Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Disertační práce

Efektivnost informačních systémů veřejné správy
Effectiveness of Information Systems of Public Administration

Autor: Ing. Tomáš Tureček

Obor: 6208V038 Management a ekonomika

Školitel: prof. Ing. Zdeněk Molnár, CSc.

Srpen 2008

PODĚKOVÁNÍ

Děkuji svému školiteli prof. Ing. Zdeňku Molnárovi, CSc. za cenné rady, připomínky, odborné vedení, konzultace a náměty vztahující se nejen k tvorbě této disertační práce, ale i k celému doktorskému studiu.

Dále děkuji svým kolegyním a kolegům z Ústavu informatiky a statistiky za jejich kritický přístup a konzultace.

Poděkování patří také mým rodičům a známým za podporu a trpělivost.

ABSTRAKT

e-Government je v současné době jednou z nejdiskutovanějších problematik vzhledem k veřejné správě. Disertační práce se zabývá efektivnosti zaváděných informačních systémů ve veřejné správě.

Literární rešerše popisuje nasazení informačních systémů ve veřejné správě. Jsou zde definovány základní pojmy, organizace veřejné správy, informační systémy, platné i plánované legislativní opatření. Nechybí informace o službách Czech POINT, elektronickém podpisu, dlouhodobém uchovávání elektronických dokumentů, na to navazující konverzi dokumentu a je zakončena stručným popisem e-Governmentu v zahraničí.

Hlavním cílem práce je na základě teoretického a terénního výzkumu identifikovat a zhodnotit současný stav informačních systémů ve veřejné správě, spokojenost s jejich využíváním jak na straně úředníků, tak na straně občana, zjistit kritická místa využívání těchto informačních systému a formou vypracování metodiky navrhnout opatření pro efektivní implementaci a využívání informačních systémů ve veřejné správě.

Součástí výzkumného problému je i stanovení hypotéz. V závěru jsou výsledky výzkumného šetření porovnávány se stanovenými hypotézami, které jsou potvrzeny, respektive zamítnuty.

Cílem této práce je zejména přispět ke zlepšení stavu řešené problematiky – efektivnost informačních systémů veřejné správy České republiky. Výsledkem práce je teoretická a praktická báze využitelná především pro úřady veřejné správy.

ABSTRACT

e-Government is in recent period one of the most discussed themes in relation to public administration. Dissertation thesis deals with effectiveness of information systems that are being implemented in public administration.

Literature research describes information systems usage in public administration. Basic terms, organization of public administration, information systems, valid and planned law measures are defined here. Not missing information about services Czech POINT, electronic signature, long term storage of electronic documents, following aforementioned conversion of documents and it is closed with brief description of e-Government in abroad.

Main aim of the thesis, based on theoretical and terrain research, is to identify and evaluate recent state of information systems in public administration, satisfaction with using them either on side of clerks thus on side of citizen, to identify critical points of usage information systems and in form of procedure to propose measurements for effectiveness implementation and usage of information systems in public administration.

Belonging to research problem is also stating of hypothesises. In the summary are results of research investigation compared with stated hypothesises that are confirmed or denied.

Aim of this work is to contribute to improve state of solved theme – effectiveness of information systems in public administration of Czech Republic. Result of this work is theoretical and practical base utilizable foremost for bureaus of public administration.

OBSAH

SEZNAM OBRÁZKŮ, GRAFŮ A TABULEK

SEZNAM ZKRATEK

CA	-	Certifikační autorita
ČÚZK	-	Český úřad zeměměřičský a katastrální
FIS	-	Finanční informační systém
GIS	-	Geografický informační systém
HW	-	Hardware – technické vybavení počítače
ICT	-	Informační a komunikační technologie
IS	-	Informační systém
ISVS	-	Informační systémy veřejné správy
IT	-	Informační technologie
KN	-	Katastr nemovitostí
MF	-	Ministerstvo financí
MI	-	Ministerstvo informatiky
MPO	-	Ministerstvo průmyslu a obchodu
MPSV	-	Ministerstvo práce a sociálních věcí
MSMT	-	Ministerstvo školství, mládeže a tělovýchovy
MSp	-	Ministerstvo spravedlnosti
MV	-	Ministerstvo vnitra
MZe	-	Ministerstvo zemědělství
MZV	-	Ministerstvo zahraničních věcí
MŽP	-	Ministerstvo životního prostředí
RES	-	Registr ekonomických subjektů
RN	-	Registr nemovitostí
ROB	-	Registr obyvatel
ROS	-	Registr osob
RPP	-	Registr práv a povinností
RÚI	-	Registr územní identifikace
SGI	-	Soubor grafických informací
SPI	-	Soubor popisných informací

SW - Software – programové vybavení počítače
ÚIR - Územně identifikační registr
VIS - Vnitřní informační systém
VS - Veřejná správa
VÚSC - Vyšší územní samosprávné celky
ZoEP - Zákon o elektronickém podpisu

SEZNAM ZÁKLADNÍCH POJMŮ

Atest – úřední doklad osvědčující kladný výsledek atestace.

Atestace – stanovení způsobilosti pro použití v informačních systémech veřejné správy na základě shody se stanovenými standardy, technickými normami, požadovaným stupněm bezpečnosti nebo na základě dosažení vyšší úrovně technických a užitných vlastností než požadují standardy a technické normy. Podle zákona o ISVS stanovuje tuto způsobilost nezávislé atestační středisko.

Atestační středisko – právnická nebo fyzická osoba provádějící atestace na základě pověření k výkonu atestací uděleného MIČR. Pracuje na základě smlouvy uzavřené s žadatelem o atestaci a za úhradu. V současnosti je na trhu deset společností pověřených k výkonu atestací.

Czech POINT – Český Podací Ověřovací Informační Národní Terminál, slouží jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby „*obíhala data, ne občan*“.

Číselník – seznam přípustných hodnost datového prvku obvykle ve formě dvojic, to znamená kódového údaje a hodnoty jeho kódu.

Dálkový přístup – přístup do informačního systému prostřednictví telekomunikačního zařízení (například prostřednictvím sítě Internet).

eGON – oranžový panáček, který symbolizuje moderní pojetí e-Governmentu v České republice.

e-Government – nová podoba veřejné správy fungující lehce, rychle a levně, a to nejen uvnitř, ale především ve vztahu k veřejnosti. Díky zapojení informačních a komunikačních technologií má být veřejná správa výkonnější, otevřenější a přívětivější ke svým uživatelům.

Elektronická podatelna – pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv.

Elektronická značka – obdoba zaručeného elektronického podpisu, elektronickou značkou však může k označení dat použít i právnická osoba nebo organizační složka státu, a to automatizovaně. I elektronická značka je založena na kvalifikovaném certifikátu.

Informační systém – funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností.

Informační systémy veřejné správy (ISVS) – jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů (o státní statistické službě, živnostenský zákon, o veřejném zdravotním pojištění, obchodní zákoník, o správě daní a poplatků).

Kvalifikované časové razítko – důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem.

Kvalifikovaný certifikát – datová zpráva, která je vydána kvalifikovaným poskytovatelem certifikačních služeb (na trhu v současnosti tři konkurující si subjekty, a to První certifikační autorita, Česká pošta, eIdentity). Spojuje data pro ověřování elektronických podpisů s podepisující resp. označující osobou a umožňuje ověřit její identitu.

Orgány veřejné správy – jsou ministerstva, jiné správní úřady, orgány územní samosprávy a další státní orgány (prosím o konkretizaci orgánů a úřadů).

Označující osoba – fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou.

Podepisující osoba – fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby. Nejčastěji občan nebo zaměstnanec orgánu veřejné správy.

Portál veřejné správy – informační systém vytvořený a provozovaný se záměrem usnadnit veřejnosti dálkový přístup k pro ni potřebným informacím z veřejné správy.

Provozní informační systém – informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku a nesouvisející bezprostředně s výkonem veřejné správy. Na provozní informační systémy se zákon o ISVS nevztahuje.

Provozovatel ISVS – subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje.

Správce ISVS – subjekt, který určuje účel a prostředky zpracování informací a za informační systém odpovídá. Jsou to ministerstva, jiné správní úřady, orgány územní samosprávy a další státní orgány (souhrnně nazývané „orgány veřejné správy“).

Standard ISVS – soubor pravidel pro výkon odborných činností spojených s vytvářením, rozvojem a využíváním informačních systémů veřejné správy uveřejněný ve Věstníku MIČR.

Uživatel – osoba nebo organizace, která používá provozovaný systém k vykonávání specifické funkce.

Veřejný informační systém – informační systém vedený správci ISVS nebo jiný informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy.

Základní registry – mají zabezpečit dostupnost základních zdrojů dat v soustavě informačních systémů veřejné správy:

- registr obyvatel,
- registr osob,
- registr územní identifikace, adres a nemovitostí,
- registr práv a povinností.

Zaručený elektronický podpis ("e-podpis") – elektronický podpis, který je jednoznačně spojen s podepisující osobou a umožňuje její identifikaci. Podepisující osoba ho může udržet pod svou výhradní kontrolou a je k datové zprávě připojen tak, že je možno zjistit jakoukoliv následnou změnu zprávy. Je určen pouze fyzickým osobám. V praxi se používá při komunikaci občana s orgánem veřejné správy, přičemž "e-podpisem" musejí být vybaveny obě strany – jak občan, tak příslušný úřad prostřednictvím svého zaměstnance. Je založen na kvalifikovaném certifikátu.

ÚVOD

Motto: „*Cílem a prioritou je „profit občanů“ a jejich společenství, nikoliv pouhé řešení informačního systému!“*

Pro vývoj současné „informační společnosti“ je charakteristický vzrůstající význam špičkových moderních technologií ve všech oblastech lidského života. Informace jsou hybnou silou a jejich efektivní využívání je předpokladem orientace a úspěchu moderní společnosti na počátku 21. století. Informace jsou a budou zbožím. Dokonalé zvládnutí způsobu jejich zpracování a využití se stává konkurenční výhodou.

Informační systémy veřejné správy (ISVS) jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů.

Informační systém je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností [15].

Důvody volby tématu disertační práce

Důvody volby mého tématu disertační práce jsem se pokusil shrnout do následujících bodů, které ovlivnily zaměření mé disertační práce:

- ***Aktuálnost*** – pojem e-Government a ISVS jsou v posledních dnech stupňován v každém pádu. Není ani divu, protože před nedávnem procházel návrh zákona o e-Governmentu poslaneckou sněmovnou, kde prošel jednotlivým čtením, ale parlament jej vrátil s určitými výhradami zpět k přepracování.
- ***Neuniknutelnost*** – toto téma se bez výjimky dotkne každého z nás, protože všichni musíme komunikovat s úřady. Někteří komunikují jednou ročně při podávání daňového přiznání, ale jsou i tací, kteří komunikují s úřady denně, a pro ně je právě e-Government a elektronizace veřejné správy cesta jak ušetřit spoustu času.
- ***Mohutnost (Ohromnost)*** – téma informačních systémů ve veřejné správě není určeno pro jednu disertační práci. Jedná se o neuvěřitelné množství „navzájem“ propojených systémů, díky kterým budeme v budoucnu moci z jednoho místa vyřídit veškerou agendu spojenou

s jednotlivými úřady (ať už se bude jednat o úřad práce, finanční úřad, bytový úřad, evidence vozidel, aj.).

- ***Zkušenosti s informačními technologiemi*** – v neposlední řadě byl důvod mého výběru tohoto tématu v oblibě oboru, kterému se již několik let důkladněji věnuji.

Všechny tyto skutečnosti ovlivnily zaměření mé disertační práce a doufám, že naplním stanovené cíle a práce bude přínosem jak po stránce teoretického poznání, tak po stránce praktického využití.

Při zpracovávání disertační práce budou analyzovány a zpracovány literární zdroje, provedena literární rešerše, na základě které budou definována teoretická východiska pro výzkumnou část disertační práce. Následně budou stanoveny hypotézy výzkumu a identifikována metodika. V závěru práce bude provedena syntéza přínosů disertační práce v třech základních oblastech - v oblasti vědecké, praktické a pedagogické - a budou formulovány závěry disertační práce.

1 SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Dnes se i v České republice stále častěji setkáváme s pojmem „*informační společnost*“. Jeho původ nacházíme v USA, kde se začátkem 90. let začalo hovořit o informačních dálnicích, globální informační infrastruktuře a následně o informační společnosti.

Ať si pod pojmem informační společnost v detailech představujeme cokoliv, shodně je za její základní charakteristiku považováno to, jak nedocenitelný význam pro život společnosti mají informace. Stávají se surovinou i výrobkem, předmětem průmyslu a obchodu, lze říci, že se život společnosti do jisté míry odhmotňuje.

Dostupnost informací, schopnost lidí je zpracovávat a používat pro rozvoj své osobnosti, při práci, v každodenním životě či správě věcí veřejných je základním kritériem pro to, zda lze konkrétní společnosti dát přívlastek informační v pravém slova smyslu či nikoliv.

1.1 Charakteristika pojmů

1.1.1 Data, informace, znalosti

Pojem informace a informační systém lze jen stěží vysvětlit bez objasnění dalších souvisejících pojmů, kterými jsou data, informace a znalosti. Tím, že je vysvětlím, přispějí k jednoznačnému chápání pojmu „informační systém“ a jeho širších souvislostí.

Daty rozumíme jakékoliv údaje, které mohou být zachyceny na nějakém nosiči. Jednoduché údaje zprostředkované člověku jeho smysly a stroji jeho zařízeními [7].

V kontextu klasické počítačové vědy se pojem data vždy používal jako označení pro čísla, text, zvuk, obraz, popř. jiné smyslové vjemy reprezentované v podobě vhodné pro zpracování počítačem, tj. digitálně [13].

Informace pak jsou data, o kterých se jejich vlastník nebo poskytovatel domnívá, že mohou u příjemce změnit stav jeho poznání nebo uspokojit informační potřebu nebo nárok. Jsou to tedy data s přiděleným významem na základě subjektivního rozhodnutí.

Na otázku, zda záznam uložený ve formě souboru na disku představuje informace nebo data, bychom měli odpovědět, že data. Teprve v okamžiku, kdy tato data začneme zpracovávat a využívat je, stanou se z nich informace. Znalosti (poznání) následně vznikají vyhodnocením informací v lidském vědomí [7].

1.1.2 Informační systém

Informační systém (IS) je systém pravidel, předpisů a způsobů řízení v určité organizaci (včetně systému pravidelných porad, neformálních setkání pracovníků). Koncepce budování IS veřejné správy vymezuje pojem jako funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý IS zahrnuje informace, které jsou uspořádány tak, aby bylo umožněno jejich zpracování a zpřístupnění a nástroje umožňující provádění informačních činností [15].

1.1.3 Informační technologie

Jednotlivé fáze procesu zpracování dat (pořízení, uchování, vlastní zpracování, prezentace, přenos) jsou realizovány a zabezpečovány informačními technologiemi (IT).

Platí, že informační technologie se rozdělují na části:

- technické prostředky (HW)
- programové prostředky (SW)

1.1.4 Informační a komunikační technologie

Pojem informační systém je definován mnoha způsoby. Odhlédneme zde od definic teorie informace, informační vědy i informatiky a vyjděme z definice, se kterou pracuje náš právní řád. Mám na mysli citaci dle zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (novější zákony a materiály ji přebírají nebo se na ni odkazují):

"Informačním systémem se rozumí celek zabezpečující cílevědomé a systematické shromažďování, zpracovávání, uchovávání a zpřístupňování informací. Každý informační systém podle této definice zahrnuje informační základnu, technické a programové prostředky, technologie a procedury a pracovníky."

Význam existence a respektování definovaných procedur pro získávání, ukládání, využívání, archivaci/zálohování dat roste s velikostí provozovaného informačního systému a s mírou heterogenity a komplexnosti prostředí, ze kterého jsou zdrojová data do systému pořizována. Konečným a limitujícím faktorem úspěchu každé technologie a nástroje, nejen informačních a komunikačních technologií a systémů, je lidský faktor. Není-li nástroj, jakkoli dokonalý, přijat subjektem, pro který je určen (u informačních systémů pro veřejnou správu je potřeba brát v úvahu dvě skupiny subjektů, úředníky veřejné správy a občany), zůstávají potenciální přínosy nevyužity.

1.1.5 Efektivnost IS/IT

Na efektivnost se můžeme dívat z několika pohledů. Nejčastěji hledáme odpověď na otázku: „*Jak máme řídit rozvoj IS/IT, abychom s danými omezenými výdaji dosahovali co nejvyšších přínosů pro organizaci?*“ „*Jaké mají být vstupy (výdaje a hodnoty faktorů), abychom dosáhli požadovaných přínosů?*“ Odpovědi na tyto otázky je třeba hledat jak na straně vstupů, které by měly být pro dosahování efektivnosti minimalizovány, tak na straně výstupů, které by měly být samozřejmě maximalizovány. Rozhodující je pak hledání hodnot faktorů ovlivňujících tuto transformaci [11].

