ISO, predstavuje riešenie web služieb na úrovni DCOM, prezentačnej vrstvy pre verejnosť, procesného manažmentu typu BPM (integrácia riadenie procesov) a lokálneho DCOM riešenia identifikácie a prístupu typu IAM,
- dátovej (databázovej) konsolidovanej vrstvy typu MDM,

Na nasledujúcom obrázku je základná technická architektúra riešenia v rozdelení na jednotlivé vrstvy:

Obrázok 3 – Základná technická architektúra riešenia DCOM



Prístupová infraštruktúra

- Prístupová infraštruktúra bude zabezpečovať bezpečné pripojenie verejnosti, samospráv, prístupových miest a štátnej správy. Cez túto vrstvu sú poskytované všetky potrebné služby pre správne fungovanie prístupových rozhraní a ich bezpečné publikovanie (napr. PKI systém).

Prístupové rozhrania

- Prístupové rozhrania sú určené pre prístup k riešeniu DCOM. Používatelia služieb budú prístupovať na základe pravidiel definovaných v systéme správy identít a prístupov. Medzi prístupové rozhrania patria:
 - prístupový portál – umožňuje bezpečný prístup používateľov (verejnosť, pracovníci samospráv, IOM) k aplikáciám DCOM prostredníctvom webového prehliadača,
 - vzdialený prístup – umožňuje pomocou bezpečného klienta samosprávam prístup k DCOM,
 - aplikačné rozhranie - zabezpečuje komunikáciu a integráciu informačných systémov DCOM, komunikáciu s ISVS a spoločnými modulmi eGov cez štandardné aplikačné rozhranie.

Správa identít a riadenie prístupov

- Zabezpečuje centrálnu správu identít používateľov a je používaná ostatnými vrstvami DCOM a aplikáciami pre potreby autentifikácie užívateľov a ich autorizáciu na prístup k jednotlivým funkciám. Tento komponent môže byť neskôr integrovaný s centrálnym systémom IAM.

Aplikačná vrstva

- Aplikačná vrstva sa skladá z dvoch hlavných častí:
 - pôvodné aplikačné programové vybavenie rozšírené o elektronické služby zodpovedajúce danej aplikácii,
 - nová spoločná vrstva pre všetky ISO pripojené do DCOM nazvaná Rozšírenie ISO. Hlavné komponenty tvoria: prezentačná vrstva, vrstva služieb samospráv a modul BPM.

Dátová vrstva (MDM)

- Vrstva je zložená z databáz jednotlivých aplikácií samospráv a konsolidovaných údajov DCOM.

BackOffice vrstva

- Slúži na podporu výkonu samospráv. Jedná sa hlavne o prevádzku kancelárskych aplikácií typu kancelársky balík, mail, manažment znalostí, vzdelávanie a iné.

Vrstva zdrojov (Resources and Management)

- Vrstva obsahuje komponenty fyzickej architektúry, virtualizačné nástroje, operačné systémy, zálohovanie a manažment uvedených zdrojov.

5.1.3.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Pri centralizovaných systémoch sa predpokladá aplikácia 3 vrstvovej architektúry klient – server a využitie virtualizácie.

5.1.3.4 Rámcovém požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých aplikácií je možné pre systém definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie dát. Pásková knižnica v záložnom DC nie je uvažovaná.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy

5.1.4 Elektronizácia služieb VÚC

5.1.4.1 Funkcionalita

Cieľom projektu je zaviesť vybrané elektronické služby (eGov služby) poskytovaných regionálnou samosprávou pre potreby verejnosti – najmä občanom a podnikateľským subjektom. Služby budú realizované prostredníctvom elektronizácie vybraných životných situácií, ktoré predstavujú uskutočnenie kontaktu medzi občanmi (podnikateľskými subjektmi) a verejnou správou.

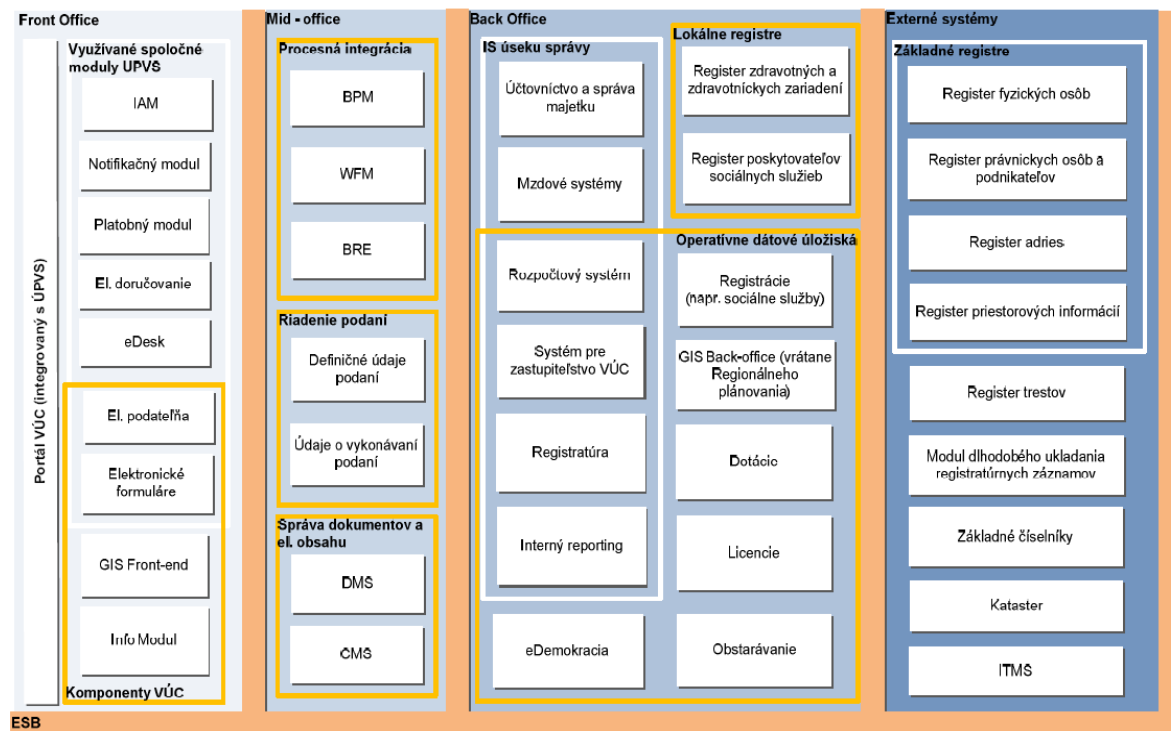
5.1.4.2 Architektúra

Architektúra informačných systémov VÚC je založená na referenčnej architektúre VÚC. O danej architektúre sa hovorí ako o referenčnej z dôvodu, že sa predpokladá autonómna implementácia eGovernmentu na úrovni každej VÚC. Avšak vzhľadom na to že kompetencie, povinnosti a teda v

konečnom dôsledku aj ponúkané eGov služby sú navzájom medzi VÚC rovnaké, mala by byť rovnaká aj cieľová architektúra pre jednotlivé VÚC. Rozdiely medzi jednotlivými VÚC sa pravdepodobne prejavajú na úrovni back-office aplikácií.

Definovaná referenčná architektúra je popisovaná v štyroch hlavných vrstvách, a je znázornená na nasledujúcom obrázku:

Obrázok 4 – Referenčná architektúra IS VÚC



Front-office

▪ Komponenty VÚC

- Portál - je základným komponentom vrstvy front-office, ktorý je prostriedkom pre zabezpečenie používateľského rozhrania tak voči verejnosti (občanom a podnikateľom), ako aj voči zamestnancom VÚC.
- Info Modul - v úzkej spolupráci s modulmi CMS a Správa podaní – prípadov umožňuje štruktúrovaný pohľad na ponúkané služby VÚC, priamo integrovaný s produkčnými definíciami služieb v systéme Správa podaní – prípadov.
- Elektronické formuláre - modul pre Elektronické formuláre pozostáva z dvoch častí - Samotný eForm modul tak ako je definovaný v NKIVS a rozšírenie pre Elektronické formuláre modulu pre potreby VÚC.
- GIS Front-end - je časť používateľského rozhrania, ktorá umožňuje vizualizáciu určitých informácií pomocou ich geopriestorového zobrazenia.

▪ Komponenty UPVS

- Vybrané komponenty ÚPVS - sú samostatné riešenia, ktoré VÚC budú využívať z dôvodov efektívneho vynakladania prostriedkov na realizáciu samostatných riešení a poskytnutia jednotného prístupu k funkcionalitám, ktoré sú ponúkané verejnou správou.

Mid-office

▪ Procesná integrácia

- Riadenie podaní
- Správa dokumentov a elektronického obsahu

Back-office

- IS úsekov správy VÚC
- Lokálne registre
- Operatívne dátové úložiská

Externé systémy

- Základné registre
- Iné externé systémy

5.1.4.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Popri existujúcich informačných systémoch na podporu konkrétnych úsekov správy a portálu VÚC, ktoré sú v aktuálnom stave prítomné v architektúre VÚC sa však predpokladá vybudovanie úplnej architektúry pre eGov služby založenej na princípoch SOA. Na základe toho vzniknú požiadavky na zabezpečenie zdieľaných dátových úložných kapacít, integráciu vzniknutých komponentov a infraštruktúry na poskytovanie elektronických služieb.

5.1.4.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých modulov je možné pre systém definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie dát. Pásková knižnica v záložnom DC nie je uvažovaná.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy

5.1.5 Ústredný portál verejnej správy (ÚPVS)

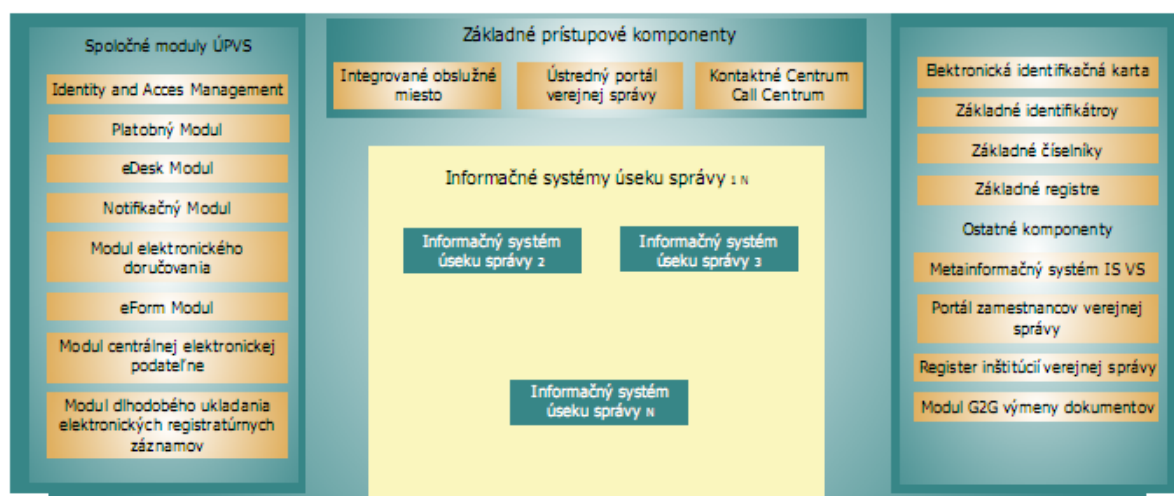
5.1.5.1 Funkcionalita

Cieľom projektu ÚPVS je zabezpečiť prístup a poskytovanie informácií o službách VS, vyhľadávanie informácií podľa životnej situácie alebo kľúčových slov a navigáciu k eGov službám podľa voľby používateľa.

5.1.5.2 Architektúra

Jednotlivé komponenty systému ÚPVS v prostredí rámcovej architektúry integrovaného informačného systému verejnej správy (IISVS) je znázornená na nasledovnom obrázku:

Obrázok 5 – Architektúra systému ÚPVS v prostredí IISVS



Architektúra ÚPVS obsahuje nasledovné hlavné moduly:

Spoločné moduly ÚPVS:

- Identity and Access management
 - Služi na identifikáciu a autentifikáciu používateľov eGov služby.
- Platobný modul
 - Zabezpečuje realizáciu platieb za spoplatnené eGov služby.
- eDesk
 - Zabezpečuje jednotnú evidenciu e-komunikácie medzi používateľom a verejnou správou
 - Zabezpečuje systém hodnotenia spokojnosti príjemcu služby s kvalitou jej poskytnutia
 - Umožňuje štatistické vyhodnocovanie kvantitatívnych a kvalitatívnych ukazovateľov poskytovaných služieb
- Notifikačný modul
 - Zabezpečuje centrálné riešenie na zasielanie informácií (notifikácií) prostredníctvom SMS správ, prípadne prostredníctvom iného elektronického komunikačného kanála
- Modul Elektronické doručovanie
 - Umožňuje zasielanie a preberanie elektronických dokumentov spolu s funkcionalitu zabezpečujúcou vytvorenie potvrdenia o doručení, respektíve o nedoručení dokumentu
- eForm modul
 - Zabezpečuje jednotný prístup používateľov, štandardné používateľské rozhranie a integráciu s ostatnými spoločnými modulmi
- Modul centrálnej elektronickej podateľne
 - Centrálna elektronická podateľňa (CEP) tvorí jeden zo základných modulov architektúry integrovaného ISVS definovanej v rámci NKIVS. Použitie CEP je prierezové – je využívaná vo všetkých elektronických službách verejnej správy, ktoré sú viazané na použitie zaručeného elektronického podpisu (ZEP), resp. vyžadujú spracovanie elektronického podania prostredníctvom CEP.
 - Zabezpečuje overenie elektronického podpisu prijatého podania a vystavenie potvrdenia o prijatí e-formulára, resp. elektronického dokumentu.

- Modul dlhodobého ukladania elektronických registratúrnych záznamov
 - Zabezpečuje trvalú čitateľnosť ukladaných elektronických registratúrnych záznamov za pomoci ukladania záznamov aj vo formáte určenom na dlhodobé uloženie.
 - Zabezpečuje udržiavanie platnosti elektronického podpisu ukladaných elektronických registratúrnych záznamov
 - Zabezpečuje integritu obsahu elektronických registratúrnych záznamov.

Základné prístupové komponenty:

- Kontaktné centrum (KC)
 - Predstavuje základný centrálny prístupový a komunikačný komponent medzi verejnosťou (občanom) a budovaným integrovaným informačným systémom verejnej správy pre vzdialených účastníkov. Pod vzdialeným účastníkom sa rozumie občan, ktorý nie je fyzicky prítomný na mieste poskytovania danej služby. Zameraný na vytvorenie prístupového subjektu pre vzdialených účastníkov prednostne pomocou hlasového kanálu.
- Integrované obslužné miesto (IOM)
 - IOM predstavuje prístupový a komunikačný komponent medzi verejnosťou (občanom) a budovaným integrovaným informačným systémom verejnej správy pre občanov, ktorí osobne prídu na pracovisko IOM (na rozdiel od KC, kde je prístup vzdialený).
- Ústredný portál verejnej správy (ÚPVS)
 - ÚPVS je hlavným bodom pre vstup do systému portálov VS a predstavuje dvojúrovňový systém portálov, tvorený samotným ÚPVS a portálmi druhej úrovne, tzv. portálmi úsekov správy prislúchajúcimi jednotlivým inštitúciám VS. Portály úsekov správy poskytujú detailnejšie informácie a môžu umožňovať realizáciu služieb jednotlivých vecných agend na danom úseku správy resp. úsekoch správy.

5.1.5.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Cieľová technická architektúra ÚPVS vrátane spoločných modulov ÚPVS bude čiastočne využívať existujúcu architektúru portálu. V rámci projektu bude potrebné obstaranie ďalšieho technického vybavenia pre sprevádzkovanie služieb ÚPVS.

5.1.5.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých aplikácií je možné pre systém definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie dát (dlhodobé ukladanie registratúrnych záznamov). Pásková knižnica v záložnom DC nie je uvažovaná.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy

5.1.6 Elektronické služby Štatistického úradu SR

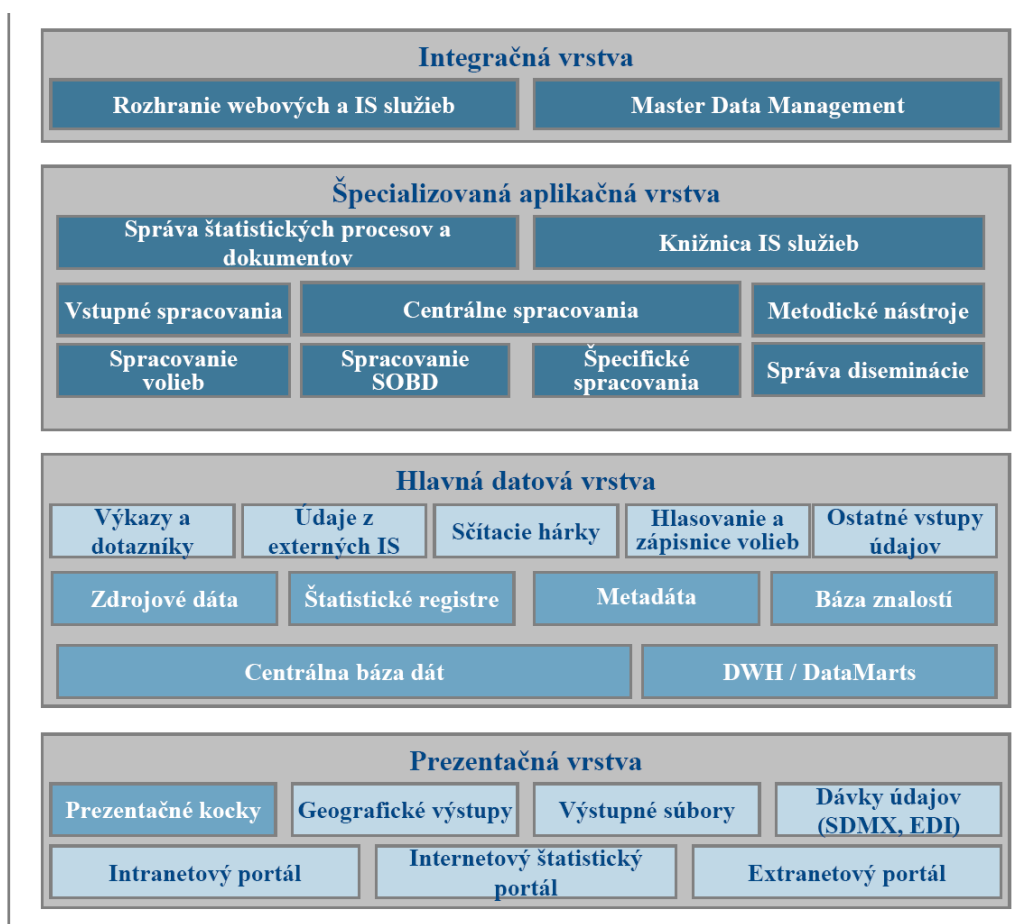
5.1.6.1 Funkcionalita

Cieľom projektu je zavedenie elektronických služieb ktoré na jednej strane znížia administratívne zaťaženie štatistických spravodajských jednotiek pomocou plnej elektronizácie zberu údajov pre všetky typy štatistických zisťovaní a na druhej strane poskytnú občanovi jednoduchý a prehľadný prístup k štatistickým informáciám a zjednodušenie úkonov súvisiacich s poskytovaním zdrojových údajov v roli respondenta. V oblasti volieb a elektronizácie ich procesov sa jedná o postupné kroky prvej etapy elektronizácie služieb spracovávaní volebných výsledkov vedúcich ku komplexným elektronickým voľbám. Služby budú realizované prostredníctvom elektronizácie vybraných životných situácií.

5.1.6.2 Architektúra

Architektúra Integrovaného štatistického informačného systému (IŠIS) so základnými komponentmi a v rozdelení do jednotlivých vrstiev je na nasledovnom obrázku:

Obrázok 6 – Architektúra IŠIS



Prezentačné komponenty

- Internetový štatistický portál – bude slúžiť na prístup k štatistickým údajom pre občanov a podnikateľov
- Extranetový portál – bude slúžiť na prístup k štatistickým údajom pre inštitúcie verejnej správy
- Intranetový portál – bude slúžiť na prístup k štatistickým údajom pre zamestnancov ŠÚ SR

Integračné komponenty

- Rozhranie Webových a IS služieb - zabezpečí prepojenie IŠIS na integrovaný ISVSa prezentačné komponenty ŠÚ SR
- Master Data Management – bude poskytovať sadu procesov a nástrojov, ktoré zabezpečia definovanie a riadenie referenčných dát pri ich zbieraní, validácii, agregáciách, priradení, konsolidácii, zaistení ich kvality, uchovávaní a distribúcii.

Špecializované komponenty

- Správa štatistických procesov a dokumentov – bude podporovať realizáciu štatistických procesov a dokumentov potrebných pre zber a spracovanie dát a prezentáciu štatistických údajov.

Štatistický informačný systém

- Knižnica IS služieb – bude obsahovať jednotlivé moduly IS služieb podporujúce definované eGov služby úradu a využívané eGov služby ISVS.
- Príprava a zber údajov – funkcie ŠIS podporujúce tento blok budú zamerané na využitie služieb IS a eGov služieb pre zber štatistických údajov v rámci štatistických zisťovaní, preberanie údajov z administratívnych zdrojov, zber a spracovanie údajov z volieb a SOBD, ako aj načítanie vstupných údajov a metadát z iných zdrojov.
- Správa metadát – tento blok bude obsahovať rozhodujúce nástroje pre vytváranie a aktualizáciu metadát.
- Centrálne spracovanie štatistických údajov – tento blok bude zameraný na realizovanie výpočtov základných a odvodených ukazovateľov podľa stanovených, agregácií s uložením do PBD centrálnej bázy dát. Taktiež bude poskytovať nástroje, umožňujúce vykonávanie analýz a výstupov v dohodnutých formách nad dátovými kockami.

5.1.6.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Pre prevádzkovanie požadovaných služieb však bude nutné vytvoriť nové technické a technologické zabezpečenie, pričom sa predpokladá nasadenie kombinácie technológie virtualizácie a technológie clustrov a bezpečnej infraštruktúry pre ukladanie dát. Predpokladá sa vytvorenie dvoch centrálnych vysoko dostupných a geograficky oddelených dátových centier a tretieho geograficky oddeleného zálohovacieho pracoviska.

Vybudovanie novej infraštruktúry bude vyžadovať rekonštrukciu alebo úpravu existujúcich priestorov IS ŠÚ SR.

5.1.6.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých modulov a rozsahu funkčnosti je možné pre systém definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie dát. Pásková knižnica v záložnom DC nie je uvažovaná. Uvažované je zálohovacie DC, kde je umiestnená pásková knižnica a 1 dátový rozvádzač.

Identifikácia rámcových požiadaviek na technické zabezpečenie

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy

- Požiadavky na záložné DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
- Požiadavky na zálohovacie DC
 - 1 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre páskové úložné systémy

5.1.7 Elektronické služby Sociálnej poisťovne

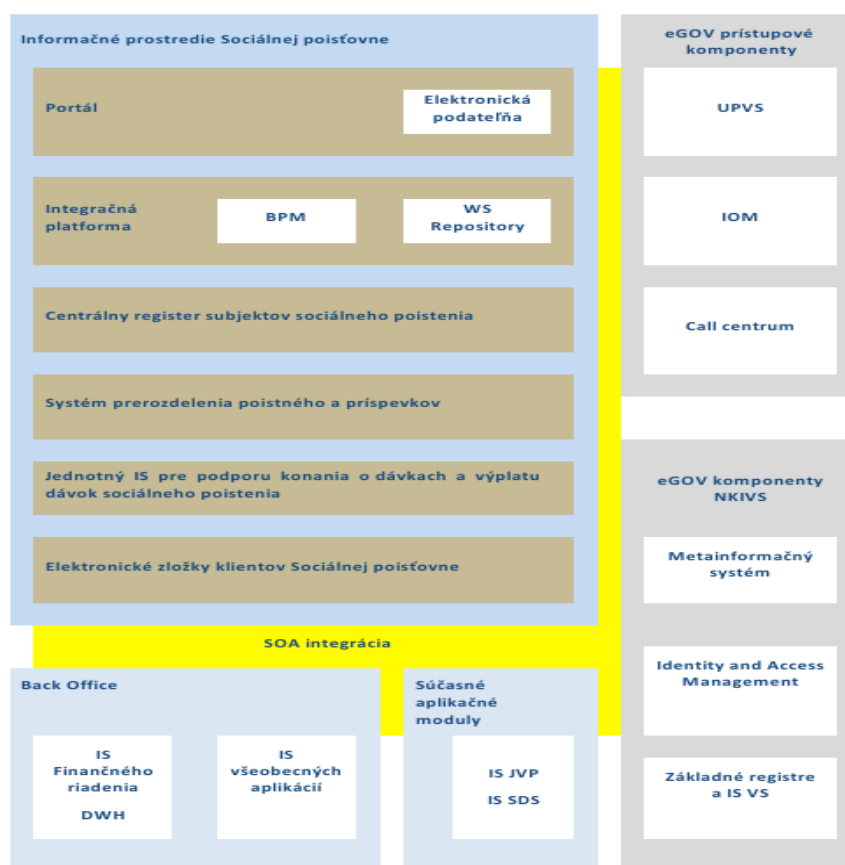
5.1.7.1 Funkcionalita

Cieľom projektu je vybudovanie komplexného informatického riešenia, ktoré zabezpečí realizáciu agendy Sociálnej poisťovne prostredníctvom elektronických služieb. V cieľovom stave bude výber poistného prebiehať v prostredí elektronickej komunikácie s klientom na báze automatizácie konaní. Budú centralizované a harmonizované registre SP a vzájomne integrované informačné systémy SP. Finančné toky sa budú jednoznačne evidovať vo väzbe na jednotlivé subjekty sociálneho poistenia a príslušné fondy. Požiadavky klientov a platby sociálnych dávok budú prebiehať elektronicky.

5.1.7.2 Architektúra

Konceptuálna architektúra informačného systému Sociálnej poisťovne so základnými komponentmi je na nasledovnom obrázku:

Obrázok 7 – Koncept architektúry IS SP



Centrálny register subjektov sociálneho poistenia - centralizácia a integrácia registrov SP

- CRSSP bude zjednocujúcim a prierezovým systémom, ktorý na jednom mieste zabezpečí centralizovanú správu a evidenciu všetkých relevantných údajov (identifikačné údaje, údaje o postavení v systéme sociálneho poistenia a ďalšie údaje nevyhnutné pre výkon sociálneho poistenia) viažucich sa k subjektom systému sociálneho poistenia.
- Špecifickou nadstavbovou časťou systému CRSSP je dátový sklad.

Systém prerozdelenia poistného a príspevkov na starobné dôchodkové sporenie – nahradenie súčasných procesov výberu poistného vo väzbe na program UNITAS

- Náhrada súčasných informačných systémov SP podporujúce výber poistného, správu pohľadávok a starobné dôchodkové sporenie budú nahradené integrovaným riešením elektronických služieb zabezpečujúcich plnenie úloh SP vo väzbe na pripravovanú reformu zjednotenia výberu daní, cla a odvodov – program UNITAS.

Jednotný IS pre podporu konania o dávkach a výplatu dávok sociálneho poistenia - zjednotenie a integrácia dávkovej agendy sociálneho poistenia

- Náhrada súčasného heterogénneho agendovo orientovaného prostredia dávkových systémov sociálneho poistenia jednotným IS pre podporu konania o dávkach a výplatu dávok sociálneho poistenia.

Systém elektronických zložiek klientov- integrácia spracovania podkladov sociálneho poistenia a výstupov konania

- Komplexné riešenie pre transformáciu procesov spracovania vstupov systému sociálneho poistenia (nárokové podklady, žiadosti o dávky, potvrdenia a pod.) a vyhovovania výstupov konania vo veciach sociálneho poistenia
- Zabezpečí tiež spracovania papierového dokumentu s uložením jeho obsahu do štruktúrovanej dátovej formy, archivovania „digitálneho obrazu“ elektronického a papierového dokumentu v rámci technológie Dokument manažment systému

Systém elektronických služieb - portál a komunikačné rozhrania

- Systém elektronických služieb SP (SES) bude sprístupnený používateľom prostredníctvom elektronického internetovského portálu, ktorý zabezpečí klientom SP aplikácie pre prístup ku všetkým relevantným informáciám spracovávaným v rámci systému sociálneho poistenia.

5.1.7.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Realizácia projektu implementácie elektronických služieb Sociálnej poisťovne si však vyžaduje zabezpečenie príslušných hardvérových a softvérových technológií, ktoré poskytnú potrebný výpočtový výkon pre prevádzku príslušných systémov pri rešpektovaní požiadaviek kladených na spoľahlivosť a bezpečnosť. Pri implementácii sa predpokladá aplikácia HW a SW virtualizácie fyzických systémov.

Súčasná technologická infraštruktúra IS SP je komplexne sústredená v ústredí SP pričom nie je vybudované záložné centrum. Z tohto pohľadu sú identifikované nasledovné doplňujúce požiadavky na infraštruktúru:

- vytvorenie permanentne aktuálnej kópie prevádzkovej údajovej základne IS SP,
- on_line plnohodnotné využitie kópie údajovej základne v prípade jej porušenia (výpadku) v centrálnom výpočtovom stredisku,
- realizácia zálohovania a archivácie údajovej základne,
- implementácia záložných systémov pre prevádzkovanie kritických aplikačných služieb IS SP,

- on_line plnohodnotné využitie záložných systémov v prípade prerušenia prevádzky (poruchy) v centrálnom výpočtovom stredisku.

5.1.7.4 Rámcové požiadavky na technické zabezpečenie

Aj keď sú definované len základné moduly riešenia, vzhľadom na zabezpečovanú funkčnosť je možné predpokladať že pôjde o robustný informačný systém, pre ktorý je možné definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj na uloženie a zálohovanie dát. Pásková knižnica v záložnom DC nie je uvažovaná.

Identifikácia rámcových požiadaviek na technické zabezpečenie

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 3 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy

5.1.8 Elektronizácia služieb Ministerstva hospodárstva SR (IIS MH)

5.1.8.1 Funkcionalita

Cieľom projektu je nasadenie a sprístupnenie všeobecne použiteľných elektronických služieb Ministerstva hospodárstva v rámcovom rozsahu:

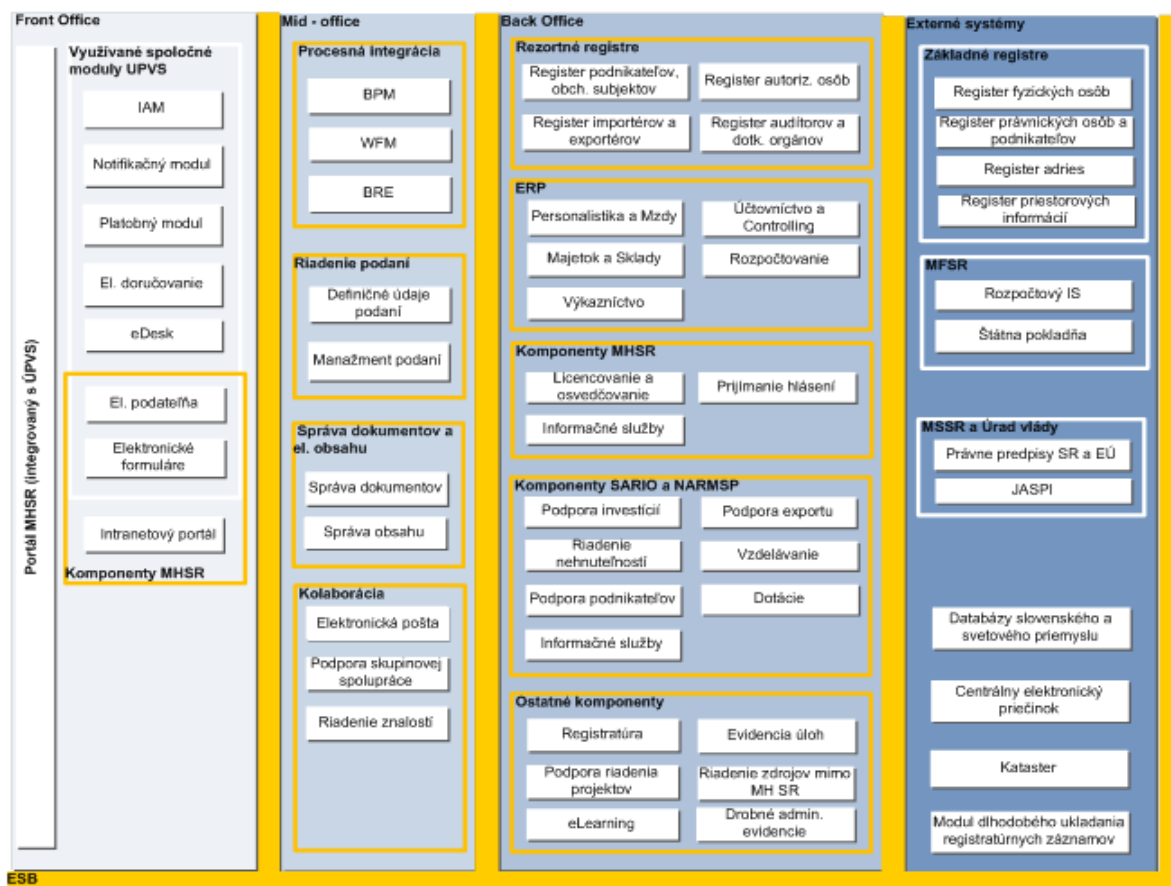
- Elektronizácia procesov Ministerstva hospodárstva SR a ich sprístupnenie občanom a podnikateľom prostredníctvom elektronických služieb:
 - zabezpečenie inteligentného využívania registrov a sofistikovaných analýz tržného prostredia,
 - elektronizácia procesov práce s klientmi pre NARMSP a SARIO,
 - sofistikácia podpory exportu,
 - elektronizácia procesu energetického auditu,
 - elektronizácia služieb pre vydávanie licencií MHSR.
- Vybudovanie integrovaného informačného systému spravujúceho procesy MH, NARMSP a SARIO na báze troch kooperujúcich celkov:
 - zavedenie kolaboračných portálov pre efektívnu prácu používateľov MH SR, SARIO, NARMSP,
 - zavedenie moderných systémov pre riadenie vzťahov s hospodárskymi subjektmi a ďalšími klientmi,
 - zavedenie dátových skladov umožňujúcim pokročilé analytické a štatistické funkcie,
 - zavedenie systémov pre efektívne riadenie zdrojov a elektronizáciu úsekov výkonu správy.
- Zabezpečenie využívania elektronických služieb Ministerstva hospodárstva SR v kontexte elektronizácie verejnej správy a NKIVS:
 - prepojenie informačného systému Ministerstva hospodárstva SR s informačným prostredím Štatistického úradu SR, MS, NKÚ, Sociálnou poisťovňou, Daňovou správou a Centrálnym elektronickým priečinkom,

- zabezpečenie využívania základných registrov podľa NKIVS pre dátovú harmonizáciu a spoločných modulov ÚPVŠ pre podporu behu obslužných procesov pre služby v informačnom prostredí Ministerstva hospodárstva SR.

5.1.8.2 Architektúra

Cieľová architektúra Integrovaného informačného systému Ministerstva hospodárstva (IIS MH) so základnými komponentmi a v rozdelení do jednotlivých vrstiev je na nasledovnom obrázku:

Obrázok 8 – Architektúra IIS MH



Front-office

- Vrstva, ktorá priamo zabezpečuje elektronickú výmenu informácií medzi občanom/podnikateľom a MH SR, jej hlavnou úlohou je zabezpečiť právne záväzné podanie na vstupe a právne relevantný výstup na druhej strane,
- Kľúčovým prvkom sprostredkujúcim tieto úlohy, na ktorý sú ostatné komponenty prepojené, je portál MH SR.

Mid-office

- Vrstva, ktorá riadi procesnú stránku podaní a súvisiacu orchestráciu zamestnancov MH SR a jednotlivých komponentov IS tak, aby na konci procesu bol k dispozícii požadovaný výstup,
- Hlavnými komponentmi sú procesné nástroje (BPM na orchestráciu systémov a WFM na procesné riadenie manuálnych aktivít) a Riadenie podaní (Case management) pre definíciu typov podaní a správu informácií o ich priebehu.

Back-office

- Služi najmä ako dátový zdroj a úložisko pre jednotlivé procesy eGov služieb a ako vnútorná IT podpora MH SR,
- Obsahuje systémy pre vnútornú správu MH SR, rezortné registre (vychádzajúce z národných registrov definovaných v NKIVS a ďalšie vyplývajúce zo špecifických potrieb MH SR) a dátové služby operatívnych dátových úložísk pre špecifické agendy MH SR.

Externé systémy

- Systémy mimo správy a kompetencie MH SR, ktorých služby sú využívané v rámci procesov MH SR, ide najmä o systémy, ktoré poskytujú informácie potrebné pre vykonávané procesy, resp. sú do nich informácie v rámci týchto procesov zasielané.

5.1.8.3 Predpokladané technické riešenie

V rámci štúdie uskutočniteľnosti je naznačená principiálna (modelová) architektúra technickej infraštruktúry. Navrhovaná modelová architektúra predpokladá využitie prevádzky systémov (aplikačných, databázových aj podporných) vo virtualizovanom prostredí, s uložením dát na SAN zariadeniach. Umiestnenie HW infraštruktúry je navrhované v dvoch lokalitách, primárnej a záložnej, s prepojením na úrovni virtualizačných klastrov a SAN zariadení.

