Konero, s.r.o.
Lázeňská 1402
562 01 Ústí nad Orlicí
http://www.konero.cz

Dlouhodobé řízení ISVS

Úplná struktura informační koncepce

Zadavatel	Ministerstvo vnitra
Řešitel	Konero, s.r.o.

Verze dokumentu	3.0
Název souboru	PIK_Struktura_final_3_0.rtf
Autor	Ing. Jiří Langr (jiri.langr@konero.cz)
Datum vytvoření	2.8.2006
Datum poslední revize	6.10.2011
Počet stran	23
Počet příloh	0
Důvěrnost	pro potřebu orgánů veřejné správy

OBSAH

1 Identifikace informační koncepce

1.1 Základní údaje informační koncepce

Tabulka základních údajů informační koncepce :

- orgán veřejné správy: název, sídlo, typ (ústřední úřad, KÚ, ORP, POÚ, ...)
- časové ohraničení informační koncepce (IK): označení počáteční verze, datum vzniku IK, datum počátku platnosti, doba platnosti resp. datum konce platnosti (vyhláška č. 529/2006 Sb. § 2 odst. 1 písm. i) a § 6 odst. 1)
- údaje o dokumentu: označení verze dokumentu, název a umístění elektronické podoby, počet stran a příloh apod.
- označení důvěrnosti dokumentu
- autor: jméno resp. jména, příjmení, útvar nebo externí organizace, funkce
- schválil: jméno resp. jména, příjmení, útvar nebo externí organizace, funkce
- datum schválení IK

1.2 Verze X informační koncepce

1.2.1 Identifikace verze informační koncepce

Tabulka identifikace verze informační koncepce (vyhláška č. 529/2006 Sb. § 6 odst. 1 a 2):

- identifikace verze: označení verze, datum vzniku, datum počátku platnosti
- údaje o dokumentu: označení verze, název a umístění elektronické podoby, počet stran a příloh apod.
- autor: jméno resp. jména, příjmení, útvar nebo externí organizace, funkce
- schválil: jméno resp. jména, příjmení, útvar nebo externí organizace, funkce
- datum schválení verze IK

1.2.2 Změny provedené ve verzi IK

Tabulka všech změn aktuální verze oproti verzi minulé (vyhláška č. 529/2006 Sb. § 6 odst. 3):

- popis změny
- odůvodnění změny
- identifikace místa v dokumentu, které bylo změněno

1.3 Verze Y informační koncepce

Obdobná struktura a náplň jako pro verzi X. Verze by měly být chronologicky řazené od nejnovější k nejstarší.

2 Informační systémy ve správě orgánu veřejné správy

Přístup k jednotlivým informačním systémům veřejné správy (ISVS) může orgán veřejné správy (VS) zvolit (vyhláška č. 529/2006 Sb. § 2 odst. 2):

- každý ISVS se charakterizuje zvlášť,
- na více informačních systémů (IS) se pohlíží jako na subsystémy jednoho ISVS.

Přístup k provozním IS s vazbami na ISVS může orgán ISVS zvolit (vyhláška č. 529/2006 Sb. § 5 odst. 2):

- popisuje pouze vazby těchto IS na ISVS,
- věnuje se těmto IS obdobně jako ISVS, pokud takový přístup považuje za účelný.

V případě potřeby může dokonce postup stanovený pro ISVS uplatnit na úplně všechny jím provozované IS bez ohledu na to, zda mají vazbu na ISVS. Informační koncepce musí především sloužit potřebám orgánu veřejné správy.

V úvodu této kapitoly se doporučuje uvést:

- jakým způsobem jsou charakterizovány jednotlivé ISVS,
- jakým způsobem jsou popisovány provozní IS, které mají vazby na ISVS,
- zda jsou popisovány všechny provozní IS nebo pouze ty, které mají vazby na ISVS,
- přehledný seznam všech IS, které jsou dále popsány s rozlišením, o jaký typ se jedná (ISVS, provozní IS s vazbou na ISVS provozní IS bez vazby na ISVS).

2.1 Informační systémy veřejné správy

2.1.1 Informační systém X

Pro každý ISVS ve správě orgánu veřejné správy obdobná struktura údajů (vyhláška. č. 529/2006 Sb. § 2 odst. 1 písm. a) viz následující podkapitoly. Kromě toho je třeba každý IS pojmenovat, popsat jeho určení (včetně případného odkazu na zřizující legislativu). Identifikace útvaru odpovědného za jeho správu, případně osobu správce - je lepší provést až v provozní dokumentaci IS.

2.1.1.1 Charakteristika informačního systému X

ISVS se charakterizuje s přihlédnutím k ustanovení (vyhl. č. 529/2006 Sb. §5 odst. 1) především s ohledem na:

- data, která jsou v něm zpracovávána,
- služby, jsou jeho prostřednictvím zajišťovány,
- použité technické a programové prostředky.

2.1.1.2 Charakteristika současného stavu informačního systému X

Uvede se stručná charakteristika stávajícího stavu (především z pohledu míry naplnění požadavků, stavu zastarávání apod.).

2.1.1.3 Předpokládané změny v informačním systému X

Uvede se stručná charakteristika předpokládaných změn včetně jejich časového a finančního horizontu, případně konstatování, že se se žádnými změnami nepočítá apod. Může zde být uveden též záměr na ukončení činnosti IS.

2.1.2 Informační systém Y

Obdobná struktura a náplň jako pro IS X.

2.2 Provozní informační systémy

Kapitola obsahuje dílčí podkapitoly pro jednotlivé provozní IS. V případě, že se zde popisují pouze provozní IS s vazbou na ISVS, pak může být uveden pouze popis těchto vazeb. V případě, že se provozní IS popisují obdobně jako ISVS, pak mohou být popsány všechny provozní ISVS, u provozních IS s vazbami na ISVS by měly být popsány též tyto vazby.

