MINISTERSTVO PRÁCE A SOCIÁLNÍCH VĚCÍ

Informační koncepce Ministerstva práce a sociálních věcí

Prosinec 2008

1. Identifikační údaje informační koncepce

Označení verze	verze 1.0 ze dne 19. 12. 2008		
Zpracovali:	Jan Jirsák Mgr. Karel Lux		
Schválil	ŘOI Ing. Roman Kučera	dne:	1. 1. 2009
Doba platnosti	do 31. 12. 2010		

Obsah:

2. Charakteristika informačních systémů veřejné správy

2.1. Model rozdělení informačních systémů MPSV

V rámci charakteristiky informačních systémů MPSV zavádíme dělení na ISVS a na podpůrné (provozní) IS.

- Informační systémy veřejné správy – jedná se o primární systémy MPSV určené k výkonu jeho pravomocí a obsahující citlivá data potřebná pro výkon státní správy v oblasti působnosti ministerstva.
- Podpůrné (provozní) informační systémy – jedná se o systémy podporující funkci ISVS a dále o interní systémy zabezpečující plynulý výkon agendy státní správy v působnosti MPSV. Do skupiny podpůrných systémů patří také systémy mající zejména provozní funkci (umožňující plynulý výkon práce MPSV bez zbytečných výpadků a rizik).

2.2. Informační systémy veřejné správy

2.2.1. IS hmotné nouze a sociálních služeb (IS HN a SS)

Charakteristika ISVS	Architektura je definována moduly: • bezpečnost - zahrnuje procesy a IT služby související s autentizací uživatelů, řízením přístupu k informacím a práci s osobními údaji, • klientská část IS HN, SS - je část infrastruktury a programového vybavení, která slouží představiteli Orgánu pro pomoc v hmotné nouzi ke komunikaci s centrální částí IS HN, • centrální část IS HN, SS - infrastruktura pro část APV IS HN, SS které je umístěna v datovém centru (resp. datových a komunikačních centrech) MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • archivace dokumentů - je vyčleněna jako samostatná část systému dovolující správu a uchování dokumentů, • integrační modul - modul pro spojení IS HN, SS s ostatními aplikacemi a systémy ISVS, • testovací prostředí - prostředí dedikované pro účely simulace chyb, ověření nových verzí apod., • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.

Předpokládané změny	Integrace se systémem OKcentrum
Přehled zpracovávaných dat	Osobní údaje – data související s výkonem vlastní agendy IS HN, SS Informace pro vnitřní potřebu – především statistické informace Informace určené pro zveřejnění – především statistické informace
Přehled zajišťovaných služeb	Výplata dávek o pomoci v hmotné nouzi v souladu se zákonem číslo 111/2006 Sb., o pomoci v hmotné nouzi, ve znění pozdějších předpisů. Služby vyplývající ze zákona 108/2006 Sb., o sociálních službách.
Použité technické a programové prostředky	Technologická architektura • Aplikace IS HN, SS jsou vybudovány ve vícevrstvé architektuře s centralizovanou datovou a aplikační vrstvou. • Na lokálních pracovních stanicích koncových uživatelů je instalována pouze prezentační vrstva. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno na centrální úrovni. • Pro uložení dat je použita databázová technologie Oracle. • Pro aplikační servery je použita technologie podporující specifikaci Enterprise JavaBeansTM 3.0. • Operační systém pro databázový server je UNIX. • Operační systém pro aplikační servery je LINUX. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace využívá bezpečné šifrované protokoly. Pro komunikaci mezi presentační vrstvou APV a aplikačním serverem je použito oboustranného protokolu SSL, při elektronickém podávání žádostí je použit jednostranný SSL protokol. SW architektura • IS HN, SS je budován a provozován ve vícevrstvé architektuře s tenkým bohatým klientem. • Vrstva relační databáze - SW, který zajišťuje služby ukládání a zacházení s daty. • Vrstva objektově relačního mapování • Střední vrstva – obsahuje sadu funkcí obchodní logiky aplikace a funkce pro komunikaci s jinými

	IS • Lehká aplikační vrstva - představuje vlastní logiku aplikace, tj. funkce pokrývající jednotlivé procesy aplikací. • Prezentační vrstva - uživatelské rozhraní, představuje nástroj na prohlížení dat a ovládání funkcí.
Vazby na ISVS	Informační systémy veřejné správy • MV - komunikace s registrem obyvatel • FÚ - získávání informací o příjmech z daňových přiznání • MO, MV, MS, IS ČSSZ a OSSZ - získávání informací o příjmech z dávek Důchodové pojištění a dávky nemocenského pojištění (péče) • Řešení duplicit (konflikty identifikačních údajů osob, duplicity žádostí, konflikty mezi doloženými údaji HN, SS aj.) Archivace písemností • Sledování pohybu písemností • Aplikace pro skenování písemností a kontrolu naskenovaných obrazů s těsnou vazbou na evidenci písemností a dopravu písemností • Komunikace s centrální spisovnou Elektronické formuláře • Zveřejnění formulářů a tiskopisů HN s použitím technologie presentace elektronických formulářů na portálu MPSV IS SSP • výše příjmu z dávek SSP • přiznání a výplata příspěvku na bydlení • informace o nezaopatřenosti • kontrola dat poskytnutých klienty za účelem ochrany proti neoprávněnému poskytování dávek IS SZ • informace z evidence uchazečů o zaměstnání (délka evidování uchazeče, spolupráce uchazeče při hledání zaměstnání aj.) • informace o výši příjmů z podpory v nezaměstnanosti, při rekvalifikaci a při insolventnosti zaměstnavatelů • kontrola dat poskytnutých klienty za účelem ochrany proti neoprávněnému poskytování dávek Infrastruktura veřejných klíčů

	Registr UIR ADR Síť WAN MPSV

2.2.2. IS státní sociální podpory (IS SSP)

Charakteristika ISVS	Architektura je definována moduly: • bezpečnost - zahrnuje procesy a IT služby související s autentizací uživatelů, řízením přístupu k informacím a práci s osobními údaji, • klientská část IS SSP - je část infrastruktury a programového vybavení, která poskytuje představiteli Orgánu podporu pro výplatu dávek státní sociální podpory a ke komunikaci s lokální částí IS SSP, • lokální část IS SSP - infrastruktura pro část APV IS SSP které je umístěna na úřadu práce, který je výkonným orgánem agendy SSP, • centrální část IS SSP - infrastruktura pro část APV IS SSP které je umístěna v datovém centru (resp. datových a komunikačních centrech) MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi lokální částí systému a uživateli a lokální částí systému s částí centrální, • archivace dokumentů - je vyčleněna jako samostatná část systému dovolující správu a uchování dokumentů, • integrační modul - modul pro spojení IS SSP s ostatními aplikacemi a systémy ISVS, • testovací prostředí - prostředí dedikované pro účely simulace chyb, ověření nových verzí a pod., • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Migrace systému do prostředí systému OKcentrum
Přehled zpracovávaných dat	Osobní údaje – data související s výkonem vlastní agendy IS SSP Informace pro vnitřní potřebu – především statistické informace Informace určené pro zveřejnění – především statistické informace
Přehled zajišťovaných služeb	Výplata dávek státní sociální podpory v souladu se zákonem číslo 117/2005 Sb., o státní sociální podpoře, ve znění pozdějších předpisů.
Použité technické a	Technologická architektura

programové prostředky	• Aplikace IS SSP jsou vybudovány v architektuře klient server s distribuovanou databázovou částí. • Na lokálních pracovních stanicích koncových uživatelů je instalováno aplikační programové vybavení, které zajišťuje spojení s lokálním databázovým serverem úřadu a zároveň zajišťuje kompletní aplikační logiku. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno nad databázovým serverem úřadu. • Pro uložení dat je použita databázová technologie Oracle. • Operační systém pro lokální databázové servery je MS Windows 2003 server. • Operační systém pro centrální databázový server je UNIX. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace využívá nativní protokoly Oracle. Ochrana dat je zajištěna na aplikační úrovni kryptografickými prostředky. Pro komunikaci mezi lokální a centrální částí systému je využívána elektronická pošta, jejímž prostřednictvím jsou vyměňovány importní / exportní soubory.
Vazby na ISVS	Informační systémy veřejné správy • MV - komunikace s registrem obyvatel • FÚ - získávání informací o příjmech z daňových přiznání • MO, MV, MS, IS ČSSZ a OSSZ - získávání informací o příjmech z dávek Důchodové pojištění a dávky nemocenského pojištění (péče) • Řešení duplicit (konflikty identifikačních údajů osob, duplicity žádostí, konflikty aj.) Archivace písemností • Sledování pohybu písemností • Aplikace pro skenování písemností a kontrolu naskenovaných obrazů s těsnou vazbou na evidenci písemností a dopravu písemností • Komunikace s centrální spisovnou Elektronické formuláře • Zveřejnění formulářů a tiskopisů SSP s použitím technologie presentace elektronických formulářů na portálu MPSV IS SZ

	• informace z evidence uchazečů o zaměstnání (délka evidování uchazeče, spolupráce uchazeče při hledání zaměstnání aj.) • informace o výši příjmů z podpory v nezaměstnanosti, při rekvalifikaci a při insolventnosti zaměstnavatelů • kontrola dat poskytnutých klienty za účelem ochrany proti neoprávněnému poskytování dávek Infrastruktura veřejných klíčů Registr UIR ADR Síť WAN MPSV

2.2.3. IS služeb zaměstnanosti (IS SZ)

Charakteristika ISVS	Architektura je definována moduly: • bezpečnost - zahrnuje procesy a IT služby související s autentizací uživatelů, řízením přístupu k informacím a práci s osobními údaji, • klientská část IS SZ - je část infrastruktury a programového vybavení, která poskytuje představiteli Orgánu podporu pro výplatu dávek v nezaměstnanosti, podporu k evidenci zaměstnavatelů a ke komunikaci s lokální částí IS SZ, • lokální část IS SZ - infrastruktura pro část APV IS SZ které je umístěna na úřadu práce, který je výkonným orgánem agendy SZ, • centrální část IS SZ - infrastruktura pro část APV IS SZ které je umístěna v datovém centru (resp. datových a komunikačních centrech) MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi lokální částí systému a uživateli a lokální částí systému s částí centrální, • archivace dokumentů - je vyčleněna jako samostatná část systému dovolující správu a uchování dokumentů, • integrační modul - modul pro spojení IS SZ s ostatními aplikacemi a systémy ISVS, • testovací prostředí - prostředí dedikované pro účely simulace chyb, ověření nových verzí a pod., • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Migrace systému do prostředí systému OKcentrum