5.1.8.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých modulov a rozsahu funkčnosti je možné pre systém definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie dát. Pásková knižnica v záložnom DC nie je uvažovaná.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1 x dátový rozvádzač – pre diskové úložné systémy
 - 1 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 4 x dátový rozvádzač – pre serverovú infraštruktúru
 - 1 x dátový rozvádzač – pre diskové úložné systémy

5.1.9 Elektronizácia služby zdravotníctva (eHealth)

5.1.9.1 Funkcionalita

Základným cieľom predmetného projektu je sprístupnenie elektronických služieb zdravotníctva (eHealth) a zabezpečenie ich všeobecnej použiteľnosti. Zo širšej množiny elektronických služieb boli ako prioritné vybrané nasledovné skupiny služieb:

- Poskytovanie verejných zdravotne relevantných informácií,
- eAlokácie,
- eMedikácia / ePreskripcia,
- Poskytovanie zdravotných informácií pacienta.

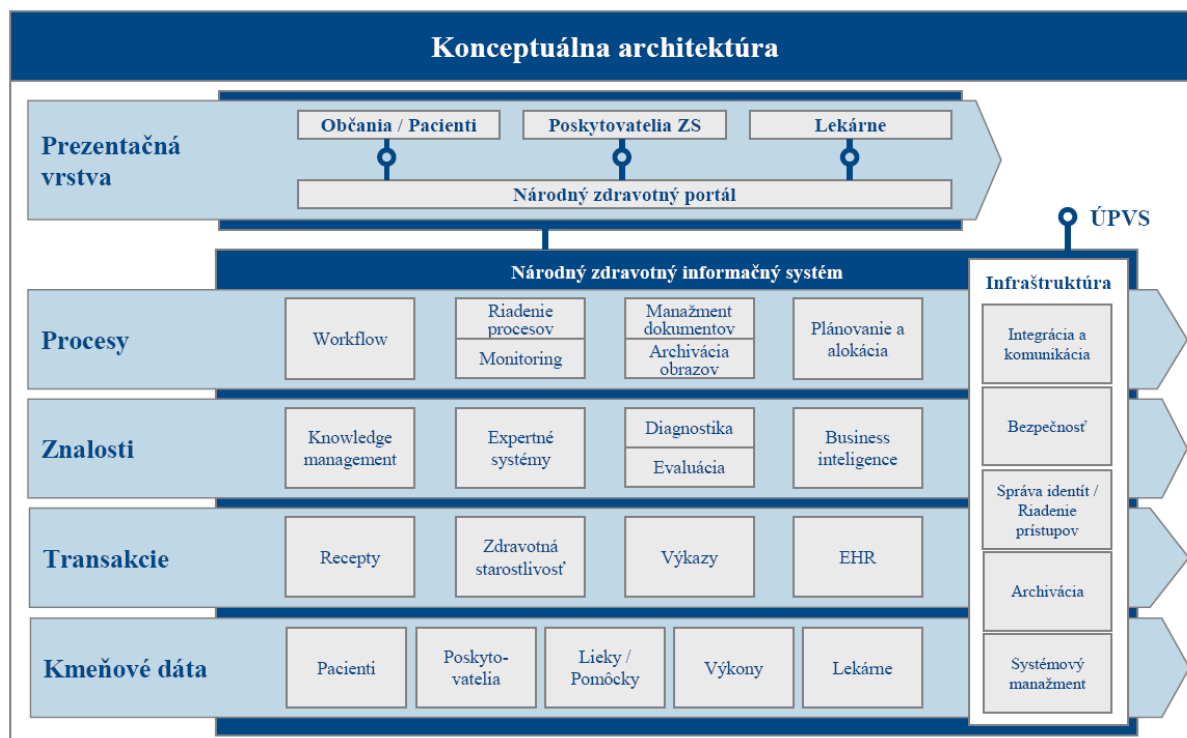
Zároveň má projekt zabezpečiť vytvorenie a konsolidáciu dátovej základne a zabezpečenie príslušnej infraštruktúry pre elektronickú zdravotnú knižku občana (pri dodržaní štandardov obsahu a štruktúry údajov ako základ budovania národného systému EHR - electronic health records) a

poskytovanie podkladov občanom, ktoré im umožnia využiť cezhraničné služby zdravotnej starostlivosti v celej EÚ (v rámci projektu EÚ s názvom epSOS).

5.1.9.2 Architektúra

Architektúra riešenia vychádza z definovaných prioritných služieb, ktoré majú byť podporené v prvej etape elektronizácie zdravotníctva. Týmto spôsobom bude vytvorené základné aplikačné prostredie a rámec do ktorého bude možné zakomponovať ďalšie komponenty a procesy. Konceptuálna architektúra riešenia, rozdelená do špecifických vrstiev, je na nasledujúcom obrázku:

Obrázok 9 – Konceptuálna architektúra riešenia platformy eHealth v prvej etape



Prezentačná vrstva – Národný zdravotný portál (NZP)

- Zabezpečuje centralizované poskytovanie interaktívnych služieb a integruje všetky zúčastnené strany (pacientov, lekární, poskytovateľov zdravotnej starostlivosti, ...).

Národný zdravotný informačný systém (NZIS) – predstavuje integráciu procesov, znalostí, transakcií a kmeňových dát.

- Procesy eHealth služby budú riadené procesmi, ktoré budú realizované prostredníctvom:
 - Systému Workflow - na definíciu procesov.
 - Systému pre manažment dokumentov, ktorý bude neskôr rozšírený o archiváciu obrazov a na podporu behu procesov.
 - Systému plánovania a kalendárov s podporou komunikácie a riadenia
- Znalosti – podporujú kvalitu dodávaných eHealth služieb, prostredníctvom expertnej integrácie a publikovania znalostí z rôznych zdrojov:
 - Knowledge management systém - pre správu neštruktúrovaných dokumentov,
 - Expertné systémy - schopné vyhodnocovať podnety na základe banky znalostí poskytovať podporu v rozhodovacích procesoch, napríklad aplikácie na podporu diagnostiky

- Aplikačné komponenty pre procesy vyhodnotenia (evaluácie) v zdravotníctve a publikovanie výsledkov
- Nástroje na analýzy a spracovanie veľkého množstva dát (Business Intelligence)
- Transakcie – predstavujú systémovú podporu pre interakcie medzi subjektmi v eHealth prostredí:
 - elektronické objekty pre recepty
 - zaznamenávanie zdravotnej starostlivosti
 - štandardizované elektronické objekty výkazníctva medzi subjektmi
 - postupné zavádzanie komponentov elektronického zdravotného záznamu
- Kmeňové dáta
 - Kmeňové dáta potrebné na výkon zdravotnej starostlivosti spravované v registroch, ktoré budú centrálné synchronizované a harmonizované systémom správy kmeňových dát (MDM).
 - Uvažuje sa o systematizácii: poistencov, poskytovateľov zdravotnej starostlivosti, databáze liekov, liečiv a zdravotníckych pomôcok, štandardizovanom číselníku výkonov a pod..
 - Základným komponentom pre uchovanie dát na centrálnej úrovni bude Národné zdravotné dátové centrum (NZDC).

5.1.9.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Pre realizáciu a zabezpečenie požadovaných služieb je však požadované vytvoriť nové technické a technologické zabezpečenie. To predstavuje vybudovanie nových vysoko dostupných a bezpečných dátových centier pre NZIS, NZP a takisto aj pre ďalšie komponenty eHealth (napr. registre, EHR, EDS, ePreskripcia, integračný middleware) a takisto aj vytvorenie vysoko dostupnej a bezpečnej sieťovej infraštruktúry za účelom komunikácie. Z uvedeného vyplýva aj potreba alokácie geograficky vzdialených lokalít pre zástupné/disaster centrá na zabezpečenie náhradného chodu a funkčnosti služieb ako aj pre potreby archivácie a zálohovania.

Predpokladá sa umiestnenie systému do priestorov DataCentra

5.1.9.4 Rámcové požiadavky na technické zabezpečenie

Aj keď sú definované len základné moduly riešenia, vzhľadom na zabezpečovanú funkčnosť je možné predpokladať že pôjde o robustný informačný systém, kde je možné definovať požiadavky pre NZP a NZIS ako pre samostatný informačný systém.

Z pohľadu predpokladaného nasadenia väčšieho počtu jednotlivých modulov a rozsahu funkčnosti je možné pre celý systém (NZP a NZIS) definovať rozšírené požiadavky na rozsah technického zabezpečenia pre prevádzku systémov aj uloženie a zálohovanie a prípadnú archiváciu dát (archivácia obrazov). Na úrovni IS ako celku sa už predpokladá optimalizácia rozmiestnenia komponentov v jednotlivých dátových rozvádzačoch.

- NZP
 - rozšírený systém, bez zvýšených požiadaviek na uloženie dát
- NZIS
 - rozšírený systém, so zvýšenými požiadavkami na uloženie dát, zálohovanie aj archiváciu (archivácia obrazov). Pásková knižnica pre potreby archivácie je uvažovaná aj v záložnom DC.

Identifikácia rámcových požiadaviek na technické zabezpečenie - NZP

- Požiadavky na primárne DC
 - 2,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - 1,5 x dátový rozvádzač – pre kompletnú infraštruktúru IKT

Identifikácia rámcových požiadaviek na technické zabezpečenie - NZIS

- Požiadavky na primárne DC
 - 3,5 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 2 x dátový rozvádzač – pre páskové úložné systémy
- Požiadavky na záložné DC
 - 2,5 x dátový rozvádzač – pre serverovú infraštruktúru
 - 2 x dátový rozvádzač – pre diskové úložné systémy
 - 2 x dátový rozvádzač – pre páskové úložné systémy

5.1.10 Kontrolórsky informačný systém (KIS NKÚ)

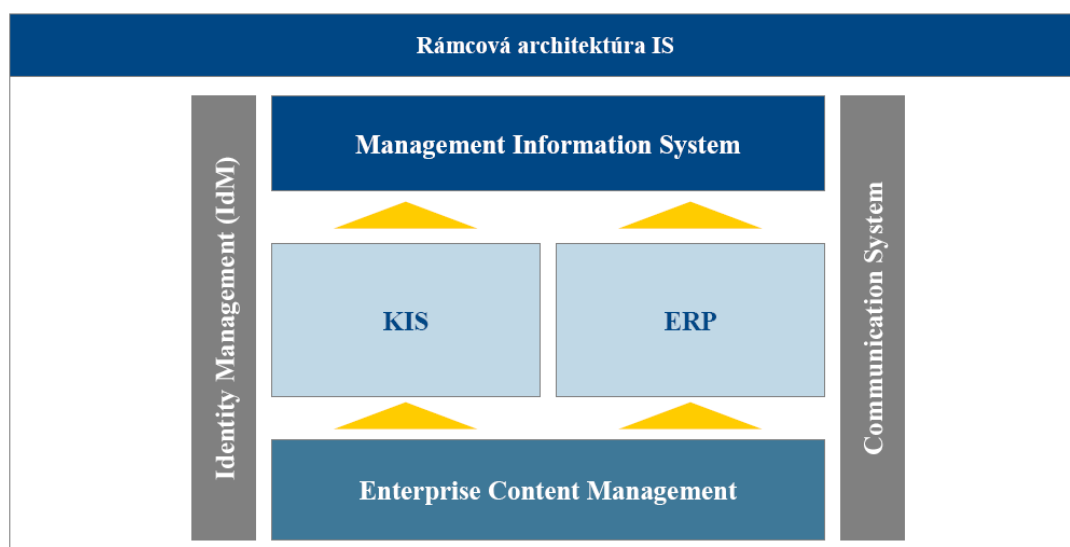
5.1.10.1 Funkcionalita

K prioritným cieľom národného projektu patrí podpora práce kontrolórov spoľahlivým pripojením k dostupným poznatkom o kontrolovateľných subjektoch, interakcia s kontrolnými systémami a kontrolórmí kontrolovaných subjektov orgány štátnej správy, obce, VÚC , tvorba databázy kontrolných akcií, kontrolných zistení, odporúčaní a správ z kontrol, súlad metodiky kontroly s medzinárodnými normami a štandardami kontrolných postupov.

5.1.10.2 Architektúra

Rámcová architektúra komplexného IS pre NKÚ so základnými modulmi je znázornená na nasledovnom obrázku:

Obrázok 10 – Konceptuálna architektúra komplexného IS pre NKÚ



Management Information System (MIS) – Manažérsky informačný systém

- Modul zahŕňajúci funkčnosti pre reporting, meranie výkonnosti a riadenie spoločnosti.
- Plánuje sa ako nový modul dodávaný formou Commercial Off-the-shelf aplikácie s predpokladanými čiastkovými úpravami a nastaveniami.

Identity Management (IdM)

- IdM bude tvoriť nadstavbu pre komponent IAM z ÚPVS a zabezpečovať autentifikácia prihlasovaní do tretích systémov bude zabezpečená pomocou IAM.

Kontrolórsky informačný systém (KIS) a systém riadenia kvality

- Modul obsahujúci funkčnosti pre podporu hlavných procesov.
- Plánuje sa ako nový modul vyvinutý podľa identifikovaných požiadaviek.

Enterprise resource planning (ERP) – Administratívno-ekonomický informačný systém

- Modul obsahujúci funkčnosti pre podporu podporných procesov.
- Plánuje sa ako rozšírenie súčasných aplikácií formou Commercial Off-the-shelf.

Communication system (CS) – Komunikačný systém

- Modul zahŕňajúci funkčnosti pre komunikáciu, monitoring a výmenu informácií.
- Plánuje sa ako rozšírenie súčasných aplikácií formou Commercial Off-the-shelf (zložené z rôznych komerčných riešení v oblasti prenosu dát a telekomunikácií).

Enterprise Content Management (ECM)

- Systém pre riadenie znalostí, elektronický archív a systém riadenia prípadov (CMS, ECM)
- Modul zaisťujúci jednotnú dátovú bázu.

5.1.10.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Pre KIS sa predpokladá aplikácia nového riešenia, ktoré bude prevádzkované v trojvrstvovej architektúre klient – server, pričom bude potrebné modernizovať hardvérové vybavenie a sieťovú infraštruktúru. Dôjde tiež k zvýšeniu nárokov na kapacitu dátových úložísk, dátových liniek, spoľahlivosti a dostupnosti sieťovej infraštruktúry, ich monitoringu a správy.

Navrhované je vývojové, testovacie a prevádzkové prostredie. Testovacie prostredie by malo svojím výkonom a konfiguráciou kopírovať prevádzkové prostredie, aby predovšetkým záťažové testy priniesli v oblasti výkonu výsledky zodpovedajúce reálnemu výkonu produktívnej prevádzky. V projekte treba uvažovať aj o školiacom prostredí pre používateľov.

5.1.10.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia menšieho počtu jednotlivých modulov a využitia komerčných aplikácií je možné pre systém definovať základné požiadavky na rozsah technického zabezpečenia.

Identifikácia rámcových požiadaviek na technické zabezpečenie.

- Požiadavky na primárne DC
 - 1 x dátový rozvážač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - 1 x dátový rozvážač – pre kompletnú infraštruktúru IKT

5.1.11 Elektronické služby úradu pre verejné obstarávanie (IS EVO)

5.1.11.1 Funkcionalita

Hlavným cieľom projektu je vybudovanie informačného systému na báze webových služieb, ktorý umožní podávanie oznámení všetkých typov v elektronickej forme a zabezpečí podporu pre elektronické verejné obstarávanie pre všetky súčasné využívané postupy verejného obstarávania s možnosťou prepojenia na iné informačné systémy verejnej správy a informačné systémy EÚ (napr. OJEÚ). Systém bude umožňovať bezpečné ukladanie celej súvisiacej dokumentácie v súlade so zákonom o archívoch a registratúrach, pričom počas doby uloženia bude umožňovať prístup v súlade so zákonom o ochrane osobných údajov.

5.1.11.2 Architektúra

Rámcová architektúra komplexného IS pre Úrad pre verejné obstarávanie (ÚVO) obsahuje nasledovné základné komponenty:

- Webové sídlo ÚVO/Publikačný portál ÚVO
 - portál bude slúžiť ako prezentačné rozhranie na zverejňovanie informácií používaných vo verejnom obstarávaní, zabezpečí prístup k službám ÚVO a zber oznámení a údajov používaných vo verejnom obstarávaní prostredníctvom formulárov systému zberu údajov. Portál IS ÚVO bude integrovaný s ÚPVS.
- Webové sídlo ÚVO/Systém zberu údajov
 - Systém umožní prostredníctvom poskytnutých formulárov zber údajov (oznámení, žiadostí, informácií atď.) používaných vo verejnom obstarávaní.
- eSender
 - Zabezpečí automatizáciu posielania povinných oznámení podávaných verejným VO/O publikačnému úradu ES spôsobom a vo formátoch vyžadovaných EÚ,
- IS EVO
 - Bude poskytovať elektronické služby elektronického verejného obstarávania pre fázy prípravy a plánovania, eNotification – posielanie oznámení, eTendering - predkladanie ponúk a žiadostí o účasť, vysvetľovanie a fázu elektronického vyhodnocovania a vyhodnocovania prostredníctvom elektronickej aukcie - eAwarding.
 - Vo fáze prípravy môže obstarávateľ využiť nástroj na vytváranie formulárov pre ponuky.
- Systém spracovania údajov
 - Bude slúžiť ako komplexný systém pre podporu všetkých činností ÚVO, pre podporu spracovania údajov používaných vo verejnom obstarávaní, generovaniu reportov, štatistických vyhodnocovaní podľa definovaných kritérií. Bude slúžiť na administráciu registrov a bude umožňovať vyhľadávanie a generovanie definovaných výstupov, kontrolách, ich stave a podobne.
- Spoločné podporné moduly
 - Document Management System (DMS) – Účelom DMS je spracovanie, evidencia a uloženie dokumentov, ktoré sú používané v rámci VO. Dokumenty sú v DMS ukladané bez ZEP. DMS zabezpečuje ich publikovanie, kontrolu verzií, podporu workflow, ako aj zaistenie bezpečnosti. Lokálny DMS je využívaný subsystémami Registratúra, Elektronická podateľňa.
 - Workflow – Komponent riadiaci jednotlivé procesy bežiace v systéme vrátane komunikácie s integrovanými komponentmi, resp. systémami.

- ePodateľňa – zabezpečí overenie elektronického podpisu prijatého podania, vystavenie potvrdenky o prijatí podania, zabezpečenie elektronického podpisu príslušného orgánu verejnej správy a aplikačnú podporu na vytváranie a overovanie elektronických podpisov.

5.1.11.3 Predpokladané technické riešenie

Predpokladané technické riešenie nebolo v rámci štúdie uskutočniteľnosti naznačené. Predpokladá sa vybudovanie integrovaného systému s viacvrstvou architektúrou pre ktorý je potrebné realizovať zmeny existujúcej technologickej platformy a modernizovať hardvérové vybavenie a sieťovú infraštruktúru. Navrhnuté je tiež prepojenie 3 oblastných pracovísk na zefektívnenie možností spolupráce pri poskytovaní služieb.

5.1.11.4 Rámcové požiadavky na technické zabezpečenie

Z pohľadu predpokladaného nasadenia menšieho počtu jednotlivých modulov a využitia komerčných aplikácií je možné pre systém definovať základné požiadavky na rozsah technického zabezpečenia.

Identifikácia rámcových požiadaviek na technické zabezpečenie

- Požiadavky na primárne DC
 - 2 x dátový rozvádzač – pre kompletnú infraštruktúru IKT
- Požiadavky na záložné DC
 - 2 x dátový rozvádzač – pre kompletnú infraštruktúru IKT

5.2 Princípy konsolidácie pre projekty OPIS PO1

Centrálne služby poskytované Dátovým centrom vytvárajú priestor pre konsolidáciu požiadaviek na IKT infraštruktúru jednotlivých projektov PO1 OPIS a z toho vyplývajúcu úsporu nákladov na obstaranie a prevádzku informačných systémov štátnej správy. Úspory spojené s využitím služieb Dátového centra vyplývajú z:

- **Konsolidácia infraštruktúry** – konsolidácia infraštruktúry umožňuje zdieľanie a efektívne využitie dostupných zdrojov. V spojení s virtualizáciou a šandardizáciou vytvára podmienky pre také riadenie kapacít, ktoré umožňuje pokryť plánované požiadavky a minimalizuje objem nevyužitých zdrojov.
- **Úspora nákladov na energie** – náklady na energie predstavujú v súčasnosti 15-20% nákladov na celkové vlastníctvo (TCO). Veľké dátové centrá sú schopné nakupovať energie za výhodnejšie sadzby. Vďaka konsolidovanej infraštruktúre sú schopné dynamicky optimalizovať záťaž a využitie zdrojov a tým efektívne riadiť aktuálnu spotrebu energie.
- **Úspora nákladov na pracovnú silu** – prostredie veľkých dátových centier umožňuje automatizáciu opakovaných úloh manažmentu IKT prostredia aj v takých prípadoch, ktoré by boli pre menšie dátové centrá finančne neefektívne. Masívna automatizácia následne umožňuje pracovníkom dátového centra obslužiť väčšie množstvo IKT prvkov a sústrediť sa na úlohy s vyššou pridanou hodnotou.
- **Kúpna sila** – Prevádzkovatelia veľkých dátových centier nakupujú hardvér, softvér a služby vo veľkom čo im dáva predpoklady na získanie výhodnejšej ceny ako v prípade menších nákupcov.

Nasadenie služieb Dátového centra bude na úrovni jednotlivých projektov PO1 OPIS vyžadovať nasledovné aktivity:

- **Analýza požadovaných služieb** – v rámci prípravy projektového plánu musia byť identifikované požadované služby IKT infraštruktúry vrátane ich rámcových charakteristík.

Identifikovaných kandidátov na služby bude potrebné posúdiť z pohľadu špecifických bezpečnostných a prevádzkových požiadaviek a rozhodnúť o:

- implementácii služby v rámci projektových výstupov
- využitií služieb dátového centra
- **Špecifikácia požadovanej úrovne služieb Dátového centra** – pre všetky služby, ktoré budú poskytované Dátovým centrom, musia byť v rámci analytických a návrhových aktivít projektu definované požiadavky, ktoré budú určovať rozsah, spôsob a kvalitu týchto služieb. Na úrovni projektovej organizácie musí byť definovaný zástupca zodpovedný za riadenie vzťahov s dodávateľom služieb dátového centra.
- **Uzavretie zmluvy o poskytovaní služieb** – v spolupráci so zástupcom dodávateľa služieb dátového centra budú definované SLA, ktoré bližšie určujú rozsah, spôsob dodávky, kvalitu, spôsob merania, reporting a podporné procesy pre odoberané služby. V prípade kladného posúdenia realizovateľnosti zo strany dodávateľa služieb bude uzavretá zmluva o poskytovaní služieb.
- **Nasadenie služieb** – samotná implementácia služieb bude realizovaná zo strany poskytovateľa (Dátového centra). Na úrovni projektu bude potrebné zabezpečiť nevyhnutnú súčinnosť potrebnú pre implementáciu a následné nasadenie definovaných služieb.
- **Testovanie a akceptácia** – úlohou akceptačného testovania je overiť vlastnosti poskytovaných služieb voči požiadavkám definovaným v zmluve a poskytovaní služieb. Úspešne ukončené akceptačné testy sú nutným predpokladom pre zahájenie produkčného využívania služieb dátového centra.

Pri analýze a posudzovaní požadovaných služieb IKT infraštruktúry je potrebné vychádzať z aktuálnych služieb poskytovaných Dátovým centrom a zo zohľadnenia nasledovných princípov:

- **Konsolidácia** – v oblasti konsolidácie je potrebné zabezpečiť čo najširšie využitie služieb centrálnej IKT infraštruktúry a centrálnych služieb pre podporu a riadenie IKT prostredia. Odklon od využitia konsolidovaných riešení je predpokladaný iba v prípadoch, ktoré sú odôvodnené špecifickými prevádzkovými a/alebo bezpečnostnými požiadavkami. Konsolidácia je motivovaná znižovaním ceny a komplexnosti správy.
- **Štandardizácia a interoperabilita** – princíp štandardizácie je zameraný na maximálne využitie štandardných a otvorených technológií. Štandardizácia musí byť zároveň zameraná na redukovanie počtu hardvérových a softvérových architektúr. Štandardizácia je nutným predpokladom pre správne fungovanie technických celkov a ich vzájomnú interoperabilitu.
- **Rozšíriteľnosť** - v rámci rozšíriteľnosti je potrebné riešiť vzťah medzi nákladmi a životným cyklom IKT technológií. Zároveň je potrebné brať do úvahy, že požiadavky na kapacitu IKT infraštruktúry budú počas prevádzky prirodzene rásť. Kľúčovým je navrhnúť optimálny počiatočný stav a stanoviť rozvojový plán tak, aby bolo možné zabezpečiť potrebnú kapacitu včas a finančne efektívne.
- **Bezpečnosť** - Na úrovni bezpečnosti je potrebné adresovať všetky základné oblasti:
 - Fyzická bezpečnosť
 - Bezpečnosť prostredia
 - Bezpečnosť informačných a komunikačných technológií

Súčasťou bezpečnosti je aj analýza rizík a dopadov, ktorá následne definuje požiadavky na dostupnosť riešenia. Dostupnosť je pritom chápaná vo vzťahu ku koncovému odberateľovi eGov služieb čo vytvára vysoké nároky na všetky komponenty infraštruktúry, ktoré sa podieľajú na poskytovaní týchto služieb.

5.3 Finančné požiadavky projektov OPIS PO1

Využitie možností DataCentra na technické zabezpečenie a podporu eGov služieb centralizovaným spôsobom, prináša so sebou aj príležitosť na optimalizáciu nákladov na jednotlivé eGov služby. Pri identifikácii nákladov na technickú infraštruktúru potrebnú na zabezpečenie prevádzky eGov služieb v rámci jednotlivých projektov OPIS PO1, uvažovaných v tejto štúdii, sa primárne vychádzalo z informácií uvedených v ich štúdiách realizovateľnosti. V štúdiách, kde neboli priamo špecifikované náklady na potrebnú technickú infraštruktúru, boli tieto náklady stanovené odhadom podľa iných porovnateľných projektov.

Prehľad alokácií finančných zdrojov na technickú infraštruktúru pre projekty OPIS PO1, uvažované v tejto štúdii, je uvedený v nasledujúcej tabuľke. Všetky sumy sú v EUR s DPH.

Tabuľka 4 - Prehľad alokácií finančných zdrojov na technickú infraštruktúru vybraných projektov OPIS PO1

Projekt	Celkové náklady	Náklady na HW	Náklady na SW	Náklady na IKT celkom	Poznámka
Národný projekt CEP	16 949 051	1 741 479	4 084 528	5 826 007	Cena HW a SW z dodatku zmluvy
Elektronické služby Finančnej správy I. oblasť daňová (program UNITAS)	49 972 765	2 210 880	1 989 120	4 200 000	Cena HW zo ŠU Cena SW odhadom (Cena za HW 4,2 mil. zo ŠU)
Datacentrum miest a obcí (DCOM)	49 772 080	8 078 786	7 888 578	15 967 364	Cena HW zo ŠU Cena SW zo ŠU
Elektronizácia služieb VÚC	4 737 000	420 012	377 833	797 845	Cena HW odhadom Cena SW odhadom Cena celkových nákladov pre jedného žiadateľa
Ústredný portál verejnej správy (ÚPVS) - spoločné moduly a prístupové komponenty	43 397 000	6 808 000	6 125 894	12 933 894	Cena HW odhadom Cena SW odhadom
Elektronické služby Štatistického úradu SR	22 600 000	2 003 855	1 802 623	3 806 478	Cena HW odhadom Cena SW odhadom
Elektronické služby Sociálnej poisťovne	46 300 000	7 264 320	6 535 680	13 800 000	Cena HW odhadom Cena SW odhadom (Cena za technologickú infraštruktúru 13,8

Projekt	Celkové náklady	Náklady na HW	Náklady na SW	Náklady na IKT celkom	Poznámka
					mil. zo ŠU)
Elektronizácia služieb Ministerstva hospodárstva SR (IIS MH)	9 999 800	665 000	1 800 000	2 465 000	Cena HW zo ŠU Cena SW zo ŠU
Elektronické služby zdravotníctva (eHealth)	49 600 000	4 600 000	6 900 000	11 500 000	Cena HW zo ŠU Cena SW zo ŠU
Kontrolórsky informačný systém (KIS NKÚ)	2 960 000	500 000	470 000	970 000	Cena HW zo ŠU Cena SW zo ŠU (štruktúra nákladov Variant III)
Elektronické služby úradu pre verejné obstarávanie (IS EVO)	3 485 000	309 002	277 971	586 972	Cena HW odhadom Cena SW odhadom
Celkom	299 772 696	34 601 333	38 252 227	72 853 559	

6 Návrh cieľového stavu zámeru

6.1 Princípy

6.1.1 Efektivita

Dátové centrum musí byť budované so zreteľom na dosiahnutie maximálnej efektivity pri využití zdrojov a minimalizácii prevádzkových nákladov pri dodržaní požadovaných parametrov poskytovaných služieb. Princíp efektivity musí byť adresovaný vo všetkých oblastiach Dátového centra. Dodržanie tohto princípu umožní v konečnom dôsledku naplniť jeden z primárnych cieľov riešenia, ktorým je znižovanie nákladov na informačné systémy verejnej správy.

6.1.2 Zohľadnenie najlepších praktík

Pri návrhu dátového centra sa vychádza zo štandardu pre telekomunikačnú infraštruktúru dátových centier ANSI/TIA-942 a ANSI/NECA/BICSI-002, ktoré definujú referenčný model (rámec požiadaviek a najlepších praktík) pre návrh a implementáciu dátových centier. Štandard TIA-942 definuje 4 kategórie dátových centier:

- I. Základné – 99,671% dostupnosť
- II. S redundantnými komponentmi – 99,741% dostupnosť
- III. So súbežnou údržbou – 99,982% dostupnosť
- IV. Odolné voči chybám – 99,995% dostupnosť

V oblasti riadenia prevádzky sú zohľadnené štandardy ISO 20000 a framework ITIL V3, ktorý mimo iné definuje procesy a funkcie pre riadenie prevádzkových činností smerujúcich k efektívnej dodávke poskytovaných služieb v rozsahu:

- Event management
- Request fulfilment
- Incident management
- Problem management
- Access management
- Service desk
- Technical management
- Application Management
- IT Operations Management

V oblasti riadenia informačnej bezpečnosti sa vychádza zo štandardu ISO 27001 a ISO 27002.

6.1.3 Dostupnosť

Zabezpečenie požadovanej dostupnosti je základnou prioritou riešenia. Dostupnosť je pritom chápaná vo vzťahu ku koncovému odberateľovi služieb čo vytvára vysoké nároky na všetky komponenty infraštruktúry, ktoré sa podieľajú na poskytovaní služieb dátového centra:

- podpornú technológiu
- komunikačnú technológiu
- informačnú technológiu

Zabezpečenie požadovanej úrovne dostupnosti budú dosiahnuté prostredníctvom redundantných komponentov a fail-over mechanizmov.

6.1.4 Modularita

Modularita umožňuje zefektívniť prevádzku, prípadné technické zásahy, obnovu technicky alebo morálne zastaraných technických prostriedkov alebo softvéru. Prevádzkovateľovi zjednodušuje dohľad a manažment. Pri hľadaní chýb umožňuje ich izoláciu a tým ich jednoduchšie a rýchlejšie odhalenie a odstránenie. Tým má zásadný vplyv aj na dostupnosť.

6.1.5 Bezpečnosť

Bezpečnosť je prioritou pri zanedbaní ktorej môže dôjsť k vážnemu ohrozeniu aktív zákazníka a jeho partnerov a môže mať kľúčový dopad na celý sektor.

Na úrovni dátového centra je potrebné venovať primárnu pozornosť nasledovným oblastiam informačnej bezpečnosti:

- Fyzická bezpečnosť
- Bezpečnosť prostredia
- Bezpečnosť informačných a komunikačných technológií

Analýza a návrh naplnenia požiadaviek jednotlivých oblastí informačnej bezpečnosti vrátane určenia spôsobov dosiahnutia trvalo udržateľnej adekvátnej úrovne informačnej bezpečnosti musí byť neoddeliteľnou súčasťou implementácie dátového centra vo forme príslušného bezpečnostného projektu.

Bezpečnosť rovnako ako modularita má zásadný vplyv aj na dostupnosť. Jednou z oblastí bezpečnosti je aj ochrana.

6.1.6 Rozšíriteľnosť

Rozšíriteľnosť v zmysle kapacít a ponúkaných služieb je ďalším kľúčovým princípom. Riešenie Dátového centra je potrebné navrhnuť tak, aby umožňovalo naplniť súčasné ako aj očakávané budúce požiadavky. V rámci rozšíriteľnosti je potrebné optimálne riešiť konflikt medzi nákladmi, predpokladanou dobou prevádzky DC a krátkym životným cyklom IKT technológií. Rovnako je potrebné brať do úvahy, že požiadavky na kapacitu dátových centier a služieb s nimi spojených budú počas prevádzky prirodzene rásť. Kľúčovým je navrhnuť optimálny počiatočný stav a stanoviť rozvojový plán tak, aby bolo možné zabezpečiť potrebnú kapacitu včas a finančne efektívne.

Princíp rozšíriteľnosti adresuje aj požiadavku na pružnosť a elasticitu výpočtových kapacít z pohľadu odberateľa služieb. Riešenie Dátového centra je potrebné navrhnuť tak, aby umožňovalo rýchlu a jednoduchú zmenu kapacít.

6.1.7 Interoperabilita

Interoperabilita na úrovni infraštruktúry a technických celkov IT je dosiahnutá využitím štandardov a musí byť riešená v rámci vypracovania detailnej architektúry a konfigurácie systémov. Táto úroveň zabezpečuje technické fungovanie infraštruktúry.

6.1.8 Virtualizácia

Virtualizácia infraštruktúry podporuje rýchle nasadenie, vysokú flexibilitu a zvyšovanie efektivity nákladov na správu a údržbu. Umožňuje vytvárať a prevádzkovať služby privátneho cloudu (IaaS) s využitím vlastnej fyzickej infraštruktúry.

6.1.9 Meranie

Všetky poskytované služby musia byť monitorované a získané dáta priebežne vyhodnocované. Meranie je dôležité pre všetky typy služieb nakoľko poskytuje komplexný prehľad o fungovaní jednotlivých služieb, aplikácií, ich výpočtových potrebách a o aktuálnom využití dostupného výkonu a kapacít. Meranie je kľúčovým princípom, ktorý vytvára nutné podmienky pre samotné riadenie poskytovaných služieb.

6.2 Služby dátového centra

Služby poskytované dátovým centrom sú na základe svojho charakteru rozdelené do troch kategórií:

- primárne – základné služby, ktoré poskytujú požadovanú infraštruktúru a zabezpečenie prevádzkových činností
- podporné – poskytujú podporu riadenia prevádzky
- telekomunikačné – služby zabezpečujúce komunikáciu v rámci verejnej správy a využívanie služieb Internetu

Pre všetky služby dátového centra budú definované:

- Charakteristika – popis základných parametrov služby udržiavaný v rámci katalógu služieb
- SLA - určuje zmluvné podmienky pre dodávku služby
- Nákladový model – definuje náklady na poskytovanie služby
- Model spoplatnenia – definuje spôsob spoplatnenia

Štúdia predpokladá postupný evolučný prechod k poskytovaniu služieb formou cloud computingu.

6.2.1 Primárne služby

6.2.1.1 Prenájom priestoru (housing)

Prenájom priestoru dátového centra určeného pre osadenie vlastnej technickej infraštruktúry odberateľa. Priestor môže byť prenajatý vo forme:

- dátového rozvádzača (racku)
- časti dátového rozvádzača
- základnej plochy dátového centra

Okrem samotného priestoru je súčasťou poskytovanej služby:

- redundantné napájanie vrátane záložného zdroja
- chladenie
- sieťová konektivita na chrbticovú sieť dátového centra

6.2.1.2 Prenájom servera (IaaS)

Poskytovanie serverov a súvisiacej technickej infraštruktúry určenej pre prevádzku informačných systémov odberateľa. Poskytovanie systémových zdrojov bude zabezpečené prostredníctvom virtualizačnej infraštruktúry, ktorá umožňuje flexibilitu a dynamickú alokáciu zdrojov, zvyšuje finančnú efektívnosť a znižuje požiadavky na správu a prevádzkovú podporu.

Služby server hostingu budú mať garantovanú vysokú dostupnosť na úrovni virtuálnej platformy v rámci lokality dátového centra.

Súčasťou poskytovania služby je:

- prenájom priestoru (housing)
- prenájom dátového úložiska

6.2.1.3 Prenájom dátového úložiska (IaaS)

Poskytovanie storage kapacít pre uloženie dát prevádzkovaných IS odberateľa.

Storage kapacita bude poskytovaná prostredníctvom zdieľaných storage zariadení, ktoré budú na základe svojich vlastností kategorizované do niekoľkých tried:

- storage tier 1 - je určený pre kritické aplikácie, ktoré vyžadujú vysokú výkonnosť a dostupnosť
- storage tier 2 – je určené pre menej kritické business aplikácie s nižšími požiadavkami na výkonnosť storage subsystému
- storage tier 3 – je určené pre testovacie a školiace prostredia, resp. pre aplikácie, ktoré nevyžadujú vysokú dostupnosť a sú orientované viac kapacitne ako výkonnostne.

Súčasťou služby je:

- redundantné napájanie vrátane záložného zdroja
- chladenie
- pripojenie a konfigurácia SAN

6.2.1.4 Prevádzka informačného systému (SaaS)

Poskytuje komplexnú starostlivosť o prevádzku informačného systému objednávateľa v prostredí dátového centra. Súčasťou služby je:

- prenájom servera
- prenájom dátového úložiska
- dohľad
- prevádzková podpora
- zálohovanie a obnova

6.2.1.5 Certifikačná autorita

Samostatná CA poskytujúca služby pre autentifikáciu s využitím certifikátov a ZEP zamestnancov verejnej správy.