Efektivnost ISVS

Tento pohled je důležitý i ve veřejné správě, ale je třeba se na úspěšnost implementace a celkovou efektivnost ISVS podívat také z pohledu občana. Z tohoto pohledu bychom měli efektivnost ISVS hodnotit kladnými odpověďmi na následující otázky:

- Cítí občan podstatné zlepšení a zjednodušení komunikace se státní správou při řešení každodenních životních situací?
- Umožnily ISVS občanovi, aby poskytoval státní správě všechny vyžadované informace pouze jednou a pohodlně nebo musí tutéž informaci poskytovat vícekrát různým úřadům?
- Využívá občan nabízené služby spontánně nebo ho odrazují neodstraněné překážky?
- Má občan stejnou (ne-li větší) důvěru v elektronickou formu komunikace se státem ve srovnání s klasickou „papírovou“ formou?
- Došlo v souvislosti se zavedením e-Governmentu k výrazné redukci administrativních nákladů na výkon veřejné správy?
- Naplnila se vize „*Obíhají data, nikoli občan*“?

1.1.6 Zákon 365/2000 Sb., o informačních systémech veřejné správy

Zákon o informačních systémech veřejné správy stanoví práva a povinnosti osob související s vytvářením, užíváním, provozem a rozvojem ISVS. Níže jsou uvedeny některé důležité pojmy.

Základní pojmy zákona o ISVS

Informační činností se rozumí získávání a poskytování informací, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče, uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat

ukládaných na hmotných nosičích. Je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků.

Informačním systémem se zde rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý IS zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností. ISVS jsou souborem IS, které slouží pro výkon veřejné správy.

Referenčním, sdíleným a bezpečným rozhraním ISVS je souhrn právních, technických, organizačních a jiných opatření vytvářejících jednotné integrační prostředí ISVS, které poskytuje kvalitní soustavu společných služeb.

Sdílením dat se rozumí umožnění přístupu (tj. poskytování příslušné služby) k daným datům prostřednictvím referenčního rozhraní více subjektům současně.

Atestace IS je stanovení jejich způsobilosti pro použití v ISVS na základě shody se stanovenými standardy, technickými normami a požadovaným stupněm bezpečnosti [19].

1.1.7 Zákon 227/2000 Sb., o elektronickém podpisu

Prvním platným zákonem o elektronickém podpisu se stal UTAH Digital Signature Act. To bylo v roce 1995. V Evropě směřoval rozvoj legislativy ke standardizaci, která se promítla do lokálních zákonů. Státy Evropské unie pochopily nezbytnost jednotného přístupu k řešení elektronického podpisu zejména v návaznosti na elektronický obchod na společném trhu. Výstupem byl dokument dodnes prakticky závazný pro členské státy EU, kterým je směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999.

Transformace požadavků směrnice do právních norem jednotlivých států byla realizována několika způsoby. Tím nejrozšířenějším je vydání zákona o elektronickém podpisu jako samostatné právní normy. Touto cestou se vydala i Česká republika, kde byl zákon o elektronickém podpisu (ZoEP) přijat v roce 2000 a ČR se tak stala třetí zemím, kde vstoupil v platnost zákon upravující užívání elektronického podpisu.

Základní pojmy zákona o elektronickém podpisu

Zákon o elektronickém podpisu definuje elektronický podpis jako „údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“, což je v podstatě rozšířená

definice daná směrnicí. Běžný elektronický podpis je řešení vhodné pro jednoduché aplikace nebo pro uzavřené systémy.

Vyšší formou elektronického podpisu je zaručený elektronický podpis. ZoEP říká, že: „Zaručeným elektronickým podpisem je elektronický podpis, který splňuje následující požadavky:

1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat“ [18].

1.2 Organizace veřejné správy v České republice

Kategorizace informačních systémů ve veřejné správě je komplexní problematikou zasluhující si detailní studium. Jejich zefektivnění pomocí technologických a softwarových komponentů (nazývaných počítačově orientované IS) nám nepřinese požadované výsledky bez bližšího seznámení se základními principy, organizací a členěním orgánů veřejné správy.

Dostávám se k vymezení pojmu veřejná správa a pojmům souvisejícím s cílem mé práce. Jednoznačné a stručné vymezení tohoto pojmu je obtížné, protože existuje několik pohledů na náplň a uspořádání veřejné správy v ČR.

Veřejnou správu nelze vnímat pouze jako mechanický součet nebo sumu jednotlivých orgánů a institucí, je třeba brát v úvahu stávající vazby mezi těmito institucemi a nahlížet na veřejnou správu jako na systém nebo komplex institucí a vazeb mezi nimi.

Pro potřeby práce a pro zjednodušení veřejnou správou nazývám soustavu veřejnoprávních institucí (VPI) a procesů, které probíhají uvnitř těchto VPI, mezi VPI navzájem, a to po vertikální i horizontální ose a mezi VS a veřejností.

1.2.1 Veřejná správa v České republice z organizačního hlediska

Veřejnou správu podle jednoho z možných výkladů lze chápat jako správu veřejných záležitostí ve veřejném zájmu [9]. Veřejnou správu vykonávají (až na výjimky) [1]:

- orgány státu,
- orgány územní samosprávy.

Z hlediska organizačního náleží pod pojem veřejné správy pouze takové orgány a instituce, pro které tvoří výkon veřejné správy hlavní nebo alespoň

podstatnou součást jejich činnosti. Na ostatní orgány a instituce vykonávající veřejnou správu se vztahují pravidla charakteristická pro veřejnou správu pouze při výkonu činnosti veřejné správy samotné, jejich ostatní vztahy jsou výkonem veřejné správy ovlivněny jen minimálně nebo vůbec ne [9].

Státní správa

Státní správa má vždy povahu veřejné správy, lze ji považovat za základní druh veřejné správy. Podstatným charakteristickým rysem je jednotná úprava výkonu pro celé území státu daná zákonem. Nositelem správy je v tomto případě stát a vykonavateli jsou orgány státu [1].

Na první pohled se může zdát, že tímto základem by měla být samospráva vzhledem ke svému bezprostřednímu odvození od občanů. Celý pohled je však složitější v důsledku omezení samosprávy vždy pouze na určité územní, zájmové nebo jinak definované společenství. Pojem samosprávy v jeho obvyklém používání neobsahuje samosprávu na úrovni státu jako celku. Státní správa plní především dvě základní funkce. První z těchto funkcí je aplikace zákonů, druhou je provádění státní politiky a sledování státních zájmů [9].

Státní správu je možné členit podle řady kritérií, základním členěním podstatným pro pochopení uplatňovaného modelu v České republice je členění na ústřední státní správu (ministerstva a ústřední správní úřady) a státní správu v území (speciální správní úřady).

Samospráva – povaha a funkce

Pro samosprávu je charakteristická demokratičnost ve vytváření základních samosprávných orgánů.

Samosprávný orgán disponuje autonomií při svém rozhodování, jeho rozhodnutí je zpravidla konečné. V samosprávě neexistuje vertikální hierarchická struktura, a to nejen ve vztahu samosprávy k orgánům státu, ale ani v rámci samosprávy samotné. Nižší samosprávný organ není podřízen vyššímu.

Funkcí samosprávy je především spravování záležitostí určitého společenství, jeho reprezentace a vyjadřování zájmů tohoto společenství, a to s účastí všech členů příslušného společenství [9].

Působnost orgánů veřejné správy

Výše uvedené charakteristiky se vztahují k výkonu vlastní samosprávy čili k tzv. samostatné působnosti. Mezi ty patří zejména:

- schvalování programu územního obvodu obce a provádění kontroly jeho plnění,
- hospodaření s majetkem obce,
- sestavování rozpočtu obce, hospodaření podle něj a vyúčtování hospodaření obce za uplynulý kalendářní rok,
- zakládání a zřizování právnických osob a zařízení, popřípadě jejich rušení,
- vydávání obecně závazných vyhlášek ve věcech patřících do samostatné působnosti,
- stanovení druhů místních poplatků a jejich sazeb podle zvláštního zákona,
- rozhodování o vyhlášení místního referenda a realizace jeho výsledků,
- úkoly v oblasti školství, sociální péče, zdravotnictví a kultury, s výjimkou výkonu státní správy,
- správa, údržba a provozování zařízení sloužících k uspokojování potřeb občanů, jsou-li ve vlastnictví obce,
- místní záležitosti veřejného pořádku a zřizování obecní (městské) policie, s výjimkou rozhodování o přestupcích,
- čistota obce, odvoz domovních odpadků a jejich nezávadná likvidace, zásobování vodou, odvádění a čištění odpadních vod.

Podstatným charakteristickým rysem státní správy je jednotná úprava výkonu na celém území státu daná zákonem. Nositelem správy je v tomto případě stát a vykonavateli jsou orgány státu [2].

Spojený model výkonu veřejné správy

Státní správu na určitém území mohou vykonávat rovněž orgány územní samosprávy. V tomto případě jde o tzv. přenesenou působnost uplatňující odlišná pravidla.

V České republice byl zvolen tzv. spojený model veřejné správy, tzn. že obce a kraje vykonávají vedle samostatných působností také státní správu v přenesené působnosti [2].

V ČR bylo k 1. 1. 2007 celkem 6 249 obcí [21], z tohoto počtu 393 obcí s tzv. pověřeným obecním úřadem. Na ně je delegován zvláštními zákony výkon státní správy v přesně vymezených oblastech. V těchto obcích působí rovněž stavební úřad nebo matriční úřad (tyto úřady působí ovšem i v dalších obcích). Zákonem č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností byl definován nový typ obcí, tzv. obce s rozšířenou působností. Obce s rozšířenou působností jsou obcemi, na které byla přenesena velká část kompetencí okresních úřadů, které 31. 12. 2002 ukončily svoji

činnost. Namísto 76 okresních úřadů vzniklo k 1. lednu 2003 celkem 205 obcí s rozšířenou působností [1].

Obce s rozšířenou působností vykonávají státní správu v přenesené působnosti, kde se v prvé řadě jedná o následující potřebné agendy:

- evidence obyvatel,
- vydávání cestovních a osobních dokladů,
- vydávání řidičských průkazů, technických průkazů, evidence motorových vozidel,
- živnostenských oprávnění,
- výplata sociálních dávek,
- sociálně právní ochrana dětí,
- péče o staré a zdravotně postižené občany,
- vodoprávní řízení, oblast odpadového hospodářství a ochrany životního prostředí,
- státní správa lesů, myslivosti a rybářství,
- oblast dopravy a silničního hospodářství.

1.2.2 Územní samospráva v České republice

Územně správní uspořádání je vyjádření způsobu, jakým je stát z administrativního hlediska rozdělen na jednotky, v nichž je vykonávána veřejná správa.

Území ČR se dělí na obce, okresy a kraje. Základními administrativními jednotkami jsou obce. Nejvyšší správní jednotkou jsou kraje. V obcích a krajích je příslušnými orgány vykonávána státní správa a samospráva [10].

Ústavní základy územní samosprávy

Ústavní zakotvení územní samosprávy nalezneme v ústavním pořádku ČR, zejména v pak Ústavě ČR [16] a Listině základních práv a svobod [17]. Čl. 8 Ústavy výslovně uvádí, že se zaručuje samospráva územních samosprávných celků. Bližší vymezení územní samosprávy na ústavní úrovni pak představuje hlava sedmá Ústavy ČR označená pojmem Územní samospráva. Zdůrazním zejména následující:

- Česká republika se člení na obce, které jsou základními územními samosprávnými celky, a kraje, které jsou vyššími územními samosprávnými celky,
- územní samosprávné celky jsou územními společenstvími občanů, která mají právo na samosprávu.

Klasifikace krajů

Ústavním zákonem č. 347/1997 Sb., o vytvoření vyšších územních samosprávných celků (VÚSC) vzniklo k 1. 1. 2000 14 VÚSC: Hlavní město Praha, Středočeský kraj (Praha), Jihočeský kraj (České Budějovice), Plzeňský kraj (Plzeň), Karlovarský kraj (Karlovy Vary), Ústecký kraj (Ústí nad Labem), Liberecký kraj (Liberec), Královéhradecký kraj (Hradec Králové), Pardubický kraj (Pardubice), Vysočina (Jihlava), Jihomoravský kraj (Brno), Olomoucký kraj (Olomouc), Moravskoslezský kraj (Ostrava) a Zlínský kraj (Zlín). Jména krajů jsou uvedena ve znění po novelizaci ústavního zákona v roce 2001, v závorce je vždy uvedeno sídlo kraje.

Zákon č. 129/2000 Sb., o krajích (krajské zřízení) definuje kraj jako územní společenství občanů, jemuž náleží právo na samosprávu. Kraj je veřejnoprávní korporací, má vlastní majetek. Kraj je spravován zastupitelstvem kraje, dalšími orgány, jsou rada kraje, hejtman kraje a krajský úřad.

Obr. 1 - Mapka členění ČR na kraje [34]

Klasifikace obcí

Podle zákona č. 128/2000 Sb., o obcích (obecní zřízení) je obec samosprávným společenstvím občanů; tvoří územní celek, který je vymezen hranicí území obce. Každá obec má svůj název (ke změně dává souhlas Ministerstvo vnitra na návrh obce). Obec je veřejnoprávní korporací, má vlastní

majetek. V právních vztazích vystupuje svým jménem a nese odpovědnost z těchto vztahů vyplývající.

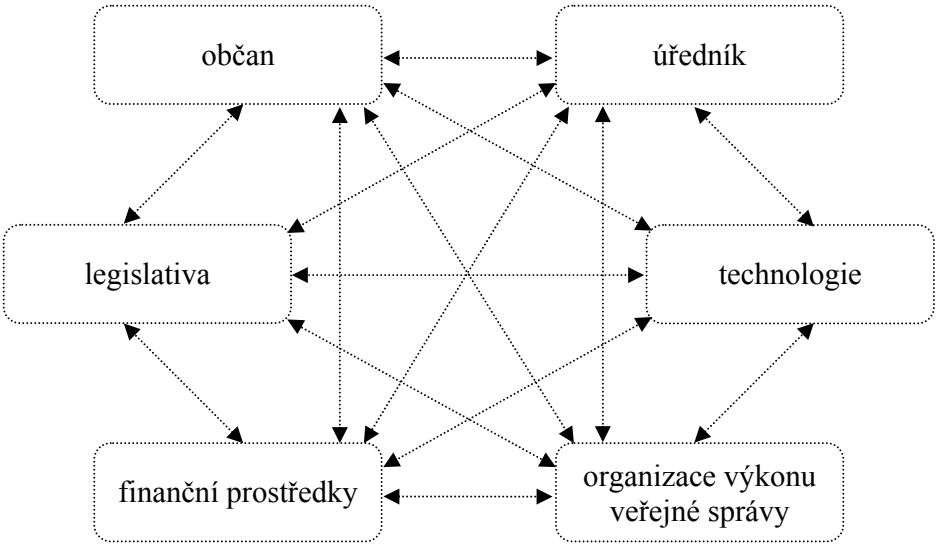
Obec je spravována zastupitelstvem obce, další orgány obce jsou rada obce, starosta, obecní úřad a zvláštní orgány obce. Obec spravuje své záležitosti samostatně (samostatná působnost). Statní orgány a orgány krajů mohou zasahovat do samostatné působnosti jen vyžaduje-li to ochrana zákona a jen způsobem, který zákon stanoví.

Obce mají všechny samosprávné uspořádání, mají základ v samostatné působnosti, ale z hlediska postavení v přenesené působnosti se liší:

- obce základní – mají rozsah výkonu státní správy, který přísluší všem obcím (6249),
- obce s matričním úřadem (900),
- obce se stavebním úřadem (772),
- obce s pověřeným obecním úřadem (393),
- obce s rozšířenou působností – výkon státní správy ze zrušených okresních úřadů (205),
- obce s magistráty – Brno, Plzeň, Ostrava – zůstaly jim všechny kompetence, které náležely okresním úřadům,
- Praha – zvláštní postavení obce a kraje současně.

1.2.3 Strategické a koncepční záměry modernizace orgánů veřejné správy

Následující kapitola shrnuje základní myšlenky, které jsou uplatňovány nejen ve strategických a koncepčních záměrech modernizace orgánů veřejné správy, ale je snahou tyto ideje zahrnout v každém realizačním kroku. Na veřejnou správu pohlížíme jako na systém znázorněný hexagonem veřejné správy.