2.2.1 Informační systém A (popsány pouze vazby na ISVS)

Uvede se název a stručný popis informačního systému pro jeho jednoznačnou identifikaci a jeho účel. Dále se uvede přehled všech vazeb na ISVS, identifikují se tyto ISVS a vazby se stručně popíší.

2.2.2 Informační systém B (popsán obdobně jako ISVS)

IS bude popsán stejně jako ISVS. V rámci popisu služeb, které jsou prostřednictvím IS zajišťovány, je třeba klást zvýšený důraz na popis vazeb na ISVS.

3 Záměry na pořízení nebo vytvoření nových ISVS

Uvede se stručný úvod k záměrům nových IS nebo konstatování, že zatím žádný takový záměr neexistuje. Pro každý záměr nového IS se uvede popis dle následující vzorové kapitoly (vyhl. č. 529/2006 Sb. §2 odst. 1 písm. b) a vyhl. č. 529/2006 Sb. §8 odst. 1 písm. a)).

3.1 Záměr na pořízení/vytvoření nového IS X

Záměr by měl obsahovat následující charakteristiky:

- název IS,
- důvod včetně odkazu na legislativu, usnesení vlády apod.
- stručná charakteristika (data, služby, technika),
- typ (ISVS, provozní IS s vazbami na ISVS, provozní IS bez vazeb),
- způsob realizace: pořízení / vytvoření
- charakteristika stávajícího stavu řešení oblasti, konstatování stavu budování (např. pobíhá veřejná soutěž) případně odkazy na existující dokumentaci (např. koncepce řešení apod.),
- základní finanční a časové specifikace projektu budování IS,
- případné další okolnosti či poznámky.

4 Řízení kvality ISVS

Obsah řízení kvality je uveden ve vyhl. č. 529/2006 Sb. §2 odst. 1 písm. c), způsob naplnění ve vyhl. č. 529/2006 Sb. §3. Pro řízení kvality ISVS je nutné stanovit dlouhodobé cíle kvality, ty transformovat do konkrétních požadavků na kvalitu a následně stanovit plán, jak má být těchto cílů resp. naplnění požadavků dosaženo.

4.1 Dlouhodobé cíle v oblasti řízení kvality ISVS

Dlouhodobé cíle v oblasti řízení kvality musí být stanoveny v následujících oblastech:

- zajištění kvality dat, která jsou v IS zpracovávána,
- zajištění kvality služeb, které jsou prostřednictvím IS poskytovány,
- zajištění kvality technických a programových prostředků.

4.1.1 Cíle z oblasti zajištění kvality dat

4.1.1.1 Aktuálnost dat

Jedním z významných prvků kvality dat je jejich aktuálnost. V závislosti na typu a provedení IS může být aktuálnost dat značně různorodá. Od systémů, kde se změny projevují okamžitě, až po komplexní systémy, kde je např. zapotřebí replikací do prezentačních částí, které mohou mít časovou prodlevu.

Důležitým prvkem je též způsob spolupráce ISVS se subsystémy či jinými spolupracujícími systémy. Zde se aktuálnost dat systému stává závislou na dodávaných datech spolupracujících zdrojů a je značně svázána s aktuálností zdrojů či způsobem, jímž jsou data ze spolupracujících zdrojů získávána.

4.1.1.2 Správnost dat

Správnost dat může být zajišťována celou řadou způsobů. Počínaje pouhou vizuální kontrolou, přes kontrolu zajišťovanou administrativně či technicky (od jednoduché kontroly typu ověření modulo 11 u rodného čísla po složité křížové kontroly dat z více zdrojů).

4.1.1.3 Integrita dat

Zajištění integrity a tedy konzistentnosti dat by mělo být prováděno co nejvíce na technologické úrovni. Vzhledem k tomu, že integrita je klíčovým prvkem k tomu, aby data byla vůbec použitelná, je vhodné na této úrovni minimalizovat chybu lidského faktoru.

4.1.1.4 Stanovení odpovědnosti

Významným prvkem zajištění kvality dat je stanovení odpovědnosti. Ta může být stanovena na vysoké úrovni, ovšem je vhodné ji delegovat až na úroveň vkládání dat. To s sebou nese často též potřebu identifikace vkladatele.

4.1.2 Cíle z oblasti zajištění kvality služeb

4.1.2.1 Dostupnost služeb

Prvek velmi svázaný s kvalitou technických prostředků. Potřeba dostupnosti ISVS by měla úměrně stoupat s významem ISVS jak pro cílové uživatele, tak i pro spolupracující

informační systémy. Informační systém musí zajistit, aby požadovaná informace byla přístupná ve stanoveném místě, v požadované formě a v určeném časovém rozmezí.

4.1.2.2 Přehlednost služeb

Potřeba přehlednosti souvisí s vizuálním návrhem rozhraní ISVS. Uživatelé by se neměli "ztrácet", ale naopak by měli mít jasný přehled, ve které části rozhraní se nacházejí.

4.1.2.3 Srozumitelnost služeb

Všechny prvky rozhraní by měly být jednoznačné, popisky by neměly být matoucí. Rozhraní by se mělo oprostit od používání odborného žargonu a naopak se snažit v rozumné míře přiblížit neznalému uživateli.

4.1.2.4 Přístupnost pro handicapované

Rozhraní služby by mělo být přístupné i handicapovaným uživatelům. Při použití webového rozhraní je vhodné využít Best practice - Pravidla pro tvorbu přístupného webu (http://www.micr.cz/scripts/detail.php?id=1588), pro jakoukoliv jinou formu je vhodné se tímto dokumentem alespoň inspirovat. (Od 1. ledna 2008 bude zmiňované best practice nahrazeno vyhláškou k zákonu č. 365/2000 Sb., o ISVS.)