Samostatná CA poskytujúca služby pre zabezpečenie dôvernosti, integrity, originality a nepopierateľnosti uchovávaných údajov ako sú:

- SSL certifikáty webových serverov
- Certifikáty pre sieťové prvky
- Certifikáty pre zabezpečenie správ vymieňaných medzi jednotlivými IS VS
- Certifikáty pre podpisovanie auditných záznamov
- Certifikáty pre službu časovej pečiatky a pod.

6.2.2 Podporné služby

6.2.2.1 Zabezpečenie trvalej kontinuity

Rozširuje službu „Prevádzka informačného systému“ o zabezpečenie kontinuity definovanej IKT infraštruktúry a príslušného aplikačného vybavenia aj v prípade katastrofickej udalosti. Súčasťou služby je:

- organizácia, príprava a údržba DRP
- testovanie DRP

Predmetom služby nie je zabezpečenie trvalej kontinuity na úrovni business služieb odberateľa.

6.2.2.2 Podpora trvalej kontinuity

Poskytuje disaster recovery (záložné) prostredie pre informačné systémy, ktoré sú primárne prevádzkované v dátovom centre zákazníka. Disaster recovery prostredie môže byť poskytované ako:

- cold stand-by
- warm stand-by
- hot stand-by

Súčasťou služby môže byť:

- prenájom servera
- prenájom dátového úložiska
- správa prostredia
- zálohovanie a obnova
- výkon DRP

6.2.2.3 Dohľad

Služba predstavuje súbor aktivít, ktoré sú vykonávané s cieľom priebežného sledovania stavu odoberaných služieb vrátane technických komponentov, ktoré sa podieľajú na ich poskytovaní. Dohľad centralizuje zber a spracovanie „systémových“ udalostí nad IKT infraštruktúrou a „bezpečnostných“ udalostí vyvolaných narušením definovaných bezpečnostných politík. Súčasťou služby je:

- analýza a riešenie udalostí v súlade s dohodnutými podmienkami
- výkon nápravných opatrení po zachytení známej udalosti
- poskytovanie informácií o stave IKT
- notifikácia určených osôb zákazníka o definovaných udalostiach
- generovanie a poskytovanie reportov

6.2.2.4 Prevádzková podpora

Služba predstavuje súbor aktivít, ktoré sú vykonávané s cieľom zabezpečenia priebežnej prevádzkovej podpory technickej infraštruktúry v rozsahu:

- správa siete
- správa SAN
- správa serverov

- správa dátových úložísk
- správa databáz a adresárových služieb
- meranie výkonnostných parametrov
- riadenie výkonnostných parametrov v súlade s dohodnutými podmienkami a potrebami

6.2.2.5 Aplikačná podpora

Služba zabezpečuje priebežnú podporu aplikačného programového vybavenia počas celého životného cyklu od identifikácie a špecifikácie požiadaviek až po podporu testovania, nasadenia a údržby. Súčasťou služby je:

- Analýza používateľských požiadaviek
- Podpora testovania
- Správa verzií a riadenie nasadenia
- Zabezpečenie činností súvisiacich so správou aplikácie
- Zabezpečenie spúšťania rutinných úloh
- Kontrola behu rutinných úloh a riešenie s nimi súvisiacich problémov

6.2.2.6 Používateľská podpora

Podpora koncových používateľov informačných systémov na úrovni:

- evidencie a riešenia servisných hlásení (incidentov a požiadaviek)
- metodologickej podpory pri používaní informačného systému

6.2.2.7 Zálohovanie a obnova

Služba zabezpečuje ochranu systémových a aplikačných dát pred stratou a poškodením prostredníctvom riadeného zálohovania a následnej obnovy. Súčasťou služby je:

- pravidelné zálohovanie operačného systému
- pravidelné zálohovanie aplikácie a aplikačných dát
- manuálne vytvorenie zálohy operačného systému na vyžiadanie
- manuálne vytvorenie zálohy aplikácie a aplikačných dát na vyžiadanie
- úplná obnova systému zo zálohy
- čiastočná obnova dát zo zálohy
- duplicitné ukladanie zálohovaných dát na požiadanie v dvoch lokalitách
- bezpečná likvidácia zálohovaných dát

Zálohovanie a obnova budú vykonávané na základe definovaných politík a postupov na infraštruktúre poskytovateľa služby.

Voliteľnou súčasťou služby je archivácia vybraných dát.

6.2.3 Telekomunikačné služby

6.2.3.1 Hlasové služby

Služba zabezpečuje vytvorenie štátnej telekomunikačnej siete založenej na princípe VoIP ako alternatívy ku komerčne dostupným hlasovým službám. Súčasťou služby je:

- CLIP
- CLIR
- SMS
- odkazová schránka
- faxové služby cez štandardné faxové zariadenia

Hlasové služby sú integrované so sieťami komerčných prevádzkovateľov telekomunikačných služieb.

6.2.3.2 Pripojenie do internetu

Služba zabezpečuje širokopásmový prístup do Internetu.

6.2.3.3 E-mail

Zabezpečuje služby email servera a správu email schránok. Súčasťou služby je:

- web klient
- antivírusová ochrana
- ochrana proti nevyžiadanej pošte (antispam)
- zálohovanie a obnova
- archivácia elektronickej pošty v súlade s dohodnutými podmienkami

6.2.3.4 Pripojenie do rezortných sietí

Zabezpečuje vysokorýchlostné pripojenie do rezortných WAN sietí. Súčasťou služby je:

- vytváranie virtuálnych sietí
- zabezpečenie VPN prístupov

6.2.4 Rozvoj služieb dátového centra

V rámci rozvoja služieb Dátového centra je prirodzeným krokom migrácia smerom ku cloud computingu, ktorý je spoločnosťou NIST (National Institute of Standards and Technology) definovaný ako model IT služieb, umožňujúci všadeprítomný, pohodlný, resp. na požiadanie možný sieťový prístup k zdieľaným oblastiam dynamicky konfigurovateľných výpočtových zdrojov, ktoré môžu byť rýchlo nasadzované a uvoľňované s minimálnymi nárokmi na jej manažment alebo vzájomnú súčinnosť s poskytovateľom tejto služby. K základným charakteristikám cloud computingu patrí:

- Samoobslužnosť – služby si môžu používatelia sami zriadiť, nakonfigurovať a používať.
- Prístup odkadiaľkoľvek – služby sú dostupné prostredníctvom štandardného internetu cez širokú paletu klientských zariadení.
- Zdieľanie zdrojov – výpočtové zdroje sú zdieľané viacerými používateľmi bez ohľadu na to, kde sú umiestnené.
- Pružnosť – elasticita, ktorá umožňuje používateľom rýchlo upraviť (škálovať) kapacitu zdrojov podľa aktuálnej potreby.
- Meranie – používateľ platí len za to čo spotrebuje.

Distribučný model cloud computingu definuje tri základné formy poskytovaných služieb:

- Infraštruktúra ako služba (IaaS) – predstavuje poskytovanie virtualizovanej infraštruktúry. Zákazník používa a ovláda základné výpočtové zdroje. Má možnosť riadiť operačné systémy,

dátové úložiská, nasadené aplikácie či sieťové komponenty infraštruktúry ale nie je mu umožnené ovládať/riadiť základnú cloud infraštruktúru, ktorá poskytuje všetky potrebné výpočtové zdroje pre užívateľské prostredie.

- Platforma ako služba (PaaS) – poskytuje komplexnú hardverovú platformu, teda zariadenia a služby potrebné pre podporu úplného životného cyklu budovania aplikácií vrátane možnosti návrhu, vývoja, testovania a nasadenia. Používateľ ovláda (riadi) aplikácie, ktoré sú spustené v tomto prostredí (a má aj možnosť riadiť niektorú funkcionality hostujúceho prostredia), ale neriadi (nemá možnosť spravovať) operačné systémy, hardwarovú a sieťovú infraštruktúru, na ktorej sú aplikácie spustené. Pre poskytovanie takejto miery abstrakcie je potrebné nasadiť služby pre vývoj a beh aplikácií, workload manažment, riadenie životného cyklu a manažment dát.
- Softvér ako služba (SaaS) – znamená poskytovanie aplikácií vo forme služieb. Používateľ nemusí, resp. nemá možnosť spravovať aplikáciu, platformu ani infraštruktúru.

Z pohľadu Dátového centra ako poskytovateľa služieb, ktorého zákazníkmi budú organizácie verejnej správy predpokladáme nasadenie cloud computingu formou privátneho cloudu. Služby budú poskytované iba pre konkrétne organizácie a poskytovaná infraštruktúra bude vytvorená na virtuálnom prostredí Dátového centra v rámci jeho uzavretej infraštruktúry. Pri privátnom cloudu je akýkoľvek IT zdroj rozprestrený naprieč medzi organizáciami a je dynamicky doručovaný jednotlivým organizáciám podľa ich požiadaviek čo umožňuje dosiahnuť oveľa väčšiu efektivitu v poskytovaní týchto zdrojov. Pre odberateľov IT služieb by sa mali zdroje cloud computingu zdať neobmedzené. Preto je podmienkou pre dlhodobu efektívne fungovanie prostredia dobré kapacitné plánovanie, bez ktorého môže dôjsť k veľkému prebytku alebo nedostatku zdrojov. Z tohto pohľadu je privátny cloud náchylnejší na chyby v plánovaní, ktoré nie je možné vzájomne eliminovať medzi väčším počtom odberateľov. Na druhej strane však privátny cloud umožňuje lepšie zabezpečenie bezpečnosti, lepšie riadenie komunikácie, lepšie riadenie SLA a pod..

V porovnaní s poskytovaním služieb v rámci virtualizovanej infraštruktúry je prechod na privátny cloud rozšírením o:

- Automatizáciu procesov a self-service rozhranie, ktoré umožňuje zriadenie služby na požiadanie.
- Vysokú automatizáciu v zmysle riadenia zdrojov, ktorá obsahuje všetko od infraštruktúry, middleware až po procesný manažment.
- Manažment prostredia s cieľom kontinuálneho zvyšovania efektívnosti prostredia.
- Sofistikované bezpečnostné a riadiace schopnosti, ktoré sú špecificky navrhnuté na základe požiadaviek organizácie.
- Prieběžné riadenie úrovne služieb na základe aktuálnych požiadaviek organizácie.

Komplexný prechod na poskytovanie služieb formou cloud computingu vyžaduje vyššiu mieru konsolidácie a štandardizácie ISVS, ktorá bude technologicky a organizačne náročná. Pred zahájením samotnej migrácie na cloud computing bude potrebné:

- analyzovať a špecifikovať očakávané ciele cloudu
- identifikovať služby
- dôkladne zvážiť predpokladané scenáre využitia
- posúdiť a ohodnotiť architektonické a technické obmedzenia aplikácií
- identifikovať a definovať legislatívne požiadavky
- identifikovať požiadavky na uloženie a ochranu údajov

- pripraviť stratégiu migrácie na cloud computing

Z pohľadu poskytovania služieb infraštruktúry (IaaS) dátového centra, je možné začať uplatňovať princípy cloud computing takmer okamžite, pričom práve infraštruktúra resp. jej virtualizácia v Government Private Cloud-e a presun existujúcich aplikácií do tohto prostredia môže položiť základ na komplexný prechod ISVS.

6.3 Procesná analýza

Poskytovanie centrálnych služieb dátového centra je komplexná a náročná úloha, ktorá vyžaduje nasadenie procesov pre riadenie odberateľských (zákazníckych) vzťahov, procesov pre plánovanie, zavedenie a prevádzku poskytovaných služieb a podporných procesov pre riadenie internej organizácie.

Procesná analýza má za cieľ identifikovať základné procesy, ktorých implementácia je nutným predpokladom pre efektívne poskytovanie služieb dátového centra pri zabezpečení takej úrovne služieb, ktorá je požadovaná jej jednotlivými odberateľmi.

6.3.1 Primárne procesy pre správu IT služieb

Základné procesy pre správu poskytovaných IT služieb budú pre zvýšenie prehľadnosti rozdelené na základe životného cyklu riadenia IT služieb do štyroch oblastí:

- plánovanie
- dizajn
- zavedenie
- prevádzka

6.3.1.1 Plánovanie

Procesy plánovania zabezpečujú strategické riadenie IT služieb na úrovni:

- požiadaviek a očakávaní
- portfólia poskytovaných IT služieb
- finančnej efektivity a udržateľnosti
- strategických rizík

V procesoch plánovania sú definované strategické ciele Dátového centra pri poskytovaní svojich služieb. Sú analyzované požiadavky a správanie zákazníkov, identifikované, posúdené riziká a vyhodnotená ekonomická efektívnosť, na základe ktorej je riadené portfólio poskytovaných služieb počas celého životného cyklu od plánovania až po odstavenie.

6.3.1.2 Dizajn

Oblasť návrhu zastrešuje aktivity, ktoré sú spojené s dizajnom nových alebo modifikáciou už poskytovaných IT služieb tak aby ich bolo možné nasadiť do produkčného prostredia a bola zabezpečená prevádzková podpora. Návrh by mal adresovať, v súlade so štandardami a definovanými konvenciami, všetky aspekty spojené s danou IT službou:

- návrh riešenia
- návrh manažment systému a nástrojov
- technickú architektúru
- procesy, metriky a systém merania

Procesy podieľajúce sa na návrhu IT služieb sú:

- Manažment dodávateľov – zabezpečuje manažment dodávateľov a nimi poskytovaných služieb tak, aby bola zabezpečená požadovaná kvalita za adekvátne náklady.
- Manažment informačnej bezpečnosti – zabezpečuje aby boli požiadavky informačnej bezpečnosti efektívne zohľadnené a implementované vo všetkých poskytovaných službách a manažment aktivitách.
- Správa katalógu služieb – zabezpečuje aby Katalóg služieb obsahoval aktuálne a správne informácie o všetkých prevádzkovaných službách.
- Správa úrovne služieb – zabezpečuje aby bola dosiahnutá dohodnutá úroveň služieb.
- Riadenie kontinuity IT služieb – zabezpečuje podporu toho, aby bola definovaná IKT infraštruktúra a IT služby obnovené v dohodnutom čase a rozsahu.
- Manažment dostupnosti – zabezpečuje takú úroveň dostupnosti poskytovaných služieb, ktorá je v súlade s dohodnutými podmienkami.
- Manažment kapacít – cieľom procesu je včas zabezpečiť potrebné a finančne zdôvodniteľné zdroje (technické, ľudské, ...) potrebné na zabezpečenie aktuálnych a plánovaných služieb.

6.3.1.3 Zavedenie

Oblasť zavádzania služieb má za cieľ zlepšiť schopnosť organizácie pri implementácii a nasadení nových alebo zmenených služieb do produkčnej prevádzky.

Procesy podieľajúce sa na zavedení IT služieb sú:

- Riadenie zmien – zabezpečuje štandardné metódy a postupy pri posudzovaní a schvaľovaní zmien tak, aby boli minimalizované negatívne dopady spojené s nasadením zmeny.
- Plánovanie zavedenia – zabezpečuje plánovanie príslušných kapacít a zdrojov potrebných pre implementáciu, testovanie a nasadenie novej, resp. zmenenej služby do produkcie.
- Validácia a testovanie – zabezpečuje aby služba spĺňala definované požiadavky
- Riadenie nasadenia – zabezpečuje nasadenie zmeny do produkčného prostredia.
- Správa konfigurácie – podporuje manažment IT služieb prostredníctvom evidencie, správy a poskytovania informácií o všetkých aktívach podieľajúcich sa na poskytovaní služieb počas celého životného cyklu.
- Riadenie znalostí – umožňuje organizácii zlepšiť kvalitu rozhodovania tím, že zabezpečuje a prístupňuje spoľahlivé informácie počas všetkých fáz životného cyklu IT služby.

6.3.1.4 Prevádzka

Oblasť prevádzky je zodpovedná za efektívnu dodávku a podporu poskytovaných služieb. Spôsob akým sú riešené procesy prevádzky priamo vplyvajú na vnímanie poskytovaných služieb zo strany koncových odberateľov. Prevádzka musí dosiahnuť vyváženie medzi:

- stabilita vs. dynamika
- kvalita vs. cena
- reaktivita vs. proaktivita
- interným pohľad vs. externý pohľad

Procesy a funkcie podieľajúce sa na dodávke a prevádzke IT služieb sú:

- Správa udalostí – prispieva k stabilite dodávky služieb cez zabezpečenie monitorovania všetkých udalostí v IKT infraštruktúre, detekciu a následnú eskaláciu identifikovaných výnimiek.

- Riadenie incidentov - zabezpečuje čo najrýchlejšie obnovenie normálnej prevádzky služby tak aby bol minimalizovaný dopad na odberateľa.
- Riadenie požiadaviek – poskytuje kanál pre spracovanie používateľských požiadaviek, poskytovanie informácií a štandardných služieb.
- Riadenie problémov – redukuje riziko opakovaných incidentov a chýb tým, že identifikuje príčiny chýb a zabezpečuje ich odstránenie.
- Riadenie prístupov – zabezpečuje prístup oprávnených a zamedzuje prístup neoprávnených používateľov k poskytovaným službám za účelom ochrany integrity, dôvernosti a dostupnosti informácií a infraštruktúry.
- ServiceDesk – vykonáva podporné aktivity pre zabezpečenie dostupnosti a využiteľnosti poskytovaných služieb.
- Manažment prevádzky IKT – zabezpečuje rutinné aktivity spojené s prevádzkou a údržbou IKT infraštruktúry.
- Aplikačný manažment – zabezpečuje podporu a údržbu aplikačného softvéru. Asistuje pri dodávke služby.
- Technický manažment – poskytuje podporu pre manažment prevádzky. Zabezpečuje údržbu, prevádzku, rozvoj a testovanie hardverových komponentov IKT infraštruktúry.

6.3.2 Zákaznícky orientované procesy

6.3.2.1 Manažment akvizícií

Je kľúčový proces, ktorý riadi aktivity smerujúce k získaniu zákazníka a k objednaníu odberu poskytovaných služieb. Súčasťou procesu je:

- zber požiadaviek
- koordinácia prípravy návrhu riešenia
- overenie technickej uskutočniteľnosti
- poskytovanie informácií zákazníkovi
- spracovanie objednávky
- vyjednanie a uzavretie kontraktu
- zahájenie interných procesov pre aktiváciu/sprístupnenie služby
- monitoring a riadenie priebehu spracovania objednávky

6.3.2.2 Aktivácia služby

Proces aktivácie služby má za cieľ umožniť prístup odberateľa k objednanej službe. Aktivácia služby má tri základné fázy:

- Plánovanie
 - overenie a plánovanie kapacít
 - kontrola technických predpokladov
 - alokácia zdrojov
 - príprava časového harmonogramu
 - poskytnutie spätnej väzby a komunikácia zo zákazníkom
- Logistika (ak je aplikovateľná)

- dodávka IKT infraštruktúry do DC
- dodávka IKT infraštruktúry k zákazníkovi
- poskytnutie spätnej väzby a komunikácia zo zákazníkom
- Aktivácia služby
 - príprava technických predpokladov
 - inštalácia a konfigurácia prostredia
 - systémové testy
 - akceptačné testy
 - aktualizácia dokumentácie
 - zahájenie prevádzky

6.3.2.3 Starostlivosť o zákazníka

Proces zabezpečuje riadenie vzťahov medzi odberateľom služieb a Dátovým centrom ako ich poskytovateľom. Cieľom procesu je, v súlade s dohodnutými podmienkami, zabezpečiť spracovanie a riešenie zákazníckych požiadaviek na odoberané služby ako sú zmenové požiadavky, sťažnosti, žiadosti o informácie, požiadavky na deaktiváciu služby a pod.. Z dôvodu zvýšenia transparentnosti poskytuje proces funkciu „kontaktného centra“, ktoré tvorí primárne miesto kontaktu.

Proces nesupluje funkciu ServiceDesk. Je orientovaný na podporu oblasti, ktorá súvisí so servisným kontraktom a nie na podporu koncových odberateľov služieb.

Súčasťou procesu je:

- evidencia a spracovanie požiadavky;
- validácia požiadavky;
- analýza a inicializácia riešenia požiadavky;
- koordinácia interných procesov súvisiacich s riešením požiadavky;
- poskytnutie spätnej väzby a komunikácia zo zákazníkom;
- aktualizácia dokumentácie.

6.3.2.4 Ocenenie a fakturácia

Proces zabezpečuje riadne ocenenie a zaúčtovanie poskytnutých služieb. Súčasťou procesu je správa modelu oceňovania, zaistenie generovania a spracovania vstupov potrebných pre ocenenie služieb, rozúčtovanie a fakturácia poskytnutých služieb.

6.3.3 Podporné procesy

6.3.3.1 Riadenie ľudských zdrojov

Proces riadenia ľudských zdrojov je zodpovedný za manažment celého životného cyklu zamestnancov organizácie (prípadne externých spolupracovníkov, brigádnikov, ...) od ich náboru až po odchod z organizácie. Zabezpečuje nasledovné aktivity:

- Stratégia a plánovanie ľudských zdrojov
- Riadenie náboru
- Administrácia zamestnancov a spolupracovníkov (pracovné zmluvy, popisy pracovných miest, výplaty, ...)

- Sledovanie a riadenie výkonnosti
- Rozvoj (vzdelávací program, sociálny program, prieskumy spokojnosti, ...)

6.3.3.2 Finančný manažment

Proces finančného manažmentu zabezpečuje komplexné služby v oblasti riadenia finančných zdrojov. Medzi jeho základné aktivity patrí:

- Plánovanie a rozpočtovanie
- Účtovníctvo
- Reporting
- Správa majetku
- Správa daní
- Správa pokladne

6.3.3.3 Obstarávanie

Proces zabezpečuje aktivity súvisiace s obstaraním hardvéru, softvéru, licencií a služieb od externých partnerov v súlade s aktuálnou legislatívou a za najlepších obchodných podmienok. Súčasťou procesu je vyjednávanie zmluvných podmienok a manažment dodávateľov a dodávateľských vzťahov.

6.3.3.4 Stratégia

Cieľom procesu je definovať stratégiu Dátového centra v súlade s potrebami a očakávaniami verejnej správy. Súčasťou procesu je:

- zber vstupov a strategická analýza
- definovanie stratégie a implementácia merateľných ukazovateľov
- stanovovanie priorít a cieľov
- monitorovanie strategických cieľov

6.3.3.5 Právne a regulácia

Proces zabezpečuje podporu v oblasti práva a regulácie pre všetky ostatné procesy.

6.3.3.6 Bezpečnosť a riadenie rizík

Proces zabezpečuje výkon aktivít súvisiacich s riadením bezpečnosti na úrovni organizácie. Jeho súčasťou je:

- Vývoj bezpečnostnej stratégie
- Definícia bezpečnostných štandardov a politík
- Implementácia a monitorovanie bezpečnostných mechanizmov a konceptov
- Riadenie rizík
- Riadenie trvalej kontinuity
- Výkon bezpečnostného auditu procesov a technológií
- Zabezpečenie súladu s požadovanými bezpečnostnými štandardami a usmerneniami

6.3.3.7 Správa budov a vybavenia

Proces zabezpečuje aktivity spojené so správou lokalít a vybavenia pre zamestnancov ako aj lokalít a vybavenia pre prevádzku dátových centier, správou vozového parku, prístupom a inžinierskym sieťam a odoberanie ich služieb a pod.

6.4 Základná koncepcia

Budovanie Dátového centra pre podporu eGov služieb predstavuje dlhodobý program, ktorý sa musí vyrovnáť z množstvom prekážok vychádzajúcich z aktuálneho stavu ISVS a spôsobu realizácie konsolidačných a štandardizačných aktivít na strane PO1 OPIS projektov. V ideálnom prípade by bolo možné budovať Dátové centrum ako poskytovateľa IT služieb vo forme cloud computingu. Za súčasného stavu ISVS a pri aktuálnych potrebách a požiadavkách projektov PO1 OPIS však považujeme za zmysuplné zahájiť rozvoj DataCentra s primárnym dôrazom na naplnenie potrieb jednotlivých projektov PO1 OPIS a zabezpečenie maximálnej prevádzkovej efektivity. Pre dosiahnutie týchto cieľov budú zavedené systémy pre riadenie služieb a podpory prevádzky, systémy riadenia informačnej bezpečnosti a nasadené moderné technológie s výraznou podporou virtualizácie. Tento „prechodný“ stav bude samozrejme budovaný v súlade s cieľovým smerovaním ku konsolidácii, štandardizácii a k poskytovaniu IT služieb formou plnohodnotného cloud computingu.

Dátové centrum predstavuje organizáciu pre poskytovanie komplexných IT služieb pre subjekty verejnej správy. Prevádzkuje podpornú infraštruktúru, IKT infraštruktúru, zabezpečuje rutinný beh služieb, informačných systémov a aplikácií vrátane používateľskej podpory v súlade s dohodnutými podmienkami. Riadi rozvoj portfólia poskytovaných IT služieb v súlade s požiadavkami svojich odberateľov, legislatívnym rámcom so zreteľom na dosiahnutie maximálnej efektivity.

Fyzicky bude dislokované do dvoch vzájomne prepojených geograficky oddelených lokalít. Lokálne dátové centrá budú konfigurované tak, aby bolo Dátové centrum schopné pre svojich odberateľov poskytovať služby s akceptovateľnou dostupnosťou aj v prípade výpadku, resp. katastrofickej udalosti na jednej lokalite.

Pri definovaní a návrhu Dátového centra sa primárne vychádza zo štandardu pre telekomunikačnú infraštruktúru dátových centier ANSI/TIA-942, ktorý spolu so štandardmi ako je ANSI/NECA/BICSI-002 definuje rámec požiadaviek a „best practices“ pre návrh a implementáciu dátových centier. Vyššie spomenuté štandardy nekladú požiadavky len na telekomunikačnú infraštruktúru, ale aj na technologickú infraštruktúru, serverové farmy, členenie a pod..

TIA-942 definuje štyri kategórie dátových centier:

Tabuľka 5 - Charakteristika dátového centra podľa ANSI/TIA-942

Oblasť	Kategória I.	Kategória II.	Kategória III.	Kategória IV.
Aktíva IKT	Neredundantné	Redundantné	Redundantné	Redundantné
Miera redundancie	N	N+1	N+1	Minimálne N+1
Distribúcia služieb	Neredundantná	Neredundantné	Redundantná pasívna	Redundantná aktívna
Segmentácia prevádzkového prostredia	Neumožňuje	Neumožňuje	Neumožňuje	Umožňuje
Údržba bez prerušenia služieb	Nie	Nie	Nie	Áno

Oblasť	Kategória I.	Kategória II.	Kategória III.	Kategória IV.
DC				
Odolnosť DC ako celku proti poruchám	Nie	Nie	Nie	Áno
Zabezpečenie personálom	Bez personálu	8 hod. zmena	12 hod. zmena	24 hod. zmena
Typická záťaž W/m ²	300	500	1600	>1600
Typická záťaž kg/m ²	400	450	700	>1000
Typická záťaž na 42'' rack v kW	3	6	12	15
Neprerušiteľný okruh chladenia	Nie	Nie	Čiastočne	Áno
Single point of failure	Veľa + ľudské chyby	Veľa + ľudské chyby	Málo + ľudské chyby	Žiadne
Maximálna doba nedostupnosti	28,8 hod.	22 hod.	1,6 hod.	0,8 hod.

Vzhľadom na koncepciu budovania ISVS podľa NKIVS, požiadavky na vysokú dostupnosť a kontinuitu eGov služieb realizovaných v rámci projektov PO1 OPIS je kategorizácia Dátového centra navrhovaná na úrovni Tier III, resp. Tier III+.

6.4.1 Geografické členenie

Geografické členenie Dátového centra predstavuje spôsob ako eliminovať riziko nedostupnosti poskytovaných služieb v prípade:

- straty konektivity
- straty napájania
- straty chladenia
- narušenej bezpečnosti
- povodne
- požiaru
- inej živelnnej pohromy
- a pod.

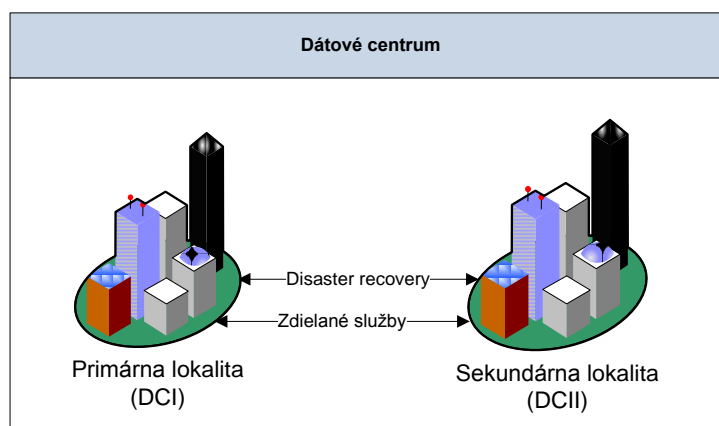
Vhodným spôsobom dosiahnutia vysokej dostupnosti a odolnosti voči katastrofám (disaster recovery) je využitie dvoch alebo viacerých fyzických lokalít a umiestnenie informačných systémov v nich tak, aby ich komponenty síce tvorili logický celok, ale boli umiestnené v dvoch alebo viacerých fyzických lokalitách. Komponenty informačného systému a dáta musia byť umiestnené tak, aby pri nedostupnosti jednej z fyzických lokalít poskytoval informačný systém, na ktorý sa kladie požiadavka na vysokú dostupnosť, stále požadované služby. Samotné informačné systémy je možné implementovať tak, aby v prípade nedostupnosti jednej fyzickej lokality poskytovali rovnaké portfólio služieb s rovnakou odozvou pre daný počet používateľov a transakcií ako v prípade, keď sú

všetky fyzické lokality dostupné alebo je možné poskytnúť alternatívne zníženú úroveň služieb počas výpadku jednej z fyzických lokalít. Často sa používa implementácia, pri ktorej je redundantná IKT infraštruktúra informačného systému použitá na testovacie účely.

Jednotlivé lokality Dátového centra si môžu vzájomne poskytovať vybrané služby ako sú monitoring IKT infraštruktúry, riadenie udalostí, manažment systémov a pod..

Odberatelia môžu využívať služby poskytované primárnou, sekundárnou alebo v prípade disaster recovery riešení oboma lokalitami Dátového centra.

Obrázok 11 – Geografické členenie Dátového centra



Z hľadiska geografickej distribúcie Dátového centra je dôležité vziať do úvahy vzdialenosť jednotlivých lokalít. Kým na jednej strane sa so zvyšujúcou vzdialenosťou znižuje riziko súčasnej nedostupnosti oboch lokalít na druhej strane rastie oneskorenie pri synchronizácii dát a rastú požiadavky na logistiku a obsluhu. Voľba a výber vhodných lokalít je preto otázkou nájdenia kompromisu. Ako jeden z faktorov pre správny výber variantu geografického rozloženia dátového centra je nutné posúdiť aj prístupnosti k existujúcej infraštruktúre zvlášť k optickým dátovým trasám.

Tabuľka 6 – Parametre geografického členenia Dátového centra

Požiadavka	Hodnota
Počet lokalít	2
Vzdialenosť	>200 km
Bezpečnosť	Žiadne prírodné a environmentálne riziká v lokalite, resp. blízkom okolí dátového centra: blízkosť rieky, záplavová oblasť, blízkosť závodu pre výrobu/spracovanie nebezpečných látok, miestnosti sanity v priestoroch DC, dopravné trasy pod.
Inžinierske siete	Možnosť napojenia na všetky inžinierske siete. Dostatočná kapacita energií.
Komunikačná infraštruktúra	Možnosť napojenia na optické dátové trasy.
Architektonické parametre objektu	Vyhovujúce architektonické členenie, ktoré umožňuje realizovať požadované stavebné členenie. Statika objektu vyhovujúca požiadavkám

Požiadavka	Hodnota
	inštalovanej technológie. Transportné trasy a manipulačné priestory. Vybudované prístupové komunikácie k objektu.
Právny vzťah k objektu	Vo vlastníctve poskytovateľa služieb, resp. štátu.
Vplyv na okolie	Minimálny dopad na blízke obydlia.

Vzhľadom na aktuálny stav v rezorte MFSR odporúčame ako primárnu lokalitu pre budovanie Dátového centra (DCI) využiť existujúce priestory DataCentra v Bratislave na Cintorínskej ulici, ktoré spĺňajú všetky požiadavky kladené na kapacitu, dostupnosť, modularitu a úroveň bezpečnosti.

Realizácia sekundárnej lokality Dátového centra (DCII) je možná tromi spôsobmi: adaptáciou existujúcich priestorov, výstavbou nového objektu, kúpou existujúceho dátového centra, ktoré vyhovuje stanoveným požiadavkám.

Všetky tri prístupy majú svoje výhody a nevýhody, z ktorých vyberáme nasledovné:

Variant A: Adaptácia priestorov v existujúcich objektoch

Výhody:

- nižšia cena stavebných prác
- jednoduchšia legislatíva a inžinierska činnosť
- kratšia doba realizácie

Nevýhody:

- riešenie sa musí prispôbiť existujúcim priestorom
- problém s optimálnym využitím inštalovanej infraštruktúry
- negatívny vplyv stavebných prác na prevádzku, najmä v prípade ak sa jedná o využívané priestory

Variant B: Výstavba nového objektu

Výhody

- optimálny návrh objektu bez obmedzení v zmysle požiadaviek na budovanie dátových centier
- minimálny, resp. žiadny vplyv na prevádzku

Nevýhody:

- vyššia cena stavebných prác
- dlhší čas realizácie
- náročnejšia inžinierska činnosť

Variant C: Kúpa existujúceho dátového centra

Výhody

- minimálny čas realizácie
- zohľadnenie požiadaviek kladených na budovanie dátových centier,
- minimálny, resp. žiadny vplyv na prevádzku existujúcej IKT

- žiadna, resp. minimálna inžinierska činnosť

Nevýhody:

- vyššia cena
- pravdepodobnosť menších úprav
- možná zastaranosť inštalovanej infraštruktúry

Voľba vhodného variantu bude predmetom samostatnej analýzy v rámci projektu, pričom kľúčovým kritériom bude ekonomická efektívnosť a udržateľnosť.

6.4.2 Stavebné a fyzické členenie

Vzhľadom na vysoké finančné nároky na výstavbu a prevádzky Dátového centra je dôležité efektívne využitie vnútorných priestorov. Pri návrhu fyzického členenia jednotlivých lokalít je potrebné zabezpečiť ergonómiu celkovej dispozície, určiť verejné a privátne zóny, napojenie na externú infraštruktúru a adresovať všetky potrebné priestory.

Na základe analýzy potrieb predpokladáme pre jednotlivé lokality nasledovné iniciálne priestorové požiadavky:

Tabuľka 7 – Predpokladané priestorové požiadavky Dátového centra

Lokalita	Plocha IKT	Celková plocha
* DCI	500 m ²	1000-1500 m ²
DCII	500 m ²	1000-1500 m ²

* V lokalite DCI je aktuálne vybudovaných a využívaných cca 250m² plochy pre IKT

Celková plocha je závislá od výkonovej hustoty na jeden dátový rozvádzač. V prípade štandardného dátového centra je pomer medzi plochou IKT a ostatnými priestormi typicky 1:1. V prípade vysokej hustoty (15kW/rozvádzač) je tento pomer 1:2.

Stavebné členenie oboch lokalít Dátového centra musí umožňovať vybudovať nasledovné priestory:

- Technologická miestnosť (serverová farma)
- Testovacia miestnosť (laboratórium)
- Priestor pre zdroje trvalého napájania (UPS)
- Priestor pre dieselagregát
- Miestnosť pre manažment systémy Dátového centra
- Pracovisko (miestnosti) pre vydávanie certifikátov
- Priestor pre SHZ
- Priestor pre logistickú podporu
- Kancelárske priestory pre obsluhu
- Vzduchotechnické zariadenia
- Priestor pre zabudovanie vonkajších klimatizačných jednotiek
- NN rozvodňa
- Trafostanica

- Centrálny bezpečnostný systém
- Káblová komora
- Priestory fyzickej ochrany objektu
- Hygienické zariadenia
- Parkovacie miesta

Modularita aspoň jednej lokality Dátového centra musí byť taká, aby umožňovala minimálne dvojnásobné rozšírenie priestorových kapacít.

Detailnejšie požiadavky pre stavebné a fyzické členenie dátového centra sú v [prílohe č. 1](#).

6.4.3 Fyzická a objektová bezpečnosť

Fyzickú bezpečnosť a objektovú bezpečnosť tvorí systém opatrení, ktorý slúži na ochranu údajov pred nepovolanými osobami a pred neoprávnenou manipuláciou v objektoch a chránených priestoroch a zároveň umožňuje prístup oprávnených osôb k chráneným údajom na základe určenia a princípu „need to know“.

Pri riešení požiadaviek fyzickej bezpečnosti a objektovej bezpečnosti vychádzame z predpokladu, že dátové centrum:

- bude potenciálne prijímať, ukladať a distribuovať utajované skutočnosti do stupňa utajenia „Dôverné“ v zmysle Zákona č. 215/2004,
- bezpečnostné projekty dátového centra budú spracované v súlade s požiadavkami legislatívy pre nakladanie s utajovanými skutočnosťami stupňa „Dôverné“.

Realizácia opatrení fyzickej a objektovej bezpečnosti je formou tzv. „hlbkovej ochrany“ v jednotlivých vrstvách. Tieto vrstvy sú tvorené opatreniami na:

- ukladanie utajovaných skutočností,
- ochranu chráneného priestoru,
- ochranu objektu,
- ochranu perimetra.

Model základného zabezpečenia chráneného priestoru dátového centra vychádza z analýzy NBÚ, ktorá zovšeobecňuje zistenia NBÚ pri realizácii chránených priestorov kategórie „Tajné“ a „Prísne tajné“. Model môže byť použitý ako referenčný model pre návrh bezpečnostných opatrení chránených priestorov jednotlivých dátových centier.