Přehled zpracovávaných dat	Osobní údaje – data související s výkonem vlastní agendy IS SZ Informace pro vnitřní potřebu – především statistické informace Informace určené pro zveřejnění – především statistické informace
Přehled zajišťovaných služeb	Zajišťované služby jsou dány zákonem číslo 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů. Jedná se především o evidenci uchazečů o zaměstnání, evidenci zaměstnavatelů, výplaty podpory v nezaměstnanosti a další.
Použité technické a programové prostředky	Technologická architektura • Aplikace IS SZ jsou vybudovány v architektuře klient server s distribuovanou databázovou částí. • Na lokálních pracovních stanicích koncových uživatelů je instalováno aplikační programové vybavení, které zajišťuje spojení s lokálním databázovým serverem úřadu a zároveň zajišťuje kompletní aplikační logiku. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno nad databázovým serverem úřadu. • Pro uložení dat je použita databázová technologie Oracle. • Operační systém pro lokální databázové servery je MS Windows 2003 server. • Operační systém pro centrální databázový server je UNIX. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace využívá nativní protokoly Oracle. Ochrana dat je zajištěna na aplikační úrovni kryptografickými prostředky. Pro komunikaci mezi lokální a centrální částí systému je využívána elektronická pošta a přenos dat protokolem FTP, jejímž prostřednictvím jsou vyměňovány importní / exportní soubory.
Vazby na ISVS	Informační systémy veřejné správy • MV - komunikace s registrem obyvatel • FÚ - získávání informací o příjmech z daňových přiznání • MO, MV, MS, IS ČSSZ a OSSZ - získávání informací o příjmech z dávek Důchodové pojištění a dávky nemocenského pojištění (péče) • Řešení duplicit (konflikty identifikačních údajů

	osob, duplicity žádostí, konflikty aj.) Archivace písemností • Sledování pohybu písemností • Aplikace pro skenování písemností a kontrolu naskenovaných obrazů s těsnou vazbou na evidenci písemností a dopravu písemností • Komunikace s centrální spisovnou Elektronické formuláře • Zveřejnění formulářů a tiskopisů SZ s použitím technologie presentace elektronických formulářů na portálu MPSV IS SSP • výše příjmu z dávek SSP • přiznání a výplata příspěvku na bydlení • informace o nezaopatřenosti • kontrola dat poskytnutých klienty za účelem ochrany proti neoprávněnému poskytování dávek Infrastruktura veřejných klíčů Registr UIR ADR Elektronická spisová služby Síť WAN MPSV

2.3. Podpůrné (provozní) informační systémy

2.3.1. Územně identifikační registr adres (UIR-ADR)

Charakteristika	Architektura je definována moduly: • klientská část - je část infrastruktury a programového vybavení, která slouží ke komunikaci s centrální částí registru. Klienty registru jsou další systémy nebo koncoví uživatelé, • centrální část služby - infrastruktura pro část aplikačního vybavení, které je umístěno v datovém centru MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • integrační modul - modul pro spojení registru s ostatními aplikacemi a systémy ISVS, • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Operativní úprava dat registru spojená se vznikem a zánikem adres.

Přehled zpracovávaných dat	Informace určené pro zveřejnění
Přehled zajišťovaných služeb	Jedná se o podpůrný systém, který poskytuje autorizovaný registr adres ostatním systémům veřejné správy a široké veřejnosti.
Použité technické a programové prostředky	Technologická architektura • Aplikace registru je vybudována ve vícevrstvé architektuře s centralizovanou datovou a aplikační vrstvou. • Pro uložení dat je použita databázová technologie Oracle. • Pro aplikační servery je použita technologie Oracle Aplication server. • Operační systém pro databázový server je UNIX. • Operační systém pro aplikační servery je LINUX. • Komunikace využívá bezpečné šifrované protokoly na bázi SSL nebo nezabezpečené protokoly na bázi HTTP. SW architektura • Pro správu dat registru je použito technologie klient server. Na pracovní stanici je instalováno aplikační programové vybavení, které zajišťuje spojení s centrálním databázovým serverem a zároveň zajišťuje kompletní aplikační logiku. • Prezentační vrstva - uživatelské a systémové rozhraní, představuje nástroj na prohlížení a čtení dat registru.
Vazby na ISVS	Síť WAN MPSV

2.3.2. Síť WAN MPSV

Charakteristika	Síť WAN MPSV je tvořena čtyřmi částmi • WAN - (Wide Area Network) celorepubliková síť spojující úřady práce, krajské úřady, obce s rozšířenou působností a další úřady. Síť je neveřejná, tvořená prvky MPSV a je dedikována pro účely provozu aplikací MPSV. • SAN - (Storage Area Network) - síť pro ukládání dat. Specificky v MPSV se sítí SAN míní Fibre Optic spojení, optické přepínače a systémy pro ukládání dat (disková pole, páskové knihovny). • LAN - lokální komunikační sítě úřadů (vzhledem k síťové topologii LAN v MPSV může LAN například obsahovat jednu VLAN rozprostřenou mezi více lokalit). • KDC – (Komunikační Datové Centrum). Jedná se o část komunikační infrastruktury datového centra, v které jsou servery (případně další

	komponenty) připojené na páteřní přepínače DC. Dle návrhu jsou cílově k těmto přepínačům mj. připojovány servery hlavních aplikací. • KCW – (Komunikační Centrum WAN) Jedná se o část komunikační infrastruktury datového centra, v které jsou komponenty připojené k páteřním přepínačům WAN. Dle návrhu jsou zde servery pro infrastrukturní a komunikační aplikace (DNS, mail, antivirová ochrana, dohledové systémy atd.). Datová a komunikační centra se dále dělí na: • Produkční datové centrum obsahuje provozní systémy, za normální situace jsou zde provozovány všechny hlavní aplikace. Disponuje plnou konektivitou k uživatelům, operátorům a správcům. • Záložní datové centrum obsahuje záložní systémy a aktuální záložní kopii uživatelských a jiných provozních dat hlavních systémů. V případě plánovaných nebo neplánovaných výpadků je schopno převzít provoz kritických systémů. Přepnutí se v optimálním případě děje automaticky a pro jednotlivé systémy odděleně (tj. jeden systém může být provozován v produkčním centru, jiný v záložním). Centrum disponuje plnou konektivitou k uživatelům, operátorům a správcům. • Havarijní centrum obsahuje záložní kopii uživatelských a jiných provozních dat hlavních systémů. Dále v případě výpadku Produkčního a Záložního centra je v něm možné provozovat kritické aplikace v předem stanoveném omezeném režimu. Přepínání se děje pro všechny zde umístěné hlavní aplikace najednou, typicky za účasti operátorských zásahů.
Současný stav	Systém se nachází v provozním stavu.
Předpokládané změny	Úpravy vyvolané potřebami ostatních ISVS.
Přehled zpracovávaných dat	Přenos veškerých dat ostatních ISVS. Síť WAN nativně uzpůsobena pro přenos dat kategorií „Pro vnitřní potřebu“ a „Informace určené pro zveřejnění“. Při přenosu dat z kategorie „Osobní údaje“ nebo „Chráněné informace“ musí být k ochraně použito přídavných mechanismů (například kryptografické ochrany).
Přehled zajišťovaných služeb	Základní služby sítě (DNS, DHCP, WINS, NTP) Adresářové služby Poštovní služby Řízení bezpečnosti (IDS, Antivir)

	Monitorování a dohled stavu sítě a služeb Připojení k veřejné síti Internet a k meziresortní síti Govbone.
Použité technické a programové prostředky	Fyzická a linková vrstva je zajištěna prostředky poskytovatelů datových a komunikačních služeb a prostředky komunikační infrastruktury veřejné správy. Síťová vrstva je na úrovni WAN sítě zajištěna vlastními směrovači podporujícími technologie oddělení datového provozu na IP vrstvě (IP MPLS VPN). Na Úrovni SAN a LAN pak přepínači datového provozu, u IP sítě s podporou VLAN. Aplikační vrstva je zajištěna bezpečnostními systémy umožňujícími řízení a kontrolu datového provozu, systémy pro správu a dohled, systémy pro přenos elektronické pošty a dalšími.
Vazby na ISVS	nemá žádné vazby

2.3.3. Elektronická spisová služba

Charakteristika	Elektronická spisová služba ARSYS-X je centrálně provozovaná na Ministerstvu práce a sociálních věcí a je využívaná všemi úřady práce v ČR. Architektura je definována moduly: • bezpečnost - zahrnuje procesy a IT služby související s autentizací uživatelů, řízením přístupu k informacím, • klientská část - je část infrastruktury a programového vybavení, která slouží ke komunikaci s centrální částí spisové služby, • centrální část spisové služby - infrastruktura pro část aplikačního vybavení, které je umístěno v datovém centru MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • integrační modul - modul pro spojení spisové služby s ostatními aplikacemi a systémy ISVS, • testovací prostředí - prostředí dedikované pro účely simulace chyb, ověření nových verzí apod., • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Probíhá testování pilotní implementace systému na vybraných úřadech práce.
Předpokládané změny	Rozšíření systému na všechny úřady práce.
Přehled zpracovávaných dat	Informace pro vnitřní potřebu

Přehled zajišťovaných služeb	Rozsah zpracovávaných dat upravuje především zákon číslo 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů. Jedná se především o • elektronické písemnosti doručené nebo odeslané z úřadu práce, • elektronická evidence identifikačních údajů písemností v papírové podobě.
Použité technické a programové prostředky	Technologická architektura • Aplikace spisové služby je budována ve vícevrstvé architektuře s centralizovanou datovou a aplikační vrstvou. • Na lokálních pracovních stanicích koncových uživatelů je instalován pouze webový prohlížeč. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno na centrální úrovni. • Pro uložení dat je použita databázová technologie Oracle. • Operační systém pro databázový server je MS Windows 2003. • Operační systém pro aplikační servery je MS Windows 2003. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace využívá http protokol. SW architektura • Spisová služba je budován a provozován ve vícevrstvé architektuře • Vrstva relační databáze - SW, který zajišťuje služby ukládání a zacházení s daty. • Presentační a aplikační vrstva - představuje vlastní logiku aplikace, tj. funkce pokrývající jednotlivé procesy aplikací. Prezentační vrstva - uživatelské rozhraní, představuje nástroj na prohlížení dat a ovládání funkcí.
Vazby na ISVS	Infrastruktura veřejných klíčů Síť WAN MPSV

2.3.4. Elektronické formuláře

Charakteristika	Architektura je definována moduly: • klientská část - je část infrastruktury a programového vybavení, která slouží ke komunikaci s centrální částí systému. Klienty

	formulářů jsou koncoví uživatelé, především klienti agend vykonávaných systémy HN, SSP a SZ, • centrální část služby - infrastruktura pro část aplikačního vybavení, které je umístěno v datovém centru MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • integrační modul - modul pro spojení formulářů s ostatními aplikacemi a systémy ISVS, • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Úprava systému vyvolaná potřebami nového systému OKcentrum.
Přehled zpracovávaných dat	Informace určené pro zveřejnění – vzorové formuláře. Osobní údaje – v okamžiku vyplnění vzorového formuláře daty o klientovi.
Přehled zajišťovaných služeb	Publikace vzorových formulářů široké veřejnosti. Předání vyplněných formulářů dalším systémům ISVS.
Použité technické a programové prostředky	Technologická architektura • Aplikace formulářů je vybudována v prostředí Oracle Aplication server s centralizovanou datovou a aplikační vrstvou. • Pro uložení dat je použita databázová technologie Oracle. • Pro aplikační servery je použita technologie Oracle Aplication server. • Operační systém pro aplikační i databázový server je LINUX. • Komunikace využívá bezpečné šifrované protokoly na bázi SSL nebo nezabezpečené protokoly na bázi HTTP. SW architektura • Prezentační vrstva - uživatelské rozhraní, představuje nástroj na čtení a vyplnění formulářů.
Vazby na ISVS	Síť WAN MPSV

2.3.5. Kontrolní registr klientů (KRK)

Charakteristika	Architektura je definována moduly: • klientská část - je část infrastruktury a programového vybavení, která slouží ke

	komunikaci s centrální částí registru. Klienty registru jsou další systémy nebo koncoví uživatelé, • centrální část služby - infrastruktura pro část aplikačního vybavení, které je umístěno v datovém centru MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • integrační modul - modul pro spojení registru s ostatními aplikacemi a systémy ISVS, • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Integrace se systémem OKcentrum
Přehled zpracovávaných dat	Osobní údaje
Přehled zajišťovaných služeb	Jedná se o podpůrný systém, který poskytuje autorizovaný seznam a informace o klientech evidovaných v systémech veřejné správy, především HN, SSP a SZ.
Použité technické a programové prostředky	Technologická architektura • Aplikace registru je vybudována ve vícevrstvé architektuře s centralizovanou datovou a aplikační vrstvou. • Pro uložení dat je použita databázová technologie Oracle. • Pro aplikační servery je použita technologie Oracle Aplication server. • Operační systém pro databázový server je UNIX. • Operační systém pro aplikační servery je LINUX. • Komunikace využívá bezpečné šifrované protokoly na bázi SSL. SW architektura • Pro správu dat registru je použito technologie klient server. Na pracovní stanici je instalováno aplikační programové vybavení, které zajišťuje spojení s centrálním databázovým serverem a zároveň zajišťuje kompletní aplikační logiku.
Vazby na ISVS	Síť WAN MPSV