4.1.2.5 Kompatibilita s běžně používanými klientskými prostředími a standardy

Kvalita služeb se týká nejen rozhraní pro uživatele, ale i pro spolupracující informační systémy. Proto je při návrhu žádoucí držet se běžně používaných standardů.

4.1.3 Cíle z oblasti zajištění kvality technických a programových prostředků

Kvalita ISVS se významně odvíjí od kvality technických a programových prostředků. Chyby v těchto prostředcích mohou mít přímý vliv na prvky kvality dat.

4.1.3.1 Kvalita technických prostředků

Kvalita technických prostředků je přímo úměrná požadované kvalitě služeb (viz níže). Je zajišťována jak kvalitou samotného technického vybavení, tak ale i prvky k odvrácení technických rizik. Začíná tedy volbou vhodných technických komponent systémů samotného ISVS, pokračuje přes zařízení schopná omezit rizika výpadku vnějších prvků (např. výpadek energie, výpadek připojení k internetu) a končí kompletními failover řešeními, schopnými snížit rizika výpadku samotného zařízení (disková pole, clustery, počítače se znásobenými komponentami pro případ jejich výpadku, apod.).

Mezi prvky k zajištění kvality technických prostředků rovněž patří další podpůrné systémy, jako např. zálohovací systémy, ale i routery, firewally apod.

Do prvků, určujících kvalitu technického vybavení můžeme zařadit i firmware použitého technického zařízení, až se svou povahou spíše jedná o prvek na rozhraní technického a softwarového vybavení.

4.1.3.2 Kvalita programových prostředků

Požadavek kvality programových prostředků postihuje širokou škálu softwarového vybavení. To lze rozdělit do několika úrovní:

Základní vrstva:

- operační systém
- certifikované ovladače
- servisní balíčky či "záplaty"
- apod.

Podpůrná vrstva:

- databázové servery (+ servisní balíčky či záplaty)
- aplikační servery (+ servisní balíčky či záplaty)
- webové servery (+ servisní balíčky či záplaty)
- run-time prostředí typu Java, .NET (+ servisní balíčky či záplaty)
- apod.

Kvalita konkrétního programového vybavení zajišťujícího vlastní funkčnost systému.

Do této oblasti také nepřímo spadá kvalita programových prostředků spolupracujících systémů.

4.2 Požadavky na kvalitu ISVS

Požadavky na kvalitu obsahují souhrn požadavků, které jsou konkretizací poněkud obecnějších cílů kvality. Požadavky by měly být pokud možno měřitelné a měly by být vázány na cíle kvality, k jejichž naplnění směřují. Požadavky mohou být specifické pro jeden IS nebo společné pro několik nebo dokonce pro všechny IS daného správce. Součástí vyhodnocování IK by mělo být mj. též vyhodnocování míry a způsobu naplnění stanovených požadavků na kvalitu IS.

4.3 Plán řízení kvality ISVS

Plán řízení kvality obsahuje popis činností, které orgán veřejné správy vykonává pro naplnění stanovených cílů kvality a uplatnění konkrétních požadavků na kvalitu IS. Součástí je též předpokládaný časový harmonogram plnění cílů a požadavků v oblasti kvality.

5 Řízení bezpečnosti ISVS

Obsah řízení bezpečnosti je uveden ve vyhl. č. 529/2006 Sb. §2 odst. 1 písm. d), způsob naplnění ve vyhl. č. 529/2006 Sb. §4. Pro řízení bezpečnosti ISVS je nutné stanovit dlouhodobé cíle bezpečnosti, ty transformovat do konkrétních požadavků na bezpečnost a následně stanovit plán, jak má být těchto cílů resp. naplnění požadavků dosaženo.

Přitom je třeba mít na zřeteli, že každý požadavek v oblasti bezpečnosti ISVS by se měl opírat o projektovou bezpečnostní a provozní bezpečnostní dokumentaci.

5.1 Dlouhodobé cíle v oblasti řízení bezpečnosti ISVS

Dlouhodobé cíle v oblasti řízení bezpečnosti musí být stanoveny v následujících oblastech:

- oblast zajištění bezpečnosti dat,
- oblast zajištění bezpečnosti technických a programových prostředků,
- oblast zajištění bezpečnosti služeb.

5.1.1 Cíle z oblasti zajištění bezpečnosti dat

5.1.1.1 Dostupnost dat

Dostupnost dat by měla být zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebě dat. Do této kapitoly jistě patří např. použití diskových polí, clusterů, i softwarových nástrojů, zajišťujících či posilujících datovou dostupnost.

Je nutné stanovit politiku zálohování a archivací, a to nejen z hlediska pravidelnosti zálohování, způsobu zálohování, způsobu archivací dat, ale i způsobu uložení dat (např. dvojí uložení do dvou fyzicky různých lokalit pro případ požáru) apod.

5.1.1.2 Důvěrnost dat

Jedná se o aplikaci základních atributů zabezpečení přístupu, což jsou:

- identifikace - každý uživatel je jednoznačně identifikován,
- autentizace - uživatel prokáže svoji totožnost (heslem, otiskem prstu apod.),
- autorizace - každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává.

K datům je nutno vést řízený přístup. Je třeba, aby data byla chráněna tak, aby k nim neoprávněné osoby neměly přístup umožňující čtení či dokonce manipulaci s nimi (pozměňování, mazání). Zde je nutné uvést, že řízený přístup je třeba vést k datům živým, ale i k zálohám a k médiím data obsahujícím (např. vadné disky apod.).

5.1.1.3 Integrita dat

Integrita dat by měla být od počátku zajištěna volbou vhodných nástrojů pro zpracování dat, tedy od databází zajišťujících referenční integritu až po archivační nástroje s ověřováním kontrolních součtů.