Tabuľka 8 – Model zabezpečenia chráneného priestoru

Bezpečnostné opatrenia	Popis	Ohodnotenie
Opatrenie ochrany chráneného priestoru	Steny z obyčajných tehál alebo tvaroviek tak, aby spĺňali typ, železobetónový strop a podlaha hrúbky najmenej 150 mm, dvere najmenej bezpečnostnej triedy 3, okenný otvor zabezpečený mrežou najmenej bezpečnostnej triedy 3.	SS3 = 3 body
Opatrenia ochrany objektu	Chránený priestor sa nachádza v objekte, pričom hranica chráneného priestoru nie je totožná s hranicou objektu. Objekt je tvorený pevnou stavebnou konštrukciou. Uzamykacie systémy, dvere, mreže, bezpečnostné	S3 = 3 body

Bezpečnostné opatrenia	Popis	Ohodnotenie
	fólie, okná a zasklenia poskytujú rovnaký stupeň odolnosti ako ostatné časti hranice objektu.	
Kontrola vstupov, náhodné prehliadky a režim návštev	Kontrola vstupu typu 2 s elektrickým systémom kontroly vstupu spĺňajúcim požiadavky triedy prístupu B a triedy rozpoznania 2 podľa príslušnej normy. Náhodné prehliadky sú realizované. Návštevy sú sprevádzané počas celého pobytu v objekte a chránenom priestore.	SS6 = 2 body SS12 = 1 bod SS7 = 2 body
Fyzická ochrana a elektrický zabezpečovací systém	Fyzická ochrana objektu je vykonávaná obchôdzkami zvonku objektu. Na stanovišti stáleho výkonu služby fyzickej ochrany sa zabezpečí nepretržitá prítomnosť najmenej jedného člena fyzickej ochrany – typ 3. Elektrický zabezpečovací systém (EVS) chráneného priestoru je typu 3 pri technickej úrovni prostriedkov EVS typu 3.	SS8 = 3 bodov SS91 = 3 body SS92 = 3 body
Opatrenia vonkajšej ochrany	Kamerová zostava zabezpečujúca monitorovanie vstupu do chráneného priestoru.	SS15 = 1 bod

Súčet celkového bodového ohodnotenia je 21 bodov. Podľa vyhlášky NBU 336/2004 Z.z. sú minimálne požadované hodnoty ohodnotenia opatrení fyzickej bezpečnosti a objektovej bezpečnosti chránených priestorov určených na manipuláciu s utajovanými skutočnosťami alebo na ich ukladanie na technických prostriedkoch pre kategóriu D:

Tabuľka 9 – Minimálne požadované ohodnotenie pre kategóriu D

Priestor určený na ukladanie utajovaných skutočností kategórie "Dôverné"	Miera rizika		
	Malá	Stredná	Veľká
Povinné: (S1)+(S2)+(S3)	4	4	5
Povinné: (S4)+(S5)	2	3	3
Nepovinné: (S6 a zvýšenie opatrení S1 až S5)	2	3	3
Celkový výsledok	8	10	11

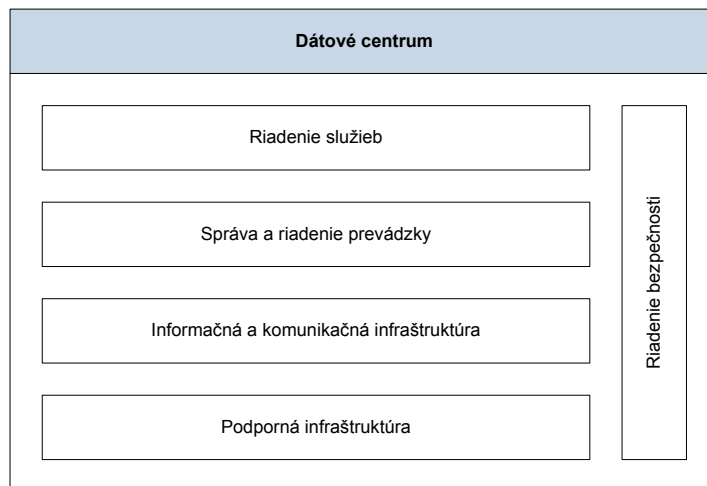
Z uvedeného vyplýva, že v modeli navrhované opatrenia fyzickej bezpečnosti a objektovej bezpečnosti chránených priestorov dátových centier spĺňajú a výrazne prekračujú minimálne požadované hodnoty týchto opatrení podľa bezpečnostného štandardu fyzickej bezpečnosti a objektovej bezpečnosti pre chránený priestor kategórie „Dôverné“ s určenou mierou rizika „Veľká“. Toto umožní v závislosti na miestnej situácii, v ktorej sa dátové centrum nachádza, variabilne prispôbiť úroveň jednotlivých opatrení bezpečnosti a tým prijať vyvážené a primerané riešenie celkovej fyzickej bezpečnosti a objektovej bezpečnosti.

Referenčná architektúra pre fyzickú a objektovú bezpečnosť je v [prílohe č. 2](#).

6.4.4 Logická architektúra

Logická architektúra Dátového centra pozostáva z piatich vzájomne sa dopĺňajúcich komponentov.

Obrázok 12 – Logická architektúra Dátového centra



Riadenie služieb

Cieľom vrstvy „Riadenie služieb“ je poskytovanie služieb Dátového centra pre koncových odberateľov. Riadi komunikáciu s odberateľom služieb, zabezpečuje naplnenie podmienok pre odber služieb, udržiava katalóg služieb (vrátane SLA) a implementuje procesy a technológie pre podporu a riadenie poskytovaných služieb.

Priebežne monitoruje stav úrovne poskytovaných služieb, zabezpečuje generovanie a distribúciu reportov. Na základe výstupov monitoringu zabezpečuje priebežnú optimalizáciu prevádzky tak aby bola požadovaná úroveň služieb dosiahnutá s maximálnou efektívnosťou.

Správa a riadenie prevádzky

Vrstva „Správa a riadenie prevádzky“ pokrýva procesy a technológie pre správu a údržbu IKT infraštruktúry Dátového centra.

Definuje a udržiava celkový model správy, procesy, politiky a jednotlivé procedúry, ktoré vstupujú do procesu správy a podpory prevádzky IKT infraštruktúry.

Pokrýva oblasť:

- technickej podpory
- aplikačnej podpory
- prevádzkovej podpory a správy príslušenstva a technického vybavenia (facilities management)

Informačná a komunikačná infraštruktúra

Predstavuje vrstvu fyzických komponentov IKT infraštruktúry, ktorá poskytuje systémové zdroje vyžívané jednotlivými službami. Je tvorená HW a SW komponentmi. Na úrovni HW typicky obsahuje sieťovú, serverovú a storage infraštruktúru. Na SW úrovni sa jedná o operačné systémy, databázové systémy, virtualizačné platformy, podporné nástroje pre správu a konfiguráciu IKT a pod..

Nosnou myšlienkou architektúry IKT infraštruktúry je virtualizácia serverov. Alokovaním potrebného výpočtového výkonu na jednotlivé aplikácie je možné dosiahnuť dynamicky sa meniace prostredie, ktoré je možné bez prerušenia poskytovania služieb prispôbiť aktuálnym požiadavkám. V prípade celkovej nedostatočnosti výpočtovej kapacity umožňuje virtualizácia efektívne rozšírenie o ďalší výpočtový výkon.

Riešenie predpokladá vytvorenie centrálnych pamäťových úložísk (storage) rozdelených do niekoľkých kategórií redundantných dátových skladov. Jeden z nich bude slúžiť na uskladnenie a sprístupnenie dát prevádzkovaných informačných systémov a je primárnym zdrojom informácií. Druhý bude vystupovať ako aktívna, resp. pasívna záloha v prípade výpadku primárneho výpočtového centra.

Podporná infraštruktúra

Predstavuje technologickú infraštruktúru Dátového centra a súvisiace technológie určené pre jej správu a údržbu. Jedná sa hlavne o:

- dátová kabeláž
- dátové rozvádzače
- napájanie
- environmentálny manažment
- protipožiarny systém

Podporná infraštruktúra bude budovaná v súlade s existujúcimi štandardmi a s použitím moderných technológií. Vybrané komponenty budú redundantné.

Riadenie bezpečnosti

Oblasť riadenia bezpečnosti sa týka prierezuvo všetkých logických vrstiev tvoriacich riešenie Dátového centra. Definuje bezpečnostné politiky a mechanizmy pre zabezpečenie integrity, dostupnosti a dôvernosti. Vykonáva audit dodržiavania stanovených bezpečnostných politik a prijíma rozhodnutia pre elimináciu nedostatkov.

Komponent „Riadenie bezpečnosti“ bude pokrývať oblasť:

- Ochrana koncových zariadení a bezpečnosť infraštruktúry
- Aplikačná bezpečnosť
- CA a PKI

Zároveň bude zabezpečovať úlohy spojené s definovaním a riadením procesov pre riadenie dostupnosti, riadenie kontinuity a DRP.

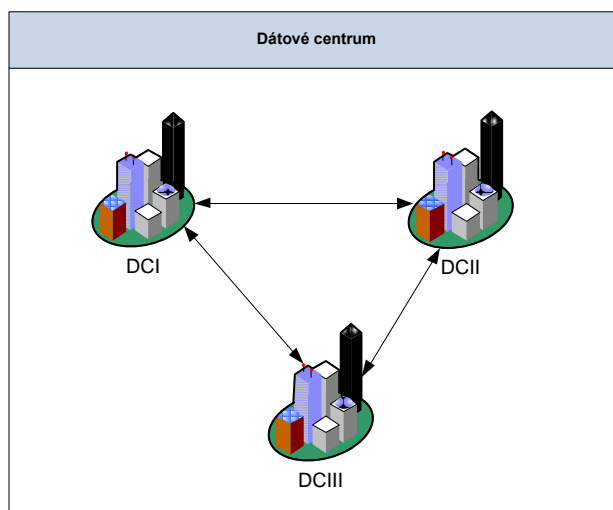
6.4.5 Rozvoj Dátového centra

Rozvoj Dátového centra je možné analyzovať z niekoľkých uhlov pohľadu:

- Kapacít a zdrojov
- Technologického
- Spôsobu poskytovania služieb

V rovine kapacitného rozvoja sa očakáva postupné zvyšovanie kapacít Dátového centra, ktoré bude realizované prostredníctvom rozširovania plochy v existujúcich lokalitách a/alebo budovaním ďalších geograficky distribuovaných lokalít s cieľom priblížiť IT služby čo najbližšie k ich odberateľom.

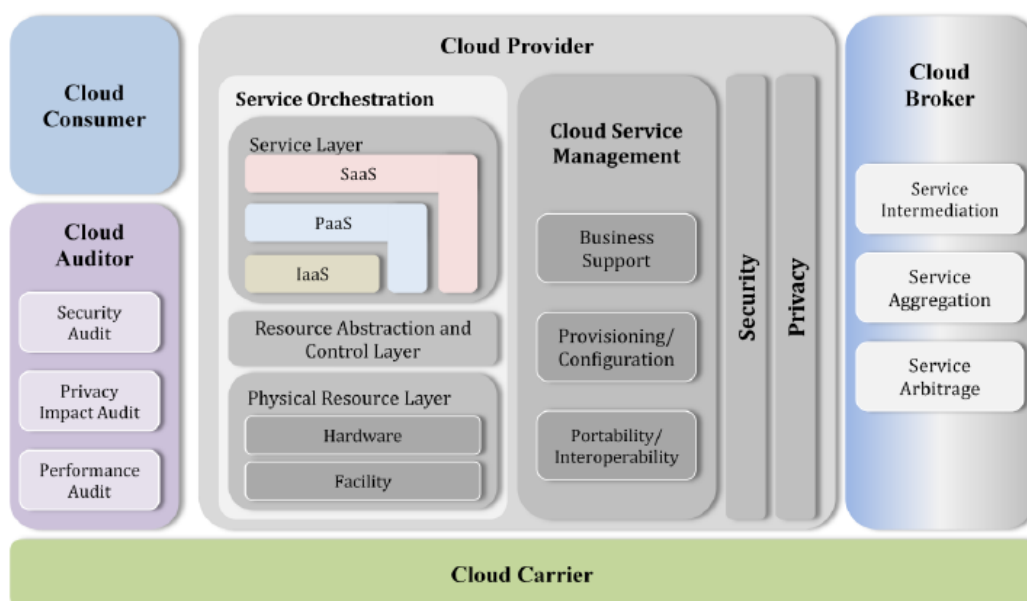
Obrázok 13 – Geografický rozvoj Dátového centra



Ďalší prirodzený rozvoj v oblasti zvyšovania kapacít a zdrojov bude viazaný na zmenu dostupných technológií. Dátové centrum musí v rámci svojej modularity umožňovať obnovu technicky alebo morálne zastaraných technických prostriedkov.

Kľúčovou oblasťou rozvoja Dátového centra je zvýšenie efektivity poskytovania služieb migráciou na poskytovateľa IT služieb formou cloud computing. Tento cieľový stav bude vyžadovať úpravu modelu a architektúry dátového centra tak, aby bolo schopné adresovať všetky nové požiadavky a výzvy, ktoré so sebou nesie cloud computing. Jedným z dostupných konceptuálnych referenčných modelov pre cloud computing je architektúra definovaná a udržiavaná v rámci National Institute of Standards and Technology¹.

Obrázok 14 – Referenčný model cloud computing



¹ NIST Special Publication 500-292, „NIST Cloud Computing Reference Architecture“, September 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

Hore uvedená referenčná architektúra rozlišuje päť základných aktérov (osoby alebo organizácie), ktorí medzi sebou komunikujú v definovaných scenároch:

Zákazník (odberateľ) – kľúčový aktér, ktorý využíva služby poskytovateľa cloud a udržiava s ním obchodný vzťah. Zákazník má prístup ku katalógu služieb, žiada o príslušné služby a uzatvára zmluvu o dodávke služieb, ktorej typickou súčasťou je SLA a cenová politika.

Poskytovateľ – je zodpovedný za poskytovanie služieb. Nadobúda a spravuje IKT infraštruktúru, prevádzkuje cloud softvér pre poskytovanie služieb a zaisťuje dodávku sieťovo prístupných služieb pre zákazníka. Aktivity poskytovateľa sa líšia v závislosti od typu služby, pričom najkomplexnejšie sú viazané na SaaS, ktorý vyžaduje nasadenie, konfiguráciu, údržbu a prevádzku infraštruktúry a softvéru v cloud infraštruktúre. Primárne aktivity poskytovateľa sú v nasledovných oblastiach:

- Nasadenie služieb
- Orchestrácia služieb
- Manažment cloud služieb
- Bezpečnosť
- Ochrana súkromia

Auditor – vykonáva nezávislé posúdenie stavu a systému riadenia cloud služieb vrátane výroku a návrhu odporúčaní. Audit je realizovaný za účelom verifikácie voči definovaným štandardom. Môže byť vykonaný pre oblasť:

- Bezpečnosti
- Ochrany súkromia
- Výkonnosti

Broker – vykonáva sprostredkovanie služby pre odberateľa v prípade ak je integrácia cloud služieb príliš komplexná. Broker je v tomto prípade entita, ktorá riadi využívanie, výkonnosť, dodávku a vyjednávanie služieb medzi poskytovateľom a zákazníkom. Vo všeobecnosti môže broker poskytovať tri kategórie služieb:

- Sprostredkovanie
- Agregácia
- Arbitráž

Carrier – poskytuje spojenie a transportnú vrstvu pre cloud služby medzi poskytovateľom a odberateľom, ktorá môže byť realizovaná prostredníctvom počítačovej siete, telekomunikačnými zariadeniami, fyzickým transportom a pod..

Na úrovni poskytovateľa definuje architektúra 4 základné komponenty:

Orchestrácia služieb – predstavuje trojúrovňový model reprezentujúci tri systémové oblasti, ktoré musí poskytovateľ pokryť aby bol schopný dodať cloud službu.

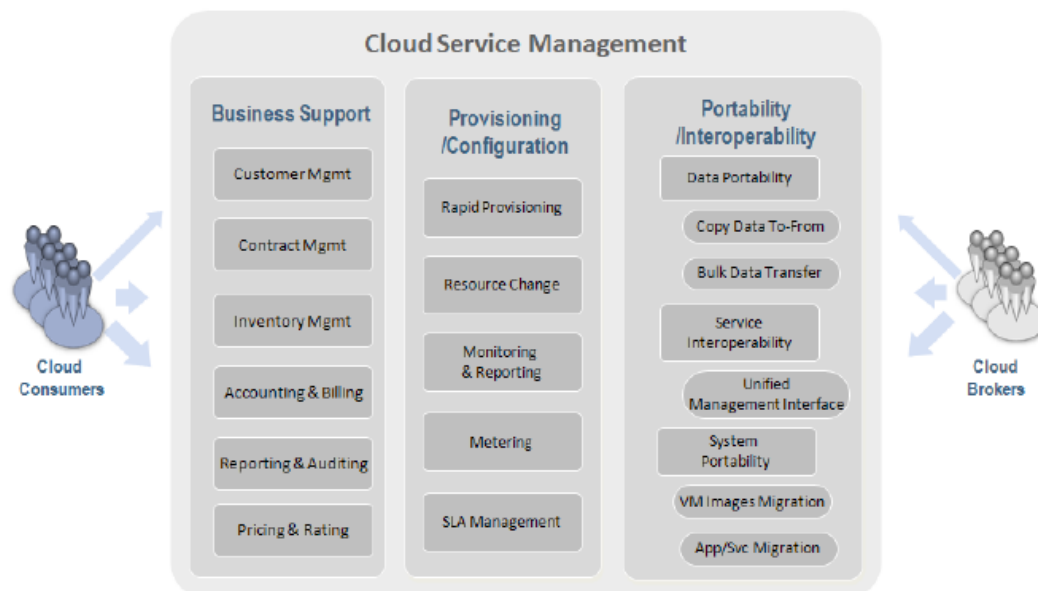
Na najvyššej úrovni je definované rozhranie pre prístup ku všetkým typom služieb (SaaS, PaaS, IaaS). Zároveň je možné, ale nie nevyhnutné, aby boli aplikácie poskytované ako SaaS budované na PaaS a komponenty PaaS budované na IaaS.

Na strednej vrstve modelu je realizovaná abstrakcia a riadenie zdrojov. Obsahuje komponenty, ktoré cez softvérové abstrakcie (hypervisor, virtuálne servere, virtuálny storage, ...), zabezpečujú a riadia prístup k fyzickým zdrojom. Úlohou abstrakcie zdrojov je zabezpečiť efektivitu, bezpečnosť a spoľahlivosť fyzických zdrojov. Riadiaci aspekt tejto vrstvy sa vzťahuje k softvérovým komponentom, ktoré zabezpečujú alokáciu zdrojov, riadenie prístupu a monitorovanie ich využitia.

Najnižšia vrstva predstavuje úroveň fyzických výpočtových zdrojov, ktoré obsahujú prvky IKT a technologickej infraštruktúry.

Manažment cloud služieb – obsahuje všetky servisne orientované funkcie, ktoré sú nevyhnutné pre prevádzku a riadenie požadovaných a poskytovaných služieb.

Obrázok 15 – Manažment cloud služieb



Business podpora predstavuje súbor obchodne orientovaných služieb zaoberajúcich sa vzťahmi so zákazníkom a súvisiace podporné procesy:

- Customer management: manažment zákazníckych účtov, riadenie používateľských profilov, riešenie požiadaviek a problémov, kontakt so zákazníkom a pod.
- Contract management: správa servisných zmlúv, príprava návrhov zmlúv, riadenie zmluvných jednaní, vypovedanie zmluvných vzťahov a pod.
- Inventory Management: zavedenie a správa katalógu služieb, riadenie konfigurácie a pod.
- Accounting and Billing: správa účtovných informácií, fakturácia a platby, upomienky a pod.
- Reporting and Auditing: monitorovanie používateľov, generovanie reportov a pod.
- Pricing and Rating: ocenenie služieb a určenie cenového modelu, správa cenovej politiky, manažment propozícií a pod.

Zriadenie a konfigurácia – obsahuje nasledovné procesy a funkcie:

- Rapid provisioning: automatické nasadenie cloud system založeného na požadovaných službách, zdrojoch a funkcionalitách.
- Resource changing: prispôsobenie konfigurácie a priradenie zdrojov na opravu, upgrade a zaradenie nových uzlov do cloud.
- Monitoring and Reporting: zisťovanie a monitorovanie virtuálnych zdrojov, monitorovanie cloud operácií a udalostí, monitorovanie výkonnosti, generovanie reportov.
- Metering: schopnosť merať s vyššou mierou abstrakcie, ktorá závisí od typu služby.
- SLA management: riadenie SLA zmlúv, monitorovanie SLA a zabezpečenie súladu medzi SLA a definovanými parametrami a politikami.

Prenositel'nosť a interoperabilita – zabezpečuje dátovú prenositeľnosť, interoperabilitu služieb a systémovú prenositeľnosť. Dátová prenositeľnosť je chápaná ako schopnosť zákazníka prenášať dátové objekty z/do cloudu. Interoperabilita služieb je schopnosť zákazníka využívať dáta a služby v prostredí viacerých poskytovateľov s využitím unifikovaného rozhrania. Systémová prenositeľnosť umožňuje prenos inštancií virtuálnych strojov alebo ich obrazov medzi poskytovateľmi, resp. migráciu aplikácií a služieb od jedného poskytovateľa k druhému. Požiadavky na prenositeľnosť a interoperabilitu sa diferencujú v závislosti od modelu, t.j. SaaS sa primárne zameriava na dátovú prenositeľnosť kým IaaS na systémovú prenositeľnosť.

Bezpečnosť – bezpečnosť je aspekt architektúry, ktorý sa týka všetkých úrovní referenčného modelu od fyzickej bezpečnosti až po aplikačnú bezpečnosť. Z toho dôvodu sa bezpečnosť cloud computing architektúry týka nie len poskytovateľa služieb ale aj zákazníka a ostatných relevantných aktérov. Systémy pre cloud musia adresovať všetky známe bezpečnostné požiadavky ako autentifikácia, autorizácia, dostupnosť, dôvernosť, integrita, správa identít, auditing, monitoring bezpečnosti, riadenie bezpečnostných incidentov a manažment bezpečnostných politík. Cloud computing však prináša do oblasti informačnej bezpečnosti aj špecifiká, ktoré vyplývajú zo zvoleného distribučného modelu a modelu nasadenia.

Pre jednotlivé distribučné modely (SaaS, PaaS, IaaS) sú využité rôzne typy manažment operácií a rôzne spôsoby prístupu ku cloud systému. Napríklad služby SaaS sú typicky prístupné po sieti cez Internet a web prehliadač čo vyžaduje dôsledne riešiť bezpečnosť web prehliadačov. V prípade IaaS, ktoré sú poskytované nad virtuálnou infraštruktúrou, je potrebné riešiť bezpečnosť hypervizora a pod..

Výrazné implikácie na bezpečnosť má aj distribučný model. Jedným z uhlov pohľadov je zabezpečenie výlučnosti zákazníka. V privátnych cloud modeloch sa napr. nemusí tak výrazne riešiť oddelenie jednotlivých odberateľov ako vo verejných. Iný pohľad na analýzu bezpečnostných dopadov v jednotlivých distribučných modeloch vychádza z ochrany prístupovej hranice do cloudu. Koncept bezpečnostného perimetra neobsahuje iba firewallly a zabezpečenie siete ale riadi hranice medzi rôznymi prístupovými úrovňami bežiacieho softvéru, hranice medzi aplikáciami a operačným systémom a pod..

V tradičných IT systémoch má organizácia plnú kontrolu nad všetkými vrstvami výpočtových zdrojov a celým ich životným cyklom. V cloud prostredí sa táto kontrola delí medzi poskytovateľa a odberateľa, ktorí sú nútení spolupracovať pri návrhu, vývoji, nasadení a prevádzke cloud systémov. Rozdelenie kontroly so sebou prináša aj rozdelenie a zdieľanie zodpovednosti za riadenie informačnej bezpečnosti. Na základe analýzy je potrebné definovať, ktorá strana má lepšiu pozíciu pre implementáciu jednotlivých bezpečnostných opatrení.

Ochrana súkromia – poskytovateľ musí zabezpečiť ochranu a konzistenciu chránených a dôverných údajov pri ich spracovaní a využívaní.

6.5 Technická architektúra

Základným princípom pre budovanie technickej architektúry Dátového centra je technologická neutralita a modulárnosť jednotlivých komponentov, ktorá minimalizuje problémy s ich vzájomnou prepojitelnosťou a obnovou.

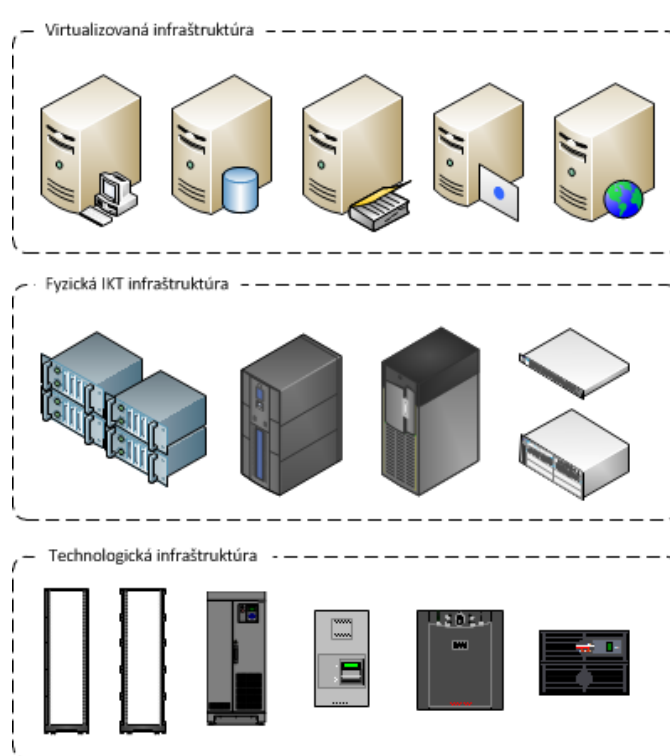
Z pohľadu cieľovej vízie, ktorou je implementácia cloud computingu, je požadovaná vysoká miera konsolidácie a virtualizácie.

Hardverová architektúra Dátového centra, jeho priestorové podmienky, výpočtová, storage a zálohovacia kapacita musí zohľadňovať požiadavky POI OPIS projektov (eGov služieb), pri ktorých sa predpokladá využitie služieb Dátového centra. Keďže v súčasnosti nie sú tieto požiadavky známe v dostatočnej miere úplnosti a detailu, nie je možné určiť cieľové výpočtové kapacity a finálnu technickú architektúru Dátového centra.

V „prechodnom“ stave, t.j. pred migráciou na cloud computing, sa predpokladá, že jednotlivé POI OPIS projekty budú primárne využívať služby housingu, resp. hostingu (IaaS) a samotná IKT infraštruktúra sa bude dodávať v rámci týchto projektov. Už v tejto etape však musí dátové centrum poskytovať plne funkčnú technologickú infraštruktúru, komunikačnú infraštruktúru a virtualizovanú infraštruktúru pre prevádzku podporných systémov:

- Zálohovanie a obnova
- Monitoring udalostí
- Monitoring bezpečnosti
- Riadenie IKT infraštruktúry
- Riadenie služieb
- Riadenie informačnej bezpečnosti

Obrázok 16 – Technická architektúra



6.5.1 Technologická infraštruktúra

Technologická infraštruktúra Dátového centra obsahuje nasledovné komponenty:

- Dátová kabeláž
- Dátové rozvádzače
- Napájanie
- Environmentálny manažment
- Protipožiarny system

Štandardy a referenčné architektúry vzťahujúce sa k jednotlivým komponentom technologickej infraštruktúry sú uvedené v [prílohe č.3](#).

6.5.1.1 Dátová kabeláž

Dátová kabeláž je dôležitou súčasťou dátového centra. Od jej funkcionality je závislá funkcionality celej IKT. Návrh riešenia musí zohľadniť nasledovné parametre:

- Štruktúrovaný návrh optických a metalických spojov
- Životný cyklus použitej technológie 10 rokov
- Konsolidovaná modulárna architektúra
- Návrh zodpovedajúci štandardom návrhu kabeláže pre dátové centrá

Predpokladáme nasledovné požiadavky na štruktúrovanú kabeláž pre každú lokalitu Dátového centra:

- minimálne dva sieťové rozvádzače
- v každom sieťovom rozvádzači budú centrálné uzly pre LAN a SAN, t.j. z každého serverového rozvádzača bude vedená vždy polovica káblov do jedného a polovica do druhého uzla
- na každý dátový rozvádzač pre serverovú infraštruktúru budú privedené metalické aj optické káble vrátane rezervy

6.5.1.2 Dátové rozvádzače

Podľa možnosti budú všetky komponenty IKT infraštruktúry umiestňované do štandardných dátových rozvádzačov 42U.

Vzhľadom na očakávaný rozsah IKT infraštruktúry pre projekty PO1 OPIS (viď kap. 7.3) predpokladáme nasledovné iniciálne požiadavky na dátové rozvádzače:

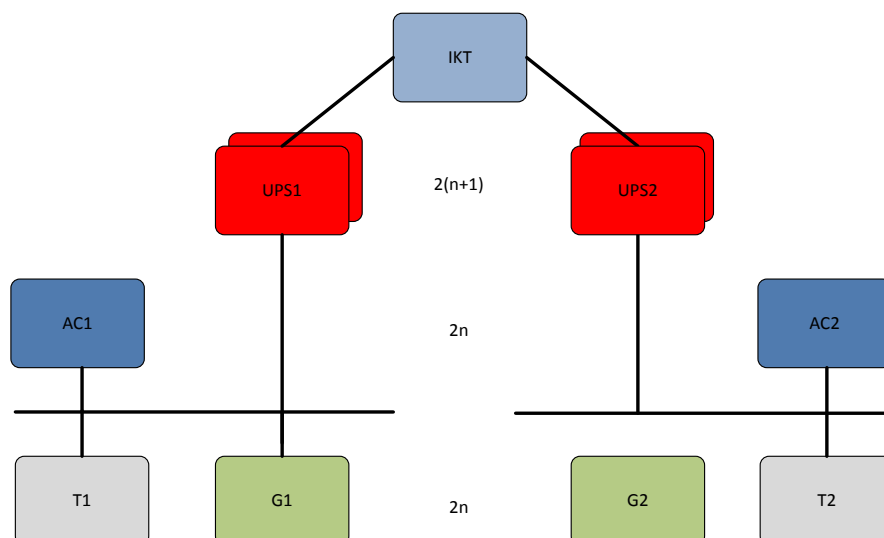
Tabuľka 10 – Predpokladané počty dátových rozvádzačov pre projekty PO1 OPIS

Typ	Počet rozvádzačov	
	DCI	DCII
Rozvádzač pre serverové zariadenia	42	35
Rozvádzač pre storage zariadenia	13	13
Sieťový rozvádzač	3	3
Rozvádzač pre ENI	1	1
Rezerva	10	10
SPOLU	69	62

6.5.1.3 Napájanie

Vzhľadom na ambíciu budovať Dátového centrum na úrovni Tier III+ navrhujeme vybudovať dve nezávislé aktívne vetvy od prívodov VN/NN prípojky do objektu až po napájanie dátového rozvádzača v dátovom centre. Obidve vetvy budú zálohované vlastnou UPS a dieselagregátorom. Rozloženie výkonu na jednotlivé vetvy bude rovnomerné, pričom každá vetva môže byť zaťažená maximálne na 50%, aby mala dostatočnú výkonovú kapacitu na prevzatie celej záťaže v prípade poruchy alebo servisu, ktorý má za následok odstavenie druhej vetvy.

Obrázok 17 – Návrh redundancie napájania



Dieselagregát umiestnený na samostatnom mieste. K jeho spusteniu dôjde automaticky pri výpadku VN napájača na povel od zálohového automatu, ktorý bude reagovať na pokles napätia alebo výpadok el. prúdu. Záložný zdroj bude zásobovať celú budovu dátového centra. Bude mať samostatný NN rozvádzač, ktorý bude prepojený s NN rozvádzačom trafostanice pomocou záložného deonu.

Pre zálohu napájania technologickým miestnosť predpokladáme modulárny systém UPS v spoločnom paralelnom zapojení s redundanciou N+1. Ku každej UPS bude priradený batériový modul s kapacitou batérií na 30 minút prevádzky pri plnom výkonovom zaťažení. Batérie budú fyzicky oddelené od UPS a budú umiestnené v špeciálnych montovateľných rozvádzačoch spolu s batériovými odpojovačmi.

6.5.1.4 Environmentálny manažment

Zdrojom chladu bude bloková chladiaca jednotka umiestnená vo vonkajšom priestore. Teplonosným médiom bude zmes s nízkym bodom tuhnutia. Konfigurácia zdrojov chladu bude n+1 pre zaistenie redundancie.

V prípade inštalácie vysokého výkonu na dátový rozvádzač bude potrebné využiť sofistikované spôsoby chladenia. Jedným z možných riešení je uzavretie studenej a teplej uličky a chladenie do uličky, resp. chladenie priamo do rozvádzača. V tomto prípade sú vnútorné jednotky inštalované vo forme rozvádzačov umiestnených medzi rozvádzače s IKT infraštruktúrou čo prináša nasledovné výhody:

- Modulárny dizajn, ktorý poskytuje škálovateľnosť riešení pridávaním chladiacich jednotiek tak, ako sa zvyšujú požiadavky na chladenie
- Umiestnenie jednotky v rade dátových rozvádzačov prináša zdroj chladu bližšie k zdrojom tepla. Tento prístup eliminuje miešanie vzduchu a poskytuje predpovedateľnú architektúru chladenia.
- Ovládanie prívodu vzduchu do dátových rozvádzačov garantuje vstupnú teplotu pre IKT zariadenia.

Chladenie miestnosti s UPS bude v zostave n+1. Chladný vzduch bude vyfukovaný pri podlahe a ohriaty bude nasávaný pri strope miestnosti.

Pre vetranie technologických miestností a miestnosti s UPS bude využité rovnotlakové vetranie. Vetranie bude zabezpečovať kompaktná vetracia jednotka, ktorá je vybavená prírodným, odťahovým ventilátorom, filtráciou vzduchu a elektrickým ohrevom vzduchu.

6.5.1.5 Protipožiarny systém

Technologické priestory budú chránené SHZ, EPS a SDP. Pre ostatné priestory bude inštalovaná EPS, v prípade, že v nich nie je inštalovaná EPS budovy. Vyhodnocovanie signálov z EPS a SDP v dátovom centre musí byť procedurálne zaistené.

Spustenie SHZ je možné dvomi spôsobmi:

- samočinne (automaticky) – signálom z externého zdroja
- ručne (manuálne) – aktiváciou spúšťacieho ventilu

Samočinne - prostredníctvom výstupu z riadiacej jednotky SHZ na základe definovaných podmienok. Počas plynutia nastaveného času od signalizácie požiaru do vyslania signálu na otvorenie ventilov bude možné automatické spustenie hasenia prerušiť pomocou tzv. deaktivčných tlačidiel. Samočinné spustenie SHZ sa rieši signálom pre otvorenie elektromagnetického ventilu na zásobníku s hasiacou látkou od riadiacej ústredne SHZ, prípadne systému EPS na základe spracovaných a vyhodnotených informácií pripojených detektorov požiaru.

Manuálne – pomocou tzv. aktivačných tlačidiel, pripojených k riadiacej jednotke SHZ.

Návrh predpokladá:

- Plynové SHZ:
 - Hasiace médium prírodný plyn IG-55
 - Systém 200 / 300 bar
 - Samostatné strojovne SHZ
 - Samostatné istenie každého HÚ
- EPS pre riadenie SHZ:
 - Dvojstupňová EPS s centrálnou ústrednou
 - Opticko-dymové hlásiče
 - Samostatné riadiace ústredne SHZ pre každý HÚ
- Skorú detekciu požiaru (doplňkový hlásič EPS)
 - Vysoko citlivý hlásič s nasávaním
 - 2 úrovne signalizácie zadymenia

6.5.2 IKT infraštruktúra

IKT infraštruktúra Dátového centra obsahuje nasledovné komponenty:

- Komunikácia (WAN, LAN, SAN)
- Ukladanie dát
- Servery
- PKI a LTA

Štandardy a referenčné architektúry vzťahujúce sa k jednotlivým komponentom IKT infraštruktúry sú uvedené v [prílohe č.4](#).

6.5.2.1 Komunikačná infraštruktúra

Pre účely tejto štúdie WAN sieť zabezpečuje:

- IP alebo TCP/IP prepojenie medzi dátovými centrami navzájom

- IP alebo TCP/IP prepojenie medzi odberateľmi služieb a poskytovateľmi týchto služieb, ktorými sú informačné systémy prevádzkované v Dátovom centre
- IP alebo TCP/IP prepojenie medzi Dátovým centrom a obslužným personálom
- synchronizáciu a výmenu dát medzi lokalitami Dátového centra cez IP alebo TCP/IP prepojenie alebo cez FC protokol.

Pre naplnenie hore uvedených požiadaviek predpokladáme IP spojenie medzi lokalitami Dátového centra s rýchlosťou 10 Gb/s a FC spojenie 8 alebo 10 Gb/s podľa dostupnej technológie. V oboch prípadoch odporúčame redundantné.

Berúc do úvahy vzdialenosť medzi dátovými centrami, požadovanú kapacitu prenosu a požiadavku na prenos IP a FC protokolov bude nevyhnutné zabezpečiť fyzické spojenie oboch centier pomocou dedikovanej optickej kabeláže. Minimálne jeden pár pre FC, ak existujúca IP WAN infraštruktúra dokáže zabezpečiť požadovanú kapacitu pre prenos IP alebo dva a viac párov, tak aby bolo možné preniesť paralelne IP aj FC.