Obr. 2 - Hexagon veřejné správy [vlastní zpracování]

Každý z šesti vrcholů hexagonu přímo ovlivňuje ostatní vrcholy a pro zajištění efektivního fungování veřejné správy proto musíme vidět, že kvalitu veřejné správy ovlivňují – legislativa, občan, úředník, technologie, finanční prostředky a také samotná organizace výkonu veřejné správy. Možnost a potřeba systémového zlepšení fungování veřejné správy, budování tzv. Smart administration znamená zabývat se programově všemi těmito vrcholy symbolického hexagonu. Každý krok či prvek v kterékoliv z uvedených oblastí je třeba chápat v kontextu vztahů všech těchto oblastí.

Souběžně s těmito klíčovými projekty je samozřejmě třeba řešit řadu souvisejících projektů a aktivit, které jsou přímo navázány na vrcholy zmíněného hexagonu veřejné správy. Jenom pro ilustraci tak rozsáhlého komplexu úkolů mohu uvést např. v oblasti legislativy potřebu provedení komplexní analýzy existující legislativy z hlediska nutnosti odstranit nadbytečnou administrativní či regulační zátěž. To představuje dále povinnost vyhodnocovat při návrhu nových legislativních aktů komplexní administrativní, ekonomické, sociální i environmentální dopady. Jedná se o použití metody RIA. Občany je nutno stále více zapojovat do procesu přípravy vládních i legislativních dokumentů, včetně možnosti uplatnění elektronických připomínkových řízení.

U úředníků je třeba intenzivně bojovat proti korupci, starat se o trvalé zvyšování jejich kvalifikace, včetně využívání e-learningu, prosazovat etický kodex úředníka veřejné správy. V oblasti technologií, s podporou zmíněných legislativních úkonů a zejména s plným nasazením systému základních registrů veřejné správy, je nezbytné pečlivě vybírat úkony vhodné k elektronizaci a zavádět plně elektronizovaný výkon vybraných agend. Je nutné vytvářet podmínky pro odstraňování duplicit či multiplicit v informační podpoře výkonu jednotlivých agend veřejné správy a využívat prvky integrace a interoperability dat, informací i informačních systémů. V oblasti finančního zabezpečení je potřebné vyřešit problematiku adekvátních nákladů na výkon jednotlivých agend, trvalým hledáním cesty k úsporám, k vyšší transparentnosti vynakládání prostředků na informatizaci. Nemalá očekávání jsou ve vztahu k čerpání finančních prostředků z fondů EU, pro tzv. Smart Administration zejména z IOP [6].

1.3 Informační systémy ve veřejné správě (ISVS)

Nové technologie jsou příležitostí pro vytváření moderní a efektivní veřejné správy, která nabízí nové nebo zlepšené služby, jež jsou výsledkem reformy dosud užívaných postupů. Veřejná správa je rovněž významný účastník na trhu, který podporuje jak vývoj, tak poptávku po produktech a službách v oblasti ICT.

Služby veřejné správy musí být pro uživatele jednoduché a musí být dostupné všem, tedy i handicapovaným či jinak znevýhodněným skupinám obyvatel. Moderní veřejné služby musí vycházet z potřeb svých zákazníků, tj. občanů a podnikatelů. Při využívání ICT musí být zamezeno zneužívání citlivých informací a je třeba důsledně dbát na ochranu osobních údajů [31].

ISVS jsou informační systémy, které jsou definovány zákonem č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů. § 3 odst. 1 výše uvedeného zákona vymezuje ISVS jako „*soubor informačních systémů, které slouží po výkon veřejné správy*“.

Dříve, než se dostaneme k podstatě toho, co je a co není ISVS, je zapotřebí říci, proč je rozdíl mezi informačním systémem a ISVS tak důležitý. Rozdíl spočívá pouze v tom, zda konkrétní informační systém bude spadat pod zákon č. 365/2000 Sb. či ne. Vzhledem k zákonným požadavkům na ISVS je zde rozdíl v dokumentaci, komunikaci a správě informačního systému. Zákon č. 365/2000 Sb. je často používán i jako podmínka veřejných zakázek právě z toho důvodu, že definuje náležitosti komunikace ISVS a jeho dokumentace, přičemž příslušný úřad se těmito technickými náležitostmi dále nezabývá.

Za ISVS můžeme u orgánu veřejné správy označit následující informační systémy:

- informační systém, o kterém zákon (který stanovuje požadavky na vznik informačního systému) stanoví, že se jedná o ISVS podle zákona č. 365/2000 Sb.,
- informační systém, který je zákonem označen jako registr, rejstřík nebo evidence,
- informační systém, u kterého je v zákoně uvedeno, že se jedná o ISVS, ale odkaz na zákon č. 365/2000 Sb. není uveden,
- informační systém, který je zákonem stanoven bez označení, že se jedná o ISVS,
- informační systémy, které nejsou upraveny zákonem, ale prostřednictvím nichž orgán veřejné správy vykonává svěřené činnosti.

ISVS je informační systém, který spravuje konkrétní orgán veřejné správy. Je potřeba popsat, jaké požadavky jsou na něj a na orgán veřejné správy kladeny [6].

Informační systém o informačních systémech ve veřejné správě (IS o ISVS)

Orgány veřejné správy musí MVČR v elektronické podobě a bez zbytečného odkladu (tzn. okamžitě s výjimkou záchrany lidských životů, hašení požáru,

poskytování první pomoci atp.) zpřístupňovat informace o jím provozovaných informačních systémech.

IS o ISVS vznikl s jasným cílem pomoci informatikům při tvorbě a vytváření komunikujících informačních systémů.

Přestože je nutné do IS o ISVS zadávat informace i všech ISVS provozovaných orgánem veřejné správy, není celá agenda příliš rozsáhlá. Z více než 95% totiž orgány veřejné správy provozují ISVS, které nekomunikují s jinými ISVS.

Pokud ISVS nekomunikuje podle výše uvedených požadavků, jsou předávané informace omezeny (jméno ISVS, právní základ, cena, správce atp.). Formulář pro vyplnění neobsahuje více než 20 povinných položek. Pokud ovšem ISVS komunikaci provádí, je situace dosti odlišná. Do popředí se dostává pravý účel IS o ISVS, kterým je poskytnutí informací o možnostech připojení a získání volně dostupných dat z ISVS. Pro tyto účely je nutné do ISVS předat datový formát včetně jeho specifikace, model přenosu, údaje o portech jednotlivých služeb a další nezbytné údaje, aby programátoři ostatních ISVS byli schopni s příslušným ISVS realizovat komunikaci [6].

Informační systém o datových prvcích (IS DP)

Je informační systém, který poskytuje informace o datových prvcích informačních systémů veřejné správy; slouží k vyhlašování datových prvků a zveřejňování číselníků. Datové prvky jsou popsány metodickým pokynem pro popis datových prvků ISVS, kde se využívají technologie XML. Pomocí XML schémat je zaručena bezpečná výměna dat pomocí referenčního rozhraní. IS DP umožňuje přístup k informacím o datových prvcích a ve své neveřejné, resp. návrhové části umožňuje oprávněným subjektům přístup pro potřeby vkládání nových objektů standardizace, opravy platných objektů standardizace a umožňuje diskuzi k předkládaným návrhům [24].

Provozní dokumentace

Orgány veřejné správy musí ke všem svým ISVS vést provozní dokumentaci. Tato provozní dokumentace se skládá z následujících dokumentů:

- bezpečnostní politika ISVS,
- bezpečnostní směrnice pro činnost bezpečnostního poradce,
- uživatelská příručka,
- systémová příručka,
- případně jiné důležité provozní dokumenty podle povahy a rozsahu ISVS [31].

1.3.1 Státní informační a komunikační politika

Ministerstvo informatiky vypracovalo a vláda v březnu 2004 schválila strategický a koncepční dokument s názvem Státní informační a komunikační politika – e-Česko 2006. Prioritními oblastmi Státní informační a komunikační politiky jsou:

1. Dostupné a bezpečné komunikační služby
2. Informační gramotnost
3. Moderní veřejné služby on-line
4. Dynamické prostředí pro elektronické podnikání

Aktuální úkoly v této oblasti se soustředí na budování elektronických služeb veřejné správy, pokračování liberalizace sektoru elektronických komunikací, podporu vysokorychlostního přístupu k internetu, pokračování legislativního zakotvení informační společnosti, zvyšování informační gramotnosti občanů a podporu rozvoje elektronického podnikání [31].

1.3.2 eGON – moderní pojetí e-Governmentu

Na jaře letošního roku na mezinárodní konferenci Internet ve státní správě a samosprávě v Hradci Králové ministr Ivan Langer představil eGona – oranžového panáčka, který symbolizuje moderní pojetí e-Governmentu v České republice. eGon je součástí procesu přerodu současné veřejné správy ve veřejnou správu fakticky novou, výrazně efektivnější, transparentnější a samozřejmě, jak by i sám eGon měl svou přívětivou tváří vyjadřovat, také veřejnou správu pro veřejnost, ale také pro pracovníky veřejné správy vstřícnější, přátelštější.

Obr. 3 - Přívětivá tvář veřejné správy - postavička eGON

Je jasné, že pokud má eGon růst a sílit, potřebuje, aby se začaly rozvíjet jeho další funkce, aby se na jeho základní pevnou strukturu začaly napojovat další informační systémy, které jsou již ve veřejné správě funkční a jsou garancí správné cesty k efektivní veřejné správě.

Tlukot jeho srdce se v současnosti zesiluje díky návrhu zákona, kterému zkráceně říkáme „e-Government Act“. Mají se v něm objevit některé základní principy elektronického úřadování, a to zejména ustanovení o autorizované konverzi dokumentu, o zřízení a provozu elektronických datových schránek, o bezvýznamovém identifikátoru. Další podmínkou pro životaschopnost e-Governmentu, vedle již účinného zákona o elektronickém podpisu, je také jednotná, patřičně zabezpečená komunikační infrastruktura (tedy oběhový systém našeho eGona), zajišťující bezpečné propojení nejen mezi orgány veřejné správy navzájem, ale také mezi nimi a veřejností. Je předpokladem pro efektivnější přístup k informacím veřejné správy, ale pouze pro ty subjekty a k těm informacím, pro které má ten který subjekt a konkrétní jednotlivec oprávnění. Mozek eGona nyní již obsahuje návrh zákonné úpravy základních registrů veřejné správy, kterými jsou registr obyvatel, registr osob (všech osob s právní subjektivitou), registr územní identifikace, adres a nemovitostí a registr práv a povinností. V úzké návaznosti na tento zákon bude iniciován legislativní proces přípravy speciálních zákonů pro realizaci všech čtyř jmenovaných základních registrů veřejné správy. Hlavní myšlenkou realizace uvedených registrů je možnost bezpečného sdílení dat orgány veřejné správy pro potřeby všech informačních systémů veřejné správy, v nichž jsou tato data využívána, spolu s umožněním oprávněného přístupu veřejnosti k veřejným datům těchto registrů. Bude také zajištěna rychlá, autorizovaná a bezpečná aktualizace dat, přičemž veškerá data budou pořizována pouze jednou. V provázané soustavě čtyř základních registrů budou veškerá data i ukládána pouze jednou [23].

1.3.3 e-Government – elektronická veřejná správa

Pod pojmem e-Government se skrývají různé úlohy zabývající se elektronizací výkonu veřejné správy. Do velké množiny těchto úloh patří zcela jistě i typy, které se snaží přiblížit veřejnou správu občanovi. A to jednak tak, že občan od orgánů veřejné správy získává požadované veřejně přístupné informace, ale i úlohy, které se zabývají obousměrným tokem informací, tzn. řeší případy, kdy občan od orgánu veřejné správy požaduje konkrétní úkon nebo kdy se občan prostřednictvím elektronické komunikace stává účastníkem správního řízení [2].

e-Government představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.

Hlavním cílem e-Governmentu je zvýšení výkonnosti státní správy, které by mělo přispět především ke zjednodušení činností veřejnosti při styku s veřejnou správou. Cestou k dosažení tohoto cíle je podpora činností správních úřadů při plnění úkolů státní správy a samosprávy vytvořením pravidel komunikačního prostředí odpovídající charakteru a obsahu úloh plněných státními orgány.

Pro správnou funkci e-Governmentu je klíčová účelná elektronizace vnitřních agend ve veřejné správě, neboť jedině taková elektronizace v konečném důsledku umožní veřejnosti volbu lokality a volbu způsobu komunikace s veřejnou správou. Právě elektronizace vnitřních agend veřejné správy je tím nejsložitějším úkolem současného e-Governmentu [28].

Tab. 1 - Zájem uživatelů internetu o e-Government*

v procentech

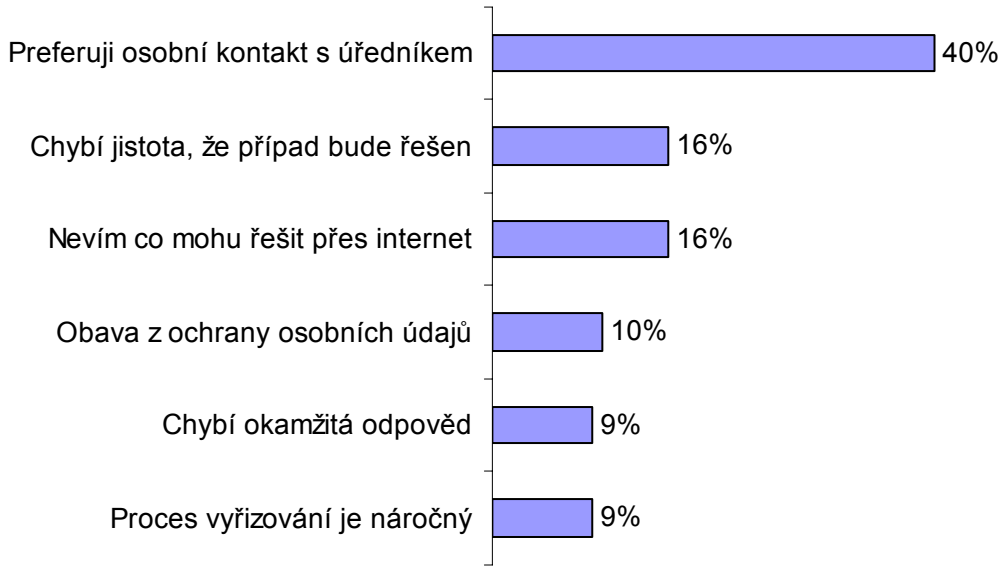
	celkem mající zájem	z toho	
		už někdy využili	**ještě nikdy nevyužili, ale rádi by využili**
celkem 16+	**45,3**	**30,3**	**69,7**
podle pohlaví			
Muži	45,6	33,3	66,7
Ženy	44,8	26,9	73,1
podle věkových skupin			
16-24	38,3	19,5	80,5
25-34	51,1	35,0	65,0
35-44	48,9	31,1	68,9
45-54	44,5	32,8	67,2
55-64	39,5	33,4	66,6
65 a více let	61,0	42,1	57,9
podle typu vzdělání			
Základní	29,0	11,2	88,8
střední bez maturity	32,9	23,6	76,4
střední s maturitou	49,1	28,9	71,1
Vysokoškolské	59,3	43,0	57,0

*Zahrnuje vyřizování osobních záležitostí na úřadech, ve smyslu omezení osobních návštěv, prostřednictvím internetu.

Podíl z celkového počtu uživatelů internetu v dané socio-demografické skupině.

Obr. 4 - Zájem uživatelů internetu o vybrané služby e-Governmentu*

*Podíl z celkového počtu uživatelů internetu, kteří mají zájem o využívání internetu k vyřizování na úřadech



Obr. 5 - Hlavní důvody nezájmu uživatelů internetu o e-Government*

*Podíl z celkového počtu uživatelů internetu, kteří nemají zájem o využívání služeb e-Governmentu

Zdroj: Šetření o využívání ICT v domácnostech, ČSÚ [25]

1.3.4 Sdílení dat a základní registry veřejné správy

Pro veřejnou správu musí platit zásada, že údaje, které již jednou fyzické a právnické osoby jednomu orgánu veřejné správy poskytly, po nich nebude jiný orgán veřejné správy znovu požadovat z jiných důvodů než za účelem odsouhlasení jejich platnosti [3].

Na konci roku 2004 vláda schválila dva klíčové dokumenty, které zahájily rozsáhlé práce na vybudování registrů veřejné správy a zavedení systému sdílení dat ve veřejné správě: věcný záměr zákona o sdílení dat a návrh dalšího postupu budování registrů veřejné správy.

Myšlenka vybudování základních registrů veřejné správy vychází z konsensu přijatého již ve strategickém dokumentu Státní informační politika – cesta k informační společnosti. Tento záměr byl dále rozpracován v dokumentu Koncepce budovaní informačních systémů veřejné správy a potvrzen dokumentem Státní informační a komunikační politika – eČesko 2006 [30].