2.3.6. Infrastruktura veřejných klíčů PKI

Charakteristika	Kartové centrum V centru je vybudováno kartové centrum v podobě kořenové Certifikační Autority (MPSV CA root) a

	provozních Certifikačních autority (MPSV CA xxx) vydávajících osobní certifikáty na čipové karty v rámci celé organizace, certifikáty serverům a službám. Certifikáty jsou strukturovány tak, že umožňují použití ve standardních aplikacích, především pro autentizaci vůči vzdálenému stroji či aplikaci a šifrování či podepisování elektronické pošty. Neumožňují však autentizaci vůči pracovní stanici uživatele zařazené do Windows NT domény, ani vůči zdrojům integrovaným do takové domény (SmartCard Logon). Detašované registrační autority zajišťují sběr dat pro potřeby kartového centra na úřadech. Lokální CA V jednotlivých subjektech MPSV (například úřad práce) jsou realizovány provozní CA integrované v rámci lokálních Windows NT domén. Tyto CA jsou nezávislé na CA kartového centra. Vydávají osobní certifikáty strukturované tak, aby umožňovaly autentizaci vůči lokální doméně. Takto získaný certifikát uživatel je přidán na čipovou kartu uživatele získanou v kartovém centru. Další CA Někteří uživatelé používají certifikáty vydávané kvalifikovanými akreditovanými CA. Tyto certifikáty jsou požívány pro styk úřadu s klienty.
Současný stav	Systém se nachází v provozním stavu.
Předpokládané změny	Nejsou předpokládány žádné úpravy systému
Přehled zpracovávaných dat	Osobní údaje – informace nutné k vydání certifikátu kartovým centrem a dalšími CA. Informace pro vnitřní potřebu – informace nutné k vydání certifikátu lokální CA. Informace určené pro zveřejnění – seznamy certifikátů.
Přehled zajišťovaných služeb	Prostřednictvím detašovaných registračních autorit zajišťovat sběr žádostí o vydání certifikátu nebo čipové karty. V kartovém centru zajistit podpis žádosti nebo vydání čipové karty. Publikovat seznamy vydaných a odvolaných certifikátů.
Použité technické a programové prostředky	Technologická architektura • Na pracovních stanicích kartového centra je instalováno aplikační programové vybavení, které zajišťuje spojení s databázovým serverem autority a zároveň zajišťuje kompletní aplikační

	logiku. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno nad databázovým serverem. • Pro uložení dat je použita databázová technologie Oracle. • Operační systém pro databázové servery je MS Windows 2003 server. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace v rámci kartového centra využívá nativní protokoly Oracle. • Komunikace mezi detašovanou registrační autoritou a kartovým centrem využívá bezpečné šifrované protokoly.
Vazby na ISVS	KRK UIR ADR Síť WAN MPSV

2.3.7. Archivace písemností

Charakteristika	Architektura je definována moduly: • bezpečnost - zahrnuje procesy a IT služby související s autentizací uživatelů, řízením přístupu k informacím a práci s osobními údaji, • klientská část archivace - je část infrastruktury a programového vybavení, která slouží ke komunikaci s centrální částí IS archivace písemností, • centrální část - infrastruktura pro část aplikačního programového vybavení, které je umístěno v datovém centru (resp. datových a komunikačních centrech) MPSV, • komunikace - je míněna ta část infrastruktury, která poskytuje spojení mezi centrální částí systému a uživateli, • integrační modul - modul pro spojení IS archivace s ostatními aplikacemi a systémy ISVS, • správa, dohled a podpora - dohledování a podpora systému.
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	Integrace se systémem OKcentrum
Přehled zpracovávaných dat	Osobní údaje – údaje obsažené na archivovaných dokumentech. Informace pro vnitřní potřebu – evidenční informace
Přehled zajišťovaných	Uchování elektronického obrazu archivované

služeb	písemnosti. Vedení evidence archivovaných písemností. Zajištění vazby na fyzický archiv písemností.
Použité technické a programové prostředky	Technologická architektura • Aplikace archivace je vybudovány ve vícevrstvé architektuře s centralizovanou datovou a aplikační vrstvou. • Na lokálních pracovních stanicích koncových uživatelů je instalována pouze prezentační vrstva. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat je zajištěno na centrální úrovni. • Pro uložení dat je použita databázová technologie Oracle. • Pro aplikační servery je použita technologie podporující specifikaci Enterprise JavaBeansTM 3.0. • Operační systém pro databázový server je UNIX. • Operační systém pro aplikační servery je LINUX. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP. • Komunikace využívá bezpečné šifrované protokoly. Pro komunikaci mezi presentační vrstvou APV a aplikačním serverem je použito oboustranného protokolu SSL, při elektronickém podávání žádostí je použit jednostranný SSL protokol. SW architektura • IS archivace je budován a provozován ve vícevrstvé architektuře s tenkým bohatým klientem. • Vrstva relační databáze - SW, který zajišťuje služby ukládání a zacházení s daty. • Vrstva objektově relačního mapování • Střední vrstva – obsahuje sadu funkcí obchodní logiky aplikace a funkce pro komunikaci s jinými IS • Lehká aplikační vrstva - představuje vlastní logiku aplikace, tj. funkce pokrývající jednotlivé procesy aplikací. • Prezentační vrstva - uživatelské rozhraní, představuje nástroj na prohlížení dat a ovládání funkcí.
Vazby na ISVS	Infrastruktura veřejných klíčů Síť WAN MPSV

2.3.8. Manažerský informační systém (MIS)

Charakteristika	Řešení MIS je možné rozdělit do následujících funkčních bloků: • BI - Business Inteligence se zabývá analýzou a vizualizací multidimenzionálních dat poskytovaných datovým skladem (DWH). Systém je určen koncovému uživateli (analytikům) s dobrou znalostí struktury dat a jejich významů. • DWH - Systém datového skladu (DWH - Datawarehouse) je klíčovou komponentou řešící vlastní dlouhodobé uchování dat získaných ze zdrojových systémů částečně či úplně v historizované formě. Datawarehouse dále poskytuje zpracovaná data do podoby datových tržišť pro potřeby BI. V rámci datového skladu probíhají ETL procesy. • ETL - ETL (Extract, Transform, Load) je systém či logika řešení zabývající se čerpáním dat ze zdrojových systémů, zajištěním jejich uložení v historizované části datového skladu, jejich transformací do tzv. multidimenzionálních databází (datových tržišť) za účelem efektivního analyzování dat podle příslušných dimenzí. • Reportovací server - RS systém (Reporting Server) je součást celkového řešení zabývající se přípravou a zpřístupnění opakovaných, předem definovaných sestav (reportů) na základě dat poskytovaných datovým skladem. • Zdrojové systémy - zdrojové systémy jsou systémy, které nejsou přímou součástí řešení, ale jsou z nich získávána základní data pro další zpracování. Zpravidla se jedná o operativní, transakční systémy sloužící pro každodenní podporu činnosti organizace či systémy třetích stran. • Podpůrné systémy – správa uživatelů, správa výkazů, dohledy, zálohování, administrace
Současný stav	Systém se nachází v provozním stavu s dokončenou implementací všech částí.
Předpokládané změny	• Přidání dalších datových zdrojů (IS HN a SS, statistické údaje, apod.) • Vytvoření nových / úprava stávajících ukazatelů a hledisek v deskriptivní části Oracle BI • Vytvoření Nových a úprava stávajících analýz, reportů a řídících panelů v aplikaci Oracle BI • Implementace změny zdrojových aplikací

	• Vytvoření nového DM nebo úprava dimenzionálního modelu v datovém skladu ze stávajících dat v historizované databázi datového skladu
Přehled zpracovávaných dat	V MIS jsou v současné době k dispozici data ze dvou základních informačních systémů MPSV - státní sociální podpory (IS SSP) a služeb zaměstnanosti (IS SZ)
Přehled zajišťovaných služeb	• Podpora rozhodovacího procesu všech uživatelů z MPSV na okresní i celostátní úrovni díky poskytování komplexních informací z oblasti trhu práce a dalších datových zdrojů • Možnost zobrazení předdefinovaných i vytvoření ad-hoc analýz, statistik a reportů podle aktuálních požadavků uživatelů.
Použité technické a programové prostředky	Technologická architektura • Řešení MIS je založené na specifické HW/SW technologii HP Neoview, která zároveň slouží jako databázová technologie pro uložení dat. • Aplikační server a uživatelská funkcionalita je zajištěna nasazením SW produktu Oracle BI Enterprise Edition Plus. • Prezentační vrstvu tvoří server odpovědný za komunikaci s aplikačním BI serverem přes zabezpečený protokol https, navíc zajišťuje jednotný způsob autentikace uživatelů. • Uživatelské rozhraní je realizované pomocí aplikace Oracle BI EE a tenkým klientem (prohlížeč www stránek) na pracovních stanicích koncových uživatelů. • Na lokálních stanicích nejsou ukládána žádná data, zálohování dat datového skladu je zajištěno pomocí specializovaného zařízení VTS (Virtual Tape System), který je dodáván jako součást systému HP Neoview. • Operační systém pro databázový server je HP Neoview Operating System, pro aplikační server Microsoft Windows 2003, pro prezentační server RedHat Enterprise Linux. • Operační systém pro pracovní stanice je Microsoft Windows 2000/XP.
Vazby na ISVS	V současné době přebírá MIS data z následujících základních informačních systémů MPSV IS SSP • osobní údaje – data související s výkonem vlastní agendy IS SSP • informace o výplatě dávek státní sociální podpory

	• informace pro vnitřní potřebu – především statistické informace • informace určené pro zveřejnění – především statistické informace IS SZ • informace z evidence uchazečů o zaměstnání (délka evidování uchazeče, spolupráce uchazeče při hledání zaměstnání aj.) • informace o výši příjmů z podpory v nezaměstnanosti, při rekvalifikaci a při insolventnosti zaměstnavatelů • kontrola dat poskytnutých klienty za účelem ochrany proti neoprávněnému poskytování dávek Síť WAN MPSV – přístup do MIS pro uživatele

3. Záměry na pořízení nebo vytvoření nových ISVS

3.1. Nový informační systém OKcentrum

OKcentrum je pracovní název připravovaného informačního systému veřejné správy, který bude na centrální úrovni integrovat stávající IS SSP a IS SZ.

Zavedení systému je plánováno ve třech etapách.

- První etapa zahrnuje registr firem a moduly „Kontrola“ a „Monitoring firem“ IS služeb zaměstnanosti.
- Druhá etapa zahrnuje IS státní sociální podpory.
- Třetí etapa zahrnuje integraci zbývajících částí IS služeb zaměstnanosti.

Zprovoznění funkčnosti první etapy je plánováno na prvním pololetí roku 2009. V prvním čtvrtletí dojde k zahájení zkušebního provoz a školení uživatelů.

3.1.1. Přínos architektury

S rozvojem technologií a trendu vývoje dochází k posilování vlivu prezentační logiky na klientské straně. Tento princip v podobě bohatého klienta je využit rovněž v rámci připravovaného IS OKcentrum. Přenesení prezentační logiky na klientskou stranu má dopad v řadě efektů na zvýšenou spolehlivost, robustnost a efektivitu celého informačního systému.