Alternatívne pri vyšších vzdialenostiach a tam kde sa páry neosvietenej optiky tzv. „dark fiber“ kupujú od prevádzkovateľov môže byť efektívnejšie využiť DWDM metódu multiplexu kde sa farebné spektrum rozloží do viacerých vlnových dĺžok tzv. farieb a na každej farbe sa potom prenáša iný protokol. Potom aj napriek vyšším obstarávacím nákladom je možné ušetriť za prevádzku služby spojenej s prenájomom párov optického kábla.

Prepojenie lokalít DCI a DCII navrhujeme realizovať kvalitnou a robustnou optickou infraštruktúrou s využitím špičkových komponentov a zariadení, ktoré zaručujú vysokú kvalitu, spoľahlivosť služby, maximálnu priepustnosť a odolnosť voči poruchám.

LAN bude podľa možnosti vytvorená s využitím zdieľanej infraštruktúry, ktorá umožní technologickú unifikáciu, optimalizáciu požiadaviek na technologickú infraštruktúru a efektivitu obsluhy. Nevýhodou môžu byť vzájomné interferencie na LAN sieťových komponentoch, ktoré sa dajú do značnej miery riadiť vhodnou topológiou siete a konfiguráciou zariadení.

LAN dátového centra odporúčame rozdeliť v kontexte ISO OSI L3 topológie do nasledovných bezpečnostných zón/vrstiev:

- Internet DMZ
- Prezentačná vrstva
- Aplikačná vrstva
- Databázová vrstva
- Vrstva manažmentu
- Vrstva pre zálohovanie a archiváciu

Návrh predpokladá optickú kabeláž medzi dátovými rozvážačmi z dôvodu vysokých prenosových rýchlostí medzi core a prístupovou vrstvou. V systéme predpokladáme výnimky ako napr. pripojenie konzoly, kde môže byť efektívnejšie metalické vedenie. S metalickou kabelážou sa uvažuje v rámci dátových rozvážačov a s prenosovými rýchlosťami na úrovni 1 Gbps a menej.

Každý server bude do LAN pripojený viacerými Ethernet portami:

- dátový „uplink“ použitý pre dátové toky (redundantné zapojenie, každý port do iného prepínača)
- manažment pre dohľad a manažment servera
- zálohovanie/archivácia

LAN sieť bude na úrovni ISO OSI L2 je rozdelená do bezpečnostných vrstiev/zón pomocou takzvaných virtuálnych LAN alebo VLAN. Ďalej odporúčame, ak to technológia umožní, izolovať

servery jednotlivých informačných systémov v rámci VLAN pomocou technológie „private“ VLAN alebo PVLAN. PVLAN definuje promiskuitné porty používané pre zdieľanú LAN infraštruktúru, ktoré môžu komunikovať so všetkými portami v rámci VLAN a izolované porty, ktoré sa spravidla využívajú pre pripojenie serverov informačných systémov.

Medzi základné LAN sieťové komponenty uvažované na úrovni tohto návrhu patria predovšetkým:

- Prepínače
- Smerovače
- Firewally
- IDS/IPS
- Lokálne a globálne loadbalancery

Na úrovni prepínačov predpokladáme dvojúrovňovú štruktúru

- Core-distribučná vrstva
- Prístupová vrstva

Core-distribučná vrstva by mala byť reprezentovaná viacerými redundantnými a fyzicky oddelenými „enterprise class“ prepínačmi, ktoré bude možné v budúcnosti rozšíriť o ďalšie prepínače (vytvorením distribučnej vrstvy) a tak zabezpečiť rast.

Prístupová vrstva bude reprezentovaná redundantnými prepínačmi na úrovni dátových rozvádzačov či už vo forme voľne stojacich prepínačov alebo vo forme prepínačov zabudovaných do „blade“ technologického puzdra.

Na úrovni smerovačov predpokladáme redundantné smerovače s podporou dynamického smerovania, MPLS a QoS. MPLS je požadované kvôli podpore pripojenia k existujúcej WAN rezortnej sieti založenej na MPLS. QoS je požadovaná kvôli limitovaniu interferencií medzi informačnými systémami a na zabezpečenie potrebnej prenosovej kvality a kapacity pre vybrané systémy.

Na úrovni firewallov predpokladáme redundantné zariadenia. Odporúčame použiť redundantné firewally od dvoch alebo viacerých výrobcov tak, aby sa zabránilo potenciálnemu prieniku spôsobeného chybou v kóde firewall. Pre pripojenie do Internetu sa odporúča firewall, ktorý pracuje na siedmej vrstve IOS OSI modelu. Firewally budú zároveň zabezpečovať izolovanie dát v jednotlivých zónach na základe vopred určených pravidiel, ktoré s pravidla povoľujú dátové toky pre vybrané služby od vybraných zdrojov k vybraným cieľom. Z pohľadu zníženia prevádzkovej náročnosti predpokladáme, podporu nasadenia virtuálnych firewallov.

Lokálne loadbalancery budú zabezpečovať distribúciu prichádzajúcich požiadaviek medzi viacerými servermi umiestnených v tom istom dátovom centre. Predpokladáme redundantné loadbalancery s možnosťou udržiavania perzistentných spojení, podporou SSL akceleratorov a možnosťou kontroly dostupnosti serverov a služieb.

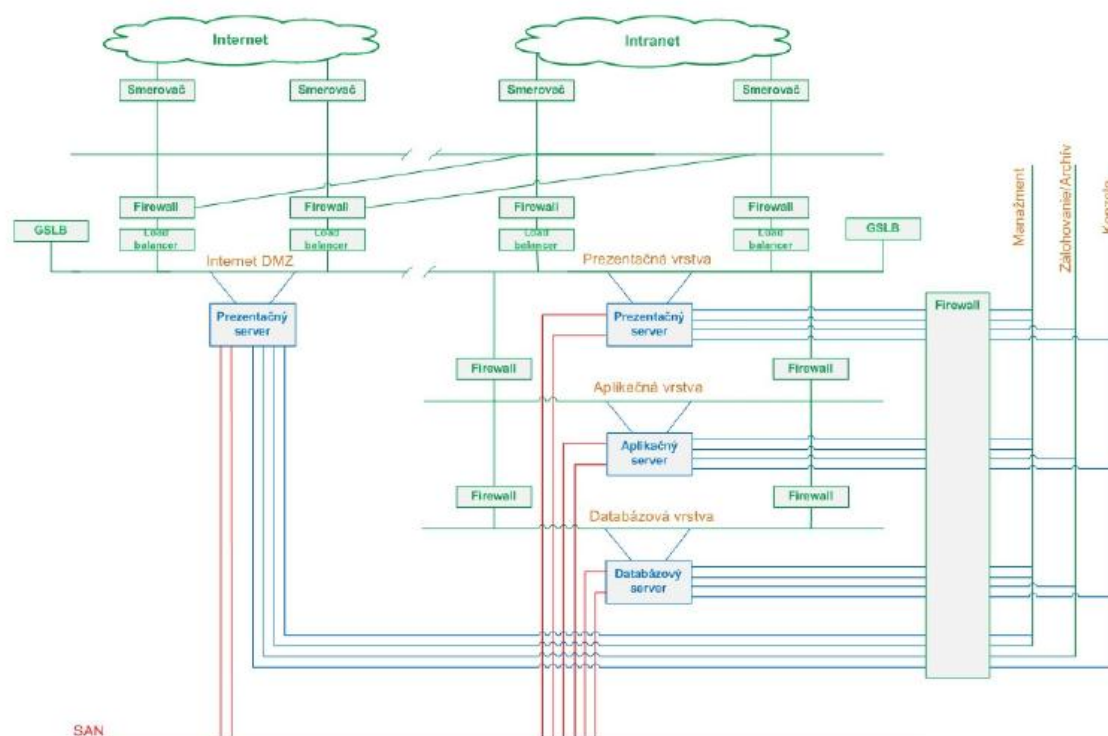
Globálne loadbalancery (Global Site Load Balancer - GSLB) majú za úlohu distribúciu prichádzajúcich požiadaviek na viaceré servery umiestnených vo viacerých geograficky distribuovaných dátových centrách. Predpokladáme podporu minimálne dvoch lokalít a „authoritative“ DNS.

IDS/IPS na základe vopred definovaných signatúr detekujú potenciálne ohrozenia a v prípade IPS aj proaktívne modifikujú pravidlá „firewall-ov“ tak, aby zabránili prienikom rizikových dát. Predpokladáme redundantné zapojenie IDS/IPS minimálne na hranici dátového centra (Internet aj intranet). Pri IDS/IPS sa predpokladá riešenie s vysokou dostupnosťou, porty pre „out of band“ manažment a v prípade „rack-mountable“ zariadení sa požaduje dostatočné množstvo voľných slotov a dostatočné bohatstvo kariet, tak aby sa dosiahla potrebná škálovateľnosť a modularita riešenia.

Tabuľka 11 – Predpokladané zariadenia LAN

Zariadenie	Počet	
	DCI	DCII
Prepínač – core vrstva	2	2
Prepínač – prístupová vrstva	2xpočet rackov	2xpočet rackov
Smerovač	2xpočet WAN pripojení	2xpočet WAN pripojení
Firewall	2	2
Lokálny loadbalancer	2	2
Globálny loadbalancer	2	2
IDS/IPS	2	2

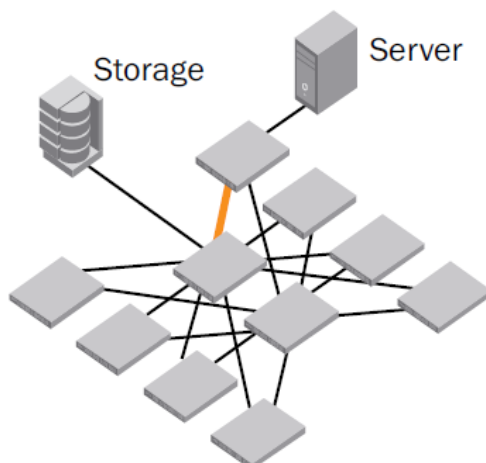
Obrázok 18 – Topológia



Ako základný protokol pre prenos dát v SAN predpokladáme využitie FC na samostatnej optickej sieti s paralelnou možnosťou vybudovania iSCSI komunikačnej infraštruktúry cez protokol IP. FC ako komunikačný protokol je v súčasnej dobe dlhodobo overený pre budovanie SAN infraštruktúry, plne podporovaný všetkými poprednými výrobcami zariadení SAN a umožňuje vybudovať dostatočne výkonnú a flexibilnú SAN.

Vzhľadom na očakávané komunikačné vzory odporúčame použiť core-edge topológiu.

Obrázok 19 – Core-edge topológia

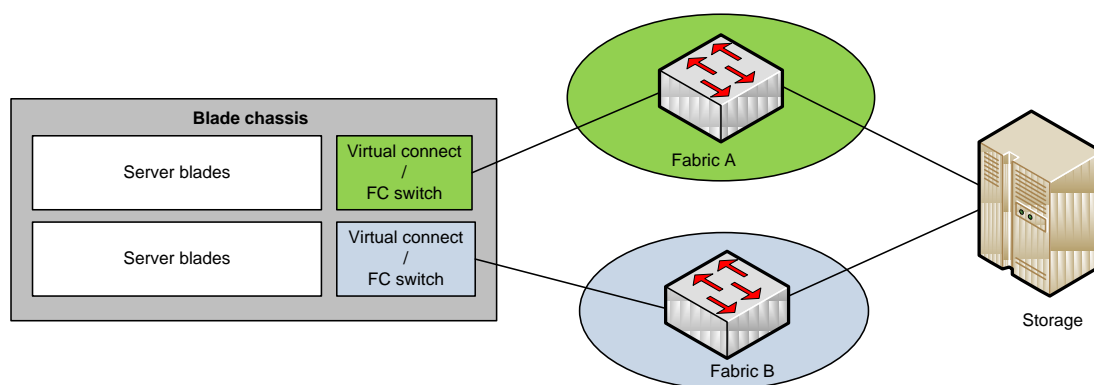


Z pohľadu odolnosti SAN voči výpadku odporúčame budovať SAN ako dva fabric. V tejto konfigurácii je dosiahnutá odolnosť voči výpadku siete (napr. z dôvodu chýb pri výmene prepínačov, nesprávnej konfigurácie siete, zlyhanie sieťových služieb a pod.), HBA servera alebo cesty na storage systém. Pri výpadku sú dáta automaticky presmerované cez alternatívnu cestu bez výpadku I/O. Topológia dvoch fabric zároveň poskytuje najvyššiu výkonnosť nakoľko sú obe siete simultánne dostupné.

Pre prenos dát z a do koncových systémov je potrebné využiť HBA v tzv. „multipath“ móde, pri ktorom je jeden server pripojený do SAN dvomi samostatnými cestami a ovládač HBA riadi smerovanie dát do SAN tak, aby bola zabezpečená vysoká dostupnosť a využitá kapacita oboch kariet (tzv. tandem).

V prípade „blade“ infraštruktúry sú technologické púzdra pripojené do SAN cez Virtual Connect alebo interný FC switch, ktorý poskytuje I/O pripojenie do SAN pre „blade“ servery.

Obrázok 20 – Pripojenie „blade“ serverov do SAN

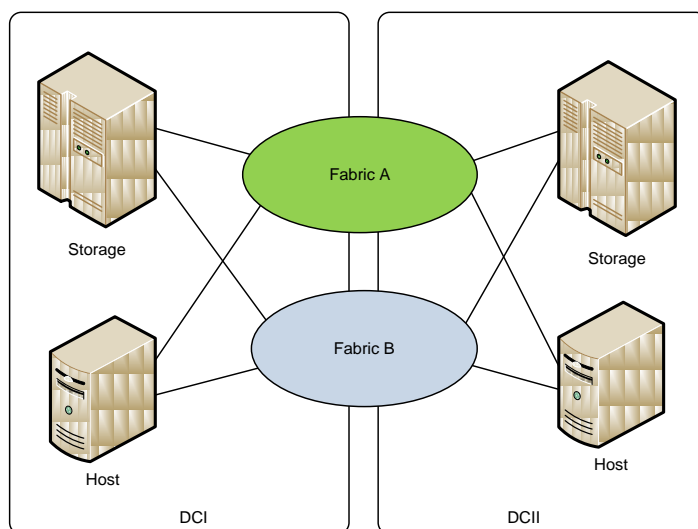


Z pohľadu rozdelenia zdrojov a riadenia bezpečnosti na úrovni prístupu k zariadeniam a portom bude fyzická SAN rozdelená na logické zóny. Pre každú zónu budú definované porty a zariadenia, ktoré sú v rámci tejto zóny adresovateľné. Samotné zónovanie bude vynútené hardvérovo prostredníctvom ASIC v SAN prepínačoch (tzv. frame-based enforcement).

Pre zvýšenie bezpečnosti v SAN prostredí bude zónovanie doplnené o LUN masking na úrovni diskového poľa, ktorý umožňuje selektívne priradiť logické jednotky storage systému (LUN) k jednému, resp. viacerým serverom v SAN sieti.

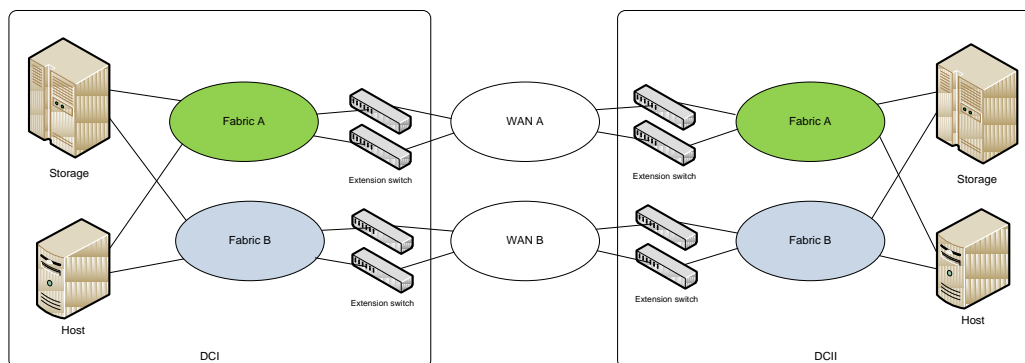
Z pohľadu geografického členenia Dátového centra navrhujeme budovať SAN ako plne rozprestretú. Táto topológia logicky neoddeľuje sieťové zóny v jednotlivých lokalitách a umožňuje aby server nachádzajúci sa v DCI plne pristupoval k dátovému úložisku v DCII a naopak. Dátové spojenie prepínačov core siete bude realizované cez prenajatú optickú trasu a multiplexovanie optického signálu technológiou DWDM (Dense Wave Division Multiplexing), CWDM (Coarse Wave Division Multiplexing) alebo TDM (Time Division Multiplexing).

Obrázok 21 – Plne rozprestretý fabric



V prípade, ak bude vzdialenosť medzi lokalitami Dátového centra taká, že nebude umožňovať synchronnú replikáciu dát a kapacita WAN bude pre replikáciu dát dostatočná, odporúčame vybudovať samostatné, logicky a fyzicky oddelené SAN siete v každej lokalite a medzi nimi vytvoriť prepojenie cez WAN sieť, ktoré bude využité pre replikáciu dát bez toho aby bolo možné pristupovať k serverom z jednej lokality do dátového úložiska v druhej lokalite. Ako nosný protokol pre replikáciu môže byť vybudovaný prepoj protokolom FC, alebo enkapsuláciou FC protokolu cez IP s následným dopadom na kvalitu a kapacitu prenosu. Pri FCoIP sa vo všeobecnosti predpokladá, že väčšina komunikácie ostáva vnútri segmentu a neprechádza na IP linky. Segmenty sú preto zvyčajne dizajnované ako core-edge, pričom core vrstva obsahuje prepínač pre IP tunelovanie. Pre zabezpečenie redundancie je potrebné osadiť dva FCoIP prepínače s nezávislými WAN linkami.

Obrázok 22 – Rozprestretý fabric s využitím IP tunelovania



SAN infraštruktúru odporúčame postaviť na „enterprise class“ SAN prvkoch, ktoré sú podporované všetkými väčšími dodávateľmi IT:

- 8Gb/s FC
- 40-80 FC ports
- No single point of failure
- Hot swap fan and power supply
- Hot code load
- Ports on demand with no downtime
- Multi-Protocol support
- Auto-sensing ports
- Dynamic Path Selection
- Enhanced ISL Trunking
- Advanced fabric services to optimize performance and resource utilization

Tabuľka 12 – Predpokladané zariadenia SAN

Zariadenie	Počet	
	DCI	DCII
SAN prepínač – core	2	2
SAN prepínač – edge	2x počet rozvádzačov osadených stojanovými servermi	2x počet rozvádzačov osadených stojanovými servermi

6.5.2.2 Storage infraštruktúra

Návrh storage architektúry vychádza zo základného princípu, pri ktorom sú všetky aplikačné dáta a dáta operačného systému pri virtualizovanej infraštruktúre uložené na centrálnom dátovom úložisku. Pri tomto variante je možné všetky servery budovať ako bezdiskové čo znižuje náklady na ich obstaranie a umožňuje využívať pokročilé funkcie diskových polí.

Dátové úložiská budú klasifikované do 4 storage tier a ich alokácia pre jednotlivé informačné systémy bude dynamická na základe zákazníckych potrieb a požiadaviek.

Pre kritické dáta (tier 1) navrhujeme pre prípad straty úložiska alebo jeho časti implementovať technológiu replikácie dát na úrovni diskových polí medzi jednotlivými lokalitami Dátového centra, t.j. všetky zápisy dát budú synchronne alebo asynchrónne zapisované do dátového úložiska umiestneného v druhej lokalite.

Pre menej kritické dáta (tier 2) navrhujeme pre elimináciu straty úložiska implementovať technológiu lokálneho zrkadlenia dát.

Na základe výsledkov analýzy v kapitole 6. „Identifikácia možností a príležitostí“ sa predpokladajú požiadavky na storage infraštruktúru normalizované na dátový rozvádzač v rozsahu:

Tabuľka 13 – Požiadavky na infraštruktúru pre ukladanie dát

Storage tier	Počet rozvádzačov v DCI	Počet rozvádzačov v DCII
Tier 1 – „enterprise“ diskové úložisko	4	4
Tier 2 – „mid-range“ diskové úložisko	2	2
Tier 3 – „high-capacity“ diskové úložisko	3	3

Storage tier	Počet rozvádzačov v DCI	Počet rozvádzačov v DCII
Tier 4 – „enterprise“ pásková knižnica	4	4
SPOLU	13	13

Nárast požadovaných kapacít dátových úložísk je možné účinne riadiť vhodne zvolenými opatreniami, ktoré spočívajú najmä v konsolidácii dát a ich zatriedení do jednotlivých tierov, nasadením mechanizmov pre deduplikáciu dát, archiváciou dát a pod.

6.5.2.3 Serverová infraštruktúra

Serverovú infraštruktúru navrhujeme implementovať v dvoch variantoch:

- stojanové servery (tier1)
- „blade“ servery (tier2)

Nasadenie samostatne stojacich serverov je vhodné aplikovať v prípadoch kedy sú požiadavky na výkon systému také, že prevyšujú možnosti „blade“ serverov. Každý samostatne stojaci server musí byť vybavený viacerými ethernet a FC portami z dôvodu zabezpečenia redundancie, priepustnosti a bezpečnosti siete. V prípade implementácie „clusteru“ je potrebné zvýšiť počet ethernet portov kvôli konfigurácii „heartbeat“. Príkladom základnej konfigurácie stojanového servera je:

- RISC server s podporou virtualizácie
- 16 core CPU
- 128 GB RAM
- 4x FC 8Gb/s
- 2x Ethernet 10 Gb/s

Nasadenie „blade“ serverov umožňuje konfiguráciu jedného stojanu s tromi „blade“ puzdrami. Každé „blade“ puzdro je možné osadiť maximálne 16 servermi polovičnej výšky alebo 8 servermi plnej výšky. Pri maximálnej konfigurácii sa dosahuje hustota 48 serverov v jednom stojane. Z prevádzkových dôvodov však niektorí prevádzkovatelia odporúčajú inštalovať maximálne dve puzdra na jeden dátový rozvádzač. Sieťová redundancia, bezpečnosť a požadovaná priepustnosť bude zabezpečená použitím viacerých ethernet prepínačov umiestnených v „blade“ puzdre. K diskovým úložiskám budú „blade“ servery pripojené pomocou FC prepínačov tak aby bola zabezpečená požadovaná redundancia. Alternatívne je možné prístupové SAN prepínače v technologických puzdách samostatne vyviesť na core SAN prepínač čo na jednej strane zvýši priepustnosť ale na druhej strane zvýši požiadavky na SAN kabeláž a počet portov core SAN prepínačov. Príkladom základnej konfigurácie stojanového servera je:

- x86/x64 „blade“ server
- 2x 6-core CPU 2,66 GHz
- 128 GB RAM
- 2x FC HBA 8 Gbit/s
- 2x Ethernet 10 Gbit/s

Na úrovni serverovej infraštruktúry odporúčame v maximálnej miere unifikovať HW a SW platformu, t.j. minimalizovať počet dodávateľov, typov, modelov a verzií jednotlivých komponentov.

Serverovú infraštruktúru zároveň odporúčame kombinovať s virtualizačnou technológiou, ktorá zabezpečuje plnú virtualizáciu. Virtualizačná platforma bude zároveň slúžiť aj pre zabezpečenie vysokej dostupnosti v prípade poruchy hardvéru alebo zlyhania operačného systému.

6.5.2.4 PKI a LTA

V rámci centrálnych služieb dátového centra bude vytvorená CA (certifikačná autorita) a PKI (Public Key Infrastructure) poskytujúca služby pre autentifikáciu s využitím certifikátov a ZEP (zaručený elektronický podpis) zamestnancov verejnej správy, pričom táto CA by mala byť súčasťou rezortu Ministerstva financií SR. Vydávanie certifikátov pre prístup zamestnancov verejnej správy k IS VS takto nebude v kompetencii externého subjektu, ale v kompetencii štátneho orgánu. CA bude poskytovať služby pre zabezpečenie dôvernosti, integrity, originality a nepopierateľnosti uchovávaných údajov, napr.:

- SSL certifikáty webových serverov
- certifikáty pre sieťové prvky, tunely
- certifikáty na zabezpečenie správ vymieňaných medzi jednotlivými ISVS
- certifikáty pre podpisovanie auditných záznamov
- certifikáty pre službu časovej pečiatky

Implementácia PKI a elektronického podpisu umožní:

- rozšírenú autentifikáciu
- ochranu elektronických dokumentov
- elektronický podpis
- využitie štandardov: ADS, PC/SC, PKCS#11, ISO 7816-1 až 4, Web Service, SOAP

Úlohou internej CA pre potreby verejnej správy bude okrem vydávania používateľských certifikátov určených na ich identifikáciu a autentifikáciu aj vydávanie tzv. technologických certifikátov pre zariadenia infraštruktúry IS VS.

Súčasťou dodávky PKI bude aj vytvorenie certifikačnej politiky a registračných procesov. Predpokladáme, že interná CA bude vydávať certifikáty rôznych úrovní, napríklad:

- certifikát bez overenia totožnosti – tento však neposkytuje žiadnu záruku totožnosti používateľa. Bude slúžiť len na testovanie, overovanie vhodnosti použitia certifikátu a pod.
- certifikát s overením totožnosti žiadateľa – na jeho vystavenie bude potrebná osobná návšteva na pracovisku registračnej autority.

V tomto projekte bude potrebné implementovať CA pre potreby identifikácie a autentifikácie používateľov, elektronické podpisovanie dokumentov a technologické zariadenia. Na tieto účely budú vybudované dve podriadené CA, jedna pre potreby vydávania certifikátov osobám a druhá pre potreby technologických zariadení.

S PKI úzko súvisí zabezpečenie dlhodobej archivácie elektronických dokumentov. Z pohľadu zabezpečenia služieb dlhodobej archivácie dokumentov budú na úrovni služieb dátového centra zabezpečené nasledujúce požiadavky:

- zachovanie integrity, dostupnosti, dôvernosti a autenticity archivovaných dát
- poskytovanie dôkazu o existencii a integrite archivovaných dát v danom čase
- interpretovateľnosť archivovaných dát
- auditovateľnosť činností

Takto budú významné nároky, ktoré sú kladené na riešenie ukladania dokumentov podpísaných zaručeným elektronickým podpisom poskytované na úrovni centrálnej služby dátového centra pre celú verejnú správu. Riešenie pre dlhodobú archiváciu bude akreditované v súlade s platnou legislatívou.

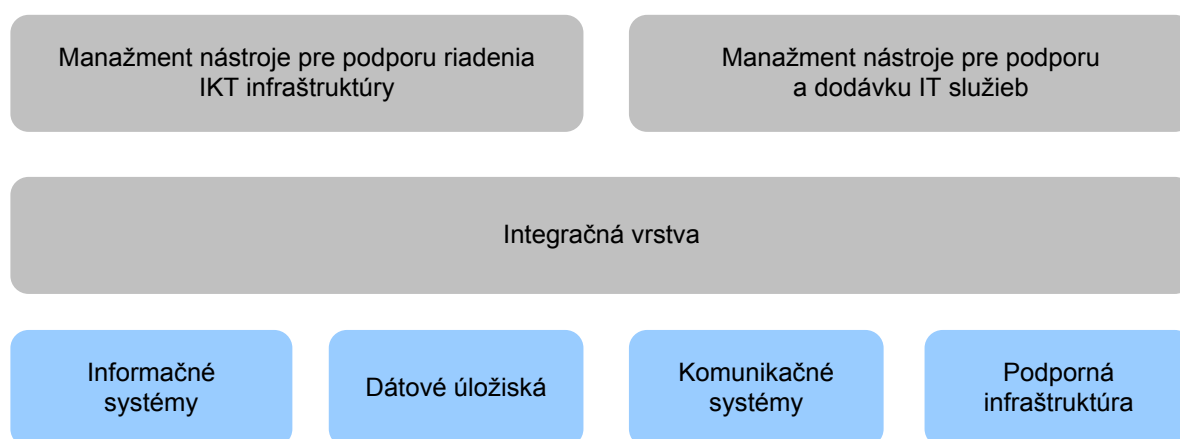
Vzhľadom na charakter uvedených služieb by bolo vysoko neefektívne, ak by tieto služby zabezpečovali jednotlivé komponenty IS VS vo vlastnej réžii. Výrazne negatívne by to vplývalo na kvalitu poskytovaných služieb a ich úroveň zabezpečenia.

6.6 Procesy riadenia služieb a podpory prevádzky

Pre zabezpečenie správy a podpory riadenia prevádzky Dátového centra je potrebné definovať komplexný a integrovaný model správy, ktorý vychádza z najlepších praktík ITSM a SMIB.

Zavedený systém bude certifikovaný na súlad s normami ISO/IEC 20000 a ISO/IEC27001.

Obrázok 23 – Logická architektúra



Integračná vrstva zabezpečuje výmenu dát, udalostí a transakcií medzi jednotlivými komponentmi IKT infraštruktúry a manažment nástrojmi. Zároveň vykonáva extrakciu dát z lokálnych dátových úložísk manažment nástrojov, ich transformáciu a uloženie do dátového skladu.

Doména manažment nástrojov pre podporu riadenia IKT infraštruktúry zastrešuje tieto oblasti:

- monitorovanie a riadenie udalostí
- manažment podpornej technologickej infraštruktúry
- manažment telekomunikačnej infraštruktúry
- manažment dátových úložísk (pamäťových priestorov)
- manažment serverov
- manažment virtualizačného prostredia
- manažment databáz
- manažment výkonnosti a záťaže
- distribúciu softvéru
- inventarizácia hardvéru a softvéru
- automatizácia prevádzkových činností
- manažment licencií

Doména manažment nástrojov pre podporu a dodávku IT služieb zahŕňa:

- konfiguračnú databázu a manažment konfigurácie
- znalostnú databázu
- Service Desk a manažment incidentov

- manažment IT zmien
- katalóg IT služieb a manažment IT služieb
- riadenie dostupnosti IT služieb
- riadenie kontinuity IT služieb

Vo všeobecnosti sa manažment nástroje dajú rozdeliť do dvoch kategórií:

- platformové riešenia (suite)
- špecializované produkty

Variant A: Platformové riešenia

Platformové riešenia sa snažia pokrývať väčšinu aktivít spojených s manažmentom IKT infraštruktúry. Ponúkajú predpripravenú integráciu jednotlivých komponentov riešenia. Sú súčasťou širšieho portfólia produktov a nástrojov čím zvyšujú pravdepodobnosť toho, že dokážu v rámci tej istej platformy naplniť aj budúce užívateľské požiadavky.

Poskytujú globálne riadenie politík, unifikovaný rámec pre kód a objekty, jednotnú, resp. integrovanú používateľskú konzolu a podobný prístup k používateľskému rozhraniu čím zjednodušujú a zrýchľujú zaškolenie personálu a prijatie nástroja ako takého.

Sledujú „best practice“ v danom odvetví a ponúkajú implementáciu s predkonfigurovanými parametrami, resp. nástroje a techniky pre rýchle zavedenie a prispôbenie riešenia aktuálnemu prevádzkovému prostrediu.

Ponúkajú širokú podporu výrobcov hardvéru a softvéru, protokolov, technológií a metód. Sledujú vývojové trendy a priebežne rozširujú a dopĺňajú svoje portfólio podporovaných technológií. Taktiež ponúkajú platformovú nezávislosť z pohľadu inštalácie samotného riešenia.

Poskytujú rozsiahle API na štandardných technológiách (JAVA, web services, CORBA, ...), ktoré umožňuje integráciu manažment nástrojov tretích strán, externých dátových zdrojov a existujúcich informačných systémov.

Riešenia sú určené pre rozsiahle IKT prostredia s nepretržitou prevádzkou a tak majú už pri dizajne a vývoji natívne zabudované požiadavky na škálovateľnosť a vysokú dostupnosť. Samotná prevádzka je obvykle zabezpečená na dedikovaných zdrojoch (server, databáza, aplikačný server a pod.), ktoré sú oddelené od ostatných informačných systémov.

Nezanedbateľná je výhoda podpory celého riešenia jedným dodávateľom, ktorá zjednodušuje zmluvné vzťahy medzi organizáciou a dodávateľom, zjednodušuje údržbu a správu riešenia z pohľadu interných zdrojov a zvyšuje efektivitu komunikácie a riešenie problémov na tretej úrovni podpory.

Nevýhodou platformového riešenia je jeho komplexita, ktorá spôsobuje nárast požiadaviek na správu a údržbu spojenú s nevyhnutným personálnym zabezpečením.

Ďalšou negatívnou črtou centrálnych platforiem je nezladený a dlho trvajúci vývoj jednotlivých komponentov spôsobený priebežnými fúziami na trhu IT spoločností, ktoré si následne vynútila proces konvergenzie a integrácie novo nadobudnutých produktov do spoločnej platformy.

Variant B: Špecializované riešenia

Požiadavky manažmentu IKT infraštruktúry je možné pokryť špecializovanými, čiastkovými nástrojmi, ktoré sú zamerané na riešenie partikulárnych oblastí a častí IKT infraštruktúry.

Výhodou tohto prístupu je rádovo nižšia komplexita v porovnaní s platformovým riešením, ktorá umožňuje rýchle nasadenie a jednoduchšiu údržbu. Obvykle nevyžaduje ďalšie personálne kapacity na správu a údržbu. Špecializované riešenia zároveň pokrývajú aj oblasti, ktoré sú mimo záujmu

veľkých platformových riešení či už z dôvodu malej zákazníckej bázy, nízkeho záujmu o danú funkcionálnosť, príliš hlbokoj špecializácie a pod.

Odporúčanie

Z pohľadu celkovej systémovej architektúry odporúčame ako preferovaný variant platformové riešenia (centrálne manažment systémy) pre oblasť:

- podporu dodávky IT služieb
- podporu riadenia IKT infraštruktúry

Centrálne manažment systémy sa v nevyhnutnej miere doplnia o špecializované nástroje.

Centrálne manažment systémy budú pokrývať IKT infraštruktúru oboch lokalít a budú budované tak, aby mali zabezpečenú trvalú kontinuitu prevádzky.

Referenčná architektúra a základné princípy budovania ITSM systému sú uvedené v [prílohe č. 5](#).

6.7 Riadenie informačnej bezpečnosti

Zavedenie SMIB bude realizované v týchto etapách:

- vypracovanie bezpečnostného projektu
- zavedenie bezpečnostných procesov a implementácia bezpečnostných opatrení
- príprava na predcertifikačný audit
- certifikačný audit

Vypracovanie bezpečnostného projektu sa zaoberá identifikáciou a ohodnotením bezpečnostných rizík a spracovaním vrcholovej bezpečnostnej politiky, ktorá popíše organizáciu bezpečnosti a základné princípy riadenia informačnej bezpečnosti dátového centra. Realizácia bude rozdelená do nasledujúcich čiastkových úloh.

- vypracovanie bezpečnostnej politiky, stanovenie organizácie riadenia informačnej bezpečnosti, stanovenie spôsobu analýzy rizík,
- analýza rizík
 - zber vstupných podkladov,
 - realizácia analýzy rizík,
 - ohodnotenie rizík a návrh správy rizika,
 - vypracovanie GAP analýzy voči ISO 27001,
 - návrh odporúčaní,
- výber cieľov riadenia a návrh bezpečnostných opatrení nariadenie rizík,
- vypracovanie vyhlásenia o aplikovateľnosti.

Zavedenie bezpečnostných procesov a implementácia bezpečnostných opatrení zabezpečí implementáciu návrhov vyplývajúcich z bezpečnostného projektu a z analýzy rizík. Opäť bude realizácia rozdelená do čiastkových úloh a to takto:

- spracovanie plánu zvládnutia rizík,
- zavedenie a implementácia bezpečnostných opatrení v týchto oblastiach
 - organizácia bezpečnosti
 - klasifikácia a kontrola aktív

- personálna bezpečnosť
 - manažment bezpečnostných incidentov
 - fyzická bezpečnosť a bezpečnosť prostredia
 - správa a prevádzka systémov
 - riadenie prístupu a pravidiel pre používanie IS
 - vývoj a údržba systémov
 - plánovanie kontinuity činností
 - súlad s legislatívou, štandardami a normami
- školenie zamestnancov.

Referenčná architektúra a základné princípy budovania systému informačnej bezpečnosti sú uvedené v prílohe [prílohe č. 6](#).

6.8 Organizácia

6.8.1 Interná organizácia

Zabezpečenie poskytovania služieb Dátového centra bude vyžadovať internú organizáciu, ktorá musí adresovať oblasť:

- riadenia
- podpory (obsluhy)
- architektúry

Požiadavky na ľudské zdroje sú rozdelené na bežnú prevádzku a pohotovosť. Bežná prevádzka je definovaná v rámci pracovných dní počas jednej 8 hodinovej zmeny v mieste dátových centier alebo na to určených administratívnych priestorov. Výnimkou je dohľad (prvá úroveň obsluhy), pre ktorú je definovaná non-stop prevádzka. Pohotovosť nemá obmedzenie v čase a je poskytovaná telefonicky mimo pracovnú zmenu. Ľudské zdroje počas pohotovosti spravidla nie sú prítomné v dátovom centre a neplnia žiadne rutinné úlohy. V prípade požiadavky na odstránenie poruchy musia zasiahnuť podľa vopred definovaných procedúr v definovanom čase.

Obsluha prvej úrovne je zdieľaná pre všetky špecializácie a je poskytovaná operátormi Dohľadového centra bez špecifických požiadaviek na ich spôsobilosti (LAN/WAN/SAN/dátové úložiská, siete a podobne). Je zodpovedná za dohľad, rutinnú prevádzku, riadenie a eskaláciu vzniknutých problémov na obsluhu druhej úrovne.