Primární cíle realizace základních registrů:

- orgány veřejné správy již nebudou od občanů vyžadovat údaje, které budou vedeny v základních registrech,
- tzv. referenční údaje, vedené v základních registrech, budou považovány za důvěryhodné a úřady již nebudou muset jejich správnost a platnost ověřovat; přitom referenčním údajem míníme jedinečný a důvěryhodný údaj vedený v jednom ze základních registrů, který je určen ke sdílení v příslušných informačních systémech veřejné správy podle jasně vymezených pravidel, jejichž dodržování zajistí potřebnou úroveň zabezpečení dat využívaných orgány veřejné správy [24].

Sdílení dat mezi orgány vykonávajícími veřejnou správu spočívá v poskytování nebo předávání údajů z jednoho informačního systému veřejné správy dálkovým přístupem jinému orgánu veřejné správy pro účely výkonu správní činnosti [30].

Za nejdůležitější registry veřejné správy je potřeba vybudovat čtyři základní registry veřejné správy:

- *registr obyvatel*, obsahující základní identifikační a lokační údaje o všech občanech ČR, cizincích s povolením pobytu v ČR a občanech jiných států, vedených v základních registrech (gestor – Ministerstvo vnitra, spolupracují Ministerstvo práce a sociálních věcí a Český statistický úřad),

- *registr osob*, tedy všech ekonomických jednotek s právní subjektivitou, obsahující identifikační a další základní údaje zejména o všech právnických osobách, podnikajících fyzických osobách, organizačních složkách státu a organizačních složkách zahraničních právnických osob (gestor – Ministerstvo spravedlnosti, spolupracují Český statistický úřad a Ministerstvo práce a sociálních věcí),
- *registr územní identifikace, adres a nemovitostí*, zachycující základní identifikační a lokalizační údaje vztahující se k územním prvkům, tedy údaje o objektech v území a jejich vzájemné časové a územní vazby (gestor – Český úřad zeměměřický a katastrální, spolupracují ministerstva vnitra, životního prostředí, zemědělství, pro místní rozvoj a také orgány samosprávy),
- *registr práv a povinností*, uchovávající informace o právech a povinnostech obecně veřejnosti a orgánů veřejné moci, tedy o právech a povinnostech obyvatel i osob; vychází se přitom z právních předpisů, podzákonných norem, samosprávných rozhodnutí, rozhodnutí orgánů veřejné moci a smluv zakládajících určitá práva a povinnosti (gestor – Ministerstvo vnitra, spolupracují všechny ústřední správní úřady i orgány samosprávy).

Podstatná však je také skutečnost, že tyto registry ve své cílové podobě a funkcionalitách musí tvořit jednotný, vzájemně provázaný a ucelený systém, který umožní v jejich klíčové funkci čerpat a sdílet data v dané oblasti z jediného relevantního datového zdroje, spolehlivě a transparentně aktualizovaného, s patřičnou úrovní zabezpečení práce s těmito daty. Tím dojde jednak k významnému zvýšení kvality dat i funkcionalit příslušných informačních systémů, jednak ke značnému zvýšení jejich efektivnosti, a tím k úsporám nemalých finančních prostředků [24].

1.3.5 Pořizování informačních systémů veřejné správy

Dne 1. 1. 2007 vstoupila v účinnost novela zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Důsledkem novelizace je mimo jiné skutečnost, že již není možné požadovat po dodavatelích informačních systémů při vypisování výběrového řízení atestaci podle kteréhokoliv standardu ISVS.

Atestaci dlouhodobého řízení ISVS (navazující na atestaci životního cyklu ISVS) si od 1. 1. 2007 zajišťují přímo orgány veřejné správy a tato atestace se provádí pro všechny jejich informační systémy veřejné správy souhrnně, nikoliv tedy pro jednotlivé informační systémy. Dodavatelé tedy nemají možnost atestaci dlouhodobého řízení zajistit [29].

Atestace ISVS podle zákona č. 365/2000 Sb.

S účinností zákona č. 81/2006 Sb., který novelizuje zákon č. 365/2000 Sb., se od 1. 1. 2007 mění podmínky udělování atestací. Ve smyslu této novely budou atestace pouze stanovovat shodu:

- způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní, nebo
- dlouhodobého řízení informačních systémů veřejné správy s požadavky tohoto zákona a prováděcích právních předpisů k tomuto zákonu [27].

1.3.6 Rada vlády pro informační společnost

O vytvoření Rady vlády pro informační společnost rozhodla vláda svým usnesením z 28. března letošního roku. Tento odborný poradní orgán vlády bude řešit koncepční a koordinační otázky rozvoje informační společnosti.

Rada bude sledovat nejnovější světové trendy v rozvoji informační společnosti a bude poskytovat vládě odbornou vědomostní základnu pro její rozhodování ve věcech informačních a komunikačních technologií a elektronizace veřejné správy [32].

1.3.7 e-Government Act - návrh zákona o e-Governmentu

Hlavní zásada občanského práva:
"Vše je dovoleno, co není výslovně zákonem zakázáno."
Pro chování státních orgánů pak platí zásada opačná:
"Vše je zakázáno, co není výslovně zákonem dovoleno."

Vláda dne 28. února tohoto roku předložila návrh zákona o elektronických úkonech, osobních číslech a autorizované konverzi dokumentů a o změně některých zákonů, pro který se vžil zkrácený název „zákon o e-Governmentu", případně „eGA". Návrh zákona byl zpracován a předložen Ministerstvem vnitra, a to ve spolupráci s Ministerstvem spravedlnosti [35].

Cílem návrhu je především dosažení zásadního zvýšení podílu elektronické komunikace v rámci veškeré komunikace, jejímž alespoň jedním z účastníků je orgán státu. Aby tohoto cíle mohlo být dosaženo, navrhuje se jednotný způsob elektronické komunikace, snadno použitelný, s nízkými náklady pro koncové uživatele.

Hlavními body návrhu je úprava:

- *datových schránek* pro komunikaci s orgány veřejné moci, provádění úkonů (tj. zasílání podání) a doručování dokumentů prostřednictvím informačního systému datových schránek,
- *jednoznačné identifikace subjektů při elektronické komunikaci* – zavedení a sjednocení systému jednoznačné identifikace fyzických osob, právnických osob a orgánů veřejné moci při elektronické komunikaci,
- *autorizované konverze dokumentů* - obousměrná konverze dokumentů, tedy převod dokumentu z listinné podoby do podoby elektronické a naopak; dokumentu, jež je výstupem, se přiznávají stejné právní účinky jako ověřené kopii.

Datové schránky

Cílem zavedení institutu datových schránek pro doručování je přiblížení orgánu veřejné moci občanovi prostřednictvím elektronických nástrojů, zefektivnění komunikace mezi občanem či podnikatelským subjektem a orgánem veřejné moci a komunikace mezi orgány veřejné moci.

Prostřednictvím datové schránky lze činit podání vůči kterémukoliv úřadu. Úřady prostřednictvím datové schránky doručují své písemnosti příslušným adresátům (fyzickým nebo právnickým osobám), stejně jako komunikují s jinými orgány veřejné moci. Veškerým úkonům, které jsou prostřednictvím informačního systému datových schránek činěny, je přiznána ekvivalence k úkonům učiněným písemně.

Bez podání žádosti budou datové schránky zřízeny pro právnické osoby zapsané v obchodním rejstříku, právnické osoby zřízené zákonem, organizační složky podniku, zahraniční právnické osoby zapsané v obchodním rejstříku, advokáty, daňové poradce a insolvenční správce. Pro tyto subjekty bude používání datových schránek povinné. Bez žádosti budou zřízeny datové schránky rovněž všem orgánům veřejné moci (mezi ty patří kromě státních orgánů a samosprávy i státní fondy, zdravotní pojišťovny, samosprávné komory zřízené zákonem, notáři a soudní exekutoři).

Do informačního systému datových schránek se uživatelé přihlašují přístupovým jménem a heslem. Přístupové údaje budou oprávněným osobám doručovány do vlastních rukou, případně bude možné je získat na Czech POINTech. Pro datové schránky fyzických osob může být přihlašování s využitím uživatelského jména a hesla dostačující, ale pro organizace, kterým může zneužitím jejich datové schránky vzniknout vyšší škoda, bude informační

systém datových schránek umožňovat použít pro přihlašování certifikáty veřejného klíče.

Možné použití datových schránek

Povinné:

- pro obousměrnou komunikaci orgánů veřejné moci, tj. mezi sebou navzájem,
- pro komunikaci orgánů veřejné moci vůči právnickým osobám a podnikajícím fyzickým osobám, kterým se zřizuje datová schránka ze zákona, a právnickým nebo fyzickým osobám, kterým byla datová schránka zřízena na základě jejich žádosti.

Nepovinné:

- pro komunikaci právnických a fyzických osob vůči orgánům veřejné moci.

Nelze využít:

- pro komunikaci mezi fyzickými a právnickými osobami.

Pokud je dokument dodán do datové schránky, okamžik doručení nastává přihlášením oprávněné osoby do příslušné datové schránky nebo 10 dnů ode dne, kdy byl do datové schránky dodán (nastává tzv. fikce doručení).

Ministerstvo vnitra připojuje k datovým zprávám odeslaným z datových schránek kvalifikovaná časová razítka vydávaná důvěryhodnou třetí stranou, a tak zajišťuje možnost zjistit, zda byla zpráva změněna a zároveň prokazuje existenci datové zprávy v čase.

Informační systém datových schránek musí reflektovat některé skutečnosti, k nimž v průběhu života osob a institucí dochází. Z toho důvodu je možné, pokud je datová schránka zřízena na žádost, znepřístupnit datovou schránku. Pokud je schránka znepřístupněna, není možné do ní zasílat datové zprávy. Datové schránky jsou znepřístupněny také v případě úmrtí držitele datové schránky, ukončení činnosti podnikající fyzické či právnické osoby, zrušení orgánu veřejné moci, a to do doby, než jsou zrušeny úplně (zrušení nastává za 3 roky).

Jednoznačná identifikace subjektů při elektronické komunikaci

Ministerstvo vnitra bude zajišťovat přidělování osobních čísel identifikujících „držitele“ datové schránky. Na základě dosavadních zkušeností je navrženo využití identifikátoru klienta Ministerstva práce a sociálních věcí. Na rozdíl od

stávající praxe, kdy je toto číslo přidělováno pouze fyzickým osobám, budou jím napříště označovány všechny subjekty, pro které se navrhuje zřizování datových schránek. Osobní číslo bude bezvýznamové a nezaměnitelné s rodným číslem. Kapacita tohoto čísla se jeví jako dostatečná s ohledem na počet subjektů, kterým může být přiděleno, a to minimálně na dobu 500 let. Osobní číslo umožňuje svou konstrukcí provést kontrolu jeho správnosti – poslední číslice je vytvořena jako zbytek po dělení prvních devíti čísel jedenácti.

Autorizovaná konverze dokumentů

Jedním ze zásadních aktuálních problémů veřejné správy je potřeba jednoznačné, podepsané a státem ověřené listiny prokazující určité skutečnosti. Příslušné dokumenty existují převážně v listinné podobě a se stoupajícím podílem elektronické komunikace je nezbytné umožnit jejich konverzi do elektronické formy. Zároveň je nutné počítat s tím, že se stoupajícím podílem elektronické komunikace bude stále více dokumentů existovat v elektronické formě a je nutné vytvořit takové prostředí, aby je v případě potřeby bylo možné konvertovat do listinné formy.

Navrhovaný zákon upravuje obousměrnou konverzi dokumentů, tedy převod dokumentu z listinné podoby do podoby elektronické a naopak. Z důvodu ztráty informací, ke které při takovém konvertování bezpochyby dojde, není přípustné konvertovat dokument, který již jednou konvertován byl. Dokumentu, jež je výstupem, se přiznávají stejné právní účinky jako ověřené kopii.

Autorizovaná konverze má dvě podoby, jednak konverzi z moci úřední, kterou mohou provádět orgány veřejné moci, pokud potřebují dokument převést pro výkon své působnosti, a konverzi na žádost, kterou provádějí za úplatu Czech POINTy. Zákon stanoví podmínky, kdy konverzi nelze provést – u konvertovaných dokumentů z listinné podoby jsou přejaty požadavky ze zákona o ověřování, u konvertovaných dokumentů z elektronické podoby jsou stanoveny některé další podmínky, které vyplývají z technických a bezpečnostních možností. Technické náležitosti provádění konverze, vstupu a výstupu konverze budou stanoveny vyhláškou.

Předpokládaný počátek účinnosti zákona je 1. červenec 2009 [24].

1.3.8 Další připravované zákony

Výčet hlavních zákonů, které vláda připravila či připravuje v rámci zdokonalování komunikace mezi státní správou a občany ČR.

Těmito zákony jsou:

- e-Government Act (podepsán prezidentem 08/08)
- Archivní zákon (připravován do vlády – 06/08)
- Zákon o občanských průkazech (e-OP) (připravován, do vlády - ??)
- Zákon o základních registrech (připravován, do vlády – 09/08)
- Zákon o ROS (o registru osob) (připravován, do vlády – 08/08)
- Zákon o RPP (o registru práv a povinností) (připravován, do vlády – 08/08)
- Zákon o RÚI (registr územní identifikace) (připravován, do vlády – 08/08)
- Zákon o ROB (o registru obyvatel) (připravován, do vlády – 08/08)
- Zákon o e-Sbírce a e-Legislativě (připravován, do vlády – 10/08)
- Zákon o svodu platných právních předpisů (připravován, do vlády – 05/09) [35]

1.3.9 Informační (sub)systémy veřejné správy

V novodobém pojetí VS znamená informační (sub)systém veřejné správy technologicky zajištěné sdílení příslušných informačních bází popisného a prostorového typu uspořádaných do věcných registrů společně se systémovým pohledem na její organizovanost za účelem efektivního podpoření správních procesů.

Příklad informačních (sub)systémů veřejné správy

V této části uvádím příklady věcně příslušných informačních (sub)systémů, které jsou rozloženy přes všechny úrovně VS a které společně s dalšími tvoří základnu faktických (současných) informací pro řiditelnost budoucího žádaného stavu.

Státní informační systém

Státním informačním systémem se rozumí takové zpřístupnění veškerých informací o státní správě pro všechny participující a kooperující VPI, které napomůže zvýšit efektivitu veřejné správy. Způsob poskytování faktických a řídících informací pro účely Státního informačního systému agreguje počítačově orientovanými IS jednotlivé údaje ve formě (on-line) registrů tak, aby místo občana obíhaly mezi veřejnoprávními institucemi elektronické informace [8].

Regionální informační systém

Regionální informační systém (RIS) tvoří mezistupeň mezi státním informačním systémem (SIS) a městským/obecním informačním systémem (MIS). Ve třístupňovém státním uspořádání se středním stupněm (VÚSC) dostává regionální řízení a RIS důležitý význam. Region ovšem nemusí být chápán pouze institucionálně (jako VÚSC), ale také přirozeným způsobem. Přirozené regiony mohou mít také své informační systémy, např. s turistickými, ekonomickými a jinými údaji [8].

Městský informační systém

Je počítačově orientovaný IS podporující jednotlivé informační (sub)systémy založené na souboru popisných a grafických informací (SPI a SGI) na úrovni městského řízení a podporující jednotlivé informační vazby mezi orgány města, veřejnoprávními institucemi a soukromoprávními subjekty. Příkladem MIS mohou být evidence:

- veřejné zeleně,
- veřejného osvětlení,
- územního plánu,
- městského a státního majetku (nemovitosti, lesy, apod.),
- městské dopravní infrastruktury,
- veřejné městské dopravy,
- inženýrských sítí (svodná a vodovodní potrubí, rozvod plynu, telekomunikačních a dálkových kabelů, energetické distribuční sítě a další specifické sítě).

Jak je patrné, jedná se o účelové provázání geografické informace s popisnou informací. Za účelem práce s geografickými informacemi se v 80. letech minulého století objevují tzv. GISy [8].

Geografický informační systém

Používá se pro označení počítačových systémů orientovaných na zpracování geografických dat prezentovaných především v podobě různých map. Výhodou GISů ve srovnání s běžnými mapovými díly je to, že důsledně oddělují obě funkce map - tedy ukládání geografických dat a jejich prezentaci a přidávají ještě další možnosti, jako jsou například prostorové analýzy. Běžné je využití GISů pro potřeby územního plánování, evidence nemovitostí, vyměřování některých typů daní, evidenci všeho druhu, správu majetku, správu dopravní infrastruktury, veřejné městské dopravy, při organizaci požární a záchranné služby, policie, apod. [8].