Zvýšení robustnosti systému

Při využití principu tenkého klienta je prezentační logika řízena vzdáleným centrálním serverem, který udržuje kompletní aktuální rozpracovaný stav, obraz uživatelské aplikace na klientské stanici. Pokud tak dojde k technickým, hardwarovým či jiným problémům na konkrétním centrálním serveru, na kterém se nachází aktuální rozpracovaný stav klientské aplikace, dojde k havárii uživatelské aplikace. Aktivní prvek rozvažující zátěž systému (Load balancer) tak sice reflektuje zátěž systému jako celku, neumožňuje však z hlediska uživatele reagovat na výpadky konkrétního serveru.

Bohatý klient odstraňuje výše uvedenou nevýhodu. Veškerá prezentační logika (ovládání aplikace) je přítomna na klientské stanici a pouze v případě, kdy je požadavek na libovolnou operaci se zpracovávanými daty, dojde k vyvolání služby obchodní logiky. Ta se nachází v centrální části systému a z jejího hlediska jsou jednotlivé servery ekvivalentní, neboť neudržují aktuální rozpracovaný stav klientské aplikace, jsou bezstavové. Výpadek libovolného stroje je tak reflektován prvkem rozvažujícím zátěž a požadavek je přesměrován na jiný funkční server.

Současně je však zachována bezpečnost ve smyslu skryté centralizované obchodní logiky, která s daty pracuje.

Zrychlení odezvy a interakce s uživatelem

Přítomnost prezentační logiky na klientské stanici zrychluje interakci s uživatelem v řadě operací, kdy událost vyvolaná uživatelem není přenášena na vzdálený centrální server, ale je vyhodnocena přímo na stanici. Výsledná odezva systému z pohledu uživatele je tak rychlejší.

Snížený vliv síťových prvků a technologie na dobu nečinnosti

Díky bezstavovému charakteru centrální obchodní logiky a přesunutí prezentační vrstvy na klientskou pracovní stanici je minimalizován vliv síťových prvků (doba max. prodlevy otevřených spojení) a technologií na dobu nečinnosti uživatele v systému, která tak teoreticky není limitována (prakticky servisními hodinami na údržbu systému apod.).

Bezpečnost

Bezpečnostními prvky, jako je např. firewall, lze omezit přístup na centrální servery tak, že na ně lze přistupovat pouze z přesně definovaných míst.

Přítomnost konfiguračních údajů pro komunikaci s databázovým systémem na centrálních aplikačních serverech rovněž nepředstavuje riziko, neboť je lze zabezpečit využitím šifrovacích mechanismů.

3.1.2. Popis komunikační architektury IS OKcentrum

Hlavní část infrastruktury

IS OKcentrum předpokládá sérii z hlediska instalovaného systému ekvivalentních centrálních serverů, na kterých bude umístěna obchodní logika a instalace prezentační části aplikace. Tyto aplikační servery jako jediné komunikují s úložištěm dat, reprezentovaným databázovým systémem. Klientské stanice, prostřednictvím kterých uživatelé pracují se systémem, kontaktují centrální prvek rozvažující zátěž, jenž dle typu požadované služby a pravidel rozvažování zajišťuje směrování na odpovídající aplikační server a vybranou aplikační součást. V případě hlavní části aplikace se jedná o instalaci prezentační části aplikace na klientskou stanici prostřednictvím JNLP protokolu a technologie Java Webstart

Mezi databází IS OKcentrum a některými stávajícími databázemi je požadováno propojení formou databázových linků. Databáze budou využity ke dvěma účelům. Konverze dat a výměna dat s IS hmotné nouze a sociálních služeb. V případě konverze dat ze stávajících systémů tak postupně požadavek na tyto komunikace bude zanikat. Potřeba výměny dat s IS HN a SS prostřednictvím DB linku závisí na vývoji IS HN a SS nebo případných zákonných změnách, které by začlenily tento systém do IS OKcentrum.

Komunikace s externími subjekty

IS OKcentrum bude vyžadovat komunikaci s řadou externích systémů, od kterých bude přebírat data nebo naopak informace poskytovat. Kartové centrum bude předávat IS OKcentrum informace o vydaných a revokovaných certifikátech s využitím web služby, portál bude získávat informace, které budou publikovány, rovněž IS HN bude vyžadovat přímou online komunikaci pro specifické typy požadavků. Všechny tyto systémy budou komunikovat prostřednictvím aplikačních serverů a nepředpokládá se žádné přímé spojení takového systému s DB IS OKcentrum. Pro tento typ komunikace se nabízí využít vnitřní adresu prvku rozvažujícího zátěž.

Dalším typem externího systému, který bude vyžadovat komunikaci s IS OKcentrum, je ČSSZ prostřednictvím webservice. V neposlední řadě bude zapotřebí poskytovat služby veřejným externím systémům, jako je např. komunikace prostřednictvím XML technologie se spisovnou v rámci archivace dokumentů.

Pokud v budoucnu bude zapotřebí poskytovat data z IS OKcentrum dalšímu externímu subjektu, předpokládá se zpřístupnění formou např. technologie web service, tedy umístění speciální aplikace na centrální aplikační servery a zprovoznění nové komunikace, nikoliv zpřístupnění DB spojení přímo na DB IS OKcentrum.

3.1.3. Provozovaná prostředí IS OKcentrum

Z hlediska výsledného stavu provozu IS OKcentrum přichází v úvahu následující prostředí.

Produkční prostředí

Produkční prostředí je prostředí pro reálný provoz IS OKcentrum, pro práci cílových uživatelů. Jeho zprovoznění se předpokládá v první polovině roku 2009 k postupnému nasazování jednotlivých modulů IS OKcentrum.

Podpůrná prostředí

Jedná se o zkušební, školicí a testovací prostředí. Tato prostředí jsou vzájemně zcela oddělená a nezávislá, rovněž jsou oddělená od produkčního prostředí. To znamená, že jednotlivá prostředí budou mít vlastní databázové a aplikační servery.

Zkušební prostředí

Zkušební prostředí slouží všem uživatelům ke zkoušení postupů a seznamování se s novou funkčností. Ve zkušebním prostředí je umístěna shodná verze aplikace jako na prostředí produkčním, obsah databází je ovšem vymyšlený a uživatelé by při zkoušení neměli zadávat skutečné osobní údaje. Při nasazování nových verzí se bude databáze upgradovat stejně jako produkční databáze, uživatelé tedy nebudou ztrácet svá zkušební data. Zkušební prostředí bude navíc využito před uvedením do provozu produkčního prostředí pro seznámení uživatelů s aplikací a k ověření funkčnosti na úřadech. Zkušební prostředí je tedy první prostředí, kde by se měla aplikace IS OKcentrum zprovoznit. Předpokládaný termín zprovoznění je počátkem roku 2009.

Školicí prostředí

Pro účely školení cílových uživatelů systému je předpoklad vybudování školicího prostředí. Uživateli tohoto prostředí jsou zejména instruktoři a školenci. Při školení mohou školenci zkoušet funkčnost kromě školicí databáze i ve zkušebním prostředí. Obsah databází je opět vymyšlený a uživatelé by neměli zadávat skutečné osobní údaje. Při nasazování nových verzí se bude databáze upgradovat stejně jako produkční databáze, instruktoři tedy nebudou ztrácet připravená data pro školení. Zprovoznění tohoto prostředí spadá rovněž na počátek roku 2009, aby mohlo být zahájeno školení uživatelů IS OKcentrum.

Testovací prostředí

Testovací prostředí je určeno pro testování nově připravovaných verzí cílovými uživateli vybraných testovacích úřadů, případně pro testování nových technologií. Při instalaci nové verze k testování bude na testovacím prostředí instalována kopie produkční databáze a proveden upgrade této databáze. Testovací úřady budou tedy testovat nové verze na kopii reálné databáze z posledního období, což je velmi důležité a užitečné. Autentizace a autorizace zde bude samozřejmě stejná jako v reálné databázi, čímž bude zachována ochrana osobních údajů. Předpokládáme, že testovací prostředí bude navíc využito pro testování konverze dat z původních IS SZ a IS SSP.

Technické podmínky podpůrných prostředí

Všechna podpůrná prostředí předpokládají samostatnou oddělenou infrastrukturu, a to nejen vzájemně mezi sebou, ale i od produkčního prostředí. Jedná se však o zjednodušenou variantu, kde není zapotřebí ekvivalentního instalovaného výkonu jako v případě prostředí produkčního.

3.1.4. Programové vybavení

Předpokládané programové vybavení aplikačního a databázového serveru a klientských stanic vychází z ověřeného modelu IS HN a SS.

- Aplikační server - LINUX, Oracle WebLogic
- Databázový server - UNIX, Oracle
- Klientské stanice - Windows XP, Vista

3.1.5. Dostupnost IS OKcentrum

IS OKcentrum musí být dostupný minimálně v pracovní době úřadů, které jej budou používat. Předpokládá se stejná dostupnost jako u IS HN/SS.

Plánované odstávky

Tyto přestávky nebudou zasahovat do stanovené provozní doby. V provozním řádu, který bude pro OKcentrum vytvořen, bude definován čas, ve kterém se budou moci tyto přestávky uskutečnit.

Neplánované výpadky

IS OKcentrum bude v případě mimořádného výpadku uvedeno opět do provozu maximálně do 24 hodin. Zařazení do konkrétní třídy dostupnosti bude záviset na smluvních podmínkách.

Dohled a správa

Pro správu a dohled předpokládáme použít dedikovaná komunikační prostředí, realizovaná přes VLAN obdobně jako v IS HN.

Cílem správy je zajištění funkčnosti softwarového vybavení IS OKcentrum. Pro její dosažení budou na systémech IS OKcentrum prováděny následující činnosti:

- Instalace a konfigurace OS a technologického software,
- automatický monitoring OS a technologického software pomocí SNMP agentů,
- monitoring funkčnosti aplikace (servlety, OVIS),
- pravidelná kontrola a údržba,
- řešení problémů, hlášení na helpline MPSV a subdodavatelům.

Předpokládáme, že pro dohled a správu budou použity následující produkty:

- Interní nástroje pro sledování funkčnosti aplikace (servlety),
- monitoring systémů pomocí SNMP dotazů a SQL dotazů ze služebního serveru,
- OVO (HP OpenView Operations) – pro dohled na úrovni operačního systému,
- OVIS (HP OpenView Internet Services) – pro monitoring dostupnosti služeb,
- MRTG (Multi Router Traffic Grapher) – pro zaznamenávání historických výkonnostních dat pro jednotlivé systémy.

3.1.6. Zálohování

Předpokládáme, že systémy tvořící IS OKcentrum budou začleněny do již osvědčeného modelu centrálního zálohování, které se mj. používá pro IS HN. Pro řízení centrálního zálohování se používají servery v různých datových centrech. Tyto servery jsou vzájemně zastupitelné a pro přepínání provozu se používá nástroj Switch. Zálohovaná data se ukládají přes SAN.

Systém zálohování bude zajišťován produktem HP Open View Data Protector. Na systémech IS OKcentrum pak budou instalovány moduly Media Agent, Disk Agent a Online Oracle Integrace (v případě databázových serverů).

Předpokládáme, že aplikační servery budou souborově zálohovány jednou měsíčně (pravděpodobně bude stačit jeden v dané zóně). U databázového serveru bude pořizována plná záloha dvakrát týdně a záloha archivních logů pak dvakrát denně.