5.1.2 Cíle z oblasti zajištění bezpečnosti služeb

5.1.2.1 Dostupnost služeb

Dostupnost služeb by měla být zajištěna vhodnou kombinací technických a programových prostředků, opět úměrně potřebnosti služeb. Sem patří použití řešení, zajišťující odolnost proti výpadku elektrické energie, komunikačních sítí, duplikování či posílení odolnosti proti výpadku hardwarových a softwarových prvků apod.

Do této oblasti spadají též nástroje pro ochranu proti útokům např. typu DoS (Denial of Service), tedy zejména nástroje síťové infrastruktury (firewally, IDS systémy apod.)

5.1.2.2 Důvěrnost služeb

Opět se jedná o aplikaci základních atributů zabezpečení přístupu:

- identifikace - každý uživatel je jednoznačně identifikován,
- autentizace - uživatel prokáže svoji totožnost (heslem, otiskem prstu apod.),
- autorizace - každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává.

Tyto atributy se uplatňují jak vůči osobám, tak i vůči spolupracujícím systémům.

Do této kapitoly spadá i ochrana důvěrnosti dat během přenosu sítěmi s tím, že informace, která to svoji povahou vyžaduje, musí být v procesu přenosu mezi zdrojem a cílem chráněna odpovídajícím způsobem.

5.1.2.3 Integrita služeb

Tento bezpečnostní cíl pokrývá zajištění integrity služeb samostatných a spolupracujících systémů. Týká se např. sdílení informací o uživateli, sdílení služeb datových zdrojů apod.

5.1.3 Cíle z oblasti zajištění bezpečnosti technických a programových prostředků

5.1.3.1 Dostupnost technických a programových prostředků

Dostupnost technických prostředků zahrnuje následující:

- záložní zdroje napájení,
- záložní síťová připojení,
- zabezpečení dostupnosti hardware duplikováním či násobením důležitých prvků (clustery apod.),
- umístěním záložních zařízení do geograficky různých lokalit.

Dostupnost programových prostředků zahrnuje zejména:

- používání výrobcem certifikovaných softwarových komponent (ovladače apod.),
- testování a včasnou aplikaci záplat programového vybavení,
- nasazení prostředků monitorování provozu a včasného upozornění jak na prostředky vlastního informačního systému, tak i na prostředky síťové infrastruktury,
- použití nástrojů softwarové ochrany (antiviry apod.),
- logické umístění do bezpečné zóny sítě, pokud je to možné (intranet, DMZ).

5.1.3.2 Důvěrnost technických a programových prostředků

Důvěrnost technických prostředků zahrnuje především:

- fyzickou bezpečnost - umístění technických prostředků do zabezpečeného prostoru, fyzická ochrana před riziky prostředí, další opatření
- zabezpečení používané telekomunikační infrastruktury - nastavení switchů, routerů apod.

Důvěrnost programových prostředků se týká zejména:

- zajištění odolnosti proti úmyslně či neúmyslně chybným vstupním datům (např. odolnost proti buffer overflow, SQL injection apod. útokům),
- zajištění ochrany proti parazitním kódům,
- zajištění ochrany proti podvržení identity spolupracujících systémů.

5.1.3.3 Integrita technických a programových prostředků

Integrita technických prostředků se týká zejména:

- ochrany proti přetížení,
- ochrany proti zničení či poškození.

Integrita programových prostředků zahrnuje:

- ochranu proti smazání softwarové komponenty,
- ochranu proti modifikaci či podvržení softwarové komponenty,
- ochranu proti modifikaci konfigurace softwarové komponenty.

5.2 Požadavky na bezpečnost ISVS

Požadavky na bezpečnost obsahují souhrn požadavků, které jsou konkretizací poněkud obecnějších cílů bezpečnosti. Požadavky by měly být pokud možno měřitelné a měly by být vázány na cíle bezpečnosti, k jejichž naplnění směřují. Požadavky mohou být specifické pro jeden IS nebo společné pro několik nebo dokonce pro všechny IS daného správce. Součástí vyhodnocování IK by mělo být mj. též vyhodnocování míry a způsobu naplnění stanovených požadavků na bezpečnost IS.

Konkrétní bezpečnostní požadavky by měly být výsledkem bezpečnostní analýzy (analýza rizik) a návrhu opatření odpovídajících míře rizika velikosti s ním svázané škody.

5.3 Plán řízení bezpečnosti ISVS

Plán řízení bezpečnosti obsahuje popis činností, které orgán veřejné správy vykonává pro naplnění stanovených cílů bezpečnosti a uplatnění konkrétních požadavků na bezpečnost IS. Součástí je též předpokládaný časový harmonogram plnění cílů a požadavků v oblasti bezpečnosti.

6 Zásady a postupy pro správu ISVS

Základní vymezení této kapitoly je uvedeno ve vyhl. č. 529/2006 Sb. §2 odst. 1 písm. e), podrobnější popis ve vyhl. č. 529/2006 Sb. §8 až §9. Uvede se souhrn základních pravidel (zásady) pro správu ISVS a postupy, které vedou k jejich naplňování.

6.1 Zásady a postupy pro pořizování a vytváření ISVS

Před tím, než orgán veřejné správy pořídí či vytvoří ISVS, musí provést některé přípravné kroky. Zásady a postupy uplatňované v této fázi budou uvedeny v této části informační koncepce, viz vyhl. č. 529/2006 Sb. §8 odst. 1.