Vnitřní informační systém

Jak už sám název napovídá, jedná se o podporu procesů probíhajících uvnitř veřejnoprávních institucí (VPI) pomocí specializovaných počítačově orientovaných IS. Informační rozsah a hloubka podpory správních procesů se u VIS liší v závislosti na pozici, velikosti, charakteru a postavení organizace.

Registr obyvatel tvoří základní „stavební kámen“ VIS. Komerčně dostupné VIS využívají agregované údaje kategorizované do čtyř základních skupin. Pro tyto skupiny se vžil název „registry“:

- Registr obyvatel (RO),
- Registr nemovitostí (RN),
- Registr územní identifikace, též nazývaný Územně identifikační registr (RÚI/ÚIR),
- Registr ekonomických činností, nazývaný Registr ekonomických subjektů (REČ/RES).

Tyto registry jsou „stavebními kameny" komerčně dostupných VIS. Mnohé GISy se s jednotlivými „registry“ integrují a vytváří jeden kompaktní celek. Obdobným způsobem dochází též i k jejich integraci s FIS [8].

Finanční informační systém

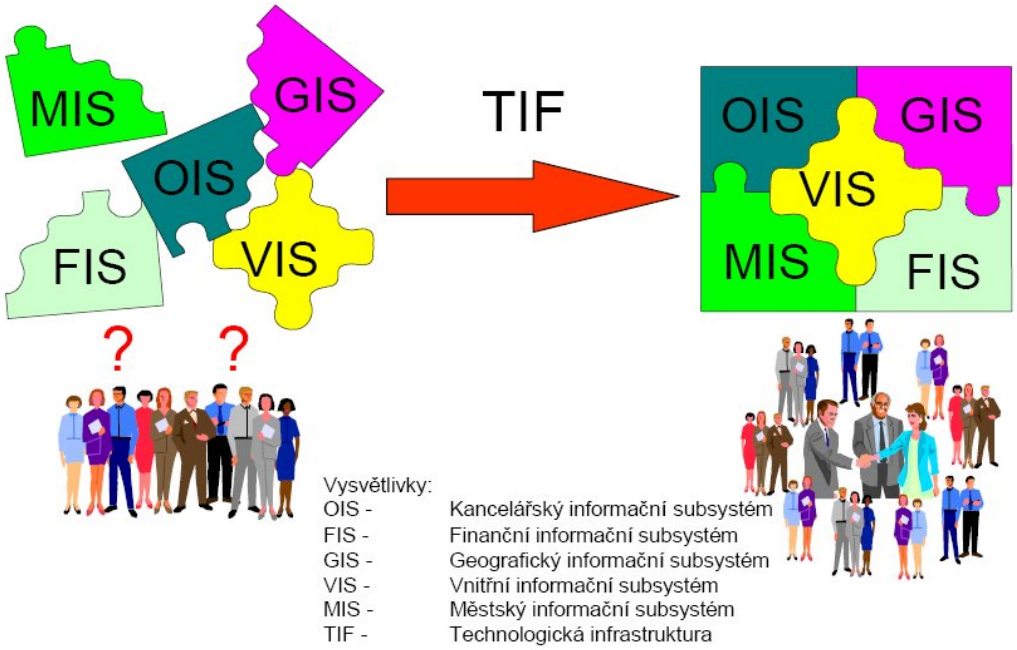
FIS je systém využívající základní „registry“, nad nimiž zajišťuje ekonomickou agendu VPI.

Finanční nástroje FIS jsou používány zejména pro integraci a automatizované zpracování finančních toků z podřízených a kooperujících VPI v oblasti výběru daní, správních poplatků, tvorby a vyvažování rozpočtu a controllingu.

FIS je postaven na základních kamenech – číselnících. Tyto číselníky jsou nositeli stálých nebo velmi málo se měnících informací. Mezi nejznámější doklady patří faktury odběratelské, dodavatelské a s tím úzce související bankovní účty a pokladny [8].

Kancelářský informační systém

Neboli Office Information System označující komerčně dostupné programové prostředky pro podporu administrativních/kancelářských činností, jakými jsou běžná korespondence, tabulkové přehledy/výkazy, sdílení/oběh dokumentů, vnitřní pošta, evidenci úkolů, poznámek, vzkazů pro rychlou informaci [8].



Obr. 6 - Logická provázanost systémů – základ systémové integrace VPI [8]

1.4 Czech POINT

Český Podací Ověřovací Informační Národní Terminál, tedy Czech POINT je projektem, který by měl zredukovat přílišnou byrokracii ve vztahu občan – veřejná správa. V současnosti musí občan navštívit několik úřadů k vyřízení jednoho problému. Czech POINT bude sloužit jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby „*obíhala data, ne občan*“.

Obr. 7 - Logo Czech POINTu

Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho universálního místa, kde bude možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany.

Projekt Czech POINT přináší značné ulehčení komunikace se státem. V některých situacích bude stačit dojít pouze na jeden úřad. V konečné fázi projektu by občan mohl své záležitosti vyřizovat i z domova prostřednictvím internetu [20].

K velmi příznivým podmínkám pro masivní celorepublikový nástup Czech POINTu považuji vládou schválení materiálu, na jehož základě každá obec, která bude od 1. ledna 2008 provozovat Czech POINT, obdrží účelový příspěvek ve výši 50 tisíc Kč na pořízení základního technologického vybavení. Jedná se o příspěvek pro více jak 1300 obcí [23].

1.4.1 Co poskytuje Czech POINT

Czech POINT v současné době poskytuje čtyři druhy výstupů. To znamená, že každý, kdo zaplatí příslušný poplatek na místě Czech POINT, může požádat o následující:

Výpis z Katastru nemovitostí

O výpis z Katastru nemovitostí České republiky může požádat anonymní žadatel. Výpis lze požadovat na základě listu vlastnictví nebo podle seznamu nemovitostí. Pokud žadatel žádá výpis podle listu vlastnictví, musí znát katastrální území a číslo listu vlastnictví. Pokud žadatel žádá o výpis podle seznamu nemovitostí, měl by znát katastrální území a dále buď parcelní číslo požadované nemovitosti, jedná-li se o pozemek, nebo stavební parcelu nebo číslo popisné, jedná-li se o stavbu. I v tomto případě je ověřený výstup zpoplatněn stejně. O výpis lze zažádat i podle seznamu jednotek, v případě že budova je dělena na jednotky, což je typické u větších staveb dělících se na jednotlivé byty, garáže atd. V tomto případě pochopitelně musí žadatel znát nejen popisné číslo domu, ale i přesné číslo bytu v domě.

Výpis z Obchodního rejstříku

O výpis z Obchodního rejstříku České republiky opět může požádat anonymní žadatel. Výpis lze požadovat na základě znalosti IČ obchodní organizace.

Výpis z Živnostenského rejstříku

I v tomto případě může o výpis z Živnostenského rejstříku České republiky požádat anonymní žadatel. Výpis lze požadovat na základě znalosti IČ obchodní organizace.

Výpis z Rejstříku trestů

Podle §11a odst. 1 zákona č. 269/1994 Sb. o Rejstříku trestů v platném znění lze vydat výpis z evidence Rejstříku trestů osobě, které se výpis týká, pouze na základě písemné žádosti. Tuto žádost není třeba ručně vyplňovat, klient ji obdrží vyplněnou k podpisu předtím, než mu je výpis z Rejstříku trestů vydán; tuto žádost úřad archivuje dle zákona. Osoba, které lze na pracovišti Czech POINT výpis vydat, musí mít platný doklad totožnosti a musí mít přiděleno rodné číslo. To znamená, že výpis se může vydat i cizincům, kteří mají například trvalé bydliště v České republice. Od 1. 1. 2008 zatím není možné na pracovištích Czech POINT vydávat výpisy zplnomocněncům, kteří žádají o výpis z Rejstříku trestů na základě plné moci.

V případě, že žádost nemohla být vyřízena elektronicky a musí být manuálně zpracována na pracovišti Rejstříku trestů, musí žadatel o výpis požádat formou papírové žádosti. Systém Czech POINT umožňuje vytisknout žadateli tuto papírovou žádost již předvyplněnou jeho osobními údaji, které sdělil obsluze pracoviště Czech POINT, a žádost úřad pošle ke zpracování na Rejstřík trestů [20].

Kolik tyto výpisy občana stojí?

Cena jako taková je závislá na počtu stran, které jsou pomocí Czech POINTu vydány. Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na 100,- Kč; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na 50,- Kč. Prozatím jedinou výjimkou je výpis z rejstříku trestů, kde je částka stanovena na 50,- Kč za tento výpis.

1.4.2 Bezpečnost Czech POINTu

Vnitro tvrdí, že Czech POINTy jsou bezpečné, experti nesouhlasí. K tomuto tématu jsem vybral názory obou stran. První jsou náměstka ministra vnitra Zdeňka Zajíčka a druhé jsou počítačového experta Davida Baiere.

- Prověrka neodhalila žádné neoprávněné přihlášení do systému Czech POINT, přesto byla přihlašovací hesla některých pracovníků některých úřadů deaktivována, protože nesplňovala zpřísněné bezpečnostní politiky.
- Hesla jsou uložena výhradně v zakryptovaném (nečitelném) formátu.

- Nevyhovující hesla byla odhalena s použitím robotických penetračních testů, které zkoumaly např. shodu uživatelského jména s heslem a jiné běžně zaužívané, a tedy lehce prolomitelné vzorce uživatelského chování při vytváření hesla.
- Pravděpodobnost prolomení přihlašovacího hesla k systému Czech POINT je asi jedna ku biliónu.

- Ochrana postavená pouze na tom, že se úředník přihlásí na internetu pod svým jménem a heslem, je naprosto nedostatečná.
- Úředník má možnost přihlásit se do systému odkudkoliv.
- Prolomení hesla je jen otázkou času. "Tedy pokud není omezený počet pokusů.“

1.4.3 92% aneb jedná se o to nejlepší, co občana na úřadě potkalo

Počátkem března 2008 uskutečnil magazín Egovernment ve spolupráci s Ministerstvem vnitra ČR anketu, kde položili tři základní otázky všem obcím, které v té době provozovaly na svých úřadech Czech POINT. Chtěli tak zmapovat, co pro tyto obce znamenalo zavádění této nové služby, jak by měla být dále rozšiřována a samozřejmě i to, s jakým ohlasem se nabídka setkala u samotných občanů. Ankety se zúčastnilo 174 úřadů.

1) Jaká je vaše dosavadní zkušenost s realizací projektu Czech POINT, především se zaváděním ve vašem úřadu?

Z odpovědí vyplývá, že zavádění Czech POINTu proběhlo vcelku hladce, neboť pouhých 14% našich respondentů pociťovalo při zavádění nějaké problémy. Těmi byla především časová náročnost, když informace přicházely na poslední chvíli, peníze byly přiděleny v prosinci s podmínkou vyúčtování do konce roku. Z technického pohledu pak byly výhrady především k tomu, že v administrátorských návodech byly závažné nedostatky a nebylo vždy jednoduché jim porozumět. Jako problematické je občas vnímáno rovněž to, že zvolené komunikační rozhraní 602XML Filler je určeno pouze pro operační systémy Windows a chybí mu tedy multiplatformnost.

Na druhou stranu 86% odpovědí hovořilo o minimálních problémech (běžných u každého projektu), nebo žádných problémech. Menší obce kvitovaly, že si při zřizování Czech POINTu mohly díky dotaci pořídit pro svůj úřad moderní vybavení.

2) Jakým směrem by podle Vás dále měla směrovat nabídka agend, které bude Czech POINT nabízet?

Odpovědi byly velice podobné od všech úřadů a týkaly se především dvou možností, o které lze rozšířit nabídku Czech POINTu – 36% odpovídajících navrhuje rozšíření o možnost nahlížet do agendy trestných bodů řidiče a 30% navrhuje rozšířit možnosti v oblasti katastru nemovitostí. Systém by podle nich měl umožnit vydat kromě listu vlastnictví také ověřený snímek katastrální mapy, většina klientů potřebuje oba dokumenty současně. U této agendy by řada úřadů ráda zavedla také možnost náhledu výpisu ještě před jeho vytisknutím, aby ještě před zaplacením poplatku mohl občan určit, zda jej opravdu chce. V neposlední řadě by úřady považovaly za rozumné, kdyby došlo ke sjednocení poplatků tak, jak jsou účtovány občanům v případě, že navštíví přímo KN.

3) Jak hodnotí tuto službu klienti vašeho úřadu – jaká je vytíženost vašeho Czech POINTu?

Z pohledu veřejné správy a jejího přechodu k přívětivé a efektivní správě je důležité, že téměř stejná byla u všech úřadů odpověď na poslední otázku. Celkově 92% z nich sdělovalo, že občané službu Czech POINT vítají. Patrně nejpregnantněji to vyjádřil tajemník Městského úřadu Sázava, který nám odpověděl, že občané Czech POINT hodnotí velmi pozitivně, protože nemusí jezdit po všech čertech. Obdobně má starosta města Rakovník odposlechnuto od jednoho z občanů, že se jedná o to nejlepší, co je za posledních X let na úřadě potkalo.

V porovnání jednotlivých agend je největší zájem o výpisy z rejstříku trestů. To je dáno pravděpodobně skutečností, že cena za výpis je stejná, jako když občan žádá přímo rejstřík, avšak z Czech POINTu si odnáší výpis obratem domů bez fronty [26].

1.4.4 Statistiky vydaných výpisů (k 31.8.2008)

Projekt Czech POINT byl spuštěn v testovacím provozu na 37 úřadech veřejné správy po celé České republice. Pilotního projektu se zúčastnily jak velká města, tak i malé obce. Zkušební provoz, kterým se systém dolaďoval, byl ukončen na konci roku 2007 a k 1.1.2008 byl zahájen ostrý provoz systému.

Z 37 kontaktních pracovišť se provoz do dnešních dnů rozrostl na 2320 kontaktních pracovišť. Občané si mohou pro jednotlivé výpisy přijít nyní na 1411 obecních úřadů, 555 poboček České pošty, 298 pracovišť Notářské komory, 49 pracovišť Hospodářské komory či na 7 zastupitelských úřadů ČR v zahraničí [20].

Tab. 2 - Počet vydaných výpisů v jednotlivých měsících [20]

Měsíc	Katastr nemovitostí	Obchodní rejstřík	Živnostenský rejstřík	Rejstřík trestů	Celkový součet
Březen 07	46	92	45	0	183
Duben 07	673	395	142	0	1 210
Květen 07	1 745	922	98	0	2 765
Červen 07	1 748	1 306	46	0	3 103
Červenec 07	1 507	1 342	81	0	2 930
Srpen 07	3 851	3 032	66	0	6 949
Září 07	3 501	3 161	56	0	6 718
Říjen 07	4 942	4 424	82	0	9 448
Listopad 07	5 765	5 090	367	0	11 222
Prosinec 07	4 601	4 381	353	0	9 335
Leden 08	14 634	8 767	642	34 460	58 503
Únor 08	19 556	9 420	413	46 318	75 707
Březen 08	19 273	10 647	354	47 451	77 725
Duben 08	19 569	12 809	402	41 694	74 474
Květen 08	16 916	12 363	334	37 489	67 102
Červen 08	16 948	12 063	426	45 832	75 269
Červenec 08	18 401	12 667	560	50 110	81 738
Srpen 08	17 347	11 488	563	47 069	76 467
Celkem	**171 023**	**114 368**	**5 032**	**350 423**	**640 846**

1.5 Elektronický podpis, elektronická značka, časové razítko

1.5.1 Elektronický podpis

Elektronický podpis je jedním z nástrojů bezpečné elektronické komunikace. Nutnou podmínkou pro praktické využití elektronické komunikace je nastavení takových postupů, přístupů a principů, které bude možné považovat za rovnocenné běžné agendě.

Na základě této úvahy lze v souladu s mezinárodními normami definovat základní bezpečnostní cíle, jejichž plnění by měl důvěryhodný komunikační systém zajistit:

- **důvěrnost informací** – systém musí zabezpečit, že přístup k důvěrným informacím mají pouze určené subjekty (osoby či systémy),
- **integrita** – systém musí zabezpečit informace proti modifikaci,
- **neodmítnutelnost odpovědnosti** – systém musí mít schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za autorství, vlastnictví, odesílání, případně přijetí zprávy.

Tyto bezpečnostní požadavky lze řešit prostřednictvím kryptografických technologií (šifrováním). Elektronický podpis umožňuje zajistit klíčové bezpečnostní atributy spojené s důvěryhodností komunikačních systémů, tedy autentizaci komunikujících stran, průkaznost jejich kroků a integritu přenášených zpráv.

Elektronický podpis (někdy také nazývaný digitální podpis) je v současné podobě zpravidla založen na kombinaci kryptografických metod, z nichž stěžejní je asymetrická kryptografie.