3.1.7. Bezpečnost

IS OKcentrum bude obsahovat osobní údaje. Z toho důvodu musí být kladen velký důraz na informační bezpečnost, která se týká neoprávněného použití osobních údajů, jejich ochrany při vzniku, přenosu, ukládání, používání a likvidaci. Zároveň musí být řešena ochrana dat před jejich modifikací, zavedením klamných dat do systému a ochrany systému jako celku. To vyžaduje komplexní ochranu hmotných i nehmotných částí IS.

Bezpečnost IS bude vycházet z bezpečnostní politiky provozovatele IS.

Součástí realizace bude zpracování bezpečnostního projektu, který bude bezpečnostní politiku provozovatele respektovat.

Nabízené řešení aplikačního vybavení bude implementovat níže uvedená bezpečnostní opatření s cílem ochrany informací proti nepovolanému přístupu, jejich modifikaci, zničení a změně a zabezpečení dostupnosti informací.

- Propracovaný systém řízeného přístupu k IS (identifikace, autentizace a autorizace uživatelů) využívající komplexní řešení PKI s využitím čipových karet uživatelů,
- využívání bezpečných šifrovaných komunikačních protokolů,
- zabezpečení dostupnosti informací a informačních služeb proti výpadkům informačního systému,
- propracovaný systém zálohování dat včetně clusterování datového serveru,
- implementace serverů do bezpečnostních zón IS centra MPSV,
- propracovaný systém obnovy IS po výpadku,
- použití spolehlivého SW s důrazem na kvalitu zvolených operační systémů, databázových serverů atd.,
- použití kvalitních technických komponent hardware IS včetně zajištění servisních služeb,
- informační podpora uživatelů subsystému (hot-line, školení),
- uchovávání údajů o přístupech do IS (žurnál) a jejich kontrola v reálném čase.

Důležité je zajištění fyzické ochrany jednotlivých technických částí IS (zabezpečení prostor, pro umístění IS, zvláště pak serverových částí, před přístupem neoprávněných osob, stabilizace elektrické energie a její dodávky, použití elektronické protipožární signalizace, klimatizace serveroven, bezpečné uložení nosičů dat aj.).

IS OKcentrum bude navržen tak, aby vyhovoval požadavkům na informační systémy veřejné správy (Standardu pro náležitosti životního cyklu informačního systému, požadavkům na bezpečnost informačních systémů), zákonu o ochraně osobních údajů a dalším příslušným zákonným normám.

4. Dlouhodobé cíle v oblasti řízení kvality ISVS

4.1. Stanovení dlouhodobých cílů řízení kvality ISVS

4.1.1. Zajištění kvality dat

ID	Popis dlouhodobého cíle
QL01	Definováním vhodné informační architektury zajistit poskytování spolehlivých a konzistentních informací a umožnit snadnou integraci aplikací do fungování MPSV (CobiT PO2).
QL02	Pořizováním a údržbou aplikačního programového vybavení získávat aplikace, které odpovídají požadavkům MPSV, jsou dostupné v požadovaném čase a za přijatelné náklady (CobiT IA2)

4.1.2. Zajištění kvality technických a programových prostředků

ID	Popis dlouhodobého cíle
QL03	Stanovením směru pro technický a programový rozvoj zajistit stabilní, cenově přijatelnou úroveň technologické infrastruktury MPSV, která bude vyhovovat stávajícím i budoucím požadavkům (CobiT PO3).
QL04	Pořizováním a údržbou technické infrastruktury zajistit fungování integrované a standardizované infrastruktury IT (CobiT IA3)

4.1.3. Zajištění kvality služeb

ID	Popis dlouhodobého cíle
QL05	Jasným definování procesů, organizace a vztahů uvnitř i vně útvaru IT zajistit pružnou reakci na požadavky, které bude MPSV klást na poskytování a rozvoj služeb IT, a určit role IT s jednoznačně definovanou odpovědností (CobiT PO4).
QL06	Řízením lidských zdrojů v útvaru IT získat kompetentní a motivované pracovníky, kteří vytváří a dodávají kvalitní služby IT (CobiT PO7)
QL07	Řízením kvality služeb IT zajistit trvalé a měřitelné zlepšování kvality dodávaných služeb IT (CobiT PO8)
QL08	Projektovým řízení zajistit dodání výstupů projektových činností v dohodnutém čase, nákladech a kvalitě (CobiT PO10)
QL09	Identifikováním vhodných řešení automatizace podporovat fungování procesů návrhem efektivních a účinných automatizovaných řešení (CobiT IA1)
QL10	Umožnit provozování a využívání služeb IT vhodnými postupy pro zaškolení koncových uživatelů a provozních pracovníků (CobiT IA4)
QL11	Provozovat služby IT v souladu s požadavky normy ČSN ISO/IEC 20000 – Informační technologie – Management služeb a doporučeními nejlepší vžité praxe (ITIL, CobiT, apod.).

4.2. Požadavky na kvalitu

ID	Popis požadavků na kvalitu	Vazba na dlouhodobé cíle kvality
QR01	Ustanovení systému řízení služeb IT, včetně politik a rámce, který umožní efektivní řízení a implementaci všech IT služeb (ISO/IEC 20000 3 a 4)	QL01, QL05, QL06, QL10
QR02	Zajištění náležité provozní dokumentace (systémová příručka, uživatelská příručka apod.) v souladu s Vyhláškou 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy)	QL11
QR03	Plánování a implementací nových nebo změněných služeb zajistit, aby nové služby a změny ve službách byly proveditelné a řiditelné při dohodnutých nákladech a kvalitě služeb (ISO/IEC 20000 5).	QL02, QL08, QL09
QR04	Pomocí řízení úrovně služeb stanovit, odsouhlasit, zaznamenávat a řídit úrovně služeb (ISO/IEC 20000 6.1).	QL07, QL11
QR05	Pomocí výkazů o službách vytvářet dohodnuté, aktuální, spolehlivé a přesné výkazy pro kvalifikované rozhodování a efektivní komunikaci (ISO/IEC 20000 6.2).	QL07, QL11
QR06	Pomocí řízení kapacit zajistit, aby poskytovatel služeb měl po celou dobu dostatečnou kapacitu ke splnění odsouhlasených současných i budoucích požadavků odrážejících potřeby MPSV a jejich odběratelů (ISO/IEC 20000 6.5).	QL03, QL11
QR07	Pomocí řízení vztahu s odběrateli služeb vybudovat a udržovat dobré vztahy mezi poskytovatelem služeb a odběrateli, založené na chápání potřeb odběratelů a hnacích sil jejich fungování (ISO/IEC 20000 7.2).	QL05, QL11
QR08	Pomocí řízení vztahů s dodavateli řídit dodavatele tak, aby bylo zajištěno poskytování nepřerušovaných, kvalitních služeb (ISO/IEC 20000 7.3).	QL05, QL11
QR09	Pomocí řízení incidentů co nejdříve obnovit dohodnuté služby pro MPSV nebo reagovat na požadavky na službu (ISO/IEC 20000 8.2).	QL07, QL11
QR10	Pomocí řízení problémů minimalizovat přerušení na straně MPSV pomocí proaktivní identifikace a analýzou příčin incidentů a řízením problémů až k jejich uzavření (ISO/IEC 20000 8.3).	QL07, QL11
QR11	Pomocí řízení konfigurace stanovovat a řídit jednotlivé prvky služeb a infrastruktury a udržovat přesné konfigurační informace (ISO/IEC 20000 9.1).	QL03, QL11
QR12	Pomocí řízení změn zajistit, aby všechny změny byly ohodnoceny, schváleny, implementovány a	QL03, QL11

	přezkoumány řízeným způsobem (ISO/IEC 20000 9.2).	
QR13	Pomocí řízení release dodat, distribuovat a sledovat jednu nebo více změn obsažených v jednom uvolnění do produkčního prostředí (ISO/IEC 20000 10.1).	QL03, QL11
QR14	Rozvoj a optimalizace technologické infrastruktury v souladu s potřebami a možnostmi MPSV zajistit efektivní využívání této infrastruktury a s přihlédnutím k technologickým trendům.	QL01, QL02, QL03, QL04
QR15	Prohlubování dostupnosti potřebných informací pomocí různých prostředků a kanálů a jejich efektivní využití (CobiT PO2-3, CobiT IA2-3).	QL01, QL02, QL03, QL04
QR16	Efektivní zajištění zpráv a informací, které jsou důležité při sledování provozu infrastruktury ICT a dovolují včas odhalit provozní odchylky a tím předcházet provozním výpadkům a problémů a poskytují údaje pro podporu správných rozhodnutí pro rozvoj infrastruktury ICT (CobiT PO2-3, CobiT IA2-3).	QL01, QL02, QL03, QL04

4.3. Plán řízení kvality

V oblasti řízení kvality ISVS budou prováděny konkrétní činnosti, které MPSV dále specifikuje a ohodnotí předpokládanou časovou náročností, která se promítne do návrhu harmonogramu plánu řízení kvality. Jednotlivé činnosti budou označeny vlastním identifikátorem (QPxx, kde xx je pořadí činnosti) a budou vloženy do třírozměrné matice, kde budou provázány s konkrétními požadavky na kvalitu ISVS a s konkrétními dlouhodobými cíli kvality ISVS.

Z pohledu informační koncepce se činnosti v oblasti kvality ISVS soustředí především na program rozvoje ICT a zavedení a využívání standardu ISO/IEC 20000:2005 v oboru managementu zlepšování kvality, zvyšování efektivity a snížení nákladů služeb ICT.

5. Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS

5.1. Stanovení dlouhodobých cílů řízení bezpečnosti ISVS

5.1.1. Zajištění bezpečnosti dat

ID	Popis dlouhodobého cíle
SL1	Bezpečnostní politikou určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení MPSV a v souladu s požadavky MPSV, příslušnými zákony a směrnicemi (ISO/IEC 27002 5.1).
SL2	Řízením bezpečnosti a minimalizací dopadů zranitelností a bezpečnostních incidentů udržovat integritu a důvěrnost informací (CobiT DS5)
SL3	Ustavit, zavést, provozovat, monitorovat, přezkoumávat, udržovat a soustavně zlepšovat dokumentovaný systém řízení bezpečnosti informací MPSV, a to v kontextu všech činností a rizik (ISO/IEC 27001 4.1)
SL4	Stanovením zásad a požadavků na řízení přístupu řídit přístup k informacím (ISO/IEC 11.1).

5.1.2. Zajištění bezpečnosti technických a programových prostředků

ID	Popis dlouhodobého cíle
SL5	Stanovením provozních postupů a odpovědností zajistit správný a bezpečný provoz prostředků pro zpracování informací (ISO/IEC 27002 10.1).
SL6	Stanovením bezpečnostní požadavků informačních systémů zajistit, aby se bezpečnost stala neoddělitelnou součástí informačních systémů (ISO/IEC 27002 12.1).