Přehled základních kroků:

- definování potřeby IS, analýza zdrojů pro jeho pořízení / vytvoření, očekávaná finanční náročnost (v případě potřeby též analýza časové dostupnosti zdrojů apod.),
- analýza výchozího stavu (též s ohledem na možnost využití služeb nebo zdrojů jiných IS téhož správce),
- stanovení požadovaného cílového stavu IS (vyplývají z definice potřeby IS),
- stanovení požadavků na kvalitu a bezpečnost (vyplývají z dlouhodobých cílů a obecných požadavků),
- analýza důsledků, které pořízení / vytvoření IS může vyvolat (např. dopad na procesy, činnost úřadu, organizační opatření apod.).

6.1.1 Pořizování ISVS

Pokud orgán veřejné správy hodlá pořizovat ISVS od dodavatele, v IK uvede (vyhl. č. 529/2006 Sb. §8 odst. 2):

- požadavky na dokumentaci IS, požadavky na oprávnění nezbytná pro provádění údržby a změn v IS, a to v závislosti na tom, zda hodlá údržbu a změny správce IS provádět vlastními silami,
- požadavky na projektové řízení u dodavatele (nemusí být definovány, či je možno ponechat výběr metody na dodavateli); doporučuje se vycházet z obecně uznávaných českých norem v této oblasti (např. ČSN ISO/IEC 15288 Systémové inženýrství - Procesy životního cyklu systému),
- požadavky na testování IS a podmínky akceptace.

6.1.2 Vytváření ISVS

Pokud orgán veřejné správy hodlá vytvářet ISVS vlastními silami, v IK uvede (vyhl. č. 529/2006 Sb. §8 odst. 3 až odst. 4):

- náležitosti dokumentování procesů vytváření IS (je vhodné apelovat na průběžnou tvorbu dokumentace),
- zásady projektového řízení dle ČSN, která stanové projektové postupy (viz výše), případně jiné vhodné normy, pokud při vytváření projektové řízení v souladu s výše uvedenou normou uplatňuje.

6.2 Zásady a postupy pro provozování ISVS

Zde jsou uvedeny zásady a postupy uplatňované při provozování ISVS v souladu s vyhl. č. 529/2006 Sb. §9. Minimální oblasti, které se v této části povinně řeší, jsou uvedeny v podkapitolách 6.2.1 až 6.2.3. Z logiky věci vyplývá potřeba plánování rozvoje ISVS, které však není vyhláškou striktně vyžadováno. V podkapitole 6.3 je návrh možného řešení této oblasti. Právní předpisy samozřejmě nevylučují v této části popsat libovolné další oblasti související s provozováním ISVS dle potřeb konkrétního orgánu VS.

6.2.1 Zajištění provozu a údržby ISVS

Zásady a postupy při zajištění provozu a údržby ISVS v souladu s vyhl. č. 529/2006 Sb. §9 odst. 1 písm. b) a vyhl. č. 529/2006 Sb. §9 odst. 3 zahrnují:

- zásady a postupy pro vytváření a údržbu provozní dokumentace (PD) (vyhl. č. 529/2006 Sb. §10 až §12),
- zásady a postupy pro zajištění souladu provozování ISVS s IK a PD,
- zásady a postupy pro vyhodnocování dodržování souladu provozování ISVS s IK a PD,
- stanovení povinností jednotlivých zaměstnanců nebo jiných fyzických osob ve vztahu k činnostem z oblasti zajištění provozu a údržby ISVS.

Proces vyhodnocování by se měl soustředit na všechny dílčí aspekty:

- soulad provozní dokumentace s informační koncepcí,
- soulad provozní dokumentace s vyhl. č. 529/2006 Sb. §10 až §12,
- soulad procesů provozování ISVS s informační koncepcí a provozní dokumentací,

6.2.2 Řízení změn v ISVS

Řízením změn se v souladu s vyhl. č. 529/2006 Sb. §9 odst. 4 rozumí zajištění činností při řízení procesů:

- navrhování změn IS,
- schvalování změn IS,
- realizace změn IS.

Řízení změn musí být dokumentováno.

V souvislosti s řízením změn je třeba stanovit hranice mezi dvěma odlišně spravovanými oblastmi (vyhl. č. 529/2006 Sb. §9 odst. 5):

- **Údržba IS** představuje provádění činností, které vedou k zachování funkcí IS v požadovaném a nezměněném stavu (například opravy chyb, bezpečnostní záplaty apod.).
- **Provádění změn v IS** zahrnuje kvalitativní změny vždy spojené se změnami funkčnosti nebo datového rozhraní (např. potřeba rozšíření funkcionality, změna datového obsahu, změna datových rozhraní, změna procesů ve kterých je IS používán, reagování na novelizaci právních předpisů apod.).

Nezbytné kroky v souvislosti s řízením změn (vyhl. č. 529/2006 Sb. §9 odst. 6):

- definování potřeby změn v ISVS
- analýza výchozího stavu pro rozvoj ISVS,

- stanovení cílového stavu ISVS,
- stanovení požadavků na kvalitu a bezpečnost vztahujících se k cílovému stavu ISVS,
- návrh transformace z výchozího do cílového stavu ISVS (může být i více alternativ, které orgán veřejné zprávy vyhodnotí),
- analýza důsledků, které změna může vyvolat (tyto analýzy jsou předpokládány pro každou navrženou alternativu a měly by být součástí podkladů pro rozhodování orgánu veřejné správy),
- promítnutí změn do provozní dokumentace a jiných dokumentů, kterých se změna dotýká (probíhá ve fázi realizace).

Předpokládá se, že v IK je řízení změn popsáno v obecné rovině společně pro všechny ISVS. IK by měla v této oblasti předepisovat pravidla pro tvorbu provozní dokumentace, v rámci níž je třeba pro každý IS stanovit (v závislosti na jeho významu a rozsahu):

- činnosti při navrhování a schvalování změn,
- pravidla pro změnové řízení,
- postupy provádění změn,
- určení rolí a odpovědností za řízení procesu změny,
- pravidla pro podrobné dokumentování změny,
- používané nástroje pro řízení verzí a konfigurační management – viz kapitola 8.