Při zjednodušeném náhledu, teoretickém minimu, můžeme říct, že pro tvorbu elektronického podpisu potřebujeme především šifrovací klíč (často nazývaný soukromý nebo privátní), tedy data pro vytváření elektronického podpisu. Pro ověření tohoto podpisu potřebujeme takzvaný certifikát, elektronický dokument, který bývá považován za obdobu průkazu totožnosti v elektronickém světě [6].

1.5.2 Certifikační autorita, certifikáty

Využití elektronického podpisu je v praxi spojeno s certifikátory. Nedílnou součástí systémů využívajících elektronický podpis a zejména zaručený elektronický podpis je proto poskytovatel certifikačních služeb, vydavatel certifikátů, takzvaná verifikační autorita (CA). Certifikační autorita vystupuje při vzájemné komunikaci dvou subjektů jako třetí, nezávislý a důvěryhodný subjekt, který prostřednictvím jím vydaného certifikátu jednoznačně svazuje identifikaci subjektu s jeho šifrovacími klíči (daty pro vytvoření a ověřování elektronického podpisu) a tím i s jeho elektronickým podpisem.

Certifikáty obsahují ve své nejjednodušší formě data pro ověření elektronického podpisu, identifikaci vlastníka těchto dat a vydavatele certifikátu. Běžné používané certifikáty též obsahují data počátku platností, datum ukončení platnosti, plné jméno certifikační autority, která certifikát vydala, sériové číslo a některé další informace spojené s použitím certifikátu.

Tvorba certifikátu má zpravidla 6 kroků:

1. Generování šifrovacích klíčů a žádosti o certifikát.
2. Příprava identifikačních dat.
3. Předání žádosti o certifikát certifikační autoritě.
4. Ověření informací.
5. Tvorba certifikátu.
6. Předání certifikátu.

Doba platnosti certifikátů je omezená a je uvedena v každém certifikátu. Tato veličina je velmi důležitá. Pokrok ve zvyšování výkonnosti výpočetní techniky a možnost objevení mezer v protokolech nebo algoritmech by ve velkém časovém horizontu mohl způsobit, že by se certifikáty staly nespolehlivými. Běžné certifikáty jsou proto vydávány s platností na jeden rok. I během této doby je možné zrušit platnost certifikátu. Důvodem pro toto opatření může být například obava z vyzrazení dat pro tvorbu elektronického podpisu. Tuto situaci je možné přirovnat ke ztrátě osobních dokladů a následujících procedur s tím spojených.

Většina bezpečnostních technologií, ty založené na certifikátech nevyjímaje, jsou spojeny s konkrétním časem. Například platnost elektronického podpisu je svázána s platností certifikátu, a ta je daná s přesností na sekundy. Nelze tedy v hraničních případech říct, že je podpis platný, aniž bychom uvedli čas, ke kterému se tento stav vztahuje. Ještě větší obtíže mohou nastat, pokud bude třeba podepsané elektronické dokumenty dlouhodobě archivovat. Řešením jsou časová razítka [6].

1.5.3 Časové razítko

Časová razítka mají stejně jako certifikáty oporu v legislativě České republiky a lze se na ně v tomto duchu i odvolat jako na důkaz. Kvalifikované časové razítko nese stejné bezpečnostní atributy jako kvalifikovaný certifikát a lze na něj tedy pohlížet jako na dokument stejně důvěryhodnosti. Klíčovým faktorem této technologie je přesný a garantovaný čas, který je vkládán do časového razítka. Je velice důležité, aby autorita, vydávající časová razítka, mohla průkazným způsobem doložit příslušnou přesnost a synchronizaci časového zdroje, a to i následně [6].

1.5.4 Ochrana osobních údajů

Z historického hlediska se ochraně osobních údajů přílišná pozornost nevěnovala. Dokud se obrovská množství dat uchovávala v kartotékách, byla jen minimální šance na jejich odcizení nebo zneužití. Pak přišla na řadu databáze a elektronická data. Spolu s tím přišla potřeba zajistit bezpečnost těchto informací.

V dnešní době, kdy používáme velké a integrované databáze osobních údajů, které komunikují on-line s jinými systémy přes internet, rizika jsou díky těmto propojeným systémům obrovská.

Data si můžeme zařadit do následujících kategorií:

Anonymní údaje jsou takové, které (a to i po zpracování) nelze vztáhnout ke konkrétní fyzické osobě. Příkladem takového údaje je „Jan Novák“. S informací „Jan Novák“ nelze jednoznačně určit, o jakou osobu se jedná.

Osobní údaje jsou takové, které umožňují jednoznačně identifikovat příslušnou fyzickou osobu, ke které se vážou, a to na základě jak jednoho, tak i více prvků. Příkladem může být rodné číslo jako jeden prvek nebo jméno v kombinaci s adresou za předpokladu, že v daném objektu nebydlí více osob stejného jména. „Jan Novák, Široká 610, Brno“

Citlivé údaje jsou takové osobní údaje, které vypovídají o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě fyzické osoby. Nebo jím může být jakýkoliv biologický či genetický údaj fyzické osoby. Tedy slina, moč, vlas, fotografie či cokoliv jiného.

Citlivé údaje lze zpracovávat a předávat pouze tehdy, pokud:

- fyzická osoba, k níž jsou citlivé údaje vázány, dá ke zpracování výslovný souhlas (vědoma si svých práv a účelu zpracování informací),
- jde o zachování a ochranu života,
- se jedná o zpracování při zajištění zdravotní péče,
- je zpracování vyžadované zákonem,
- je zpracování prováděno v rámci pracovního práva a zaměstnanosti,
- fyzická osoba tyto údaje sama zveřejnila.

Na rozdíl od utajovaných informací nejsou na ochranu osobních a citlivých údajů v ISVS kladeny žádné konkrétní požadavky. ISVS nejsou certifikovány, atestovány ani jinak kontrolovány. Je tedy pouze na správci, aby zajistil ochranu údajů v potřebném rozsahu. Je třeba podotknout, že toto zabezpečení a ochrana osobních a citlivých údajů mimo ISVS jsou předmětem zájmu každého dobrého informačního auditu [6].

1.6 Dlouhodobé uchovávání elektronických dokumentů

Problematika dlouhodobého uchovávání je pro dnešní informatiky jedním z hlavních úkolů k řešení. Pro mnoho uživatelů „elektronického styku“ je totiž právě problematika dlouhodobého uchovávání brzdou zavedení e-fakturace, elektronického zadávání veřejných zakázek, e-Governmentu apod. Bez

problémů lze dnes mnoho administrativních úkonů realizovat čistě elektronicky, a to jak směrem do státní správy, tak i mezi komerčními subjekty.

Otázka, kterou si položí každá právnická či fyzická osoba, zní: „Jak dokumenty v elektronické podobě uchovám? Jak zajistím jejich dostupnost a čitelnost při finanční kontrole za 10 let? Jak prokáži, že jsem nemovitost opravdu koupil před 50 lety?“

České právo v oblasti uchovávání elektronických dokumentů se odkazuje jen na zákon o archivnictví. V tomto zákoně se o elektronických dokumentech hovoří celkem dvakrát. Poprvé v §2 písm. d), který uvádí, že dokumentem je každý písemný, obrazový, zvukový, elektronický nebo jiný záznam. A druhá zmínka je v §8 odst. 8, kde se dočteme, že: „Dokument v digitální podobě musí být zapsán ve formátu, který zaručí jeho neměnnost a umožní jeho následné čtení. Pokud tuto podmínku nemůže původce zabezpečit, převede takové dokumenty do analogové formy odpovídající době jejich vyřízení a opatří je náležitostmi originálu, a to nejpozději před jejich zařazením do skartačního řízení.“ Tato formulace je v dnešní době obtížně realizovatelná. Jisté je, že formát, který by zaručil neměnnost a umožnil následné čtení dokumentu (po „neomezeně“ dlouhou dobu), dnes není k dispozici.

V oblasti dlouhodobého uchovávání dokumentů nám bohužel nepomůže ani technologie. Stoprocentní technologické řešení, které by umožnilo uchovávat elektronický dokument „neomezeně“ dlouhou dobu a navíc ještě zajistilo jeho autenticitu (například ve vztahu k připojenému elektronickému podpisu, elektronické značce nebo časovému razítku), neexistuje.

Pro dlouhodobé uchovávání elektronicky podepsaných elektronických dokumentů lze využít tří základních metod. Tyto metody jsou teoretickými východisky problematiky dlouhodobého uchovávání. Všechny tři již byly (v omezeném rozsahu) implementovány různými odbornými a pracovními skupinami na světě. Zajímavé je, že pohled na to, jakou metodu vybrat, se stále liší. Všechny nejasnosti musí nakonec řešit finanční stránka projektů, která je z hlediska výběru metody jasná a neúprosná.

První metodou dlouhodobého uchovávání je emulace

Jedná se o metodu, jejímž základem je emulace původního prostředí (které zná a podporuje formát konkrétního dokumentu). Emulace skýtá mnoho výhod (zejména týkajících se autenticity dokumentů), ovšem z jiných hledisek je metodou nepoužitelnou. Prvním z těchto hledisek je spolehlivost emulátorů, a to zejména v případech, kdy pracuje několik emulátorů současně. Při tomto provozu dochází k vysoké chybovosti. Druhým hlediskem je cena vývoje

emulátorů, která je vzhledem k neustálému vývoji a množství formátů, hardwaru i operačních systémů velmi vysoká.

Druhou metodou dlouhodobého uchovávání je virtualizace

Tato metoda je založena na existenci UVC (Univerzální virtuální počítač). UVC je „strojovou řečí“ pro současný, minulý i budoucí hardware, která bude všemi typy hardwaru podporována. Potom stačí každý soubor uchovat s programem, ve kterém byl vytvořen. Program musí podporovat interpretaci formátu pro UVC. U této metody je třeba podotknout, že je pro dlouhodobé uchovávání mimořádně datově náročná.

Třetí metodou dlouhodobého uchovávání je migrace

Tato metoda je založena na transformaci formátu dokumentu. V případě, že by daný formát přestal být podporován nebo byl nahrazen formátem novějším nebo perspektivnějším, byl by dokument vytvořený ve straším formátu migrován do formátu novějšího. Tato metoda bohužel přináší problémy se změnou dokumentu. Jsou například problémy s vlastností migrační metody (komprese), problémy se změnou struktury dokumentu nebo ztrátou autentizace.

Jednoduchým příkladem migrace může být převod dokumentu. Při převodu dokumentu v rozsahu cca 500 stran vytvořeném v MS Word 95 do formátu MS Word 2003 dojde i přesto, že oba formáty jsou kompatibilní, ke změně formátování a změně délky dokumentu až o několik stran. Migrace ovšem přináší oproti předchozím metodám řadu výhod. Jsou to v současné době nízké náklady na dlouhodobé uchovávání, které však budou v budoucnosti vyváženy vyšší pracností při správě většího množství těchto dokumentů, dále je tu fakt, že některé elektronické dokumenty (např. ve formátu pdf nebo txt) jsou poměrně stálé a dnes se zdá, že v blízké budoucnosti nebude tyto dokumenty třeba migrovat.

Dokument, který obsahuje elektronický prvek autenticity, je následně dlouhodobě uchováván. Formát tohoto elektronického dokumentu zastarává, až dochází k tomu, že je potřeba jej migrovat. Migrací dokumentu dojde ke změně jeho binárního zápisu. Hash migrovaného dokumentu již není shodný s hash, který byl vypočítán přej jeho migrací, Dochází tedy k tomu, že spojení mezi elektronickým dokumentem a jeho podpisem, které je na hash založeno, dále neexistuje. Není tedy možné prokázat, že elektronický podpis náleží k migrovanému elektronickému dokumentu, protože se vypočítaný hash liší.

V případě použití migrace jako metody dlouhodobého uchovávání není tento problém technologicky odstranitelný a je třeba jej legislativně řešit.

Vztah stárnutí kryptografických algoritmů a migrace je následující. Elektronický dokument, který je dlouhodobě uchováván a má elektronický podpis a kryptografický algoritmus, na jehož základě byl elektronický podpis vytvořen stárne (dnes se odhaduje bezpečná doba uchování cca 10 let). I pokud byl elektronický dokument ve formátu, který není třeba migrovat, je zapotřebí důvěryhodnou cestou ošetřit to, že kryptografický algoritmus může být prolomen.

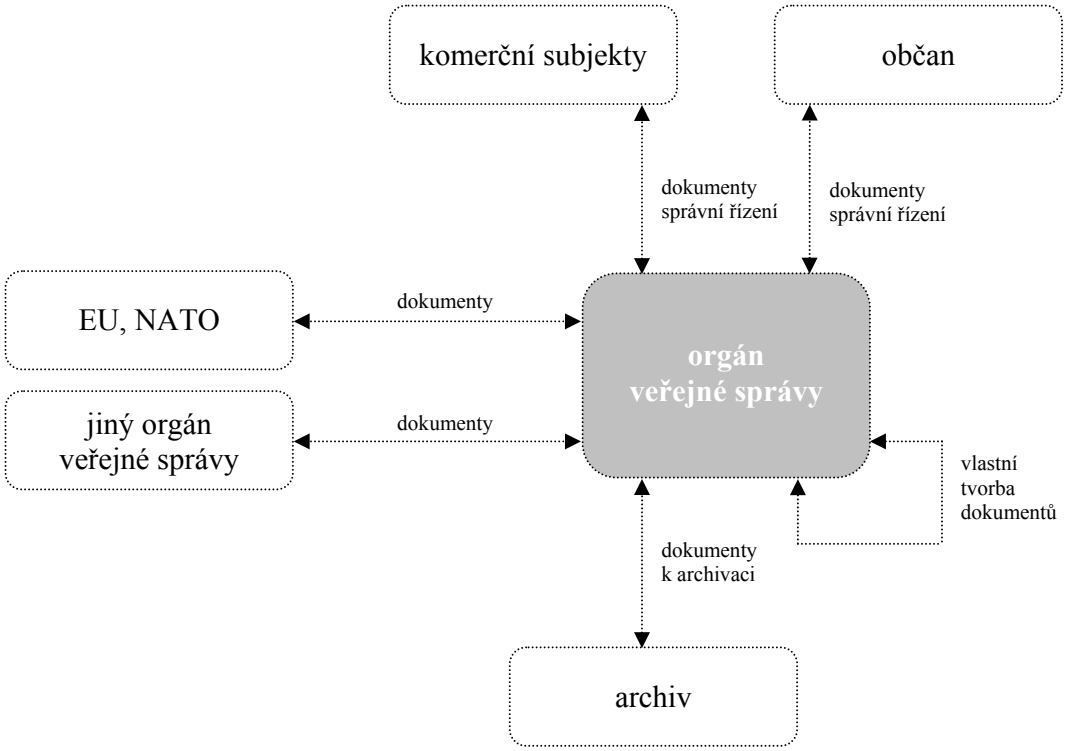
1.6.1 Formáty

Počet formátů, které budou archivním pracovištěm přijímány, musí být omezen. Pro jednotlivé formáty musí být jasně vymezen způsob jejich dlouhodobého uchovávání včetně postupů při jejich migraci.

Předpokládanými druhy formátů pro dlouhodobé uchovávání jsou:

- textové formáty – ODF, TXT, všechny formáty typu DOC, RTF, 602, WPD, SAM, EML, MSG, PDF,
- tabulky – ODS, XLS, SXC,
- prezentace – PPT, PPS, ODT, SXI,
- rastrová grafika – TIFF, BMP, JPG, PCX, PNG, XCF,
- vektorová grafika – WMF, AI, CDR, SXD,
- audiovizuální soubory – WMA, WAV, MP3, OCG, AAC, MPEG, AVI
- databáze – CSV, DBF, MDB, MS-SQL, My-SQL, Lotus Notes, Oracle,
- jiné – HTML, XML.

Z obrázku č. 8 vyplývá, že dokumenty, které jsou archivovány, vznikají v konkrétním orgánu veřejné správy, jsou mu poskytovány ostatními orgány veřejné správy a jsou předávány komerčními subjekty a občany [6].