5.1.3. Zajištění bezpečnosti služeb

ID	Popis dlouhodobého cíle
SL7	Pomocí ohodnocení a řízení rizik IT analyzovat a komunikovat rizika a jejich možné dopady na cíle a fungování MPSV resp. na poskytování služeb IT (CobiT PO9, BS 31100, ISO/IEC 27005).
SL8	V rámci všech činností spojených se službami efektivně řídit bezpečnost informací (ISO/IEC 20000 6.6).
SL9	Pomocí řízení kontinuity a dostupnosti služeb zajistit, že jsou vůči zákazníkům za všech okolností splněny dohodnuté závazky v oblasti kontinuity a dostupnosti služeb (ISO/IEC 20000 6.3) a že jsou minimalizovány případné dopady při přerušení dodávky služeb IT (CobiT DS4)

5.2. Požadavky na bezpečnost

ID	Popis požadavků na bezpečnost	Vazba na dlouhodobé cíle bezpečnosti
SR01	Zajištění náležité bezpečnostní dokumentace (bezpečnostní politika, bezpečnostní směrnice apod.) v souladu s Vyhláškou 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy)	SL1
SR02	Řídit bezpečnost informací v organizaci (ISO/IEC 27002 6.1).	SL1, SL3
SR03	Zachovat bezpečnost informací organizace a prostředků pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty (ISO/IEC 27002 6.2).	SL5, SL4
SR04	Pomocí řízení informačních aktiv nastavit a udržovat přiměřenou ochranu aktiv MPSV (ISO/IEC 27002 7.1).	SL7, SL4
SR05	Pomocí klasifikace informací zajistit, aby informace získaly odpovídající úroveň ochrany (ISO/IEC 27002 7.2)	SL4
SR06	Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace (ISO/IEC 27002 8.1).	SL1, SL3, SL5
SR07	Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spojených, svých odpovědností a povinností a aby byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby (ISO/IEC 27002 8.2).	SL1, SL2
SR08	Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem (ISO/IEC 27002 8.3).	SL1, SL4
SR09	Předcházet neautorizovanému fyzickému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace (ISO/IEC 27002 9.1).	SL1, SL3, SL4
SR10	Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace (ISO/IEC 27002 9.2).	SL1, SL3, SL4
SR11	Řízením dodávek služeb třetích stran zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávání služeb ve shodě s uzavřenými dohodami (ISO/IEC 27002 10.2).	SL2
SR12	Plánováním a přejímáním systémů minimalizovat riziko selhání systémů (ISO/IEC 27002 10.3).	SL8
SR13	Ochranou proti škodlivým programům a mobilním	SL5, SL6, SL8

	kódům chránit integritu programového vybavení a dat (ISO/IEC 27002 10.4).	
SR14	Zálohováním udržovat integritu a dostupnost informací a prostředků pro jejich zpracování (ISO/IEC 27002 10.5).	SL5, SL6, SL8
SR15	Správou bezpečnosti sítě zajistit ochranu informací v počítačových sítích a ochranu podpůrné infrastruktury (ISO/IEC 27002 10.6).	SL5, SL6, SL8
SR16	Bezpečností při zacházení s médii předcházet neoprávněnému vyzrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činností organizace (ISO/IEC 27002 10.7).	SL5, SL6, SL8
SR17	Vhodnými postupy při výměně informací zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty (ISO/IEC 27002 10.8).	SL5, SL6, SL8
SR18	Zajistit integritu veřejně dostupných informací (webů) a bezpečnost služeb elektronického obchodu a jejich bezpečné použití (ISO/IEC 27002 10.9).	SL2, SL5, SL6, SL8
SR19	Monitorováním detekovat neoprávněné zpracování informací (ISO/IEC 27002 10.10).	SL2, SL5, SL6, SL8
SR20	Řízením přístupu uživatelů zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům (ISO/IEC 27002 11.2).	SL4, SL1, SL8
SR21	Stanovením odpovědnosti uživatelů předcházet neoprávněnému uživatelskému přístupu, vyzrazení nebo krádeži informací a prostředků pro zpracování informací (ISO/IEC 27002 11.3).	SL4, SL1, SL2, SL3
SR22	Řízením přístupu k síti předcházet neautorizovanému přístupu k síťovým službám (ISO/IEC 27002 11.4)	SL4, SL1, SL2, SL8
SR23	Řízení přístupu k operačnímu systému předcházet neautorizovanému přístupu k operačním systémům (ISO/IEC 27002 11.5).	SL4, SL1, SL2, SL8
SR24	Řízením přístupu k aplikacím a informacím předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech (ISO/IEC 27002 11.6).	SL4, SL1, SL2, SL8
SR25	Zajistit bezpečnost informací při použití mobilní výpočetní techniky a zařízení pro práci na dálku (ISO/IEC 27002 11.7).	SL4, SL1, SL2, SL8
SR26	Správným zpracování v aplikacích předcházet chybám, ztrátě, neoprávněné modifikaci nebo zneužití informací v aplikacích (ISO/IEC 27002 12.2).	SL6, SL5
SR27	Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků (ISO/IEC 27002 12.3).	SL2, SL8
SR28	Zajistit bezpečnost systémových souborů (ISO/IEC 27002 12.4)	SL5, SL6

SR29	Bezpečností procesů vývoje a podpory udržovat bezpečnost programového vybavení a informací aplikačních systémů (ISO/IEC 27002 12.5).	SL5, SL6
SR30	Řízením technických zranitelností snížit rizika vyplývající z využívání zveřejněných technických zranitelností (ISO/IEC 27002 12.6).	SL5, SL6, SL2
SR31	Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě (ISO/IEC 13.1).	SL1, SL2, SL3, SL8, SL9
SR32	Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů a provedení kroků k nápravě (ISO/IEC 27002 13.2)	SL2, SL3, SL5, SL8
SR33	Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit včasnou obnovu činností (ISO/IEC 27002 14.1)	SL9
SR34	Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků (ISO/IEC 27002 15.1)	SL1, SL3, SL7
SR35	Zajistit shodu systémů s bezpečnostními politikami organizace a normami (ISO/IEC 27002 15.2).	SL1, SL3, SL7
SR36	Maximalizovat účinnost auditu a minimalizovat zásahy do/z informačních systémů (ISO/IEC 27002 15.3).	SL2, SL3
SR37	Ustavit, zavést, provozovat, monitorovat, přezkoumávat, udržovat a soustavně zlepšovat dokumentovaný systém řízení kontinuity činností služeb IT (BS 25999, BS27999)	SL9

5.3. Plán řízení bezpečnosti

V oblasti řízení bezpečnosti ISVS budou prováděny konkrétní činnosti, které MPSV dále specifikuje a ohodnotí předpokládanou časovou náročností, která se promítne do návrhu harmonogramu plánu řízení bezpečnosti ISVS. Jednotlivé činnosti budou označeny vlastním identifikátorem (SPxx, kde xx je pořadí činnosti) a budou vloženy do třírozměrné matice, kde budou provázány s konkrétními požadavky na bezpečnost ISVS a s konkrétními dlouhodobými cíli bezpečnosti ISVS.

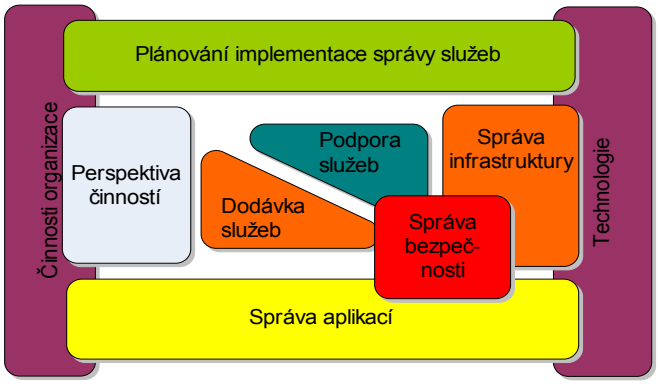
Z pohledu informační koncepce se činnosti v oblasti bezpečnosti ISVS soustředí především na program rozvoje ICT a zavedení a využívání standardu třídy ISO/IEC 27000 v oboru řízení bezpečnosti ICT.

6. Soubor základních pravidel pro správu ISVS

6.1. Zásady pořizování a vytváření ISVS

6.1.1. Zásady a postupy pro definování potřeby ISVS

Při návrhu procesu zařazování nového systému do prostředí MPSV vycházíme z doporučení ITIL, jehož rámcový model je uveden na následujícím obrázku.



Moduly lze stručně charakterizovat následujícím způsobem:

- Dodávka služeb pokrývá procesy potřebné pro plánování a dodávku kvalitních služeb IT a zaměřuje se na procesy s delším časovým dopadem, spojené se zlepšováním kvality dodávaných služeb IT.
- Podpora služeb popisuje procesy spojené s každodenními aktivitami podpory a údržby spojenými s poskytováním služeb IT.
- Správa infrastruktury pokrývá všechny aspekty ICT Infrastructure managementu od identifikace požadavků přes nabídkový proces k testování, instalaci, rozšíření a k následným operacím a optimalizaci komponent ICT a služeb IT.
- Plánování implementace správy služeb se zaměřuje na problémy a úkoly související s plánováním a zaváděním a zlepšováním procesů Správy služeb v organizaci. Zaměřuje se rovněž na problémy související s kulturními a organizačními změnami, s rozvojem vize a strategie a s nejvhodnějšími metodami přístupu. Například vytvoření předloženého metodického dokumentu spadá do této oblasti.
- Správa aplikací popisuje, jak spravovat aplikace od výchozí potřeby služeb přes všechny fáze životního cyklu aplikace až po vyřazení. Zejména klade důraz na to, aby projekty a strategie IT byly v těsném souladu s projekty a strategiemi činností organizace v celém životním cyklu aplikace, a tím aby bylo zajištěno, že činnosti jsou ICT podporovány nejefektivnějším způsobem.
- Perspektiva činností (u komerčních organizací perspektiva businessu) poskytuje personálu IT radu a návod pro porozumění, jak mohou přispět k cílům činností a jak jejich role a služby mohou být lépe přizpůsobeny a využity pro maximalizování jejich příspěvku.

- Správa bezpečnosti popisuje proces plánování a správy definované úrovně bezpečnosti informací a služeb IT, počítaje v to všechny aspekty související s reakcí na bezpečnostní incidenty. Zahrnuje rovněž analýzu a správu rizik a zranitelností a implementaci nákladově zdůvodněných protiopatření.

6.1.2. Zásady a postupy pro analýzu výchozího a cílového stavu

Analýza výchozího stavu nového informačního systému je definována v rámci systémového projektu nebo studie proveditelnosti. Analýza musí obsahovat základní informace, mezi které patří

- přesný popis zadání,
- manažerský popis,
- určení uživatelů,
- požadavky personálního obsazení,
- varianty řešení, pokud existují,
- harmonogram,
- záruční a pozáruční servis a provoz po předání do běžného provozu.

6.1.3. Zásady a postupy pro stanovení kvalitativních požadavků

Kvalitativní požadavky nových systémů jsou definovány v rámci bezpečnostní politiky systému a dále během procesu definice dostupnosti. Pro účely definice dostupnosti systému (služby) je vytvořeno rozdělení podle požadavků na dostupnost do tříd na základě požadavků na dobu uvedení do provozu a maximální akceptovatelnou ztrátu dat.

Údaje v následujícím rozdělení mají charakter maximálních hodnot:

<table>
<tr><td colspan="2" rowspan="2">Třídy dostupnosti</td><td colspan="4">Doba uvedení do provozu (RTO)</td></tr>
<tr><td>< 4 hod</td><td>< 1 den</td><td>< 1 týden</td><td>> 1 týden</td></tr>
<tr><td rowspan="3">Ztráta dat (RPO)</td><td>< 4 hod</td><td>A</td><td rowspan="2">B</td><td></td><td></td></tr>
<tr><td>< 1 den</td><td></td><td rowspan="2">C</td><td></td></tr>
<tr><td>> 1 den</td><td></td><td></td><td>D</td></tr>
</table>

RTO - maximální doba uvedení systému do provozu po výpadku.

RPO - maximální akceptovatelná ztráta dat. Při klasifikaci je nutno zvážit, zda aplikace obsahuje primární data, nebo zda jsou data součástí jiné aplikace.

Zařazení systému do třídy dostupnosti podle uvedeného rozdělení je provedeno přiřazením písmena, které vyjadřuje požadovanou dostupnost resp. požadavky na zotavení po neplánovaném výpadku.