6.2.3 Ukončení činnosti ISVS

V IK budou stanoveny zásady a postupy při definování potřeby ukončení činnosti ISVS (vyhl. č. 529/2006 Sb. §9 odst. 6).

Vlastní ukončení provozu IS by mělo být řízeným procesem s definovanými rolemi a odpovědnostmi. Za nejdůležitější část tohoto procesu se považuje bezpečné naložení s daty, která ukončovaný ISVS zpracovává (vyhl. č. 529/2006 Sb. §9 odst. 7).

Obvykle se jedná o jednu (či více) z následujících možností:

- převedení dat do jiného IS,
- uchování, zde je nutné definovat celou řadu atributů:
  - kde budou data uchována (fyzické omezení přístupu, podmínky),
  - jak budou data uchována (způsob uložení, šifrování, média),
  - jak bude zajištěna jejich čitelnost (pravidla pro údržbu médií, kontrola čitelnosti či cyklické opakování zálohování),
  - stanovení odpovědnosti za dostupnost dat.
- zničení dat (více by mělo být součástí skartačního řádu organizace).

6.3 Plánování rozvoje ISVS

Oblast plánování rozvoje ISVS se objevila ve fázi návrhu vyhl. č. 529/2006 Sb., avšak do schváleného znění se nedostala. Přesto byla tato část v Úplné struktuře IK ponechána s tím, že se jedná o část nepovinnou. Náplní této části IK by měly být zásady a postupy pro plánování rozvoje ISVS v podobě pravidel pro vytváření a údržbu plánu rozvoje ISVS.

Informační koncepce ve svých jednotlivých částech bude obsahovat různá pravidla, jak řídit budování ISVS, avšak nikde není striktně řečeno, že by bylo vhodné všechny zamýšlené

kroky konkrétně specifikovat a schválit jako aktuální plán rozvoje ISVS na nejbližší období (jeden až dva roky), což je zřejmé z následujícího přehledu plánovaných kroků v rámci IK:

- předpokládané změny v ISVS jako součást jeho popisu (kapitola 2.1.1.3),
- záměry na pořízení nebo vytvoření nových ISVS (kapitola 3),
- plán řízení kvality (kapitola 4.3),
- plán řízení bezpečnosti (kapitola 5.3),
- výsledky přípravy budování nových ISVS v souladu se zásadami a postupy pro pořizování a vytváření ISVS (kapitola 6.1),
- definované potřeby změn v souvislosti s procesem řízení změn ISVS (kapitola 6.2.2),
- definované potřeby změn ukončení činnosti v souvislosti s procesem řízeného ukončení činnosti ISVS (kapitola 6.2.3),
- plán financování naplánovaných kroků v oblasti řízení ISVS (kapitola 7).

7 Způsob financování ISVS

Obsah IK v oblasti financování ISVS je dán vyhl. č. 529/2006 Sb. §2 odst. 1 písm. f). Dále je třeba respektovat povinnosti dané dalšími právními předpisy, jako např. zák. č. 365/2000 Sb. §5 odst. 2 písm. b) a zák. č. 137/2006 Sb., o veřejných zakázkách.

Orgán veřejné správy popisuje způsob financování svých informačních systémů v souladu s pravidly danými obecnými předpisy v této oblasti pro daný typ orgánu veřejné správy. Součástí mohou být též pravidla a povinnosti při zadávání veřejných zakázek a zakázek malého rozsahu na ISVS, jako jsou např. povinné požadavky na dodávky v této oblasti (např. testování IS před jejich akceptací, požadavky na akceptační protokoly, požadavky na technickou podporu, případné požadavky na certifikaci jakosti IS, případně certifikaci řízení jakosti u dodavatele apod.).

Je vhodné stanovit role a odpovědnosti v procesu zadávání zakázek v oblasti ISVS a při činnostech v oblasti získávání finančních prostředků na realizaci záměrů v této oblasti.

Financování ISVS se řeší ve třech oblastech - viz následující dílčí kapitoly. Na základě záměrů a plánů v jednotlivých oblastech je vhodné sestavit pro celý orgán veřejné správy jednotný plán zdrojů jejich financování, a to včetně časového harmonogramu čerpání prostředků.

7.1 Financování záměrů na pořízení nebo vytvoření nových ISVS

Náplň kapitoly vychází ze záměrů na pořízení nebo vytvoření nových ISVS (viz kapitolu 3), kde je uveden přehled všech plánovaných nových IS, a to včetně finančních specifikací. V této části je třeba naplánovat zdroje financování záměrů (vlastní rozpočet, dotační programy, ISPROFIN, fondy EU apod.). V IK je třeba zakotvit též povinnosti, které v této oblasti vyplývají v oblasti schvalování investičních záměrů Ministerstvem vnitra.

7.2 Financování naplnění dlouhodobých cílů

Naplnění dlouhodobých cílů představuje ve své podstatě realizaci požadavků na kvalitu a požadavků na bezpečnost, a to formou změn stávajících ISVS nebo specifických požadavků na budování nových ISVS. V případě budování nových ISVS by tyto požadavky měly být součástí záměru ISVS a tudíž by měly být řešeny v předchozí kapitole. U stávajících IS orgán veřejné správy popíše způsob financování projektů, plánovaných v této oblasti, popíše též způsob zajištění potřebných zdrojů a vytvoří příslušný plán.

7.3 Financování správy ISVS

Financování správy ISVS zahrnuje provoz, údržbu a rozvoj samotných ISVS, ale též další podpůrné činnosti včetně dlouhodobého řízení ISVS. Orgán veřejné správy popíše způsob financování činností, prováděných v této oblasti, vytvoří příslušný plán a případně popíše též způsob zajištění potřebných zdrojů.