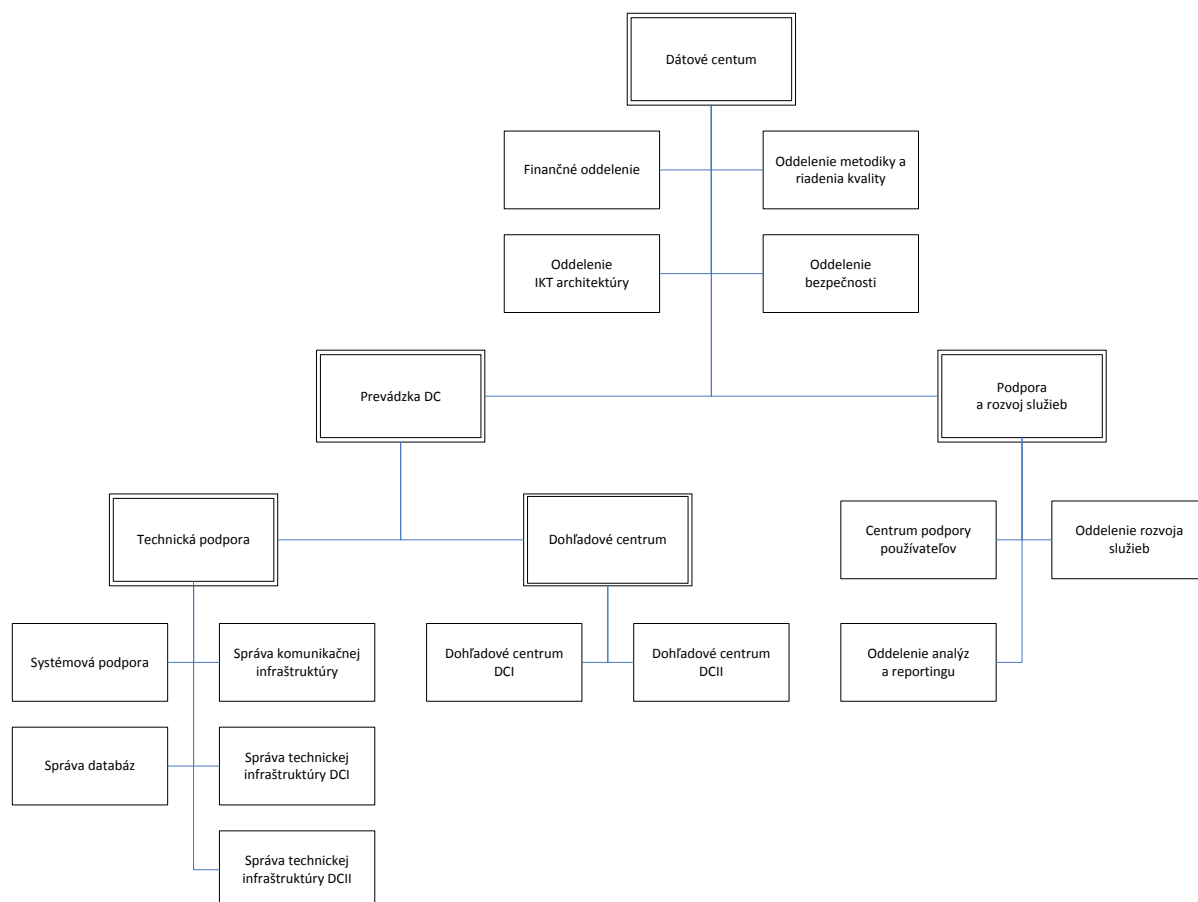
Obsluha druhej úrovne predstavuje špecialistov, ktorí sú v rámci svojej špecializácie zodpovední za návrh, plánovanie, technickú podporu, nasadenie a prevádzku komponentov IKT.

Obsluha tretej úrovne bude zabezpečovaná dodávateľsky prostredníctvom servisného kontraktu s definovanými SLA. Obsluha tretej úrovne je zodpovedná za servisnú údržbu, odstraňovanie chýb eskalovaných podporou druhej úrovne a prípadnú iniciálnu konfiguráciu IKT komponentov.

Riadenie a architektúru dátových centier bude potrebné zabezpečiť v rámci pracovných dní počas jednej 8 hodinovej zmeny v mieste dátových centier alebo na to určených administratívnych priestorov.

V rámci zabezpečenia hore uvedených oblastí predpokladáme nasledovnú modelovú organizačnú štruktúru:

Obrázok 24 – Model internej organizácie Dátového centra



Modelová organizačná štruktúra (viď tabuľka 14.) popisuje primárne odborné funkcie potrebné pre zabezpečenie služieb Dátového centra.

Pri podporných funkciách ako je riadenie ľudských zdrojov, ekonomika, právne služby a pod. sa predpokladá štandardný rozsah, ktorý je typický pre samostatné rozpočtové organizácie. Z tohto dôvodu štúdia tieto funkcie bližšie nešpecifikuje.

V rámci realizácie projektu Dátového centra bude potrebné detailne analyzovať existujúcu organizačnú štruktúru DataCentra a vykonať mapovanie hore uvedeného organizačného modelu. V prípade, ak existujúca organizácia DataCentra nebude reflektovať všetky požiadavky kladené na zabezpečenie služieb Dátového centra bude potrebný jej redizajn.

Tabuľka 14 – Predpokladaný nárast požadovaných ľudských zdrojov

Názov prac. funkcie	Manažér prevádzky DC
Zaradene v OŠ	Prevádzka DC
Prevádzková doba	8 hodinová
Pracovný profil	Plánovanie rozvoja IKT infraštruktúry Schvaľovanie zmien v technickej infraštruktúre Vyhodnotenie a riziková analýza zmien z pohľadu ich dopadu na IKT infraštruktúru Zabezpečenie primeranej administrácie komponentov IS infraštruktúry

	<p>Plánovanie, nábor a rozvoj pracovníkov určených pre podporu riadenia IS infraštruktúry</p> <p>Vzťahy s dodávateľmi a partnermi. Zabezpečenie aktuálnych a efektívnych zmlúv o technickej podpore s tretími stranami</p> <p>Zabezpečenie príslušnej štandardizácie</p> <p>Pravidelné prehodnotenie a optimalizácia procesov manažmentu IS infraštruktúry</p>
--	--

Názov prac. funkcie	Manažér dohľadového centra
Zaradene v OŠ	Dohľadové centrum
Prevádzková doba	8 hodinová
Pracovný profil	<p>Riadi operatívne prevádzkové aktivity</p> <p>Definuje a kontroluje naplnenie akceptačných kritérií pre zavedenie riešenia do prevádzky</p> <p>Eskaluje prevádzkové problémy na príslušnú autoritu</p> <p>Zaisťuje dodržiavanie prevádzkových postupov a procedúr dohľadového centra</p> <p>Zabezpečuje školenie personálu dohľadového centra</p> <p>Rieši úlohy spojené s personálnym zabezpečením dohľadového centra</p>

Názov prac. funkcie	Špecialista dohľadového centra
Zaradenie v OŠ	<p>Dohľadové centrum DCI</p> <p>Dohľadové centrum DCII</p>
Prevádzková doba	24 hodinová (trojsmenná prevádzka)
Pracovný profil	<p>Zabezpečuje nepretržitý dohľad dátového centra</p> <p>Vyhodnocuje a odstraňuje udalosti, upozornenia a poplachy, ktoré sú zaznamenané počas prevádzky IKT infraštruktúry</p> <p>Monitoruje úroveň IT služieb</p> <p>Monitoruje záťaž a výkonnosť</p> <p>Zabezpečuje údržbu zariadení v súlade s prevádzkovými podmienkami a pravidlami</p> <p>Spravuje a udržiava prevádzkovú dokumentáciu</p> <p>Vykonáva rutinné úlohy</p> <p>Poskytuje podporu v procese zálohovania a archivácie</p> <p>Vytvára podporné prevádzkové skripty a procedúry</p> <p>Implementuje prevádzkové zmeny v súlade s procesom riadenia zmien a riadenia nasadenia</p> <p>Vedie a aktualizuje zoznam (katalóg) zariadení</p> <p>Udržiava plán prevádzkových rutinných úloh</p>

Názov prac. funkcie	Manažér technickej podpory
Zaradenie v OŠ	Technická podpora
Prevádzková doba	8 hodinová

Pracovný profil	<p>Zaisťuje primeranú technickú podporu pre ďalšie procesy</p> <p>Pripravuje a aktualizuje postupy, procedúry a štandardy</p> <p>Zabezpečuje vypracovanie a distribúciu reportov</p> <p>Zabezpečenia priebežného zvyšovania kvalifikácia celého tímu technickej podpory</p> <p>Poskytuje podporu pri analýze problémov spojených s prevádzkou IKT infraštruktúry</p> <p>Participuje na štúdiách realizovateľnosti</p> <p>Implementuje zlepšenia IKT infraštruktúry na taktickej úrovni</p> <p>Rieši úlohy spojené s personálnym zabezpečením dohľadového centra</p>
------------------------	---

Názov prac. funkcie	Systémový špecialista
Zaradenie v OŠ	Systémová podpora
Prevádzková doba	<p>8 hodinová</p> <p>Pracovná pohotovosť mimo pracoviska</p> <p>Pracovná pohotovosť na pracovisku</p>
Pracovný profil	<p>Zabezpečenie serverovej infraštruktúry</p> <p>Rozvoj serverových systémov</p> <p>Odborno-konzultačná a poradenská činnosť</p> <p>Podpora pri analýze problémov spojených so správou operačných systémov a systémového softvéru</p> <p>Technické poradenstvo</p> <p>Inštalácia a konfigurácia operačného systému a systémového SW</p> <p>Správa a konfigurácia pamäťových priestorov a SAN</p> <p>Zabezpečenie súladu systémovej infraštruktúry s požiadavkami bezpečnosti</p> <p>Správa užívateľov</p> <p>Priebežná analýza logov s cieľom odstránenia slabých miest v systémovej konfigurácii</p> <p>Zálohovanie a archivácia operačného systému a súborových systémov</p> <p>Príprava štandardov v oblasti prevádzky OS a systémového SW</p> <p>Reportovanie prevádzkových aspektov celého systémového prostredia</p>

Názov prac. funkcie	Databázový špecialista
Zaradenie v OŠ	Správa databáz
Prevádzková doba	<p>8 hodinová</p> <p>Pracovná pohotovosť mimo pracoviska</p> <p>Pracovná pohotovosť na pracovisku</p>
Pracovný profil	<p>Zabezpečenie databázovej infraštruktúry</p> <p>Rozvoj databázových systémov</p> <p>Odborno-konzultačná a poradenská činnosť</p> <p>Podpora pri analýze problémov spojených so správou databázových</p>

	<p>systémov</p> <p>Technické poradenstvo</p> <p>Inštalácia a konfigurácia databázových systémov a podporného systémového SW</p> <p>Zabezpečenie súladu databázového prostredia s požiadavkami bezpečnosti</p> <p>Správa užívateľov</p> <p>Priebežná analýza databázového prostredia s cieľom odstránenia slabých miest, ladenia výkonnosti, zvyšovania stability a pod.</p> <p>Zálohovanie a archivácia databázových systémov</p> <p>Príprava štandardov v oblasti prevádzky databáz a podporného systémového SW</p> <p>Reportovanie prevádzkových aspektov celého databázového prostredia</p>
--	--

Názov prac. funkcie	Sieťový špecialista
Zaradenie v OŠ	Správa komunikačnej infraštruktúry
Prevádzková doba	<p>8 hodinová</p> <p>Pracovná pohotovosť mimo pracoviska</p> <p>Pracovná pohotovosť na pracovisku</p>
Pracovný profil	<p>Zabezpečenie komunikačnej infraštruktúry</p> <p>Rozvoj komunikačných a telekomunikačných systémov</p> <p>Odborno-konzultačná a poradenská činnosť</p> <p>Podpora pri analýze problémov</p> <p>Inštalácia a konfigurácia sieťových prvkov</p> <p>Zabezpečenie súladu komunikačnej infraštruktúry s požiadavkami bezpečnosti</p> <p>Priebežná analýza logov s cieľom odstránenia slabých miest v systémovej konfigurácii</p> <p>Príprava štandardov v oblasti LAN/WAN</p> <p>Reportovanie prevádzkových aspektov sieťového prostredia</p>

Názov prac. funkcie	Špecialista technickej infraštruktúry
Zaradenie v OŠ	<p>Správa technickej infraštruktúry DCI</p> <p>Správa technickej infraštruktúry DCII</p>
Prevádzková doba	8 hodinová
Pracovný profil	<p>Správa technickej infraštruktúry</p> <p>Analýza technických problémov spojených s IS infraštruktúrou</p> <p>Diagnostika problémov</p> <p>Poskytovanie technického poradenstva</p> <p>Podpora, vývoj, konfigurácia a integrácia manažment nástrojov</p> <p>Podpora pri nasadzovaní zmien a nových riešení</p>

,	Manažér podpory a rozvoja služieb
----------	--

Zaradenie v OŠ	Podpora a rozvoj služieb
Prevádzková doba	8 hodinová
Pracovný profil	Riadenie portfólia služieb Participácia v riadiacich orgánoch (CAB, ...) Zabezpečenie kvality poskytovaných služieb Zabezpečenie efektivity poskytovaných služieb Riadenie odberateľských vzťahov Riadenie externých subdodávateľských vzťahov pre poskytované služby

Názov prac. funkcie	Špecialista ServiceDesk
Zaradenie v OŠ	Centrum podpory používateľov
Prevádzková doba	12 hodinová
Pracovný profil	Zabezpečuje funkciu ServiceDesk v zmysle ITIL odporúčaní Zabezpečuje 1. úroveň podpory riadenia incidentov v zmysle ITIL odporúčaní Poskytuje metodickú podporu pre používateľov IS Plánuje a organizuje školenia a pracovné semináre

Názov prac. funkcie	Špecialista riadenia kvality služieb
Zaradenie v OŠ	Riadenie kvality služieb
Prevádzková doba	8 hodinová
Pracovný profil	Správa a aktualizácia Katalógu služieb, SLA, OLA, UC Vyjednávanie a dohodnutie Katalógu služieb Zabezpečenie dodržiavania parametrov SLA a OLA Špecifikácia nápravných opatrení Monitoring, analýza a vyhodnotenie stavu a úrovne poskytovania služieb Reporting

Názov prac. funkcie	Špecialista rozvoja služieb
Zaradenie v OŠ	Rozvoj služieb
Prevádzková doba	8 hodinová
Pracovný profil	Analýza zákazníckych požiadaviek a potrieb Odborno-konzultačná a poradenská činnosť Spracovanie analýz dopadov Spracovanie štúdií uskutočniteľnosti Príprava, koordinácia implementácie a podpora nasadenia nových služieb Príprava, koordinácia implementácie a podpora nasadenia zmien existujúcich služieb

Názov prac. funkcie	Architekt
Zaradenie v OŠ	Oddelenie IKT architektúry
Prevádzková doba	8 hodinová
Pracovný profil	<p>Definuje a udržiava celkovú architektúru DC.</p> <p>Definuje a udržiava pravidlá pre IKT infraštruktúru.</p> <p>Poskytuje poradenstvo vo fázach návrhu a plánovania pre ITSM procesy.</p> <p>Poskytuje podporu analytikom a dizajnérom tretích strán.</p> <p>Spolupodieľa sa na posudzovaní a výbere nových technológií.</p> <p>Spolupracuje pri finančných (nákladových) analýzach.</p>

Názov prac. funkcie	Špecialista bezpečnosti
Zaradenie v OŠ	Oddelenie bezpečnosti
Prevádzková doba	8 hodinová
Pracovný profil	<p>Zodpovedá za vývoj bezpečnostnej stratégie DC</p> <p>Definuje a udržiava celkovú bezpečnostnú politiku DC</p> <p>Pripravuje návrh rozpočtu pre bezpečnosť všetkých aktív DC</p> <p>Riadi tvorbu riadiacich dokumentov bezpečnosti</p> <p>Riadi implementáciu bezpečnostných mechanizmov a metód ochrany</p> <p>Audituje dodržiavanie bezpečnostnej politiky</p> <p>Zodpovedá za uplatňovanie fyzickej, personálnej a informačnej bezpečnosti</p> <p>Zodpovedá za aktivity súvisiace s tvorbou, aktualizáciou a funkčnosťou havarijných plánov</p> <p>Koordinuje a zabezpečuje prijatie adekvátnych opatrení pri mimoriadnych udalostiach týkajúcich sa bezpečnosti DC</p> <p>Zodpovedá za výkon dohľadu nad ochranou osobných údajov v určenom rozsahu</p> <p>Vykonáva riadiacu a kontrolnú činnosť dodržiavania predpisov vydaných na ochranu utajovaných skutočností</p> <p>Spolupodieľa sa na posudzovaní a výbere nových technológií</p>

Názov prac. funkcie	Špecialista finančného riadenia
Zaradenie v OŠ	Finančné oddelenie
Prevádzková doba	8 hodinová
Pracovný profil	<p>Príprava rozpočtu DC</p> <p>Controlling</p> <p>Reporting</p> <p>Správa aktív</p> <p>Analytická a metodická podpora pri riadení a rozvoji služieb</p>

Názov prac. funkcie	Špecialista riadenia kvality
---------------------	-------------------------------------

Zaradenie v OŠ	Oddelenie metodiky a riadenia kvality
Prevádzková doba	8 hodinová
Pracovný profil	Správa a údržba celkového procesného modelu DC Metodická podpora pre oblasť ITSM Zavádzanie a optimalizácia ITSM procesov

Vzhľadom na aktuálny stav DataCentra a očakávaný nárast kvantity a kvality poskytovaných služieb predpokladáme nasledovné navýšenie v oblasti ľudských zdrojov:

Názov pracovnej pozície	Počet
Špecialista dohľadového centra	8
Systémový špecialista	4
Databázový špecialista	3
Sieťový špecialista	3
Špecialista technologickej infraštruktúry	2
Špecialista rozvoja služieb	1
Manažér dohľadového centra	2
SPOLU	23

6.8.1 Externé vzťahy

Väzby Dátového centra s externými organizáciami je možné rozdeliť na vzťahy s:

- poskytovateľmi služieb
- odberateľmi služieb

Pod poskytovateľmi služieb sa primárne rozumejú externé subjekty, ktoré budú pre Dátové centrum zabezpečovať podporu a údržbu IKT infraštruktúry a informačných systémov. Vzájomné vzťahy budú formálne riadené zmluvami o poskytovaní služieb. Kvalita odoberaných služieb bude priebežne monitorovaná a vyhodnocovaná voči zmluvne definovaným podmienkam. Za aktuálnosť a finančnú efektívnosť týchto zmlúv bude zodpovedný manažér prevádzky DC.

Odberateľmi služieb Dátového centra budú v zmysle cieľov tejto štúdie žiadatelia, ktorí realizujú projekty elektronizácie verejnej správy. Vzhľadom na celkovú komplexnosť prostredia verejnej správy bude nasadenie služieb Dátového centra vyžadovať dôslednú koordináciu a riadenie minimálne na úrovni:

- strategické plánovanie - definuje záväzný plán pre zabezpečenie konzistencie medzi jednotlivými projektami POI OPIS a DataCentrom ako nadrezortným poskytovateľom centrálnych služieb dátového centra pre elektronizáciu verejnej správy. Plánovanie a koordinácia zohľadňuje mimo iné aj to, že IKT infraštruktúra dodávaná v rámci jednotlivých projektov bude súčasťou celkovej zdieľanej infraštruktúry Dátového centra.
- presadenie a výkon stratégie – riadi výkon stratégie voči jednotlivým projektom POI OPIS (monitoruje projekty, vyhodnocuje súlad so stanovenou stratégiou, poskytuje súčinnosť, ...). Definuje štandardy pre IKT infraštruktúru, rieši konflikty a prípadné prekryvy medzi projektami.
- pripojenie žiadateľa – riadi pripájanie žiadateľa k odberu služieb. Súčasťou je detailná analýza požiadaviek, špecifikácia požadovanej úrovne služieb, nasadenie služieb, overenie pripravenosti na strane odberateľa, testovanie a bezpečnostný/výkonnostný audit.

Kompetenciu na realizáciu hore uvedených aktivít predpokladáme na strane DataCentra, na ktoré ju deleguje MFSR ako ústredný orgán štátnej správy pre oblasť informatizácie spoločnosti, bližšie viď „Štúdiá uskutočniteľnosti projektov prioritnej osi č. 1 Elektronizácia verejnej správy a rozvoj elektronických služieb Operačného programu Informatizácia spoločnosti zameranej na rozvoj komunikačno-technologickej infraštruktúry informačných systémov verejnej správy na centrálnej úrovni“ vypracovaná spoločnosťou Logica.

Pri rešpektovaní podmienok kladených na infraštruktúru môže ktorákoľvek zúčastnená strana navrhnúť a presadiť riešenie voči druhej strane. V prípade ak nevznikne dohoda je právo a povinnosť zvoliť riešenie na strane arbitra, ktorým bude na základe svojej riadiacej kompetencie MFSR.

Celková koordinačná, riadiaca a kontrolná kompetencia nad Dátovým centrom bude realizovaná MFSR, ktoré bude v jej intenciách:

- definovať minimálny rozsah štandardných služieb, ktoré bude Dátové centrum poskytovať
- definovať parametre a cenové hranice jednotlivých štandardných služieb
- definovať kvalitatívne parametre, ktoré budú musieť Dátové centrum splniť v stanovenej lehote
- rozhodovať o umiestnení aplikácií v Dátovom centre
- kontrolovať kvalitu Dátového centra
- kontrolovať rozsah a kvalitu poskytovaných služieb

7 Finančný plán

7.1 Predpoklady

Ekonomická analýza vychádza z metodiky pre CBA projektov OPIS pričom rešpektuje špecifiká projektu, ktorý je zameraný na technické zabezpečenie a podporu poskytovaných e-Gov služieb, centralizovaným spôsobom.

Obsahom analýzy je vyčíslenie budúcich nákladov a prínosov životného cyklu projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“. Výstupom analýzy nákladov a prínosov (Cost Benefit Analysis - CBA) je súhrnný ukazovateľ čistej súčasnej hodnoty (NPV – Net Present Value) a určenie návratnosti investície (ROI – Return of Investment), obsahujúci porovnanie nákladov a prínosov poskytovaných služieb na strane poskytovateľa a používateľa:

Súčasný stav (As-Is, alternatíva 1) – poskytovanie služieb bez realizácie projektu tak ako doposiaľ plánované – decentralizovaným spôsobom, samostatne na úrovni každého projektu OPIS PO1.

Budúci stav (To-Be, alternatíva 2) – realizácia projektu a zabezpečenie poskytovania e-Gov služieb centralizovaným spôsobom.

Základné referenčné hodnoty pre výpočet CBA sú uvedené v nasledovnej tabuľke:

Tabuľka 15 – Referenčné hodnoty pre CBA

Názov faktora	Popis	Referenčná hodnota
Životnosť projektu (t)	Referenčné obdobie je počet rokov, na ktorý sa v analýze nákladov a výnosov uvádzajú predpovede.	15 rokov
Diskontná sadzba (r)	Systém riadenia ŠF a KF v prípade verejných investičných projektov spolufinancovaných z fondov stanovuje 5 % finančnú diskontnú sadzbu pre výpočet čistej súčasnej hodnoty investície v stálych cenách roku predloženia žiadosti o NFP.	5,5 %
Osobné náklady (C _{per})	<p>$C_{per} = 990,00 \cdot 1,358 / 160$, pričom 990,00 EUR je priemerná hrubá mzda vo verejnej správe za rok 2010, (zdroj: http://portal.statistics.sk/showdoc.do?docid=24136), odvody (SP, ZP, SF) tvoria 35,8% a fond pracovnej doby na 1 mesiac je 160 hodín.</p> <p>Priemerná mzda v NH je 769,00 EUR, (zdroj http://portal.statistics.sk/showdoc.do?docid=24135).</p> <p>Osobné náklady vo verejnej správe predstavujú potom 8,40 EUR/hod.</p> <p>Osobné náklady v národnom hospodárstve predstavujú potom 6,53 EUR/hod.</p> <p>Hrubá mzda v národnom hospodárstve 4,81 EUR/hod.</p> <p>Dané náklady sú faktorom prevádzkových variabilných nákladov.</p>	<p>8,40 EUR/hod Verejná správa</p> <p>6,53 EUR/hod Národné hospodárstvo</p>

Názov faktora	Popis	Referenčná hodnota
RFPD	Ročný fond pracovnej doby (hodiny)	1920

Náklady

Predpokladané náklady na technické zabezpečenie a podporu eGov služieb sú odvodené od rámcových požiadaviek na ich technické zabezpečenie, ktoré je definované prostredníctvom vzťahnej jednotky (jeden dátový rozvádzač). Metodika výpočtu a hodnoty týchto požiadaviek pre jednotlivé projekty OPIS PO1 (počet rozvádzačov potrebných pre projekt), ktoré boli uvažované ako relevantné pre túto štúdiu, sú identifikované v kap. 5.1.

Keďže náklady na technické zabezpečenie a podporu eGov služieb nie sú v rámci OPIS projektov definované pre každú eGov službu, pre identifikovanie nákladov na jednotlivé eGov služby sa vychádza z kumulácie služieb na úrovni projektu – t.j. jeden projekt OPIS dodáva jednu eGov službu.

Pre takto definované eGov služby budú identifikované náklady v dvoch alternatívach:

- Súčasný stav – poskytovanie služieb bez realizácie projektu tak ako doposiaľ plánované – decentralizovaným spôsobom, samostatne na úrovni každého projektu OPIS PO1.
- Budúci stav – poskytovanie služieb po realizácii projektu a zabezpečenie poskytovania a podpory e-Gov služieb centralizovaným spôsobom.

Pre potreby finančného vyjadrenia je v analýze nákladov definovaná štruktúra nákladových položiek, zodpovedajúca štandardným požiadavkám na technické zabezpečenie a podporu eGov služieb, ktorú je možné rozdeliť na niekoľko oblastí:

- Náklady na technologickú infraštruktúru DC – predstavujú náklady spojené s vytvorením a udrжанím potrebného prostredia dátovej sály (definované ako „Technológia“)
 - Systém elektrického napájania – systémy primárneho aj záložného napájania pre dátové centrum (IT infraštruktúru aj technológie)
 - Centrálny chladiaci systém – systém centrálného chladenia dátovej sály
 - Protipožiarny systém – automatický hasiaci systém
 - Bezpečnostný systém – systémy fyzickej bezpečnosti (kamerový systém, prístupový systém)
 - Dátová kabeláž – interné dátové rozvody metalické a optické
- Náklady na IT infraštruktúru DC – predstavujú náklady spojené s vytvorením a udrжанím potrebného prostredia IT infraštruktúry (definované ako „IT infraštruktúra“)
 - Serverové systémy – HW infraštruktúra fyzických serverov
 - Infraštruktúra pre ukladanie dát – fyzické HW komponenty a špecifická infraštruktúra určená pre ukladanie dát (diskové polia, páskové systémy, komponenty SAN infraštruktúry)
 - DR Infraštruktúra – špecifická infraštruktúra pre zabezpečenie kontinuity (napr. zrkadlenie diskových polí, vzájomné prepojenie DC, a pod.)
 - Zálohovacie systémy – systémy pre riadenie zálohovania
 - Monitorovacie systémy – infraštruktúra systémov pre monitorovanie IT infraštruktúry (servery, siete, databázy, aplikácie, bezpečnosť infraštruktúry)
 - Prístupová infraštruktúra – komplex IT systémov potrebných na vytvorenie bezpečného prístupu používateľov k poskytovaným službám

- Service desk – infraštruktúra systému (aplikácie) pre podporu používateľov
- Licencie – licencie pre serverové operačné systémy, databázy, monitorovacie systémy, ...
- Náklady na prevádzku IT infraštruktúry – predstavujú náklady priamo spojené s prevádzkou IT infraštruktúry a systémov (definované ako „Prevádzka“)
 - Elektrická energia pre IKT – napájanie systémov v dátovom rozvážači
 - Elektrická energia pre chladenie – elektrická energia potrebná na chladenie systémov IKT a ďalšie systémy
 - Dátové komunikácie – náklady na dátové komunikácie v oblasti WAN
- Náklady na zabezpečenie podpory a prevádzky systémov – predstavujú náklady spojené s činnosťami ktoré sú potrebné pre zabezpečenie prevádzky a podpory IT infraštruktúry a systémov (definované ako „Podpora“)
 - HW údržba (maintenance) – štandardné poplatky za údržbu HW komponentov a podpora
 - SW údržba (maintenance) – štandardné poplatky za údržbu SW licencií a podpora
 - Administrácia a správa systémov,
 - Administrácia a správa databáz,
 - Zálohovanie – administrácia a správa zálohovacieho systému a výkon zálohovania,
 - Monitoring – výkon dohľadu nad IT infraštruktúrou,
- Náklady spojené s prevádzkou DC – predstavujú ostatné náklady spojené s existenciou DC (definované ako „Réžia“)
 - Štandardizácia prevádzky – zavedenie a udržanie štandardov riadenia prevádzky a poskytovania IT služieb v zmysle noriem radu ISO 20000 a informačnej bezpečnosti v zmysle noriem radu ISO 27000,
 - Vzdelávanie – náklady na udržanie trvalej vedomostnej úrovne špecialistov z oblasti IT infraštruktúry aj riadenia IT služieb (školenia a certifikácie),
- Riadenie – náklady na riadenie organizácie.

Identifikácia nákladov budúceho stavu vychádza z predpokladov úspor pri technickom zabezpečení a podpore poskytovaných eGov služieb prostredníctvom centralizovaného a konsolidovaného dátového centra – t.j. z rozdielov proti dobudovaniu, prípadne budovaniu samostatných dátových centier pre potreby jednotlivých projektov OPIS (identifikovaných bolo 11 projektov) a centralizovanému dátovému centru.

V oblastiach technologickej („Technológie“) je možné predpokladať vyššiu efektívnosť vynaložených prostriedkov pri budovaní technologickej infraštruktúry jedného (dvoch) dátového centra ako pri budovaní viacerých DC (napr. znížením počtu dieselagregátov pre záložné napájanie, znížením počtu hasiacich systémov a pod.)

V oblasti IT infraštruktúry („IT infraštruktúra“) je situácia pri optimalizácii nákladov prostredníctvom centralizovaného DC obdobná:

- V oblasti serverových systémov je už aplikovaná určitá miera optimalizácie na úrovni jednotlivých projektov (každý projekt predpokladá aplikáciu virtualizácie systémov). Aj napriek tomu je však možné očakávať určitú optimalizáciu nákladov pri začlenení týchto systémov, do virtualizovanej infraštruktúry centralizovaného DC, kde je virtualizačný pomer možné špecifikovať na úrovni jednotlivých projektov začlenených do centralizovaného DC.

- Nie je potrebné budovať (rozširovať) infraštruktúru pre ukladanie dát pre viaceré lokality DC inštaláciou nových diskových polí a páskových knižníc (kde je potrebné obstarat' x krát riadiacu jednotku diskového poľa, alebo páskovej knižnice) ale prostredníctvom konsolidácie a virtualizácie infraštruktúry pre ukladanie dát je možné vytvoriť infraštruktúru vybudovanú na optimálnom počte zariadení (diskových polí, páskových knižníc) na úrovni centralizovaného DC. Vzhľadom na to, že dané zariadenia sú väčšinou zapojené do SAN infraštruktúry, prejaví sa optimalizácia nákladov aj v tejto oblasti.
- Pri DR infraštruktúre je úspora nákladov jednoznačná lebo sa odvíja od nižšieho počtu DR lokalít.
- Optimalizácia nákladov v oblasti zálohovacej infraštruktúry vychádza z možností vybudovania jedného príp. dvoch centralizovaných zálohovacích systémov (podľa charakteru prevádzky jednotlivých lokalít), oproti nutnosti budovania viacerých zálohovacích systémov pre väčší počet lokalít DC.
- Optimalizácia nákladov v oblasti monitorovacích systémov vychádza z predpokladu zníženia celkových počtov monitorovaných systémov prostredníctvom optimalizácie IT infraštruktúry v centralizovanom DC.
- Service Desk, ako primárny technický prostriedok pre podporu používateľov, je možné vytvoriť na úrovni jedného dátového centra, s využitím pre všetkých používateľov prevádzkovaných IS, oproti budovaniu viacerých obdobných systémov.
- Optimalizácia nákladov v oblasti licencií opätovne vychádza z predpokladu zníženia celkových počtov prevádzkovaných systémov prostredníctvom optimalizácie IT infraštruktúry v centralizovanom DC.

V oblasti prevádzky („Prevádzka“) je možné predpokladať úspory hlavne prostredníctvom zlepšenia energetickej efektivity dátového centra, ktorý je vyjadrený pomerom medzi celkovou spotrebou dátového centra a spotrebou IKT (bližšie v prílohe č.12 v kap. 12.3). Pritom môže niekedy dôjsť k určitým paradoxom, tým že v centralizovanom DC je možné aj zvýšenie príkonu na jeden dátový rozvádzač, zvýšením počtu systémov v tomto rozvádzači, čo je však vynahradené nižším celkovým počtom rozvádzačov.

Optimalizácia v oblasti podpory a prevádzky systémov („Podpora“) vychádzajú z možností optimalizácie ľudských zdrojov potrebných pre zabezpečenie daných činností – t.j. predpokladaným znížením počtov jednotlivých administrátorov a špecialistov IT na úrovni centralizovaného DC, oproti potrebe týchto špecialistov (alebo ich ekvivalentu prostredníctvom dodávky externých služieb) v prostredí viacerých DC.

Náklady spojené s prevádzkou DC („Réžia“) sú odvodené od samotnej existencie DC, preto je pri využívaní jedného centralizovaného DC možné predpokladať nižšie náklady ako pri súčte identických nákladov na viaceré DC. Dané úspory je možné očakávať z dôvodu optimalizácie ľudských zdrojov, aplikácie štandardov len na jeden subjekt ako aj zníženie nákladov na externé zdroje prostredníctvom napr. množstevných zliav.

Všeobecne sa udáva:

- Optimalizácia IT infraštruktúry a virtualizácia prinášajú úspory TCO v rozsahu 30-40 %.
- Zvýšenie energetickej efektívnosti IT znižuje energetické náklady o vyše 30 %.
- Optimalizácia a konsolidácia infraštruktúry dátového centra spolu s energetickým auditom redukuje náklady o 15-40 % s návratnosťou do 2 rokov.

Prínosy

Pre projekt „Centrálne služby dátového centra pre elektronizáciu verejnej správy“, je možné pri rešpektovaní jeho špecifik v podobe zamerania na technické zabezpečenie eGov služieb, identifikovať nepriame ekonomické prínosy vo forme časovej úspory používateľa služby, vyplývajúcej z lepšej dostupnosti elektronických služieb. Takéto prínosy formulované ako „zníži sa časová náročnosť poskytnutia služby, t.j. kratšie vybavenie jednotlivých agend“ sú prepokladané aj v schválenom projektovom zámere.

Pri identifikácii týchto prínosov sa vychádza primárne z rámca ITIL® (bližšie v prílohe č. 5), ktorý prostredníctvom aplikácie manažmentu IKT infraštruktúry založeného na jeho procesných princípoch, prináša pre svojich odberateľov (zákazníkov) hlavne:

- Zvýšenie dostupnosti a kvality služieb
- Efektívne riešenie problémov a incidentov
- Redukovanie rizika výpadku, resp. minimalizácia dopadu pri prípadnej poruche

Z pohľadu aplikácie centralizovaného dátového centra a jeho služieb sa jedná hlavne o zníženie nedostupnosti služby prostredníctvom efektívnejšieho riešenie incidentov na centrálne spravovanej IKT infraštruktúre a aj zo zníženého počtu incidentov, ktoré vyplýva z nižšieho počtu komponentov centralizovanej IKT infraštruktúry.

Druhú oblasť prínosov projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“, sú ušetrené náklady pri poskytovaní eGov služieb prostredníctvom centralizovaného dátového centra, oproti variante decentralizovanej – prostredníctvom parciálnych DC.

7.2 Rozpočet

V nasledujúcej tabuľke je uvedený prehľad nákladov na vybudovanie riešenia na technické zabezpečenie a podporu poskytovaných e-Gov služieb, centralizovaným spôsobom – vytvorenie dátového centra:

Tabuľka 16 – Prehľad nákladov na riešenie (rozpočet)

Názov nákladu	Suma celkom bez DPH	Suma celkom s DPH	Kód výdavkov
Analýza a návrhy riešenia pre celý projekt	800 000 €	960 000 €	637 005
Vypracovanie projektu - projektová dokumentácia	400 000 €	480 000 €	716
Technologická infraštruktúra DC a HW infraštruktúra DC	18 400 000 €	22 080 000 €	713 002
Služby pre technologickú infraštruktúru	1 500 000 €	1 800 000 €	637 005
Služby pre IT infraštruktúru	1 600 000 €	1 920 000 €	637 005
Licencie	3 900 000 €	4 680 000 €	711 004
Systémová integrácia	1 500 000 €	1 800 000 €	637 005
Vybudovanie organizácie	950 000 €	1 140 000 €	637 005
Školenia	150 000 €	180 000 €	637 001
Projektový manažment	200 000 €	240 000 €	637 005
Propagácia, reklama a inzercia	100 000 €	120 000 €	637 003
Celkom EUR	29 500 000 €	35 400 000 €	

Rozpočet predpokladá vytvorenie dvoch dátových centier v geograficky oddelených lokalitách. Rozpočet je kalkulovaný na celé trvanie projektu - 24 mesiacov (kap. 8.4). V ďalšom texte je rámcovým spôsobom popísaný obsah jednotlivých rozpočtových položiek ktoré sú uvedené v tabuľke.