Při klasifikaci lze vycházet z následujícího rámcového dělení podle účelu aplikace:

- Třída A - Kritické služby s nejvyšší požadovanou dostupností. Jedná se zejména o služby, které MPSV poskytuje klientům prostřednictvím elektronických kanálů.
- Třída B - Hlavní služby, pro které není nutná nepřetržitá dostupnost.
- Třída C - Ostatní služby, zejména interní služby, které nejsou bezprostředně třeba pro vykonávání zákonné činnosti MPSV.

- Třída D - Pomocné služby, u kterých je akceptovatelný i delší výpadek, resp. MPSV je ochotno nést riziko delšího výpadku.

6.1.4. Zásady a postupy pro stanovení požadavků na bezpečnost

Bezpečnostní požadavky jsou definovány v rámci bezpečnostní politiky. Bezpečnostní politika definuje zásady a pravidla řízení bezpečnosti informací, které jsou v systému zpracovávány. Bezpečnostní informací se rozumí zajištění dostupnosti, důvěrnosti a integrity informací v průběhu celého životního cyklu, počínaje vznikem informace, její změnou a konče skartací.

Bezpečnostní politika musí být zpracována dle standardů BS ISO/IEC 17799:2005 nebo ISO/IEC 27001. Součástí bezpečnostní politiky musí být také

- stanovení parametrů kvality služby (SLA),
- klasifikace a značení informací,
- použité bezpečnostní mechanismy.

Vlastní dokument „Bezpečnostní politika“ bude v souladu s příkazem ministra klasifikace a značení informací zařazen do kategorie „Chráněné informace“.

6.1.5. Zásady a postupy pro analýzu možných důsledků a dopadů

Důsledky a dopady nového systému jsou zkoumány v analýze rizik. Analýzou rizik se rozumí proces, ve kterém jsou zjišťována aktiva, hrozby působící na aktiva, zranitelná místa a pravděpodobnost zneužití hrozbou, včetně odhadu rizik způsobených hrozbou. Výsledky analýzy rizik budou zohledněny v bezpečnostní politice.

Analýza rizik musí být zpracována dle standardů ČSN ISO/IEC TR 13335 a musí obsahovat

- identifikaci a ohodnocení aktiv,
- identifikaci a ohodnocení hrozeb,
- odhad zranitelnosti aktiva ve vazbě na hrozby,
- stanovení mezní míry zranitelnosti.

Vlastní dokument „Analýza rizik“ bude v souladu s příkazem ministra klasifikace a značení informací zařazen do kategorie „Chráněné informace“.

6.1.6. Zásady a postupy projektového řízení

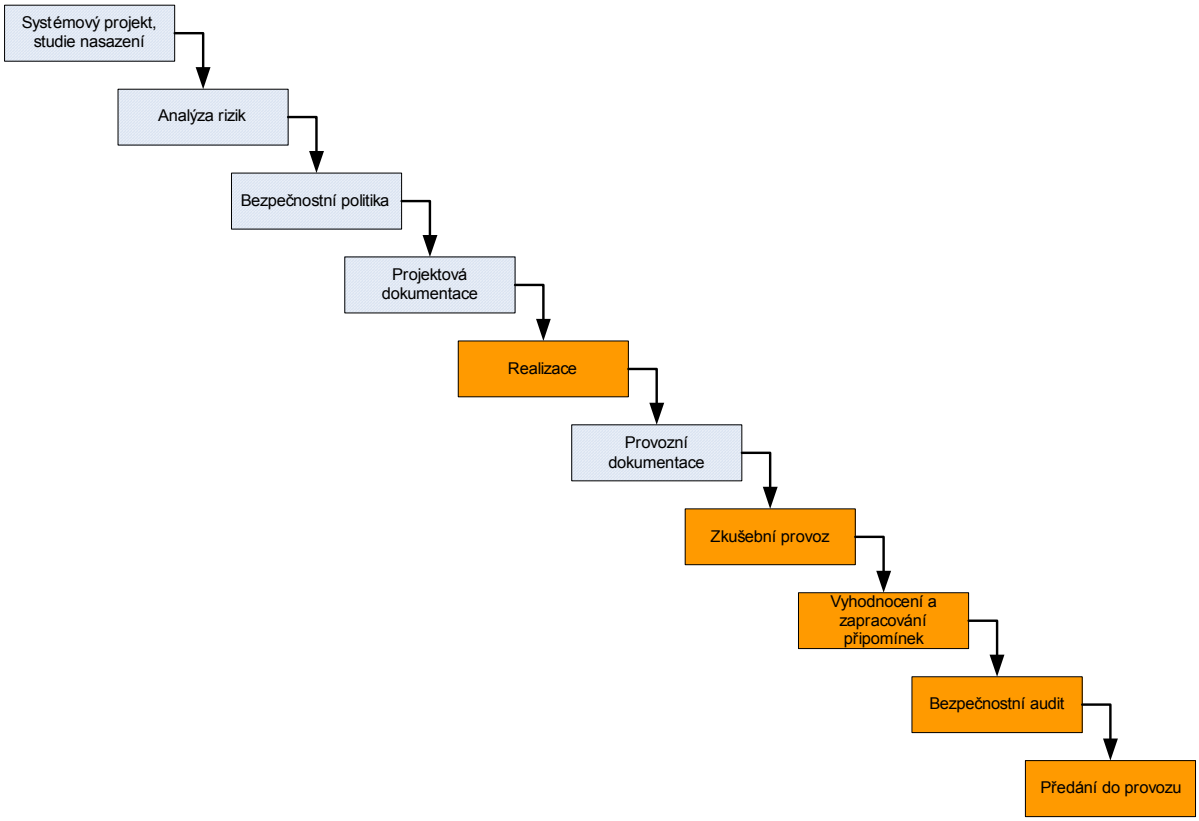
Součástí projektového řízení je dokumentace systému. Rozsah a struktura předávané dokumentace je uvedena v dalších odstavcích. Podle typu projektu může být rozsah dokumentace upraven.

- Systémový projekt, studie nasazení
  - Základní popis
  - Kdo bude uživatelem služby nebo systému
  - Personální obsazení
  - Varianty řešení
- Analýza rizik provedená dle standardů ČSN ISO/IEC TR 13335
  - Identifikace a ohodnocení aktiv
  - Identifikace a ohodnocení hrozeb
  - Odhad zranitelnosti aktiva ve vazbě na hrozby

- Stanovení mezní míry zranitelnosti

- Bezpečností politika dle standardů BS ISO/IEC 17799:2005, nově ISO/IEC 27001
  - SLA
  - Klasifikace a značení zpracovávaných informací (musí být v souladu s příkazem ministra č.27/2007, klasifikace a značení informací)
- Projektová dokumentace
  - Soupis použitého HW, SW, licence
  - Komunikační požadavky
  - Síťové služby
  - Dohled funkčnosti
  - Požadavky na zdroje (napájení, chlazení, umístění)
- Provozní dokumentace + pracovní postupy
  - PP pro dohledové centrum
  - PP pro obsluhu ze strany MPSV
  - Kontaktní informace
  - Evidenční list aplikace, systémy, serveru, atd.

Typický postup projektového řízení prochází kroky znázorněnými v obrázku.



Šedou barvou a šrafováním jsou označeny kroky, jejichž výstupem je dokumentace. Oranžovou barvou jsou označeny kroky, jejichž výstupem je provedení činnosti:

- Realizace může být zahájena teprve v okamžiku schválení systémové, bezpečnostní a projektové dokumentace. Samotný proces realizace postupuje podle kroků definovaných v projektové dokumentaci.
- Zkušební provoz slouží k ověření funkčnosti aplikace nebo systému, proškolení obsluhy a uživatelů a k ověření veškerých pracovních postupů. V průběhu zkušebního provozu budou shromážděny připomínky. Délka zkušebního provozu bude stanovena v rozmezí dvou až čtyř týdnů v závislosti na složitosti. V průběhu zkušebního provozu musí být vyškoleni uživatelé, obsluha i zaměstnanci dohledového centra.
- Vyhodnocení a zapracování připomínek. Zadavatel společně s dodavatelem vyhodnotí vzniklé připomínky a dohodnou se na způsobu vypořádání, včetně časových a finančních nároků.
- Bezpečnostní audit bude zaměřen na klíčové body systémové, bezpečností, projektové a provozní dokumentace. Zároveň bude posouzen vliv nové aplikace nebo systému na prostředí informačního systému MPSV.
- Předání do provozu. Proces zavedení nového systému do prostředí IS MPSV bude ukončen potvrzením akceptačních protokolů.

6.1.7. Zásady a postupy při pořizování ISVS pomocí dodavatele nebo interními zdroji

Veškeré služby z oblasti informačních a komunikačních technologií dodávané třetí stranou (speciální aplikace, outsourcing, servis a podobně) musí být ještě v době přípravy konzultovány s odborem informatiky. S finální podobou dodávané služby musí souhlasit vedoucí zaměstnanec odboru informatiky.

Ve smlouvě o dodávce aplikace vytvořené na zakázku musí být řešena i otázka přístupu ke zdrojovým kódům takovéto aplikace.

Ostatní oblasti pořizování systému dodavatelem se řídí pravidly definovanými v předešlých odstavcích.

6.2. Zásady provozování ISVS včetně řízení změn a rozvoje

6.2.1. Zásady a postupy pro zajištění provozu ISVS

Provoz informačních systémů je zajištěn s ohledem na jejich dostupnost, důvěrnost a integritu. Naplnění základních zásad je realizováno prostředky dokumentace systému, klasifikace informací a přiřazení rolí v systému.

Klasifikace informací umožňuje zpracovávané informace rozdělit do kategorií a následně s nimi nakládat rozdílnými způsoby. V prostředí MPSV jsou informace na základě příkazu ministra „Klasifikace a značení informací“ rozděleny a následně označeny kategoriemi

- osobní údaje,
- chráněné informace,
- informace pro vnitřní potřebu,
- informace určené pro zveřejnění.

Z hlediska správy a řízení informačního systému jsou definovány role a jim přiřazeny příslušné odpovědnosti.

- Provozovatel, vlastník systému – vytváří podmínky pro provoz informačního systému a definuje pravidla, za kterých je možno poskytovat informace uchovávané v informačním systému.
- Vlastník dat, informací – je vedoucí / řídící zaměstnanec organizační jednotky, která je zodpovědná za jejich tvorbu a která by byla nejvíce ovlivněna jejich ztrátou.
- Správce systému – je odpovědný za funkčnost a provoz systému. Správce dále provádí práce spojené s provozem systému a zajišťuje sledování vlastností systému.
- Uživatel – přistupuje k informacím a službám prostředky informačního systému.

Dokumentace systému je s ohledem na obsah dělena do částí, přičemž každá část dokumentace náleží jiné roli uživatele.

- Bezpečnostní dokumentace – je určena provozovatelům systému a vlastníkům informací.
- Systémová příručka – je určena správci systému.
- Uživatelská příručka – je určena uživateli systému.

6.2.2. Zásady a postupy pro řízení změn ISVS

Proces řízení změn ISVS v prostředí ministerstva práce je zajištěn a kontrolován mechanismy centrálního Help Desk systému. Vzhledem k rozsahu a odlišným požadavkům systémů jsou pro každý ISVS definovány samostatné procedury.

Na obecné rovině lze implementovaný proces řízení změn popsat následujícími klíčovými milníky.