8 Naplňování informační koncepce

Základní specifikace této kapitoly je uvedena v vyhl. č. 529/2006 Sb. §2 odst. 1 písm. g) a h). Jsou zde popsány postupy pro údržbu IK (provádění změn), její vyhodnocování a dále jsou konkretizovány odpovědnosti v oblasti naplnění IK a zákonných povinností v oblasti dlouhodobého řízení ISVS.

8.1 Postupy při provádění změn IK

Zásady pro provádění změn IK jsou uvedeny v vyhl. č. 529/2006 Sb. §6. V této kapitole je třeba popsat konkrétní postupy pro naplnění těchto zásad. Součástí přípravy těchto postupů by mělo být např. rozhodnutí, zda změny budou prováděny formou vydání nové verze IK nebo dodatku k ní (lze doporučit vydání nové verze - viz např. zákony, kde se vydávají novely, ale pro praktický život se stejně musí vytvořit úplné znění).

8.1.1 Postup pro zajištění včasné změny IK

Ve vyhl. č. 529/2006 Sb. §6 odst. 4 je stanovena povinnost provádět změny IK tak, aby byl zachován soulad jejího obsahu se skutečným stavem a aktuálními požadavky orgánu veřejné správy. Za tímto účelem je třeba stanovit periodu, se kterou bude informační koncepce revidována z pohledu změn v oblasti dlouhodobého řízení ISVS a v případě zjištění potřeby promítnutí těchto změn do IK, bude vydána její nová verze nebo připojen dodatek. Doporučuje se, aby tyto revize byly prováděny častěji, než vyhodnocování dodržování IK, tedy např. jednou za 12 nebo 6 měsíců, a to v závislosti na velikosti orgánu veřejné správy, počtu jím spravovaných IS a jím vedených agend apod. Je možné, že u velkých a komplikovaných ústředních úřadů bude třeba IK revidovat např. každý 1 až 2 měsíce. Doporučuje se též zvážit, jaké podrobnosti bude orgán veřejné správy v IK uvádět, protože změny IK jsou předmětem schvalovacího procesu a IK má být spíše dokumentem koncepčním – nemělo by tedy docházet k jejím častým změnám.

Dále je vhodné stanovit události, které povedou na nutnost aktualizace IK i mimo stanovenou periodu, např. významná změna organizační struktury orgánu, vznik nového záměru pořízení nebo vytvoření IS, dokončení realizovaného IS, významné změny v právních předpisech, nové požadavky v oblasti kvality a bezpečnosti IS apod.

8.1.2 Postup zápisu změny do dokumentu IK

Zde budou popsány technické postupy pro vydávání změn IK. Bude zde řečeno, zda se vydávají nové verze IK nebo její dodatky (vyhl. č. 529/2006 Sb. §6 odst. 2). Bude popsán postup a způsob identifikace verze IS, popisu a odůvodnění změny a identifikace změněné části dokumentu (viz kapitolu 1.2, vyhl. č. 529/2006 Sb. §6 odst. 1 a vyhl. č. 529/2006 Sb. §6 odst. 3).

8.1.3 Postup schvalování změny IK

Bude popsán postup schvalování změn IK. Obecně by mělo platit, že změny podléhají obdobnému postupu schvalování, jako původní verze IK.

8.1.4 Postup přípravy nové IK

S ohledem na omezení platnosti IK v čase je vhodné, aby bylo zajištěno, že před uplynutím této doby bude vznikat nová IK. Lze např. stanovit začátek přípravy nové IK v několikaměsíčním předstihu před skončením platnosti aktuální IK apod. Dále by zde měly být stanoveny postupy přípravy nové IK a role v této oblasti.

8.2 Postupy při vyhodnocování dodržování informační koncepce

Zásady pro vyhodnocování dodržování IK jsou uvedeny v vyhl. č. 529/2006 Sb. §7. V této kapitole je třeba popsat konkrétní postupy pro naplnění těchto zásad. Součástí přípravy postupů by mělo být mj. rozhodnutí o periodicitě vyhodnocování IK (max. 24 měsíců). Měla by být dodržena také obecná zásada, že vyhodnocování by mělo být nezávislé na realizaci, tzn. vyhodnocovat by měly osoby, které nezodpovídají za realizaci IK.

V této části by měly být popsány postupy pro vyhodnocování dodržování v následujících oblastech:

- IK je včas aktualizována, v souladu s postupy pro provádění změn, aktuální verze je schválena, náležitě označena včetně vyznačení provedených změn, všichni relevantní pracovníci mají k dispozici aktuální verzi IK a je zajištěno, aby neplatná verze nebyla používána.
- IK obsahuje charakteristiky všech orgánem veřejné správy spravovaných ISVS a IS s vazbami na ISVS (případně všech spravovaných IS). Charakteristiky současného stavu IS jsou aktualizovány.
- IK obsahuje všechny existující záměry na pořízení nebo vytvoření ISVS. Jednotlivé záměry jsou náležitě charakterizovány.
- Požadavky na kvalitu jsou v rámci jednotlivých IS dodržovány a vyhodnocovány, případně se provede přímo vyhodnocení naplnění těchto požadavků. Je prakticky naplňován a dodržován plán řízení kvality.
- Požadavky na bezpečnost jsou v rámci jednotlivých IS dodržovány a vyhodnocovány, případně se provede přímo vyhodnocení naplnění těchto požadavků. Je prakticky naplňován a dodržován plán řízení bezpečnosti.
- Správa ISVS je vykonávána v souladu s přijatými zásadami a postupy:
    - Před pořízením nebo vytvořením ISVS jsou vykonány všechny potřebné kroky. Při pořizování ISVS jsou naplňovány všechny stanovené požadavky, které jsou následně zakotveny ve smlouvě. Při vytváření ISVS jsou všechny procesy náležitě dokumentovány a v případě projektového řízení jsou prakticky uplatňovány zásady a postupy projektového řízení.
    - Jsou uplatňovány zásady a postupy pro plánování rozvoje ISVS, zajištění provozu a údržby ISVS, řízení změn ISVS a ukončování činnosti ISVS.
- Financování ISVS probíhá v souladu se schválenými postupy a platnými předpisy. Existuje pravidelně aktualizovaný plán financování ISVS, který sestává z plánů financování záměrů na pořízení nebo vytvoření ISVS, financování naplnění dlouhodobých cílů a financování správy ISVS.
- Prováděné vyhodnocení nastalo v předepsaném časovém úseku od minulého. Zápisy z minulých vyhodnocení jsou dostupné obdobně, jako aktuální verze IK. Opatření přijatá při minulých vyhodnocováních byla promítnuta do aktualizované verze IK. Přijatá opatření jsou uplatňována v praxi. Přijatá opatření přinesla předpokládaný účinek - dříve zjištěné nedostatky byly odstraněny.