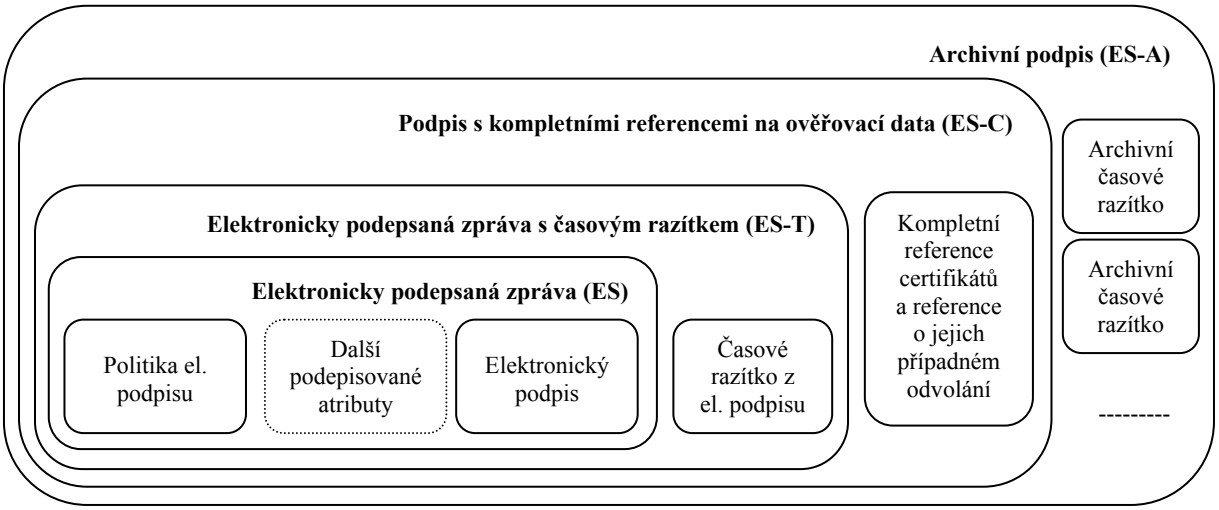


Obr. 8 - Vstupy elektronických dokumentů do orgánu veřejné správy

1.6.2 Opatření proti stárnutí kryptografických algoritmů

Tato problematika je u různých světových projektů řešena systémem „nabalování časových razítek“. Vždy, když je kryptografický algoritmus, na němž je založen současný e-podpis/značka nebo časové razítko, slabý (tzn. teoreticky nebo kryptograficky prolomen), dojde k tomu, že dokument je orazítkován časovým razítkem, které je založeno na algoritmu v dané době silným.

Tímto způsobem dochází k „*nabalování časových razítek*“ na daný elektronický dokument. Dobu, po kterou je kryptografický algoritmus silný (při použití PSA šifrovacího algoritmu, SHA 256 hash funkce a soukromého klíče v délce 2 048 bitů), odhadují odborníci vzhledem k rozvoji informačních technologií na 5 let [6].



Obr. 9 - Zjednodušené schéma el. podpisu

ERS

Standard ERS (*Evidence Record Syntax*), který vyšel pod označením RFC-4998, se věnuje případu, kdy je třeba v čase zakonzervovat současně větší množství dokumentů (např. i elektronicky podepsaných dokumentů). Dokumenty tak konzervuje v tzv. skupinách dokumentů.

Postup je zase velice jednoduchý. Z jednotlivých dokumentů ve skupině se sečtou otisky (hash). Z nich se vytvoří redukovaný Mertlův strom, který se zakonzervuje časovým razítkem nebo provázaným otiskem (linkage hash). Strom otisků doplněný a archivní časové razítko vytváří tzv. ERS záznam, pro který se u nás v Česku vžil termín „Důkazní záznam“ [24].

OAIS

Reference Model for an Open Archival Information System (OAIS), jež byla vydána i jako norma ISO pod označením ISO 14721. Tato norma si vzala za cíl definovat obecný model informačního systému sloužícího k archivaci elektronických dat (bohužel bez vazby na standardy ICA).

V oblasti dlouhodobé archivace digitálních dat je zkratka OAIS srovnatelná se zkratkou PC v oblasti počítačů. Jedná se o formální model, jak by archiv měl vypadat. Pokud se k popisu tohoto modelu nepoužije nějaká zamlžující terminologie, je model OAIS naprosto logický a zřejmý: Původce archiválii (producer) předává data k archivaci do archivu. Archiv je spravován managementem (archiváři). Archiválie (dokumenty) jsou pak zpřístupňovány badatelům (*consumer*). Vlastností archivů OAIS je, že výstup nemusí být pouze pro badatele, ale může být vstupem do dalšího archivu OAIS.

Základním termínem je balík informací (*Information Package*). Balík informací je základní archivační jednotka, kterou původce zasílá do archivu, kterou archiv archivuje či kterou si badatel z archivu vyzvedne pro svůj výzkum. Rozeznáváme tři typy balíků informací:

- Balík informací zaslaný původcem do archivu (*Submission Information Package*);
- Balík informací udržovaný v archivu (*Archive Information Package*);
- Prezentační balík (*Dissemination Information Package*), což je balík informací, který je archivem vydáván např. badateli [24].

1.7 Konverze dokumentů, zrovnoprávnění elektronické a papírové formy komunikace

I přes legalizaci e-fakturace, e-podpisu a mnohých dalších institutů mnohostranné využití e-komunikace často pokulhává. Jedním z hlavních faktorů této situace je i možnost konverze elektronických a listinných dokumentů. Pro rovnocennou komunikaci je zapotřebí definovat tyto zákonné pilíře:

- právní úprava elektronického podpisu,
- právní úprava zrovnoprávnění listinné a elektronické formy komunikace,
- pravidla elektronického doručování a podávání,
- pravidla závazkových vztahů v digitálním prostředí.

V moderní legislativě se v oblasti zrovnoprávnění elektronické a papírové formy komunikace řeší následující body:

1.7.1 Důkazní síla datových zpráv

Jde o ustanovení zrovnoprávňující elektronické a papírové důkazní prostředky. Legislativa se obvykle zaměřuje na úpravu dvou témat:

- datová zpráva by neměla mít nižší důkazní sílu pouze proto, že se jedná o datovou zprávu,
- jaké aspekty je třeba sledovat při posuzování důkazní síly datových zpráv (zejména jde o spolehlivost způsobu, jakým byla datová zpráva vytvořena, uchovávána nebo komunikována, jak byla zajištěna integrita informací obsažených v datové zprávě, zda je možné určit původce datové zprávy a jakékoliv další relevantní skutečnosti).

1.7.2 Originál

V prostředí papírové komunikace je originál dokumentu velmi důležitým pojmem, jehož předložení je vyžadováno v celé řadě případů, resp. s jehož předložením právo velmi často spojuje prokázání určitých skutečností (např. obsah smlouvy v případě soudního sporu). Tento právní institut je velmi důležitý pro úpravu zrovnoprávnění papírových a elektronických dokumentů, neboť pro elektronické dokumenty nelze použít ustálený výklad originálu v oblasti papírových dokumentů jako média/nosiče, v němž byla určitá informace poprvé vyjádřena. Při elektronické komunikaci totiž každý adresát obdrží kopii původní datové zprávy.

Jde tedy o to, jak upravit používání pojmu „*originál*“ jak pro papírové, tak pro elektronické dokumenty. V některých státech se pojem originálu prakticky přestává používat a namísto toho se používá pojem „*autentického dokumentu*“. V jiných zemích je pojem originálu upraven obdobně jako autentický dokument.

Za originál, resp. autentický dokument, bývá považována datová zpráva, která splňuje následující:

- je zachována integrita informací obsažených v dokumentu od okamžiku jeho dokončení v libovolné formě,
- datová zpráva je v písemné formě,
- informace zůstanou nezměněné a kompletní ve srovnání s právě dokončeným dokumentem, s výjimkou připojení příslušných potvrzení nebo certifikátů zajišťujících integritu, anebo s výjimkou nezbytných změn vzniklých při komunikaci, úschově nebo předvedení informací.

1.7.3 Konverze dokumentů

Dalším aspektem zrovnoprávnění elektronických a papírových dokumentů je oblast úschovy a archivace dokumentů. Zrovnoprávnění elektronické formy zde znamená možnost bezpečně transformovat papírové dokumenty do elektronické formy a uchovávat pouze dokumenty v elektronické formě.

Legislativa umožňuje převedení informací obsažených v příslušných dokumentech do elektronické formy a uchování pouze elektronických dokumentů, pokud jsou splněny následující podmínky:

- informace jsou v písemné podobě,
- jedná se o autentický dokument, resp. originál,

- je možné určit původce datové zprávy a datum a čas, kdy byla datová zpráva odeslána nebo doručena,
- požadavek úschovy se netýká informací, jejichž jediným účelem je komunikace příslušné informace.

V současné době je v České republice problematika konverze dokumentů zapracována do návrhu zákona o elektronických úkonech, osobních číslech a autorizované konverzi dokumentů. Vzhledem k tomu, že návrh je zatím po meziresortním připomínkovém řízení, nelze hovořit o jeho finální podobě. Základní principy však s největší pravděpodobností zůstanou zachovány.

Zákon hovoří o tzv. autorizované konverzi, což znamená „*úplné převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě, ověření shody obsahu těchto dokumentů a připojení ověřovací doložky*“, nebo opačný směr konverze. Oba uvedené dokumenty mají shodné právní účinky.

V Česku budou autorizovanou konverzi provádět například notáři, krajské úřady, matriční úřady, stanovené obecní úřady, stanovené zastupitelské úřady atp. Při konverzi dokumentu do listinné formy bude ověřena platnost kvalifikovaného časového razítka vstupu, platnost kvalifikovaného certifikátu vydaného akreditovaným poskytovatelem certifikačních služeb, platnost zaručeného elektronického podpisu nebo platnost uznávané elektronické značky.

Subjekt, který konverzi provedl, opatří výstup konverze (listinný výstup) ověřovací doložkou, v případě elektronického výstupu konverze je tento výstup opatřen elektronickou značkou nebo uznávaným elektronickým podpisem osoby, která konverzi provedla, a současně je opatřen kvalifikovaným časovým razítkem [6].

1.8 Fungování e-Governmentu v zahraničí

Základní úprava právních otázek spojených s e-Governmentem se datuje do roku 1996, jedná se o UNCITRAL Model Law on Electronic Commerce. Tento modelový zákon je od doby svého vzniku inspirující pro nejrozvinutější státy světa při přípravě národní legislativy a vychází z něj např. i Evropská komise při přípravě evropské legislativy řešící některé aspekty elektronické komunikace.

UNCITRAL Model Law vychází ve své úpravě z důsledného technologicky neutrálního přístupu a z rozlišení pojmu „písemnost“, „originál“, „podpis“, „úřední/notářské ověření“, „právní účinek/důkazní síla“ a „archivace dokumentů“ [33].

1.8.1 e-Government v USA

V USA byl v roce 1999 vypracovali americkou obdobu UNCITRAL Model Law, tzv. Uniform Electronic Transactions Act. V mezidobí tento zákon přijala naprostá většina států USA. V roce 2000 byl přijat federální zákon o elektronickém podpisu, tzv. E-Sign Act. Oba právní dokumenty vycházejí v podstatné míře z UNCITRAL Model Law, tento právní model však dále rozvíjejí. Oba legislativní texty přestavují v současné době pravděpodobně nejmodernější komplexní právní úpravu elektronických obchodních transakcí uznávanou mezi odborníky na celém světě.

Další úpravou v USA, která reflektuje novodobý vývoj, je od 1. prosince 2006 účinná změna občanského soudního řádu. Dodatek schválený Nejvyšším soudem odráží nutné změny v procesním právu, neboť tradiční procesní pravidla vztahující se na důkazy v papírové formě nelze použít pro úpravu problematiky elektronických dokumentů.

Novela občanského soudního řádu specificky zahrnuje elektronické informace mezi důkazní prostředky. Množství elektronických informací může být v rámci společnosti obrovské, což může vést mimo jiné k neúměrným výdajům v souvislosti s obstaráváním důkazů. Proto byla stanovena další pravidla, která specifikují formát, ve kterém elektronické informace mají být předloženy.

1.8.2 e-Government ve Velké Británii

Velká Británie dosáhla obdobného právního stavu jako USA, nikoliv však na základě zvláštních zákonů, ale zejména na základě soudních rozhodnutí. Anglické právo prakticky zrušilo požadavek na originál dokumentů. Ve Velké Británii byla rovněž vydána první soudní rozhodnutí, která přiznala plný právní účinek a důkazní sílu elektronickým dokumentům.

Anglický zákon o elektronických komunikacích stanovuje, že elektronický podpis je důkazním prostředkem v soudním řízení a slouží k autentizaci. Je však vždy na soudci, aby zvážil, zda byl elektronický podpis řádně použit. Všeobecné lze říci, že znakem britské legislativy je do určité míry liberální přístup.

1.8.3 e-Government ve Francii

Francouzské právo bylo významně upraveno ve vztahu ke sledované problematice v roce 2000. Francouzský občanský zákoník opět vychází z UNCITRAL Model Law. Zákon přiznává dokumentu, který byl původně vytvořen v elektronické podobě, hodnotu originálu, ale je jej třeba vybavit možností ověření a integrity obsahu.

Zákon uznává, že elektronický dokument má stejnou průkazní sílu jako dokument v papírové podobě. Ovšem pokud se jedná o elektronické dokumenty, které byly původně uzavřeny v papírové formě, francouzské právo je považuje pouze za kopie. Originál proto může být kdykoli požadován. Je třeba, aby byl náležitě identifikován autor dokumentu a zaručena integrita dokumentu.

I kopie může sloužit jako důkazní materiál, a to zejména v případně náhodné ztráty nebo ztráty v důsledku vyšší moci nebo proto, že originál nebyl zachován, a to v případě, že kopie je věrná a trvalá. Zda jde o kopii věrnou a trvalou, záleží na posouzení soudu.

Zákon ve Francii neukládá přesně podmínky archivnictví. Na národní úrovni vytvořilo sdružení AFNOR (Association Française de Normalisation) několik norem týkajících se elektronického archivnictví. Uvádí opatření technického a organizačního charakteru, která směřují k záznamu (přepisu), uchování a obnovení elektronických dokumentů tak, aby byla spolehlivě zajištěna integrita a uchování takových dokumentů. Upřednostňovány jsou nepřepisovatelné disky pro zápis dat. Obsah záznamu uchovávaného na optickém disku WORM (Write Once Read Many), který nelze měnit, může být nejspíše považován za integrovaný a věrný originálnímu dokumentu.

1.8.4 e-Government v Belgii

V roce 2006 byl v Belgii přijat zákon týkající se elektronického soudního řízení. Tento zákon upravuje rámec elektronizace soudního procesu, kdy procesní úkony vyplývající ze zákona či prováděcích předpisů vznikají, provádějí se, podepisují se, komunikují, archivují a jsou k nahlídnutí elektronicky. Jde o systém Phenix založený na konceptu „*elektronického spisu*“. Jeho implementace do soudního systému je předpokládána v několika etapách během několika let. Elektronický spis je v současné době naplánován v trestních věcech. Legislativa předpokládá přechodnou duální formu spisu jak elektronickou, tak papírovou, nicméně přehledy budou vedeny vždy v elektronické formě.

Zákon z roku 2004 již neváže elektronickou fakturaci na předchozí povolení úřadu. Belgická legislativa umožňuje uchovávání elektronických faktur bez ohledu na to, kde je úložiště (nelze mimo území EU) a nosič, pokud lze zaručit integritu a čitelnost faktur po celou dobu, po kterou je nutné faktury uchovávat (10 let) včetně nutnosti tyto atributy doložit. Faktury nelze převést z papírové do elektronické podoby, aniž by byl papírový originál zničen, neboť faktury musí být uchovávány v původním formátu, je však možné požádat o odchylku od tohoto pravidla.

1.8.5 e-Government v Německu

Aby byly odstraněny nedostatky ve vztahu k užívání elektronické formy smluv, byl přijat zákon na změnu občanského práva ve vztahu k požadavkům na formu a další předpisy na modernizaci právních transakcí.

Jedním ze základních principů německého práva je, že neexistuje žádný požadavek na formu. Z tohoto pravidla samozřejmě existují výjimky. V Německu vláda financuje rozsáhlý projekt, jehož účelem je elektronická transformace státních archivů. V rámci tohoto významného projektu se klade důraz právě na bezpečnou elektronickou transformaci papírových dokumentů opatřených vlastnoručními podpisy.

1.8.6 e-Government ve Finsku

Zákon o elektronických službách a komunikacích ve veřejném sektoru upravuje elektronickou archivaci v rámci spisové služby, kdy stanovuje povinnost zaregistrovat příchozí elektronický dokument vhodným způsobem, včetně označení času doručení a kontroly původu a integrity obsahu dokumentu, a stanovuje povinnost do budoucna ověřit původ a integritu archivovaného elektronického dokumentu. Tím zákon nepřímo vyžaduje i archivaci verifikačních údajů týkajících se elektronického dokumentu, např. certifikátu elektronického podpisu.

Od roku 2004 běží ve Finsku projekt SÄHKE v pilotní formě. Cílem projektu SÄHKE je mimo jiné zkoumat, jak zajistit právní hodnotu elektronických archivovaných dokumentů včetně stanovení požadavků týkajících se integrity a autenticity archivovaných záznamů. Národní archivy musí udělit povolení, aby dokumenty mohly být archivovány trvale pouze v elektronické formě.