- Požadavek na změnu zaznamenává do Help Desk systému koncový uživatel systému. Součástí požadavku na změnu je podrobný popis požadované změny.
- Schválení změny je zajištěno koordinátorem ISVS, který zhodnotí veškeré dostupné informace. V případě potřeby si vyžádá další informace a sám nebo na základě konzultací rozhodne o změně.
- Plánování a realizace změny. V případě schválení změny je naplánována a zajištěna realizace u správce nebo dodavatele systému.
- Testování a zavedení změny. Dle rozsahu a charakteristiky změny je zajištěno nejprve testování a následné uvolnění změny do provozu.
- Zhodnocení případně odstranění změny. Po ukončení fáze implementace je opětovně koordinátorem ISVS zhodnocen dopad změny na systém. V případě negativních dopadů je zavedená změna odstraněna.
- Dokumentace změny. Po ukončení všech fází změnového řízení je aktualizována dokumentace systému nebo dotčené části systému.

6.2.3. Zásady a postupy pro ukončení činnosti ISVS

V případě požadavku na ukončení činnosti ISVS je kladen velký důraz na zachování důvěrnosti zpracovávaných dat i v době po ukončení činnosti systému a na jeho případné opětovné zprovoznění. Proces ukončení činnosti je možné popsat v následujících sedmi krocích.

- V souvislosti s ukončením činnosti systému je nutné vyvolat změnového řízení v systémech, které mají vazby na systém, jehož činnost má být ukončena.
- Veškerá data systému, včetně provozních a bezpečnostních logů musí být archivována po dobu jednoho roku od ukončení činnosti systému nebo dle požadavků zákona, na jehož základě byl systém provozován.
- Bezpečnostní, systémová i uživatelská dokumentace musí být archivována po dobu jednoho roku od ukončení činnosti systému nebo dle požadavků zákona, na jehož základě byl systém provozován.
- Zdrojové kódy aplikací, instalační média a jiné související softwarové vybavení systému musí být archivováno po dobu jednoho roku od ukončení činnosti systému nebo dle požadavků zákona, na jehož základě byl systém provozován.
- Nosiče informací systému (paměťové i listinné) musí být bezpečně skartovány nebo vymazány. Vymazání informací je nutné i u paměťových médií, které budou opětovně užity v jiných systémech.
- Hardwarové vybavený systému musí být dle možností přednostně použito k jiným účelům. V případě, že jej z důvodu zastaralosti nelze použít, je možné provést fyzickou likvidaci.
- Všichni uživatelé systému, a to v jakýchkoli rolích, musí být seznámeni s povinnostmi vyplývajícími z jejich funkčního zařazení v systému, jehož činnost má být ukončena.

7. Způsob financování záměrů ISVS

V této kapitole je popsán způsob financování informačních systémů MPSV, které jsou blíže popsány v této informační koncepci. Náplň této kapitoly je vymezena vyhláškou č. 529/2006 SB. §2 odst. 1 písm. f), přičemž musí respektovat i další související předpisy, jako např. zákon č. 365/2000 Sb. §5 odst. 2 písm. b) a zák. č. 137/2006 Sb., o veřejných zakázkách.

Způsoby financování záměrů ISVS obsažených v této Informační koncepci jsou v rámci MPSV zajišťovány z rozpočtu MPSV či různých fondů, které má MPSV možnost využít v dané problematice.

Způsoby financování záměrů ISVS jsou rozděleny do třech oblastí, které jsou blíže popsány v následujících podkapitolách.

7.1. Způsob financování záměrů na pořízení nebo vytvoření nových ISVS

Seznam předpokládaných požadavků na pořízení či vytvoření nových ISVS je uveden v kapitole 3 této informační koncepce, kde jsou blíže specifikovány i finanční nároky.

Financování záměrů na pořízení nebo vytvoření nových ISVS bude provedeno z následujících finančních zdrojů:

- vlastní rozpočet MPSV
- dotační programy
- ISPROFIN
- fondy EU.

Oproti jiným aktivitám, které vyplývají z této informační koncepce, vyžaduje zpravidla pořízení nebo vytvoření nových ISVS důkladné plánování a nedílnou součástí plánování musí být i přesná specifikace finančních nákladů a jejich pokrytí v průběhu realizace záměru.

7.2. Způsob financování naplnění dlouhodobých cílů

Naplňování dlouhodobých cílů je prvořadým smyslem této koncepce a proto způsob jejich financování je nutné správně připravit.

Dlouhodobé cíle specifikované v této informační koncepci MPSV, ať už zaměřené na kvalitu či bezpečnost ISVS, jsou úzce provázány s konkrétním souborem požadavků. Definované požadavky na kvalitu jsou pak definovány v rámci kapitoly 4.2 a definované požadavky na bezpečnost jsou definované v rámci kapitoly 5.2. Nicméně jak dlouhodobé cíle, tak i definované požadavky nelze optimálně ohodnotit, a proto v rámci této informační koncepce jsou definovány i jednotlivé činnosti, které jsou svázány s jednotlivými požadavky a jednotlivými dlouhodobými cíli. Jednotlivé činnosti vyžadují konkrétní finanční zdroje a tedy i vytvoření příslušného plánu jejich alokace a čerpání.

7.3. Způsob financování správy ISVS

MPSV, jako vlastník ISVS, zajišťuje financování správy ISVS ze zdrojů, které zahrnují provoz, údržbu a rozvoj samostatných ISVS. Tyto finanční zdroje jsou plánovány pro konkrétní období, zpravidla čtyřletá, a konkrétní činnosti (v návaznosti na plnění dlouhodobých cílů). Plány investic, ať už z pohledu provozu či dalšího rozvoje ISVS v oblasti kvality a bezpečnosti ISVS jsou zpřesňovány a jsou předmětem veřejné soutěže, které jsou vypisovány na čtyřleté období.

8. Postupy při vyhodnocování dodržování informační koncepce

Vyhodnocení a případná aktualizace informační koncepce je prováděno pravidelně jednou za dva roky. V rámci samotných systémů jsou kontroly rozděleny na část administrativní, technickou a finanční.

Administrativní kontrola

Činnosti spojené s administrativní kontrolou provádí zaměstnanci oddělení koncepce informatiky a archivu. Součástí kontrol je dohled nad dodržováním organizačních postupů informační koncepce stanovených pro

- dlouhodobé cíle v oblasti řízení kvality,
- dlouhodobé cíle v oblasti bezpečnosti,
- zásady pořizování a vytváření systémů.

V rámci vlastní informační koncepce je kontrola zaměřena na

- aktuálnost z hlediska postupů provádění změn,
- aktuálnost z hlediska spravovaných ISVS, včetně vazeb na další systémy.

Technická kontrola

Kontrola technických parametrů systémů a pravidel řízení bezpečnosti je v rámci odboru informatiky zajištěna bezpečnostním správcem. Při vlastních kontrolách je kladen důraz na

- zásady provozování systémů,
- kvalita systémů dosahuje požadovaných parametrů,
- stav bezpečnosti odpovídá zásadám stanoveným pro systém,
- provozní správa odpovídá dokumentaci.

Finanční kontrola

Součástí kontrol informační koncepce je i kontrola dodržování způsobu financování informačních systémů. V rámci ministerstva práce jsou finanční kontroly zajištěny nezávislým oddělením interního auditu a kontroly.

9. Funkční zařazení útvaru pro řízení činností informační koncepce

9.1. Odpovědnosti za realizaci informační koncepce

V rámci MPSV byla vrcholná odpovědnost za realizaci informační koncepce stanovena na útvar **Odbor informatiky MPSV**.

Dílčí odpovědnosti za jednotlivé oblasti informační koncepce jsou uvedeny v následující tabulce:

Oblast	Dílčí odpovědnost
Vytváření záměrů na pořízení nebo vytvoření nových IS	Ředitel odboru informatiky
Schvalování záměrů na pořízení nebo vytvoření nových IS	Ředitel odboru financování a majetku
Řízení kvality ISVS (stanovování dlouhodobých cílů kvality a konkrétních požadavků na kvalitu IS, sestavení a údržba plánu řízení kvality, vyhodnocování naplnění požadavků a dodržování plánu)	Vedoucí oddělení koncepce informatiky a archivu
Řízení bezpečnosti ISVS (stanovování dlouhodobých cílů bezpečnosti a konkrétních požadavků na bezpečnost IS, sestavení a údržba plánu řízení bezpečnosti, vyhodnocování naplnění požadavků a dodržování plánu)	Bezpečnostní administrátor
Koordinace činností v oblasti rozvoje ISVS, příprava plánu rozvoje ISVS	Vedoucí oddělení koncepce informatiky a archivu
Schvalování plánu rozvoje ISVS	Ředitel odboru financování a majetku
Řízení postupů při pořizování a vytváření ISVS (včetně zajištění veřejných zakázek apod.)	Ředitel odboru informatiky
Vyhodnocování dodržování souladu provozování ISVS (soulad provozní dokumentace s IK a PD s vyhláškou, soulad skutečných procesů s provozní dokumentací)	Vedoucí oddělení koncepce informatiky a archivu
Koordinace a vyhodnocování řízení změn	Vedoucí oddělení koncepce informatiky a archivu
Řízení ukončování provozu IS	Ředitel odboru informatiky
Vytváření a údržba plánu financování ISVS	Ředitel odboru informatiky
Schvalování plánu financování ISVS	Ředitel odboru financování a majetku
Příprava změn IK	Vedoucí oddělení koncepce informatiky a archivu
Schvalování změn IK a jejích nových verzí	Ředitel odboru informatiky
Příprava nové IK před ukončením platnosti stávající	Vedoucí oddělení koncepce informatiky a archivu

Provádění vyhodnocování dodržování IK a vyhotovení zápisu o vyhodnocování	Vedoucí oddělení koncepce informatiky a archivu
Návrh opatření na základě zjištění při vyhodnocování	Vedoucí oddělení koncepce informatiky a archivu
Schvalování opatření na základě zjištění při vyhodnocování	Ředitel odboru informatiky
Schválení zápisu z vyhodnocení	Ředitel odboru informatiky

9.2. Splnění zákonných povinností

V rámci MPSV byla vrcholná odpovědnost za splnění zákonných povinností stanovena na útvar **Odbor informatiky MPSV**.

Dílčí odpovědnosti za jednotlivé oblasti informační koncepce jsou uvedeny v následující tabulce:

Zákon	Oblast	Dílčí odpovědnost
Zák. č. 365/2000 Sb. §5 odst. 2 písm. a	Spolupracovat s Ministerstvem vnitra při plnění jeho úkolů	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. a	Spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. b	Předložit Ministerstvu vnitra k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií	Ředitel ekonomického odboru
Zák. č. 365/2000 Sb. §5 odst. 2 písm. b	Předložit Ministerstvu vnitra k vyjádření investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií - přesné podmínky viz zákon	Ředitel ekonomického odboru
Zák. č. 365/2000 Sb. §5 odst. 2 písm. c	Uveřejňovat číselníky, pokud jsou jejich správci a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. c	Předávat Ministerstvu vnitra údaje do informačního systému o datových prvcích v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. d	Zajistit, aby vazby jimi provozovaného informačního systému na informační systémy	Ředitel odboru informatiky

	jiného provozovatele byly uskutečňovány prostřednictvím referenčního rozhraní s využitím datových prvků vyhlášených ministerstvem a vedených v informačním systému o datových prvcích	
Zák. č. 365/2000 Sb. §5 odst. 2 písm. d	Prokázat atestem způsobilost informačního systému k realizaci výše uvedených vazeb	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. e	Zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi provozovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v IS o ISVS	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5 odst. 2 písm. f	Odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5a odst. 1	Vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5a odst. 2	Vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5a odst. 3	Zajistit si atest dlouhodobého řízení ISVS	Ředitel odboru informatiky
Zák. č. 365/2000 Sb. §5b odst. 1 až odst. 2	Zajišťovat bezpečnost ISVS v rozsahu odpovídajícím alespoň minimálním bezpečnostním požadavkům k zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací dle prováděcího předpisu	Ředitel odboru informatiky