Analýza a návrhy riešenia pre celý projekt

Položka predstavuje náklady na vypracovanie definičnej časti realizačného projektu dátového centra - analýzu, špecifikáciu požiadaviek, rámcový a detailný projekt dátového centra (bližšie špecifikované v kap. 8.3.2).

Vypracovanie projektu - projektová dokumentácia

Položka predstavuje náklady na vypracovanie zodpovedajúcej projektovej dokumentácie, ktorá je potrebná k realizácii dátového centra (bližšie špecifikované v kap. 8.3.2).

Technologická infraštruktúra a HW infraštruktúra DC

Položka predstavuje náklady na vytvorenie prostredia dátovej sály - technologické vybavenie DC – napájanie, chladenie, dátové rozvody, protipožiarny systém, zabezpečenie bezpečnosti a pod. a náklady na vybavenie DC zodpovedajúcimi IKT komponentmi – servery, diskové polia, zálohovacie zariadenia, dátové rozvádzače, komponenty pre komunikačnú infraštruktúru (LAN, SAN, WAN, ...) a pod.

Služby pre technologickú infraštruktúru

Položka predstavuje náklady na inštaláciu dodaného technologického vybavenia a jeho uvedenia do prevádzky, v hodnote 10% z nákladov na technologickú infraštruktúru.

Služby pre IT infraštruktúru

Položka predstavuje náklady na inštaláciu dodaných HW komponentov IKT infraštruktúry DC a SW komponentov IKT infraštruktúry (v rozsahu dodaných licencií) a ich uvedenie do prevádzky.

Licencie

Položka predstavuje náklady na licencie pre HW infraštruktúru DC – aplikačné servery, virtualizačné nástroje, databázy, SW pre riadenie zálohovania, monitorovacie nástroje, a pod..

Systémová integrácia

Položka predstavuje náklady na služby spojené s integráciou (umiestnením) informačných systémov a aplikácií (napr. IS projektov OPIS) prostredia IT infraštruktúry DC (bližšie špecifikované v kap. 8.3.1).

Vybudovanie organizácie

Položka predstavuje náklady na zavedenie systému riadenia IT služieb podľa ISO20000 a systému manažérskej informačnej bezpečnosti podľa ISO27001 (bližšie špecifikované v kap. 8.3.4).

Školenia

Položka predstavuje náklady na školenia súvisiace s projektovou aktivitou „Vybudovanie organizácie“ (kap. 8.3.4), ale aj s implementáciou dodaných HW a SW komponentov IKT infraštruktúry (napr. administrátorské školenia, produktové školenia...).

Výkon projektového manažmentu

Položka predstavuje aktivity štandardného projektového riadenia, finančného riadenia a monitorovania realizácie projektu po celú dobu trvania projektu v rozsahu 10 000,- EUR mesačne.

Propagácia, reklama a inzercia

Položka predstavuje štandardné aktivity publicity a informovanosti projektov OPIS, ktoré sú definované v Manuáli pre informovanie a publicitu.

7.3 Analýza nákladov

Identifikácia nákladov súčasného stavu - poskytovanie eGov služieb prostredníctvom parciálnych DC:

- Pre vyššie uvedené nákladové položky budú špecifikované ich hodnoty, ktorých súčet predstavuje jednotkové náklady na vzťažnú jednotku, ktorou je jeden dátový rozvádzač.
- Budú vypočítané náklady na poskytnutie eGov služieb pre jednotlivé projekty OPIS PO1, uvažované v tejto štúdii, ako súčin jednotkových nákladov a počtu dátových rozvádzačov potrebných pre daný projekt (identifikované v kap. 5.1),

Celkové náklady súčasného stavu budú následne vyrátané ako súčet nákladov na poskytnutie eGov služieb pre jednotlivé projekty OPIS PO1, uvažované v tejto štúdii.

Vzhľadom na to, že pre aktivity súvisiace so zabezpečením a prevádzkou DC posudzovaných projektov nie sú k dispozícii relevantné informácie, vychádza z predpokladaných nákladov modelového DC – s rozlohou 250m², v ktorom je umiestnených 80 dátových rozvádzačov, s odberom priemerne 2,5kW na dátový rozvádzač, s nákladmi na DC (technologickú infraštruktúru) v hodnote približne 8 mil.- EUR a nákladmi IKT infraštruktúry v hodnote približne 9 mil. EUR (čo napr. rámcovo zodpovedá nákladom na IKT infraštruktúru cca 16 mil. EUR pre projekt DCOM). Adresácia nákladov jednotlivých položiek vychádza z princípov definovaných pre potrebu výpočtu prevádzkových nákladov projektu (kap. 7.4.1).

Špecifikácia celkových nákladov súčasného stavu na dátový rozvádzač po jednotlivých položkách:

Tabuľka 17 – Náklady na dátový rozvádzač – poskytovanie eGov služieb prostredníctvom parciálnych DC

Nákladová položka	Náklad (EUR/rok)
Systém elektrického napájania	1 100
Centrálny chladiaci systém	1 100
Požiarny systém	1 000
Bezpečnostný systém	700
Dátová kabeláž	800
Serverové systémy	5 400
Infraštruktúra pre ukladanie dát	5 200
DR infraštruktúra	1 000
Zálohovacie systémy	500
Monitorovacie systémy	500
Service Desk	300
Licencie	500
Elektrická energia pre IKT	4 205
Elektrická energia pre chladenie a ďalšie systémy	4 205
Dátové komunikácie	1 000
HW maintenance a podpora	18 178
SW maintenance a podpora	13 128
Administrácia a správa systémov	2 016
Administrácia a správa databáz	1 210
Monitoring	1 613

Nákladová položka	Náklad (EUR/rok)
Podpora používateľov	6 451
Štandardizácia prevádzky	150
Vzdelávanie	300
Riadenie	2 419
Celkom	72 975

Špecifikácia celkových nákladov súčasného stavu, po jednotlivých projektoch OPIS je uvedená v nasledovnej tabuľke:

Tabuľka 18 – Celkové ročné náklady – poskytovanie eGov služieb prostredníctvom parciálnych DC

Projekt	Náklady -as is (EUR/rok)
Národný projekt CEP	291 898
Elektronické služby Finančnej správy I. oblasť daňová	1 678 414
Datacentrum miest a obcí (DCOM)	875 694
Elektronizácia služieb VÚC	875 694
Ústredný portál verejnej správy (ÚPVS)	875 694
Elektronické služby Štatistického úradu SR	1 094 618
Elektronické služby Sociálnej poisťovne	875 694
Elektronizácia služieb Ministerstva hospodárstva SR (IIS MH)	802 720
Elektronické služby zdravotníctva (eHealth)	1 313 541
Kontrolórsky informačný systém (KIS NKÚ)	145 949
Elektronické služby úradu pre verejné obstarávanie (IS EVO)	291 898
Celkom	9 121 816

Identifikácia nákladov budúceho stavu - poskytovanie eGov služieb po realizácii projektu, prostredníctvom centrálného DC:

- Pre každú nákladovú položku budú špecifikované upravené hodnoty, vyplývajúce z aplikácie centralizácie technického zabezpečenia a podpory eGov služieb, ktorých súčet predstavuje nové jednotkové náklady na vzťažnú jednotku, ktorou je jeden dátový rozvádzač,
- Pre jednotlivé projekty OPIS PO1, uvažované v tejto štúdii, budú upravené počty dátových rozvádzačov, vyplývajúce z aplikácie centralizácie technického zabezpečenia eGov služieb,
- Pre jednotlivé projekty OPIS PO1, uvažované v tejto štúdii, budú vypočítané nové náklady na poskytnutie eGov služieb ako súčin upravených jednotkových nákladov
- Celkové náklady budúceho stavu budú následne vyrátané ako súčet upravených nákladov na poskytnutie eGov služieb pre jednotlivé projekty OPIS PO1, uvažované v tejto štúdii.

Upravené hodnoty nákladových položiek, po aplikácii centralizácie sú uvedené v nasledovnej tabuľke:

Tabuľka 19 – Upravené náklady na dátový rozvádzač

Nákladová položka	Možnosti centralizácie	Pôvodný náklad (EUR/rok)	Faktor optimalizácie (%)	Upravený náklad (EUR/rok)
Systém elektrického napájania	Optimálnejšie vybudovanie jedného veľkého systému, ako viacerých malých	1 100	3%	1 067
Centrálny chladiaci systém	Optimálnejšie vybudovanie jedného veľkého systému, ako viacerých malých	1 100	3%	1 067
Požiarny systém	Optimálnejšie vybudovanie jedného veľkého systému, ako viacerých malých	1 000	3%	970
Bezpečnostný systém	Optimálnejšie vybudovanie systému pre jeden objekt, ako pre viac menších	700	2%	686
Dátová kabeláž	Optimálnejšie vybudovanie systému pre jeden objekt, ako pre viac menších	800	2%	784
Serverové systémy	Optimalizácia (zníženie) počtov systémov	5 400	5%	5 130
Infraštruktúra pre ukladanie dát	Optimalizácia (zníženie) počtov systémov	5 200	25%	3 900
DR infraštruktúra	Optimalizácia (zníženie) počtov systémov	1 000	70%	300
Zálohovacie systémy	Optimalizácia (zníženie) počtov zálohovacích systémov	500	25%	375
Monitorovacie systémy	Optimalizácia (zníženie) počtov monitorovaných systémov	500	70%	150
Service Desk	Vybudovanie len jedného centralizovaného systému	300	70%	90
Licencie	Vychádza z optimalizácie systémov	500	5%	475
Elektrická energia pre IKT	Odber na rovnakej úrovni, lepšia cena energií pri väčších odberoch	4 205	2%	4 121
Elektrická energia pre a chladienie ďalšie systémy	Chladienie na rovnakej úrovni , lepšia cena energií pri väčších odberoch	4 205	2%	4 121
Dátové komunikácie	Optimálnejšie využitie kapacity liniek, lepšia cena pri vyšších kapacitách	1 000	3%	970

Nákladová položka	Možnosti centralizácie	Pôvodný náklad (EUR/rok)	Faktor optimalizácie (%)	Upravený náklad (EUR/rok)
HW maintenance a popora	Vychádza z optimalizovného stavu HW	18 178	30%	12 724
SW maintenance a podpora	Vychádza z optimalizovného počtu licencií	13 128	5%	12 472
Administrácia a správa systémov	Optimalizácia ľudských zdrojov	2 016	15%	1 714
Administrácia a správa databáz	Optimalizácia ľudských zdrojov	1 210	15%	1 028
Monitoring	Optimalizácia ľudských zdrojov	1 613	15%	1 371
Podpora používateľov	Optimalizácia ľudských zdrojov	6 451	15%	5 484
Štandardizácia prevádzky	Aplikácia štandardizácie a jej certifikácie len na jednu inštitúciu	150	70%	45
Vzdelávanie	Vychádza z optimalizácie ľudských zdrojov	300	10%	270
Riadenie	Vychádza z optimalizácie ľudských zdrojov a infraštruktúry	2 419	10%	2 177
Celkom		72 975		61 490

Optimalizácia počtu dátových rozvádzačov vychádza primárne z možností optimalizácie počtov zariadení pre ukladanie dát na úrovni dátových rozvádzačov a čiastočne aj umiestnenia systémov v jednotlivých rozvádzačoch.

Špecifikácia celkových nákladov budúceho stavu – to be predstavuje predpokladané optimalizované náklady na poskytovanie eGov služieb po realizácii projektu, prostredníctvom centrálného DC je uvedená v nasledovnej tabuľke:

Tabuľka 20 – Celkové náklady budúceho stavu – to be

Projekt	Náklady - to be (EUR/rok)
Národný projekt CEP	184 471
Elektronické služby Finančnej správy I. oblasť daňová (program UNITAS)	922 353
Datacentrum miest a obcí (DCOM)	368 941
Elektronizácia služieb VÚC	368 941
Ústredný portál verejnej správy (ÚPVS)	491 922

Projekt	Náklady - to be (EUR/rok)
Elektronické služby Štatistického úradu SR	553 412
Elektronické služby Sociálnej poisťovne	368 941
Elektronizácia služieb Ministerstva hospodárstva SR (IIS MH)	491 922
Elektronické služby zdravotníctva (eHealth)	614 902
Kontrolórsky informačný systém (KIS NKÚ)	122 980
Elektronické služby úradu pre verejné obstarávanie (IS EVO)	184 471
Centrálna infraštruktúra pre ukladanie dát	1 598 746
Celkom	6 272 003

7.4 Ekonomický model

7.4.1 Prevádzkové náklady

Pre potreby projekcie prevádzkových nákladov projektu, ktorých zabezpečenie je predpokladom trvalej udržateľnosti projektu, je potrebné identifikovať predpokladané náklady na prevádzku dátového centra. Tieto náklady je možné z hľadiska ich povahy rozdeliť na dve základné oblasti:

Prvou oblasťou sú náklady spojené s vlastníctvom infraštruktúry DC (IKT / technologickej), ktorá je nevyhnutná na zabezpečenie dodávky definovaných služieb v požadovanej kvalite a rozsahu, pričom je možné ich chápať ako náklady na vlastnú prevádzku DC – bez poskytovania služieb. Tieto náklady majú fixný charakter vzhľadom na to, že pri zachovanom portfóliu služieb v tom istom rozsahu a kvalite sú relatívne nemenné. Dané náklady je možné definovať v nasledovnej základnej štruktúre:

- náklady na technologickú infraštruktúru DC
 - predstavujú náklady spojené so zabezpečením prevádzky (servisu) a udržaním (obnovou) systémov potrebných na vytvorenie prostredia dátovej sály
- náklady na IKT infraštruktúru DC
 - predstavujú náklady spojené so zabezpečením prevádzky (HW, SW maintenance) a udržaním (obnovou) systémov potrebných na vytvorenie prostredia IKT infraštruktúry DC
- náklady na prevádzku infraštruktúry DC – technologickej aj IKT
 - energie (primárne elektrická)
 - náklady na dátové komunikácie
- náklady na zabezpečenie podpory prevádzky technologickej infraštruktúry DC
 - správa a prevádzková údržba
 - majú charakter personálnych nákladov
- náklady spojené so zabezpečením podpory prevádzky systémov IKT
 - administrácia a správa systémov, databáz, počítačových sietí, dohľad (monitoring), ...
 - majú charakter personálnych nákladov
- náklady spojené s prevádzkou a riadením DC ako organizácie

- riadenie, rozvoj služieb, bezpečnosť, kvalita
- majú charakter personálnych nákladov
- ostatné náklady spojené s prevádzkou DC ako organizácie
 - školenia, audit a recertifikácie spojené s udrzaním získaných štandardov, ...

Druhou oblasťou sú náklady spojené s poskytovaním služieb, kde veľkosť daného nákladu je závislá primárne od druhu a rozsahu poskytovanej služby, preto majú variabilný charakter. Dané náklady je možné definovať v nasledovnej štruktúre:

- majoritné náklady
 - náklady na službu prenájom priestoru (housing)
 - vyplývajú z rozsahu umiestenej IKT infraštruktúry
 - primárne sú to náklady na energie
 - v rámci projekcie nákladov je možné ich vyčíslit'
- minoritné náklady
 - špecifické náklady vyplývajúce z rozsahu a charakteru poskytnutej služby, pričom ich charakter a veľkosť, vzhľadom na predpokladaný rozsah poskytovanej služby, ich už neumožňuje zaradiť do prvej oblasti nákladov (fixné náklady)
 - jedná sa napr. o náklady na páskové zálohovacie médiá pri poskytnutí služby zálohovania (archivácie) dát
 - v rámci projekcie nákladov je problematické ich vyčíslit'

Projekcia nákladov

Projekcia prevádzkových nákladov vychádza z vyššie uvedenej štruktúry. Z dôvodu zjednodušenia je projekcia pre všetky položky definovaná rovnomerne na ročnej báze, je uvažovaná na vyhodnocované obdobie 15 rokov a vychádza z obstarávacích nákladov projektu (z definovaného rozpočtu).

- náklady na technologickú infraštruktúru DC
 - prevádzkové náklady na priebežnú údržbu a opravy DC
 - predpokladajú sa náklady na úrovni 10 % nákladov z implementačných služieb na technologickú infraštruktúru DC (Služby pre technologickú infraštruktúru)
 - náklady na obnovu technologickej infraštruktúry DC
 - hodnota životnosti DC je všeobecne predpokladaná v rozmedzí 10 až 15 rokov,
 - obnova technologickej infraštruktúry DC sa predpokladá na hornej hranici životnosti – t.j. 15 rokov, nie celá výška obstarávacích nákladov predstavuje náklady priamo na technológie, preto je uvažovaných 80% nákladov na technologickú infraštruktúru DC, ktoré sú rozpustené do celého vyhodnocovacieho obdobia 15 rokov
- náklady na IKT infraštruktúru DC
 - náklady na ročné udržiavacie poplatky (maintenance) sa líšia od typu HW zariadenia / SW produktu a predpokladajú sa na úrovni
 - HW maintenance a podpora – HW maintenance je uvažovaný v priemernej hodnote 16% + podpora 2%, z obstarávacích nákladov HW

- SW maintenance a podpora – SW maintenance je uvažovaný v priemernej hodnote 12% + podpora 3%, z obstarávacích nákladov SW licencií
- obnova HW komponentov infraštruktúry DC sa predpokladá na úrovni 5 rokov,
 - vzhľadom na vývoj IT technológií sa dá predpokladať znižovanie jednotkových nákladov vo vzťahu k ich charakteristickým parametrom (procesorový výkon, diskový priestor, a pod.)
 - z tohto dôvodu je rozpustených 80% obstarávacích nákladov HW do 5 rokov a premietnutých na vyhodnocovacie obdobie, v čom sú rátané aj dodatočné náklady na prácu
- obnova SW komponentov infraštruktúry DC sa predpokladá na úrovni 5 rokov,
 - vzhľadom na platený SW maintenance sa predpokladá kontinuálna dostupnosť nových SW produktov, je však potrebné rátať s prácami pri upgarde alebo zmene produktov, pričom časť týchto prác je možné realizovať v réžii DC
 - z tohto dôvodu je rozpustená 1/4 nákladov na služby pre IT infraštruktúru do 5 rokov a premietnutá na vyhodnocovacie obdobie
- náklady na prevádzku infraštruktúry DC – technologickej aj IKT
 - energie (primárne elektrická)
 - pre potreby projekcie nákladov je uvažované s prevádzkou 102 dátových rozvádzačov (vychádza sa z optimalizovaného počtu dátových rozvádzačov – tab. 22),
 - ráta sa s priemernou spotrebou 4 kW na dátový rozvádzač a s rovnakou spotrebou na chladenie a pre ďalšie zariadenie (UPS, osvetlenie, ...)
 - ráta sa s priemernou cenou elektrickej energie 180.- € / MWh
 - náklady na dátové komunikácie
 - predpokladé sú náklady v hodnote 200 000.- € na rok
- náklady spojené s prevádzkou DC ako organizácie
 - personálne náklady
 - personálne náklady vychádzajú z predpokladaného nárastu ľudských zdrojov, v počte 23 osôb, ktorý bol definovaný v rámci návrhu riešenia (kap. 6.8.1)
 - ostatné náklady spojené s prevádzkou DC ako organizácie
 - predpokladé sú náklady v hodnote 80 000.- € na rok

Projekcia komplexných ročných prevádzkových nákladov je uvedená v nasledovnej tabuľke:

Tabuľka 21 – Komplexné ročné prevádzkové náklady projektu

Nákladová položka	Náklad (EUR/rok)
Náklady na technologickú infraštruktúru DC	
Náklady na prevádzku a údržbu technologickej infraštruktúry DC	180 000
Náklady na obnovu technologickej infraštruktúry DC	960 000
Náklady na IKT infraštruktúru DC	
HW maintenance a podpora	734 400
SW maintenance a podpora	702 000
Náklady na obnovu HW infraštruktúry DC	652 800
Náklady na obnovu SW infraštruktúry DC	96 000
Náklady na prevádzku infraštruktúry DC	
Elektrická energia pre IKT	643 334
Elektrická energia pre chladenie + ďalšie zariadenia	643 334
Dátové komunikácie	200 000
Náklady na prevádzku DC ako organizácie	
Personálne náklady	370 944
Ostatné náklady	80 000
Celkom	5 262 813

7.4.2 Návrh modelu spoplatňovania služieb

Náklady uvedené v rámci projekcie nákladov predstavujú prevádzkové náklady projektu vyplývajúce z jeho realizácie a následnej prevádzky. Vzhľadom na to že projekt má za cieľ poskytovať služby pre zabezpečenie podpory a prevádzky IKT infraštruktúry eGov služieb, predstavujú aj nákladový dopad na štátny rozpočet, ktorý sa bude kumulovať na úrovni prevádzkovateľa centralizovaného DC - DataCentra.

Aby sa sprehľadnili tieto finančné toky je potrebné definovať hodnotu jednotlivých služieb a model účtovania a spoplatňovania – t.j. definovať ekonomický model DC. Pri definovaní ekonomického modelu centralizovaného DC sa vychádzalo z princípov IT Service Managementu podľa ITIL (v.3).

Vzhľadom na existenciu DataCentra ako rozpočtovej organizácie je pre ocenenie dodávaných služieb vhodné použiť koncept ocenenia služieb na základe nákladov ich dodávky (Provisioning Value), ktorý adresuje všetky nákladové položky (priame aj nepriame) na zabezpečenie dodávky služby.

Pre spôsob účtovania a následného spoplatňovania služieb existuje viacero modelov, ktoré sa líšia úrovňou komplexnosti (zložitosti) kalkulácii a schopnosti odberateľov služieb porozumieť im. Niektoré ukážky modelov spoplatnenia zahŕňajú:

- Notionálne (predstavované) spoplatňovanie
 - tieto alternatívy spoplatnenia určujú aké účtovné zápisy budú zaznamenané v podnikových finančných systémoch. Jednou z možností je metóda tzv. ‘dvoch (účtovných) kníh’. Pri tejto metóde sa do podnikového finančného systému účtujú náklady jedným spôsobom (napr. IT ako nákladové stredisko), a do „druhej knihy“ sa náklady zaznamenávajú ale neúčtujú sa. Druhá kniha poskytuje tie isté informácie ako prvá kniha, ale odráža situáciu v prípade účtovania nákladov alternatívnym spôsobom. Tento spôsob predstavuje vhodný prechodový model pri zmene spôsobov spoplatňovania z jedenej metodiky na inú.
- Odstupňované predplácanie

- daný spôsob zahŕňa rôzne úrovne garancií a/alebo prínosov ponúkaných pre služby alebo balíčky služieb, kde pre ohodnotenie každej z nich bol aplikovaný zodpovedajúci model spoplatnenia. Pre definovanie úrovne služieb sa vo všeobecnosti najčastejšie používa zlatá, strieborná a bronzová úroveň služieb. Slabou stránkou tohto modelu je to, že nepodporuje rozdielne správanie zákazníkov vo využívaní služieb.
- Meraná spotreba
 - daný spôsob vyžaduje vyspelejšie finančné prostredie a zodpovedajúce možnosti v oblasti prevádzky IT. Predpokladá sa modelovanie požiadaviek spolu s modelom dodávky služieb, pre ktorú je k dispozícii infraštruktúra IKT a jej manažment, umožňujúci poskytovať a merať výpočtové zdroje podľa aktuálnych potrieb zákazníka (utility computing). Informácie o spotrebe zdrojov sú následne aplikované pre potreby spoplatnenia zákazníka a sú založené na rôznych, vopred dohodnutých, prírastkoch služby (napr. hodiny, dni, týždne).
- Priame (náklady) plus
 - predstavuje zjednodušený model, pri ktorom náklady ktoré môžu byť priradené priamo k službe sú spoplatnené primerane s určitým percentom spoločných nepriamych nákladov.
- Fixné alebo používateľské náklady
 - jedná sa o najviac zjednodušený model spoplatnenia, kde sú náklady rozdelené prostredníctvom dohodnutého kľúča, ktorým môže byť napr. počet používateľov. Daný model však len minimálnym spôsobom zohľadňuje správanie používateľov prípadne identifikáciu skutočných požiadaviek na službu alebo jej spotrebu. Tento model však v prípade potreby umožňuje najjednoduchším spôsobom alokovať náklady na konkrétnu organizačnú zložku spoločnosti.

Pre realizáciu spoplatňovania a teda špecifikáciu spôsobu financovania prevádzky DC môže byť aplikovaný jeden alebo kombinácia viacerých spôsobov spoplatňovania. Konkrétny model spoplatňovania, ktorý bude aplikovaný, závisí od detailných požiadaviek na spoplatnenie, možnosti použitého finančného systému ako aj možnosti IKT infraštruktúry a jej manažmentu. Tento model bude definovaný a následne aplikovaný počas činností spojených so zavedením systému riadenia IT služieb podľa ISO 20000, v rámci aktivity „vybudovanie organizácie“ podľa definovaného implementačného plánu.

Dá sa však predpokladať, že s rozvojom využívania cloud computingu (vzhľadom na jeden z jeho základných princípov – pridelovanie zdrojov podľa požiadaviek) bude v rámci modelu spoplatňovania stále viac vystupovať do popredia aplikácia meranej spotreby (výpočtových zdrojov), ktorá najviac odráža realitu vo využívaní zdrojov zákazníkom.

Atraktivnosť služieb pre odberateľa je aj bez ohľadu na úroveň ich spoplatnenia možné identifikovať na viacerých úrovniach:

- nie je potrebná vynaložiť investičné náklady, či už pre potreby rozvoja technologickej infraštruktúry vlastného dátového centra alebo IKT infraštruktúry potrebnej na zabezpečenie daných eGov služieb,
- paralelne s investičnými nákladmi je tu aj faktor implementačných nákladov a faktor časový,
- nie je potrebná následná organizácia zabezpečenia prevádzky a údržby,
- vzhľadom na to, že DataCentrum je štátnou rozpočtovou organizáciou je spoplatnenie služieb len na úrovni nákladov (bez tvorby zisku).

Aby sa ešte viac zatraktívnil služby pre predpokladaných odberateľov, je vhodné spoplatňovať len určitú časť z celkových nákladov identifikovaných v rámci projekcie nákladov. Jendou z možností je napr. rozdelenie z hľadiska investičných a prevádzkových nákladov. DataCentrum by na seba prevzalo všetky náklady ktoré majú charakter investičných nákladov – t.j. náklady projektu, z definovaných nákladov na prevádzku by na seba prevzalo náklady na udržanie (obnovu) technologickej aj IKT infraštruktúry potrebnej na poskytovanie služieb a v budúcnosti aj náklady na jej rozvoj, v súlade s predpokladaným rozvojom poskytovania služieb.

Pre potreby spoplatňovania by boli následne uvažované len náklady ktoré majú charakter prevádzkový. Z tohto pohľadu by ročné prevádzkové náklady projektu boli znížené o príspevky spoplatnenia a vyzerali by nasledovne:

Tabuľka 22 – Znížené ročné prevádzkové náklady projektu

Nákladová položka	Náklad (EUR/rok)
Náklady na technologickú infraštruktúru DC	
Náklady prevádzku a údržbu technologickej infraštruktúry DC	0
Náklady na obnovu technologickej infraštruktúry DC	960 000
Náklady na IKT infraštruktúru DC	
HW maintenance a podpora	0
SW maintenance a podpora	0
Náklady na obnovu HW infraštruktúry DC	652 800
Náklady na obnovu SW infraštruktúry DC	96 000
Náklady na prevádzku infraštruktúry DC	
Elektrická energia pre IKT	0
Elektrická energia pre chladenie + ďalšie zariadenia	0
Dátové komunikácie	0
Náklady na prevádzku DC ako organizácie	
Personálne náklady	0
Ostatné náklady	0
Celkom	1 708 800

Jednou z výhod tohto modelu je napr. jednoduchosť zmluvného zabezpečenie podpory, vzhľadom na to že všetka infraštruktúra (technologická aj IKT) je vo „vlastníctve“ jedného subjektu.

Daný model by tiež podporoval kľúčovú oblasť rozvoja Dátového centra a to zvýšenie efektivity poskytovania služieb migráciou na poskytovateľa IT služieb formou cloud computing. Takto zadefinovaný cieľový stav bude totiž vyžadovať úpravu architektúry dátového centra tak, aby bolo schopné adresovať všetky nové požiadavky a výzvy, ktoré so sebou nesie cloud computing, čo predpokladá aj rozvoj zodpovedajúcej infraštruktúry IKT. Preto je „vlastníctvo“ investičných nákladov jedným z dôležitých predpokladov na systémový rozvoj IKT infraštruktúry pri jej smerovaní ku cloud computingu.

Z hľadiska časového by daná investícia do IKT infraštruktúry mala byť zosúladená s nutnou obnovou IKT infraštruktúry jednotlivých projektov OPIS, ktorú je možné predpokladať na úrovni jej morálnej životnosti – t.j. v rozmedzí 4 až 6 rokov od jej implementácie. To znamená že projekty OPIS u ktorých je z hľadiska dnešného vývoja projektu možné prepokladať primárne využitie služieb housigu by neobnovovali už vlastnú IKT infraštruktúru, ale by postupne prechádzali na poskytovanie eGov služieb prostredníctvom cloud computingu na úrovni centralizovaného DC. Časový horizont 4 rokov sa tiež javí ako adekvátny na zodpovedajúcu prípravu jednak z hľadiska definície novej architektúry, aplikácie potrebnej IKT infraštruktúry ale aj prípravy procesnej a organizačnej.

7.5 Analýza prínosov

Kvantifikáciu nepriamych prínosov projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ ktorá vychádza z ušetrenia času používateľov eGov služieb prostredníctvom efektívnejšieho riešenie incidentov na centrálne spravovanej IKT infraštruktúre a aj zo zníženého počtu incidentov, ktoré vyplýva z nižšieho počtu komponentov centralizovanej IKT infraštruktúry na ktoré je možné poukázať prostredníctvom nasledujúcich príkladov:

Na základe štúdie od spoločnosti Glomark – Governan (ITIL Benefits Benchmarks Study Release Based on the Research Study Conducted by Glomark-Governan), ktorá bola realizovaná niekoľko mesiacov (ukončená v apríli 2008), so zameraním na zistenie prevádzkových prínosov zavedenia ITSM- ITIL procesov do prevádzky, je možné konštatovať, že prostredníctvom zlepšenia Manažmentu Incidentov a Problémov sa dá v organizácii dosiahnuť výrazné zníženie výpadkov služieb pre používateľov.

Štúdia bola realizovaná na 55 spoločnostiach a vládnych organizáciách v Severnej a Južnej Amerike ako aj v Európe, ktoré implementovali ITIL v2 procesy. Výsledkom štúdie je zistenie, že prostredníctvom zavedenia Manažmentu incidentov bolo v konkrétnych spoločnostiach dosiahnuté zníženie doby výpadkov služieb v rozmedzí 10% - 28% a prostredníctvom Manažmentu problémov bola dosiahnutá redukcia incidentov v rozsahu 7% - 13% ako aj znížená priemerná doba riešenia problémov o 9,4%. Výška percenta bola v rôznych spoločnostiach rôzna a závisela na rôznych faktoroch (napr. spoločnosti, ktoré implementovali viacej ITIL procesov dosiahli lepšie výsledky, spoločnosti, ktoré využili externých ITIL expertov dosiahli tak isto lepšie výsledky,).

Ďalším príkladom zlepšenia dostupnosti služieb v organizácii je príklad spoločnosti Plan-net (Return on Investment from ITIL Service Management „White Paper“). Tá zavedením Manažmentu Incidentov do organizácie z finančného sektora dosiahla až 24% zníženie výpadkov služieb pre používateľov a prostredníctvom implementácie Manažmentu problémov bola dosiahnutá 16% redukcia počtu opakujúcich sa incidentov.

V prostredí jednotlivých organizácií (jednotlivých projektov OPIS PO1) je možné predpokladať na určitej (nižšej alebo vyššej) úrovni systémové zabezpečenie prevádzky v zmysle ITSM – ITIL. V rámci projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ je však plánované zavedenie systému riadenia IT služieb podľa ISO 20000, čo prináša štandardizáciu úrovne poskytovania a podpory služieb naprieč celým spektrom používateľov, pre všetky prevádzkované informačné systémy, s ich neustálym zlepšovaním do budúcnosti. Zavedenie štandardov podľa ISO 20000 spolu so znížením komplexnosti centralizovanej IKT infraštruktúry (zníženie počtu komponentov IKT, optimalizácia DR architektúry len na úroveň jedného DR DC), dáva predpoklad na zníženie nedostupnosti poskytovaných eGov služieb prostredníctvom efektívnejšieho riešenie incidentov na centrálne spravovanej IKT infraštruktúre a aj z dôvodov zníženého počtu incidentov a problémov, ktoré vyplýva z nižšieho počtu komponentov centralizovanej IKT infraštruktúry.

Prostredníctvom centralizovaného dátového centra a jeho služieb nie je dosiahnuteľné také výrazné zníženie nedostupnosti služieb, ako bolo identifikované vo vyššie uvedených príkladoch, kde sa jednalo o prvé zavedenie procesov ITSM – ITIL. Na základe vyššie popísaných predpokladov a zistení, je však možné prostredníctvom projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ očakávať zníženie nedostupnosti poskytovaných eGov služieb o hodnotu v rozmedzí 3% až 10%.

Na základe zníženia nedostupnosti poskytovaných eGov služieb je možné predpokladať ušetrenie priemerne 7 % času (faktor optimalizácie) používateľov eGov služieb zo všetkých projektov OPIS PO1, ktoré boli zahrnuté do tejto štúdie z celkovej hodnoty ušetrného času používateľov, ktorý bol identifikovaný v ich štúdiách uskutočniteľnosti. Pokiaľ neboli prínosy z ušetrného času používateľov v rámci jednotlivých projektov OPIS, uvažovaných v tejto štúdii, špecifikované, boli stanovené na úrovni 95% z celkových prínosov daného projektu.

Očakávané prínosy projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ sa predpokladajú až po ukončení realizačného projektu DC – t.j. po druhom roku trvania projektu.

Finančné vyjadrenie prínosov projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ z ušetreného času používateľov sú je v nasledovnej tabuľke:

Tabuľka 23 – Nefinančné prínosy projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ z ušetreného času používateľov

Rok	Prínosy zo zahrnutých projektov OPIS PO1	Faktor optimalizácie	Prínosy projektu
1	19 317 188 €	0,00%	0 €
2	37 141 972 €	0,00%	0 €
3	61 313 032 €	7,00%	4 291 912 €
4	76 558 891 €	7,00%	5 359 122 €
5	103 296 313 €	7,00%	7 230 742 €
6	120 119 072 €	7,00%	8 408 335 €
7	134 036 440 €	7,00%	9 382 551 €
8	144 218 828 €	7,00%	10 095 318 €
9	154 715 155 €	7,00%	10 830 061 €
10	109 411 835 €	7,00%	7 658 828 €
11	75 181 401 €	7,00%	5 262 698 €
12	84 797 952 €	7,00%	5 935 857 €
13	95 714 314 €	7,00%	6 700 002 €
14	106 144 233 €	7,00%	7 430 096 €
15	115 514 058 €	7,00%	8 085 984 €
Celkom	1 437 480 685 €		96 671 507 €

Úspora nákladov

Úspory nákladov vyplývajúce z projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“ predstavujú rozdiel (ušetrené náklady) medzi nákladmi na realizáciu a prevádzku parciálnych dátových centier a nákladmi na realizáciu a prevádzku centralizovaného dátového centra. Očakávané úspory nákladov sa predpokladajú až po ukončení realizačného projektu DC – t.j. po druhom roku trvania projektu. Pokiaľ by sa projekt nerealizoval bolo by potrebné budovať infraštruktúru parciálnych dátových centier, kde je predpoklad ich celkového dobudovania a teda aj nábeh nákladov v priebehu dvoch rokov (súčasný stav).

Celková úspora nákladov na zabezpečenie poskytovania e-Gov služieb centralizovaným spôsobom je uvedená v nasledovnej tabuľke:

Tabuľka 24 – Celková úspora nákladov na poskytovanie eGov služieb po zavedení projektu

Rok	Náklady - súčasný stav	Náklady - budúci stav	Úspora
1	4 560 908	0	4 560 908
2	6 081 210	0	6 081 210
3	9 121 816	6 272 003	2 849 812
4	9 121 816	6 272 003	2 849 812

Rok	Náklady - súčasný stav	Náklady - budúci stav	Úspora
5	9 121 816	6 272 003	2 849 812
6	9 121 816	6 272 003	2 849 812
7	9 121 816	6 272 003	2 849 812
8	9 121 816	6 272 003	2 849 812
9	9 121 816	6 272 003	2 849 812
10	9 121 816	6 272 003	2 849 812
11	9 121 816	6 272 003	2 849 812
12	9 121 816	6 272 003	2 849 812
13	9 121 816	6 272 003	2 849 812
14	9 121 816	6 272 003	2 849 812
15	9 121 816	6 272 003	2 849 812
Celkom	129 225 721	81 536 044	47 689 677

7.6 CBA analýza

7.6.1 Výpočet nákladov CBA

Pre výpočet CBA v časti nákladov sú v stave as-is (alternatíva 1) uvažované nulové hodnoty, čo predstavuje súčasný stav DataCentra bez realizácie projektu. V stave to-be (alternatíva 2) sú uvažované len fixné náklady, kde sú rozvrhnuté plánované náklady projektu na dobu jeho trvania – t.j. 2 roky a následne sú kalkulované náklady na prevádzku riešenia v dvoch variantách

- Variant 1 – komplexné náklady na prevádzku uvedené v kap. 7.4.1,
- Variant 2 - znížené náklady na prevádzku riešenia uvedené v kap. 7.4.2..

Výpočet nákladov pre CBA, pre variant 1 - s uvažovaním komplexných nákladov na prevádzku (kap. 7.4.1) je uvedený v nasledovnej tabuľke.