Dále by měly být popsány postupy pro vyhotovení zápisu o vyhodnocení (včetně pravidel pro jednoznačnou identifikaci zápisu), návrh opatření a jejich schválení a schválení celého zápisu. Zápis o vyhodnocení by měl obsahovat následující části:

- datum vyhodnocení, číslo či jiná identifikace zápisu,
- kdo vyhodnocení prováděl (jméno resp. jména, příjmení, útvar nebo externí organizace, funkce),
- průběh vyhodnocení,
- poznatky a závěry z vyhodnocení,
- přijatá opatření,
- schválení zápisu z vyhodnocení (kdo: jméno resp. jména, příjmení, útvar nebo externí organizace, funkce a kdy).

9 Osoba, která řídí provádění činností podle IK a zákona, nebo její funkční zařazení

Stanovení odpovědností je zakotveno ve vyhl. č. 529/2006 Sb. §2 odst. 1 písm. h).

9.1 Odpovědnosti za realizaci informační koncepce

Základní rolí v této oblasti je řízení provádění činností vedoucích k dosažení cílů, naplňování zásad a uplatňování postupů, které jsou v IK uvedeny. Měl by být určen zaměstnanec nebo jiná fyzická osoba (jméno resp. jména, příjmení, útvar nebo externí organizace, funkce) případně organizační útvar (název útvaru), který odpovídá za tuto oblast jako celek.

Dále lze specifikovat dílčí role a povinnosti, kterým mohou být přiřazeny jiné odpovědné osoby nebo útvary. Základní přehled dílčích odpovědností vyplývá ze struktury IK:

- vytváření záměrů na pořízení nebo vytvoření nových IS,
- schvalování záměrů na pořízení nebo vytvoření nových IS,
- 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),
- 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),
- koordinace činností v oblasti rozvoje ISVS, příprava plánu rozvoje ISVS,
- schvalování plánu rozvoje ISVS,
- řízení postupů při pořizování a vytváření ISVS (včetně zajištění veřejných zakázek apod.),
- vyhodnocování dodržování souladu provozování ISVS (soulad provozní dokumentace s IK a PD s vyhláškou, soulad skutečných procesů s provozní dokumentací),
- koordinace a vyhodnocování řízení změn,
- řízení ukončování provozu IS,
- vytváření a údržba plánu financování ISVS,
- schvalování plánu financování ISVS,
- příprava změn IK,
- schvalování změn IK a jejích nových verzí,
- příprava nové IK před ukončením platnosti stávající,
- provádění vyhodnocování dodržování IK a vyhotovení zápisu o vyhodnocování,
- návrh opatření na základě zjištění při vyhodnocování,
- schvalování opatření na základě zjištění při vyhodnocování,
- schválení zápisu z vyhodnocení.

9.2 Splnění zákonných povinností

Základní rolí v této oblasti je řízení provádění činností vedoucích ke splnění povinností, které orgánu veřejné správy stanoví zákon. Měl by být jmenován zaměstnanec nebo jiná

fyzická osoba (jméno resp. jména, příjmení, útvar nebo externí organizace, funkce) případně organizační útvar (název útvaru), který za tuto oblast odpovídá.

Zákonné povinnosti jsou dány především zák. č. 365/2000 Sb. §5 až §5c. Jedná se především o následující povinnosti orgánů veřejné správy:

- **zák. č. 365/2000 Sb. §5 odst. 2 písm. a)**: spolupracovat s Ministerstvem vnitra při plnění jeho úkolů podle § 4 odst. 1,
- **zák. č. 365/2000 Sb. §5 odst. 2 písm. a)**: spolupracovat s Ministerstvem vnitra při provádění kontroly na místě dle zákona o státní kontrole,
- **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,
- **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,
- **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,
- **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,
- **zák. č. 365/2000 Sb. §5 odst. 2 písm. d)**: zajistit, aby vazby jimi provozovaného informačního systému na informační systémy 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,
- **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 ISDP a IS o ISVS,
- **zák. č. 365/2000 Sb. §5 odst. 2 písm. f)**: odstranit zjištěné nedostatky ve lhůtě stanovené Ministerstvem vnitra,
- **zák. č. 365/2000 Sb. §5a odst. 1**: vytvářet a vydávat informační koncepci, uplatňovat ji v praxi a vyhodnocovat její dodržování,
- **zák. č. 365/2000 Sb. §5a odst. 2**: vytvářet a vydávat provozní dokumentaci k jednotlivým ISVS, uplatňovat ji v praxi a vyhodnocovat její dodržování,
- **zák. č. 365/2000 Sb. §5a odst. 3**: zajistit si atest dlouhodobého řízení ISVS (neplatí pro obce, které vykonávají přenesenou působnost pouze v základním rozsahu),
- **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.