Tabuľka 25 – CBA - výpočet nákladov – variant 1. komplexné prevádzkové náklady

Obdobie	Fixné náklady			Náklady spolu		
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel
t1	0	17 700 000	17 700 000	0	17 700 000	17 700 000
t2	0	17 700 000	17 700 000	0	17 700 000	17 700 000
t3	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t4	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t5	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t6	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t7	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t8	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t9	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t10	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t11	0	5 262 813	5 262 813	0	5 262 813	5 262 813

t12	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t13	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t14	0	5 262 813	5 262 813	0	5 262 813	5 262 813
t15	0	5 262 813	5 262 813	0	5 262 813	5 262 813
SPOLU				0	103 816 566	103 816 566

Výpočet nákladov pre CBA, pre variant 2 - s uvažovaním znížených prevádzkových nákladov (kap. 7.4.2) je uvedený v nasledovnej tabuľke:

Tabuľka 26 – CBA - výpočet nákladov – variant 2. znížené prevádzkové náklady

Obdobie	Fixné náklady			Náklady spolu		
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel
t1	0	17 700 000	17 700 000	0	17 700 000	17 700 000
t2	0	17 700 000	17 700 000	0	17 700 000	17 700 000
t3	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t4	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t5	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t6	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t7	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t8	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t9	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t10	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t11	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t12	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t13	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t14	0	1 708 800	1 708 800	0	1 708 800	1 708 800
t15	0	1 708 800	1 708 800	0	1 708 800	1 708 800
SPOLU				0	57 614 400	57 614 400

7.6.2 Výpočet prínosov CBA

Pre výpočet CBA v časti prínosov sú v stave as-is (alternatíva 1) uvažované nulové hodnoty, čo predstavuje súčasný stav DataCentra bez realizácie projektu. V stave to-be (alternatíva 2) sú uvažované len nepríjmy prínosy v dvoch oblastiach, tak ako boli uvedené v analýze prínosov:

- Prínosy z ušetreného času používateľov.
- Kvalitatívne prínosy ktoré predstavujú úspory vyjadrené ako rozdiel (ušetrené náklady) medzi nákladmi na realizáciu a prevádzku parciálnych dátových centier a nákladmi na realizáciu a prevádzku centralizovaného dátového centra.

Výpočet prínosov je uvedený v tabuľke 30.

7.6.3 Výpočet NPV

Výpočet čistej súčasnej hodnoty je rátaný ako rozdiel medzi prínosmi a nákladmi, kde je zahrnutý aj faktor času, prostredníctvom diskontnej sadzby v zmysle referenčných hodnôt pre výpočet CBA, tak ako je uvedená predpokladoch pre finančný plán. Výpočet je urobený pre obidve varianty prevádzkových nákladov.

Z výpočtu NPV, pre variant 1 - komplexné prevádzkové náklady, ktorý je uvedený v tabuľke 31, vyplýva že investície do projektu sa začnú vracat' v 9. roku jeho realizácie a využívania.

V prípade aplikácie spôsobu spoplatnenia uvedeného v kap. 7.4.2, keď sú pre výpočet NPV uvažované znížené prevádzkové náklady podľa variantu 2 (náklady znížené o príspevok spoplatnenia), vychádza návratnosť investície v 6. roku realizácie a využívania projektu. Výpočet je uvedený v tabuľke 32.

Tabuľka 27 – CBA - výpočet prínosov

Obdobie	Nepriame prínosy						Prínosy spolu		
	Cena ušetreného času používateľa			Kvalitatívne prínosy vo finančnom vyjadrení			Ekonomické prínosy		
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel
t1	0	0	0	0	4 560 908	4 560 908	0	4 560 908	4 560 908
t2	0	0	0	0	6 081 210	6 081 210	0	6 081 210	6 081 210
t3	0	4 291 912	4 291 912	0	2 849 812	2 849 812	0	7 141 724	7 141 724
t4	0	5 359 122	5 359 122	0	2 849 812	2 849 812	0	8 208 935	8 208 935
t5	0	7 230 742	7 230 742	0	2 849 812	2 849 812	0	10 080 554	10 080 554
t6	0	8 408 335	8 408 335	0	2 849 812	2 849 812	0	11 258 147	11 258 147
t7	0	9 382 551	9 382 551	0	2 849 812	2 849 812	0	12 232 363	12 232 363
t8	0	10 095 318	10 095 318	0	2 849 812	2 849 812	0	12 945 130	12 945 130
t9	0	10 830 061	10 830 061	0	2 849 812	2 849 812	0	13 679 873	13 679 873
t10	0	7 658 828	7 658 828	0	2 849 812	2 849 812	0	10 508 641	10 508 641
t11	0	5 262 698	5 262 698	0	2 849 812	2 849 812	0	8 112 510	8 112 510
t12	0	5 935 857	5 935 857	0	2 849 812	2 849 812	0	8 785 669	8 785 669
t13	0	6 700 002	6 700 002	0	2 849 812	2 849 812	0	9 549 814	9 549 814
t14	0	7 430 096	7 430 096	0	2 849 812	2 849 812	0	10 279 909	10 279 909
t15	0	8 085 984	8 085 984	0	2 849 812	2 849 812	0	10 935 796	10 935 796
SPOLU							0	144 361 184	144 361 184

Tabuľka 28 – CBA - kalkulácia čistej súčasnej hodnoty – variant 1 - komplexné prevádzkové náklady

Obdobie	Čisté prínosy						Čistá súčasná hodnota z projektu			
	Finančné prínosy			Ekonomické prínosy			koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návratnosť ENPV
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel				
t1	0	-17 700 000	-17 700 000	0	-13 139 092	-13 139 092	0	-17 700 000	-13 139 092	-13 139 092
t2	0	-17 700 000	-17 700 000	0	-11 618 790	-11 618 790	1	-16 857 143	-11 065 514	-24 204 606
t3	0	-5 262 813	-5 262 813	0	1 878 912	1 878 912	2	-4 773 526	1 704 228	-22 500 378
t4	0	-5 262 813	-5 262 813	0	2 946 122	2 946 122	3	-4 546 216	2 544 971	-19 955 407
t5	0	-5 262 813	-5 262 813	0	4 817 741	4 817 741	4	-4 329 729	3 963 568	-15 991 839
t6	0	-5 262 813	-5 262 813	0	5 995 334	5 995 334	5	-4 123 552	4 697 501	-11 294 338
t7	0	-5 262 813	-5 262 813	0	6 969 550	6 969 550	6	-3 927 192	5 200 786	-6 093 552
t8	0	-5 262 813	-5 262 813	0	7 682 317	7 682 317	7	-3 740 183	5 459 680	-633 873
t9	0	-5 262 813	-5 262 813	0	8 417 060	8 417 060	8	-3 562 079	5 696 998	5 063 125
t10	0	-5 262 813	-5 262 813	0	5 245 828	5 245 828	9	-3 392 456	3 381 507	8 444 633
t11	0	-5 262 813	-5 262 813	0	2 849 698	2 849 698	10	-3 230 911	1 749 467	10 194 100
t12	0	-5 262 813	-5 262 813	0	3 522 856	3 522 856	11	-3 077 058	2 059 741	12 253 841
t13	0	-5 262 813	-5 262 813	0	4 287 001	4 287 001	12	-2 930 531	2 387 163	14 641 003
t14	0	-5 262 813	-5 262 813	0	5 017 096	5 017 096	13	-2 790 982	2 660 673	17 301 676
t15	0	-5 262 813	-5 262 813	0	5 672 984	5 672 984	14	-2 658 078	2 865 242	20 166 919
SPOLU	0	-103 816 566	-103 816 566	0	40 544 618	40 544 618	SPOLU	-81 639 634	20 166 919	

Tabuľka 29 – CBA - kalkulácia čistej súčasnej hodnoty – variant 2 - znížené prevádzkové náklady

Obdobie	Finančné prínosy			Ekonomické prínosy			koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)	Kumulovaná diskont. návratnosť ENPV
	Alternat. 1	Alternat. 2	rozdiel	Alternat. 1	Alternat. 2	rozdiel				
t1	0	-17 700 000	-17 700 000	0	-13 139 092	-13 139 092	0	-17 700 000	-13 139 092	-13 139 092
t2	0	-17 700 000	-17 700 000	0	-11 618 790	-11 618 790	1	-16 857 143	-11 065 514	-24 204 606
t3	0	-1 708 800	-1 708 800	0	5 432 924	5 432 924	2	-1 549 932	4 927 823	-19 276 783
t4	0	-1 708 800	-1 708 800	0	6 500 135	6 500 135	3	-1 476 126	5 615 061	-13 661 723
t5	0	-1 708 800	-1 708 800	0	8 371 754	8 371 754	4	-1 405 834	6 887 463	-6 774 260
t6	0	-1 708 800	-1 708 800	0	9 549 347	9 549 347	5	-1 338 890	7 482 163	707 904
t7	0	-1 708 800	-1 708 800	0	10 523 563	10 523 563	6	-1 275 133	7 852 845	8 560 748
t8	0	-1 708 800	-1 708 800	0	11 236 330	11 236 330	7	-1 214 412	7 985 450	16 546 198
t9	0	-1 708 800	-1 708 800	0	11 971 073	11 971 073	8	-1 156 583	8 102 493	24 648 692
t10	0	-1 708 800	-1 708 800	0	8 799 841	8 799 841	9	-1 101 508	5 672 456	30 321 148
t11	0	-1 708 800	-1 708 800	0	6 403 710	6 403 710	10	-1 049 055	3 931 323	34 252 470
t12	0	-1 708 800	-1 708 800	0	7 076 869	7 076 869	11	-999 100	4 137 699	38 390 169
t13	0	-1 708 800	-1 708 800	0	7 841 014	7 841 014	12	-951 524	4 366 170	42 756 339
t14	0	-1 708 800	-1 708 800	0	8 571 109	8 571 109	13	-906 213	4 545 442	47 301 781
t15	0	-1 708 800	-1 708 800	0	9 226 996	9 226 996	14	-863 060	4 660 260	51 962 041
SPOLU	0	-57 614 400	-57 614 400	0	86 746 784	86 746 784	SPOLU	-49 844 512	51 962 041	

8 Plán implementácie

8.1 Metodika projektového riadenia

V tejto kapitole je popísaný jeden z možných variantov riadenia projektu. V prípade, ak zákazník nemá definovaný proces riadenia tohto projektu, môže zvoliť nasledovnú metodológiu ako celok prípadne použiť iba jej časti.

Popísaná metodika sa opiera o metodiku PRINCE 2, ktorá rozsahom svojho využívania vo svete predstavuje nepísaný štandard v danej oblasti. PRINCE alebo „PRojects IN Controlled Environments“ (projekty v riadenom prostredí) predstavuje procesne orientovanú metodiku riadenia projektov, ktorá obsahuje štruktúrovaný postup zahŕňajúci riadenie, kontrolu a organizáciu projektu. PRINCE2® je ochrannou známkou OGC (Office of Government Commerce), ktorý je súčasťou Britského ministerstva financií.

Metodika riadenia projektu, v zmysle princípov PRINCE2, je zostavená z troch základných prvkov:

- komponentov
- procesov
- techník

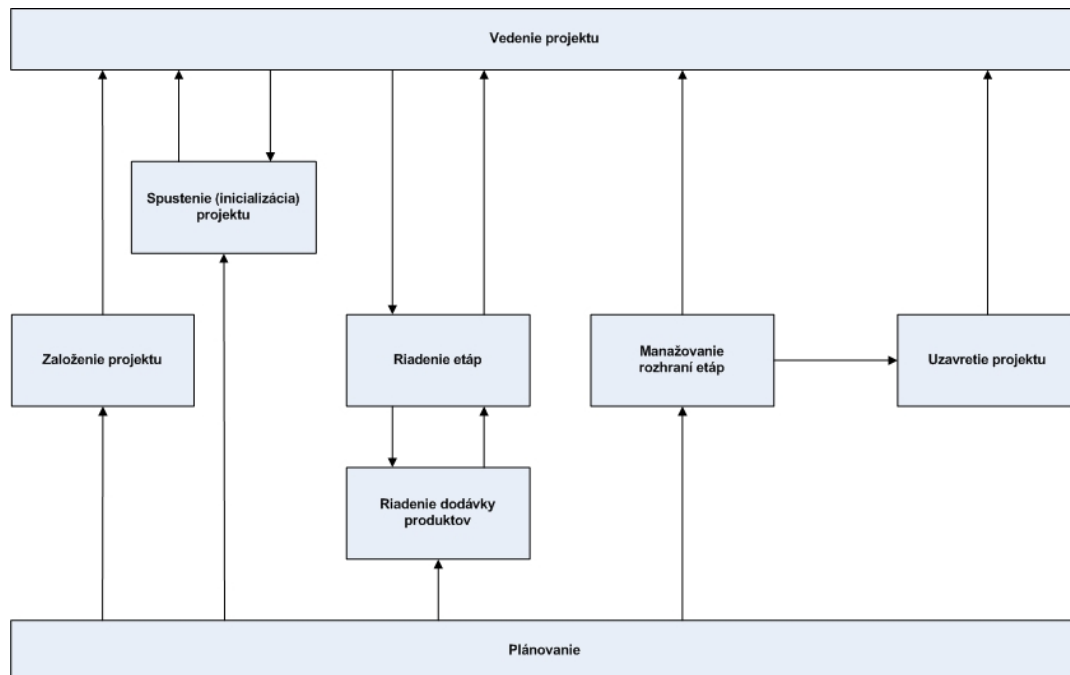
Prostredníctvom komponentov sú popísané a vysvetlené hlavné elementy projektového manažmentu a ich vzájomné prepojenie. Tieto komponenty predstavujú základné „stavebné kamene“ projektového manažmentu, vrátane manažmentu kvality a manažmentu rizík v prostredí projektu. Definované sú nasledovné komponenty:

- Organizácia
- Plánovanie
- Riadenie
- Etapy
- Manažment rizík
- Kvalita v prostredí riadenia projektu
- Konfiguračný manažment
- Riadenie zmien

Procesy predstavujú samotný procesný model metodiky, ktorý popisuje použitie jednotlivých komponentov metodiky s účelom dosiahnutia plánovaných projektových cieľov. Definovaných je 8 základných procesov:

- Otvorenie projektu
- Inicializácia projektu
- Riadenie etáp
- Manažovanie dodávky projektových výstupov
- Manažovanie rozhraní etáp
- Plánovanie
- Vedenie projektu
- Uzavretie projektu

Obrázok 25 – Základné procesy metodiky a ich vzťahy



Prostredníctvom techník sú popísané rôzne postupy, ktoré sú špecifické práve pre prostredie PRINCE:

- plánovanie na báze produktov
- prístup k riadeniu zmien
- postupy pre vyhodnotenie kvality
- vedenie dokumentácie

8.2 Projektová organizácia

Vytvorenie efektívnej projektovej organizačnej štruktúry je pre riadenie projektu jedným z rozhodujúcich faktorov jeho úspešnosti. Organizácia projektu predstavuje vytvorenie dočasných kontrolných, riadiacich a výkonných organizačných štruktúr potrebných pre zabezpečenie dodávky projektových výstupov. Všetky definované role, s výnimkou predsedov kolektívnych orgánov a pomocných rolí (napr. asistent), by mali byť súhlasne definované na strane odberateľa (objednávateľa) aj dodávateľa.

Objednávateľ je zodpovedný za zabezpečenie dohodnutých podmienok pre dodanie predmetu projektu. Oneskorenie alebo zanedbanie povinností zo strany objednávateľa, môže spôsobiť oneskorenie v harmonograme alebo neúspech realizácie zo strany dodávateľa za ktoré nemôže byť dodávateľ zodpovedný. Objednávateľ typicky:

- poskytuje informácie, údaje a rozhodnutia. Ak informácie nie sú dostupné a sú nevyhnutné pre projekt, zabezpečí ich vypracovanie v termíne podľa vzájomnej dohody.
- Zaručí splnenie dohodnutých požiadaviek a predpokladov pre realizáciu činností.
- Plánuje a koordinuje formálne pracovné stretnutia.
- Zabezpečuje prístup k osobám pre doplnkové informácie.
- Zabezpečuje vstupy pracovníkov dodávateľa na pracoviská objednávateľa, v zmysle interných predpisov objednávateľa.

Dodávateľ je zodpovedný za zabezpečenie splnenia predmetu projektu, na základe zmluvne dohodnutých podmienok. Dodávateľ typicky:

- Riadi prácu svojich subdodávateľov.
- Zodpovedá za plnenie predmetu projektu svojím subdodávateľom v takej miere ako keby ho plnil sám.
- Predkladá výstupy projektu na testovanie, pripomienkovanie a preberanie objednávateľovi.
- Plánuje a koordinuje pracovné stretnutia v spolupráci s objednávateľom.

Pre potreby zostavenia projektovej organizácie budú definované nasledovné organizačné štruktúry projektu:

- Riadiaci výbor - predstavuje kontrolné štruktúry vedenia projektu. Je tvorený predsedom a členmi riadiaceho výboru. Riadiaci výbor projektu je zodpovedný za celkové vedenie projektu a je nevyhnutné, aby v ňom mali zastúpenie všetky zainteresované skupiny.
- Manažment projektu - predstavuje riadiace štruktúry projektu. Je tvorený garantom projektu a projektovým manažérom.
- Realizačný tím - predstavuje výkonné štruktúry projektu. Pre zabezpečenie koordinácie a výkonu prác sú definované dedikované realizačné tímy za ucelené oblasti realizácie alebo špecifické odborné činnosti, ktoré sú reprezentované vedúcimi týchto tímov. Je potrebné aby vedúci jednotlivých realizačných tímov na strane odberateľa aj dodávateľa zodpovedali predmetne za rovnaké oblasti.
- Asistent projektového manažéra - vykonáva podporné činnosti v zmysle pokynov projektového manažéra.
- Manažér kvality - je zodpovedný za definovanie kvalitatívnych kritérií projektu. Sleduje dané kritériá počas priebehu celého projektu. V spolupráci s projektovým manažérom rieši odchýlky od stanovených kvalitatívnych kritérií.

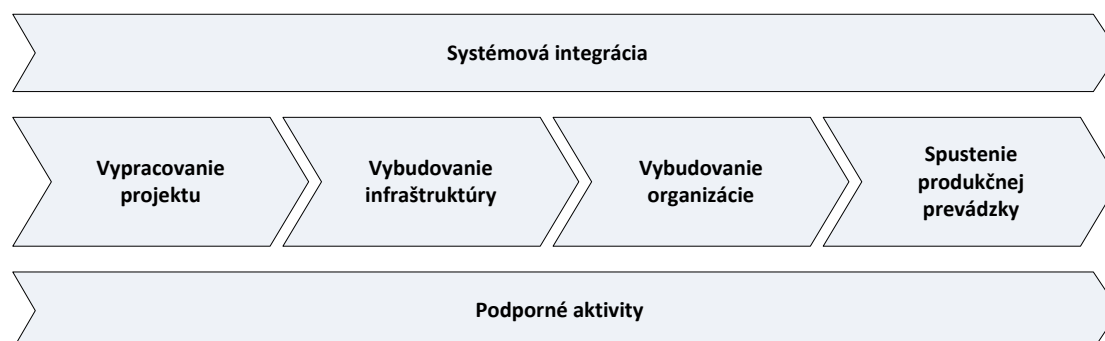
Všetky projektové role v rámci organizačnej štruktúry musia byť jasne a jednoznačne popísané, pričom ich povinnosti sa nesmú prekrývať. Každá rola musí mať presne definované úlohy, právomoci, zodpovednosti, zručnosti, vedomosti a skúsenosti, ako aj rozhranie s ostatnými rolami.

Charakteristickou črtou projektu je to, že ide o dočasné riadiace prostredie a potrebuje odlišnú organizačnú štruktúru ako je tomu pri líniovom riadení. Táto musí byť flexibilnejšia a vyžaduje širokú škálu vedomostí v relatívne krátkom čase. Na zaručenie úspechu projektu je nevyhnutné, aby bol dobre spropagovaný, uznaný a podporovaný v rámci príslušného líniového riadenia.

8.3 Aktivity a dodávky

Aktivity projektu sú rozdelené do piatich základných oblastí, ktoré adresujú primárne dodávky pri budovaní Dátového centra.

Obrázok 26 – Primárne projektové aktivity



8.3.1 Systémová integrácia

Za vedenie, obsahovú stránku a celkovú implementáciu projektu a jeho úspešné spustenie do prevádzky je zodpovedný Systémový integrátor, ktorý obsahovo riadi implementačné tímy a aktívne participuje na ich každodennej práci. Táto pravidelná aktivita vyžaduje podľa preukázateľných domácich a medzinárodných skúseností približne 10% z celkovej ceny projektu. Touto položkou sa teda nemyslí podporné projektové riadenie v zmysle Systému riadenia štrukturálnych fondov a Kohézneho fondu, ktoré spadá do podporných aktivít projektu a ktorého maximálna výška môže byť do 3% z hodnoty hlavných aktivít projektu. Systémový integrátor vykonáva funkcie, ktoré daný projekt sprevádzajú počas celého životného cyklu. Jeho úlohou je zabezpečiť aby sa z jednotlivých komponentov riešenia vytvoril funkčný, efektívny a komplexný systém, ktorý je vnútorne konzistentný a napĺňa požiadavky zákazníka. Systémová integrácia pokrýva strategickú, riadiacu a technickú časť. Medzi jej základné aktivity patrí najmä: návrh architektúry a celkovej koncepcie riešenia, identifikácia a riešenie závislostí, analýza a riadenie rizík, monitoring projektových aktivít po obsahovej stránke, posúdenie a koordinácia zmenových požiadaviek, integrácia a prepojenie jednotlivých častí riešenia, riešenie technických otázok a pod..

8.3.2 Vypracovanie projektu

Uvedená aktivita je rozdelená na štyri hlavné podaktivity:

- detailná analýza súčasného stavu v oblasti dátových centier a prevádzkovanvej IKT infraštruktúry verejnej správy. Zároveň bude nevyhnutné zozbierať všetky relevantné a uskutočniteľné požiadavky na IKT infraštruktúru a služby dátových centier z projektov PO1 OPIS.
- špecifikácia požiadaviek pre poskytovanie centrálnych služieb dátového centra pre elektronizáciu verejnej správy
- vypracovanie Rámcového projektu Dátového centra, ktorý predstavuje koncepciu riešenia a vysoko úrovňový návrh jednotlivých komponentov dátového centra. Súčasťou tejto aktivity je:
 - definícia princípov budovania dátových centier
 - návrh celkovej architektúry riešenia
 - definícia požiadaviek na stavebné úpravy
 - stanovenie priorít riešenia a postup implementácie
 - návrh celkovej architektúry manažment systémov
 - definícia základných prevádzkových potrieb a požiadaviek
 - definícia poskytovaných služieb
 - návrh stratégie v oblasti BCP a DRP

V rámci tejto aktivity bude pripravený plán realizácie riešenia s konkretizovanými etapami a časovým harmonogramom. V prípade viacerých alternatív riešenia prebehne v rámci stanovenia koncepcie posúdenie a výber optimálnych alternatív v jednotlivých častiach celkového riešenia.

- vypracovanie Detailného projektu Dátového centra, ktorý predstavuje detailný návrh pre vybudovanie rozloženého Dátového centra. Projekt musí adresovať všetky aspekty a oblasti Dátového centra od stavebného a fyzického členenia až po procesy a podporné manažment nástroje tak, aby Dátové centrum bolo schopné efektívne poskytovať definované služby v požadovanej kvalite.

8.3.3 Vybudovanie infraštruktúry

Aktivita vybudovania infraštruktúry nadväzuje na ukončenie aktivity „Vypracovanie projektu“. Aktivita adresuje tri primárne oblasti:

- prípravu lokality (stavebné a fyzické členenie, fyzická objektová bezpečnosť)
- technologickú infraštruktúru
- IKT infraštruktúru
- nástroje pre manažment technologickej infraštruktúry
- nástroje pre manažment IKT infraštruktúry

Pre oblasť technologickej a IKT infraštruktúry bude súčasťou aktivity:

- dodávka hardvéru
- dodávka nevyhnutného softvéru a licencií pre oživenie a otestovanie systémov
- inštalácia
- oživenie a základná konfigurácia
- testovanie

S nasadením IKT infraštruktúry úzko súvisia aj služby integrácie, ktoré zabezpečia vzájomnú prepojitelnosť jednotlivých komponentov ako aj komunikáciu celého riešenia s vonkajším svetom.

Oblasť testovania pokrýva oblasť prípravy a plánovanie testovania cez návrh plánu testov, stanovenie testovacej stratégie a prípravy testovacích prípadov. Samotné testovanie prebehne na úrovni integračných a akceptačných testov. Predpokladá sa niekoľko testovacích cyklov tak, aby bolo možné opätovne overiť odstránenie chýb z predchádzajúcich iterácií. Predpokladom pre zahájenie integračných a akceptačných testov je ukončenie interných testov dodávateľa, ktoré sú realizované v jeho vlastnej réžii.

8.3.4 Vybudovanie organizácie

Aktivita „Vybudovanie organizácie“ zastrešuje činnosti spojené so zavedením systému riadenia IT služieb podľa ISO 20000 a systému manažérskej informačnej bezpečnosti podľa ISO27001. Pre oba systémy riadenia prebehne:

- vypracovanie projektu
- zavedenie procesov a implementácia opatrení
- príprava na predcertifikačný audit
- certifikačný audit

Súčasťou zavedenia procesov bude implementácia podporných manažment nástrojov pre riadenie IT služieb a riadenie bezpečnosti, ktorá prebehne v súlade so štandardným cyklom:

- analýza a špecifikácia požiadaviek
- návrh riešenia
- implementácia riešenia
- testovanie
- nasadenie do produkcie

8.3.5 Spustenie produkčnej prevádzky

V rámci spustenia produkčnej prevádzky budú realizované činnosti smerujúce ku konfigurácii a nastavení všetkých komponentov riešenia tak, aby bolo Dátové centrum schopné poskytovať služby pre svojich odberateľov.

Dátové centrum bude prepojené do definovaných sietí verejnej správy, resp. samosprávy.

Po spustení do produkčnej prevádzky bude potrebné na určitý čas zabezpečiť zvýšenú úroveň podpory tak, aby bolo možné rýchlo reagovať na prípadné nedostatky a chyby, ktoré neboli odstránené počas testovacích iterácií.

Súčasťou spustenia produkčnej prevádzky sú školiace aktivity pre pracovníkov Dátového centra. Vyškolenie personálu je nutnou podmienkou pre úspešnú realizáciu a akceptáciu výsledkov projektu. Za neoprávnené sa považujú aktivity zamerané na školenie konečných používateľov služieb (občanov a podnikateľov). Fyzickému školeniu môže predchádzať aj kurz vo forme e-learning. Do tejto nákladovej položky patrí takisto príprava kompletnej sady školiacich materiálov a samotná organizácia a koordinácia týchto školení, prenájom školiacich priestorov a pod..

8.3.6 Podporné aktivity

Medzi podporné aktivity, ktoré definuje Systém riadenia štrukturálnych fondov a Kohézneho fondu patria aktivity formálneho a administratívneho charakteru, ktoré vyplývajú priamo z riadiacej dokumentácie pre čerpanie štrukturálnych fondov. Sú nimi riadenie dodávok, monitoring a finančné riadenie. Medzi podporné aktivity patria aj aktivity publicity a informovanosti, ktoré sú potrebné pre účely rozšírenia informácií o výhodách elektronického vybavovania služieb medzi verejnosťou a pre účely propagácie celého projektu.

8.4 Časový harmonogram implementácie

Odhad trvania projektu je 24 mesiacov od ukončenia verejného obstarávania. Navrhovaný rámcový implementačný plán projektu počíta s ukončením projektových aktivít do polovice roku 2014 a to za predpokladu ukončenia verejného obstarávania celého projektu do polovice roku 2012 nasledovaného „okamžitým“ zahájením implementačných aktivít.

Tabuľka 30 – Harmonogram implementácie

Aktivita projektu	2012				2013				2014			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Vypracovanie projektu												
Vybudovanie infraštruktúry DCI												
Príprava lokality DCI												
Rozšírenie technologickej infraštruktúry DCI												
Rozšírenie IKT infraštruktúry DCI												
Nasadenie manažment nástrojov DCI												
Vybudovanie infraštruktúry DCII												
Príprava lokality DCII												
Nasadenie technologickej infraštruktúry DCII												
Nasadenie IKT infraštruktúry DCII												
Nasadenie manažment nástrojov DCII												
Vybudovanie organizácie												
Vypracovanie projektu												
Zavedenie procesov												
Príprava na predcertifikačný audit												
Certifikačný audit												
Nasadenie podporných nástrojov												
Spustenie do prevádzky												

9 Riadenie rizík

9.1 Použitá metodika

Predmetom riadenia rizík je identifikácia možných ohrození (hrozieb) pri realizácii projektu „Centrálne služby dátového centra pre elektronizáciu verejnej správy“, určenie pravdepodobnosti ich výskytu a možných dopadov. Pre identifikované hrozby budú následne definované predbežné opatrenia, ktoré ohrozenia a ich dopad znížia alebo úplne eliminujú.

Analýza rizík neadresuje bezpečnostné riziká a riziká, ktoré sú relevantné pre prevádzku samotného Dátového centra, ako sú prírodné hrozby, hrozby vplyvom ľudskej činnosti, zlyhanie infraštruktúry a pod..

Pre potreby tejto štúdie bolo zvolená jednoduchá a intuitívna metodika, ktorá vychádza z 5 rôznych úrovní dopadu ohrozenia a 5 úrovni pravdepodobnosti, že ohrozenie nastane. Definícia dopadu a pravdepodobnosti je do istej miery voľná a zaradenie do jednotlivých úrovní je subjektívne na základe informácií dostupných autorskému tímu.

Tabuľka 31 – Ukazovatele dopadu ohrozenia

Úroveň	Charakteristika	Popis
1	Nevýznamný	Minimálne ohrozenie projektu, malé finančné straty, ciele nie sú ohrozené
2	Malý	Ohrozenie parciálnych cieľov projektu, stredné finančné straty, malý dopad na zákazníkov, zmena projektového plánu
3	Stredný	Niektoré parciálne ciele projektu nebudú dosiahnuté, vysoké finančné straty, významný dopad na zákazníkov, dobré meno mierne poškodené
4	Veľký	Niektoré základné ciele projektu nebudú dosiahnuté, veľké finančné straty, výrazné poškodenie dobrého mena
5	Katastrofálny	Základné ciele projektu nebudú dosiahnuté, enormné finančné straty, strata dobrého mena

Tabuľka 32 – Ukazovatele pravdepodobnosti vzniku ohrozenia

Úroveň	Charakteristika	Popis
1	Takmer isté	Očakáva sa, že nastane vo väčšine prípadov
2	Asi nastane	Vo väčšine prípadov pravdepodobne nastane
3	Možno nastane	Niekedy by azda mohlo nastať
4	Asi nenastane	Vo väčšine prípadov by nemalo nastať
5	Sotva nastane	Môže nastať iba za výnimočných okolností

Matica dopadov a pravdepodobnosti vzniku rizika definuje 4 úrovne rizika, ktoré následne určujú voľbu opatrení na jeho elimináciu, resp. zníženie.

- Extrémne riziko (E) - vyžaduje okamžitú nápravu
- Vysoké riziko (V) - treba dať do pozornosti vrcholovému manažmentu
- Stredné riziko (S) –je potrebné určiť konkrétnu zodpovednosť manažmentu
- Malé riziko (M) - riadi sa bežnými postupmi

Tabuľka 33 – Úrovně rizika

Pravdepodobnosť vzniku	Dopad					
		1 (nevýznamný)	2 (malý)	3 (stredný)	4 (veľký)	5 (katastrofálny)
	1 (takmer isté)	V	V	E	E	E
	2 (asi nastane)	S	V	V	E	E
	3 (možno nastane)	M	S	V	E	E
	4 (asi nenastane)	M	M	S	V	E
	5 (sotva nastane)	M	M	S	V	V

9.2 Analýza rizík

Ohrozenia projektu budovania Dátového centra je možné rozdeliť do 3 kategórií:

- Projektové
 - Oneskorenie počas obstarania
 - Nedodržanie cieľov, zdrojov a termínov projektu
 - Časová disharmonizácia s projektmi PO1 OPIS
 - Negatívny dopad na existujúce prostredie DataCentra
- Organizačné a procesné
 - Strata trvalej udržateľnosti
 - Nízka akceptácia DataCentra ako centrálného poskytovateľa služieb dátového centra
 - Nedostatočné skúsenosti a odborná úroveň personálu Dátového centra
- Technologické
 - Strata interoperability

9.2.1 Oneskorenie počas obstarania

Pravdepodobnosť: možno nastane

Dopad: veľký

Úroveň rizika: extrémne riziko

Popis: Doterajšie skúsenosti s obstarávaním komplexných projektov v oblasti IKT sa spájajú s výraznými oneskoreniami prípadne opakovanými vyhláseniami súťaže.

Opatrenia: Je potrebné sa detailne venovať príprave verejného obstarania a spolupracovať pri vypracovaní súťažných podkladov s Riadiacim orgánom OPIS. Niektoré časti riešenia je možné obstarávať aj separátne.

9.2.2 Nedodržanie cieľov, zdrojov a termínov projektu

Pravdepodobnosť: možno nastane

Dopad: veľký

Úroveň rizika: extrémne riziko

- Popis:* Vybudovanie Dátového centra je náročný a komplexný projekt, ktorý vyžaduje rigidné projektové riadenie a silnú, priebežnú koordináciu všetkých dodávateľov. V opačnom prípade hrozí nedodržanie cieľov, termínov a/alebo navýšenie rozpočtu.
- Opatrenia:* Využiť služby skúseného integrátora, ktorý zabezpečí kvalitu projektových dodávok.

9.2.3 Časová disharmonizácia s projektmi PO1 OPIS

- Pravdepodobnosť:* možno nastane
- Dopad:* veľký
- Úroveň rizika:* extrémne riziko
- Popis:* Projekt Dátového centra musí byť ukončený tak, aby ním poskytované služby boli reálne využiteľné v definovaných projektoch PO1 OPIS. V opačnom prípade budú musieť jednotlivé PO1 OPIS projekty riešiť IKT infraštruktúru individuálne čím im vzniknú dodatočné náklady a na strane Dátového centra dôjde k zásadnému ovplyvneniu predpokladanej návratnosti.
- Opatrenia:* Detailne analyzovať požiadavky projektov PO1 OPIS a vzájomne koordinovať projektové plány všetkých zúčastnených strán. V prípade konfliktov pripraviť náhradné (dočasné) scenáre.

9.2.4 Negatívny dopad na existujúce prostredie DataCentra

- Pravdepodobnosť:* možno nastane
- Dopad:* stredný
- Úroveň rizika:* vysoké riziko
- Popis:* Projekt budovania Dátového centra si vyžiada zásah do prostredia DataCentra vo všetkých oblastiach (organizačná, technologická, legislatívna, ...).
- Opatrenia:* Dôsledné dodržanie procesu riadenia zmien, vrátane dôkladnej analýzy dopadov a prípravy náhradných, resp. back-out scenárov. Vyhodnotenie každej zmeny z pohľadu dopadu na existujúce prostredie a priebežné zapracovanie nápravných opatrení.

9.2.5 Strata trvalej udržateľnosti

- Pravdepodobnosť:* možno nastane
- Dopad:* veľký
- Úroveň rizika:* extrémne riziko
- Popis:* Nedostatok prostriedkov na prevádzku systému bude ohrozovať trvalú udržateľnosť vybudovaného Dátového centra. Nedodržanie podmienok udržateľnosti OPIS by viedlo k vráteniu poskytnutého NFP.
- Opatrenia:* Navýšiť prostriedky na údržbu a prevádzku Dátového centra po skončení projektu. Potrebné náklady zahrnúť do prípravy rozpočtu MF SR v nasledujúcich obdobiach.

9.2.6 Nízka akceptácia DataCentra ako centrálneho poskytovateľa služieb dátového centra

<i>Pravdepodobnosť:</i>	možno nastane
<i>Dopad:</i>	veľký
<i>Úroveň rizika:</i>	vysoké riziko
<i>Popis:</i>	Dátové centrum ako poskytovateľ dátových služieb pre systémy zabezpečujúce eGovernment služby by mal byť verejnou správou akceptovaný ako dôveryhodný, stabilný a finančne efektívny partner. V opačnom prípade to môže vyvolať rezistenciu jednotlivých rezortov voči využívaniu služieb Dátového centra a snahu riešiť oblasť IKT infraštruktúry individuálne čím dôjde k celkovému zníženiu efektivity prevádzky IKT infraštruktúry vo verejnej správe.
<i>Opatrenia:</i>	Na strane DataCentra zabezpečiť a priebežne sledovať požadované parametre poskytovaných služieb. Na strane riadiacich orgánov OPIS vynútiť zohľadnenie existencie centrálneho poskytovateľa služieb dátového centra pri príprave a implementácii projektov.

9.2.7 Nedostatočné skúsenosti a odborná úroveň personálu Dátového centra

<i>Pravdepodobnosť:</i>	možno nastane
<i>Dopad:</i>	malý
<i>Úroveň rizika:</i>	stredné riziko
<i>Popis:</i>	Zníženie dostupnosti a kvality IKT infraštruktúry.
<i>Opatrenia:</i>	Poskytnúť potrebné školenie a tréning. Zabezpečiť priebežné vzdelávanie.

9.2.8 Strata interoperability

<i>Pravdepodobnosť:</i>	asi nenastane
<i>Dopad:</i>	stredný
<i>Úroveň rizika:</i>	stredné riziko
<i>Popis:</i>	Rozsah a efektivita využívania služieb Dátového centra závisí na technologickej interoperabilite.
<i>Opatrenia:</i>	V technickej a technologickej oblasti je nutné dôsledne vyžadovať dodržiavanie otvorených a neutrálnych štandardov.