V zákoně o elektronických službách a komunikací ve veřejném sektoru je elektronický dokument definován velmi obecně jako jakákoli elektronická zpráva týkající se záležitosti nebo rozhodnutí. Elektronická zpráva sama je jakákoliv informace, která byla zaslána prostředky umožňující elektronický přenos dat a vlastně umožňuje zpětnou transformaci do papírové formy, neboť uvádí, že pokud je potřeba, je možné uchovávat elektronické zprávy v písemné formě (a naopak). Pokud je však požadovaný dokument podepsaný, musí být podepsán zaručeným elektronickým podpisem založeným na kvalifikovaným certifikátu.

Zároveň pro zjednodušení komunikace zákon stanovuje domněnku, že elektronický dokument nemusí být podepsaný, pokud obsahuje informaci o odesilateli a neexistuje nejistota ohledně původu a integrity dokumentu. Z této domněnky vyplývá, že elektronický podpis je zapotřebí pouze u dokumentů, kde zákon specificky vyžaduje podpis, v ostatních případech je však technicky

neutrální a vyžaduje u elektronických dokumentů průkaznost jejich původu, integrity a nepřímo i čitelnost.

Ve Finsku neexistují žádné právní předpisy upravující specificky elektronickou fakturaci. Elektronická úschova faktur je umožněna v souladu s finskými zákony o účetnictví tak dlouho, dokud je bude možné snadno opět získat. Zároveň není požadováno, aby faktury byly archivovány v původní formě, což umožňuje jejich transformaci pro účely archivace, aniž by bylo nutné archivovat původní formát (elektronický či papírový).

1.8.7 e-Government ve Švédsku

Právní rámec úpravy týkající se státních a úředních záznamů sestává z Freedom of the Press Act, Archives Act 1990, Secrecy Act, Data Act a prováděcích předpisů, převážně Archive Ordinance 1991, který zmocňuje Národní archivy (SNA) k vydávání instrukcí týkajících se dokumentů veřejnoprávních institucí.

Zákon specificky požaduje po každém úřadu následující:

- vybrat vhodné materiály a metody pro tvorbu záznamů, aby bylo zajištěno, že informace bude srozumitelná a uchovatelná po potřebnou dobu,
- organizovat archiv tak, aby k němu byl snadný přístup veřejnosti,
- vytvořit popis archivu za účelem jeho představení a vytvoření katalogu za účelem vyhledávání.

SNA od roku 1991 vydala nařízení Regulations and recommendations concerning recordings from automatic data processing a Regulations concerning delivery of recordings form automatic data processing. První nařízení se týká usnadnění dlouhodobé archivace elektronických dokumentů. Doporučuje migraci dat na nové nosiče (požadavky na bezpečnost, kopírování, převod, organizaci, úschovu atd.). Druhé se týká převodu elektronických dokumentů do SNA. Cílem těchto nařízení je, aby SNA dostala elektronické dokumenty ve formě, která je co nejvíce nezávislá na původním hardwaru a softwaru. Data jsou obecně migrována na magnetické pásky (magnetic storage media) minimálně jednou za 10 let.

1.8.8 e-Government v Nizozemí

Již v roce 1994 měly být vyvinuty standardy, doporučení a best praktice zacházení s elektronickými záznamy. Nový zákon Archives Act od roku 1995

specificky pokrývá elektronické záznamy a vztahuje se jak na veřejnoprávní, tak na soukromoprávní instituce. V roce 2000 neexistoval žádný přístup veřejnosti k oficiálním elektronickým dokumentům. V roce 2002 měl být ukončen projekt Ministerstva vnitra Digital Longevity, který byl podkladem pro vznik projektů veřejnoprávních institucí moderního workflow dokumentů – přístup, uchování a správa elektronických dokumentů.

Od roku 1988 finguje Nizozemský historický archiv dat (NHDA), který shromažďuje a uchovává elektronické verze materiálů, jež vznikly transformací na elektronické formáty, ať už přepisem nebo např. scanováním. Aktivní v oblasti získávání elektronických publikací je také Královská knihovna, která se i účastnila výzkumu autentizace elektronických dokumentů, digitálních podpisů, šifrování a různých způsobů migrace elektronických dokumentů.

1.8.9 e-Government v Dánsku

Zákon o archivnictví (Archival Law) z roku 1992 je doplněný o podzákonný předpis (Executive order). Elektronické dokumenty jsou předávány do státního archivu, kde by měly být uchovány ve formě, jež umožňuje přepis dat do formátu, který umožňuje další přepis – a to bez ztráty dat. Období archivace je stanoveno obecně na 5 let. Data se uchovávají na CD-R nosičích.

V Dánsku existuje od roku 2004 nový zákon. Vyžaduje, aby byly uchovávány nejen tiskoviny, ale i statické elektronické dokumenty. Cílem tohoto zákona bylo zajistit, aby všechny dokumenty uveřejněné v Dánsku byly shromažďovány a zachovány do budoucna, předchozí úprava vztahovala povinnosti k archivaci jen u dokumentů, které byly vytištěny. Pokud jde o dokumenty v elektronické podobě, zachovávají se pouze dokumenty statické – a to zejména na nosičích, jako jsou diskety, CD nebo další disky.

Dánsko začalo vydávat elektronické podpisy v jednodušší formě (založené pouze na softwaru) svým občanům zdarma. Elektronické podpisy mají velmi krátkou trvanlivost – 2 roky. Dalším obecným pravidlem je, že elektronický podpis má stejnou váhu jako podpis vlastnoruční. Od února 2005 jsou všechny veřejné úřady povinny přijímat elektronické podpisy.

Faktury je třeba uchovávat v tištěné formě nebo elektronicky. Pokud jde o elektronickou formu, přesný způsob archivace není předepsán. Informace je třeba uchovávat v takové formě, aby je bylo možné zpřístupnit daňovým úřadům. Společnosti, které vydávají elektronické faktury, je musí uchovávat v jejich původní formě a v původním formátu, tj. elektronicky [6].

1.8.10 e-Government v Rakousku

Tuto zemi jsem si nechal záměrně nakonec z jistého důvodu. V dnešní době už totiž nehovoříme o tom, zda napodobovat Velkou Británii nebo Litvu, hovoříme o tom, zda přejmout rakouský model. Co je tedy ten rakouský model, kdy vznikl, jak dlouho vznikal, za jakých podmínek a hlavně s jakými výsledky? A co jsme si z toho schopni vzít my k nám domů? [22]

Podívejme se na dva protichůdné názory českých expertů (Edvard Kožušník, vedoucí projektu eStat.cz a Jiří Polák, prezident sdružení SPIS) na rakouský model a poté na názor rakouského nejvyššího IT odborníka. (Reihard Posch, CIO Federal Government Austria)

Rakouská inspirace? Zajímavá, ale nepřenositelná!

Jako vedoucí iniciativy eStat.cz, která se snaží propagovat myšlenky a konkrétní projekty vedoucí k malému, zato silnému a efektivnímu státu, jsem rakouský model poměrně podrobně studoval. Nezajímalo mě ani tak technické řešení, ale samotný proces přípravy, prosazení a realizace. Z tohoto důvodu jsem skeptický k bezhlavému přenosu uvedeného modelu. Nejzávažnějším argumentem je z mého pohledu čas. V oblasti moderních technologií je rychlý vývoj normou. Rakouský model vznikal na úrovni myšlenky někdy kolem roku 1998, tedy ve stejném čase jako tehdejší Zemanova „*Státní informační politika*“.

Základním nosným prvkem rakouských a českých myšlenek totiž byla centralizace průřezových aktivit ve vazbě na budoucí e-government. V Rakousku „centralizovali a koordinovali“ politickou vůli, legislativu a finance s vizí, že se stanou lídrem. A opravdu se jím stali. Pokud ale chceme nabídnout občanům stejné služby a pokud chceme podnikatelům nabídnout stejné moderní technologické prostředí jako v Rakousku, musí se v této oblasti politická reprezentace, včetně opozice, shodnout na programu, který bude obsahovat prvek centralizace a koordinace.

Centrální registry jsou tím trikem, který umožňuje z pohledu státu, samosprávy i dalších subjektů nabídnout nebývalé množství nových služeb.

Stejně jako v Rakousku vyžaduje zapojení do informační společnosti i v ČR aktivní vůdčí úlohu vlády a celé veřejné státní správy tak, jak tomu bylo ve většině vyspělých států. Vláda by měla jasným a uceleným způsobem udávat směr technologické modernizace v Česku. E-správa tvoří nepřehlédnutelný motor v procesu sociálně-ekonomické transformace ČR směrem k informační společnosti. Možnost elektronického přístupu občanů do veřejné správy musí být neodkladně uznána jako jejich právo.

O čem se moc nemluví, je fakt, že sousedé podpořili celý program velmi výrazně finančně [22].

Rakouská zkušenost? Zajímavá a inspirativní!

Po půlroční analýze projektu Digital Austria může Sdružení pro informační společnost (platforma Klub SPIS) konstatovat, že je nanejvýš žádoucí vzít si příklad z rakouského „tahu na branku" vedeného z nejvyšší úrovně, inspirovat se finančně-organizačním zajištěním projektu a po odborné stránce těžit ze systému identifikace a autentifikace (včetně zapojení bankovního sektoru). Integrujme v Rakousku ověřený princip identifikace/autentifikace s návrhem připravovaných centrálních registrů, s napojením na již běžící agendové informační systémy (podle návrhu MI ČR/MV ČR) a Czech POINT.

Úspěch v oblasti e-governmentu vyžaduje jasné, srozumitelné, fungující a prakticky realizovatelné přístupy k identifikaci a autentizaci osob, k využití registrů, k možnostem podávání a doručování v elektronické podobě a v neposlední řadě i k organizaci a řízení celého e-governmentu.

Zahraniční zkušenosti, zejména z Rakouska, ukazují, že zcela zásadní a rozhodující podmínkou pro úspěch e-governmentu je high-level commitment („odhodlání a zapojení na nejvyšší úrovni"). A to skutečně na úrovni nejvyšších orgánů státu, včetně premiéra a klíčových ministrů, kteří budou e-government sami aktivně prosazovat a poskytnou mu i nezbytnou „politickou záštitu".

Klíčem k možnosti provozovat nejrůznější agendy e-governmentu v elektronické podobě je spolehlivá, bezpečná a současně rychlá a pohodlná identifikace fyzických i právnických osob a orgánů veřejné moci a jejich autentizace.

Základem pro identifikaci je použití bezvýznamových identifikátorů a základem pro autentizaci je využití metod elektronického podpisu.

Důležitým principem je to, že každá agenda bude pro identifikaci konkrétních osob využívat různé identifikátory, tzv. agendové identifikátory, které nebudou přímo převoditelné mezi sebou. Jejich převod bude možný jen se souhlasem dotčené osoby a bez jejího souhlasu jen tam, kde k tomu existuje opora v zákoně. Proto žádná agenda nebude moci (bez souhlasu dotčené osoby či opory v zákoně) zjišťovat, co o stejné osobě obsahuje jiná agenda.

Praktické použití identifikačních a autentizačních nástrojů ze strany občanů bude velmi snadné. Bude založeno na využití nosičů identity, jejichž roli mohou plnit jak jednoúčelové čipové karty („elektronické občanské průkazy"), tak například bankovní platební karty, či mobilní telefony apod. – stejně jako se tyto

nástroje již dnes používají pro identifikaci a autentizaci například u elektronického bankovnictví.

Veškeré informace, se kterými veřejná správa pracuje, si uchovávají v registrech. Aby se zabránilo duplicitám a nekonzistentnostem v jejich obsahu, musí se relevantní informace uchovávat vždy na jednom místě a také jen z jednoho místa získávat. Proto musí být několik málo registrů prohlášeno za tzv. referenční registry, zatímco ostatní registry odvozují co největší část svého obsahu z těchto registrů.

Komunikace mezi registry bude možná pouze skrze prostředníka v podobě (jednotného) komunikačního rozhraní. To zajistí realizaci požadavků na bezpečnost i případné konverze dat a agendových identifikátorů a v neposlední řadě umožní pouze oprávněnou komunikaci mezi dvěma registry (buďto se souhlasem dotčené osoby, nebo s oporou v zákoně).

Základním principem však stále bude možnost volby formy podání (tj. klasické listinné či elektronické formy podání) a stejně tak možnost volby doručení. Implicitní přitom bude tradiční doručování v listinné podobě, zatímco doručování v elektronické formě bude pouze na explicitní vyžádání [22].

Rozhovor s profesorem Reinhardem Poschem

Co je z vašeho pohledu na rakouském modelu a obecně na fungujícím modelu e-governmentu nejpodstatnější?

Celý model našeho e-governmentu má několik aspektů, přičemž za ten velice důležitý, možná nejdůležitější, považuji organizační. Podobně jako u vás, i u nás jsou tři úrovně veřejné správy: federální, regionální a místní. Je tedy jasné, že musí fungovat model, který přenáší informace z federální úrovně směrem dolů, a zároveň aby tyto úrovně fungovaly v nějakém souladu. Na vrcholu této naší „pyramidy“ je platforma Digital Austria. Jedná se o skupinu zástupců z ministerstev, krajských zastupitelstev a místních správních orgánů a rovněž o zástupce profesní komunity.

O úroveň níže je platforma Federal ICT strategy. Jedná se o skupinu 70 osob. Tyto osoby v podstatě vytčené strategie dávají do souladu s legislativou. Přímo na Federal ICT Strategy je napojeno oddělení Public Relations, tedy vztahy s veřejností. Zajišťuje efektivní komunikaci veškerých výstupů na všechny úrovně veřejné správy i směrem k veřejnosti jako takové. Poslední jednotkou této úrovně je EGIZ – Egovernment inovační centrum, které především sleduje možnosti nových technologií v souvislosti s e-governmentem a potřebami veřejné správy.

Aby nebyl model e-governmentu jen knižním příkladem, ale byl lidmi využívaný, je nutné jim něco nabídnout. Co to bylo u vás?

Byla to karta. V elektronickém světě je důležitá identifikace občanů. Kdo jste a jste-li to vy? To jsou základní otázky v elektronické komunikaci. A je to podstatné nejen v kontaktu občana s veřejnou správou, ale i mezi podniky a veřejnou správou. Kontakt konkrétního podniku jde vždy přes konkrétní osobu, a tu je nutné identifikovat. Řekli jsme si, že nebudeme vytvářet nové věci, ale použijeme to, co je na trhu. Proto tyto karty obsahují elektronický podpis.

Každý člověk v Rakousku má takovou kartu s elektronickým podpisem. Pro identifikaci občana slouží klíč – bezvýznamový identifikátor. V kombinaci s registrem obyvatel a podniků už získáváme velké možnosti.

Karta mi tedy umožňuje kontakt s centrálními registry?

Samozřejmě, kolem toho se to vše točí. Vy se můžete za nějakým účelem spojit s centrálním registrem a pořídit si konkrétní výpis, nebo na tom svém stávajícím nějaké údaje měnit.

Znamená to, že všechny úřady všech úrovní akceptují elektronickou cestu úředního kontaktu pro veškeré úřední úkony?

To bohužel ještě ne, ale je to samozřejmě cíl, k němuž směřujeme. Ale už teď platí, že každý státní úředník musí mít přístup do registrů. Zároveň platí, že například ministerstva nesmí posílat žádné papíry, jsou-li schopny toto realizovat v rámci spisové služby elektronicky. To je nařízeno zákonem.

Jakou váhu mají elektronicky doručené dokumenty a jak se prokazuje jejich platnost?

Jakýkoliv výpis, který pořídíte elektronickou cestou a je elektronicky podepsán příslušným úřadem, je stejně platný i v této elektronické podobě. Elektronická verze v sobě skrývá onen elektronický podpis, který jasně prokazuje platnost daného dokumentu. Pokud si takto získaný dokument vytisknete, je opatřen podpisovou tabulkou, která v sobě nese řadu informací o dokumentu, jeho vydání i podpisovém certifikátu. To samo o sobě nahrazuje „razítko“ a podpis. Navíc platnost tohoto úkonu můžete kdykoliv ověřit na webu pomocí kódu, který je obsažen v této tabulce. Vlastně je to jistější, než papír s razítkem a podpisem.

Co je tedy při realizaci fungujícího e-governmentu podstatné?

Technologie existují, jen si je správně vybrat. Peníze jsou důležité, vždy se vše točí kolem nich, ale nejpodstatnější je přesto politická vůle. Stát, vláda, ministři se musí shodnout, musí chtít a jít společnou cestou [22].

2 HYPOTÉZY A CÍLE DISERTAČNÍ PRÁCE

Hypotéza představuje předběžné tvrzení, představu o vztahu mezi zkoumanými proměnnými a s tím související předpoklad budoucího chování systému.

Cíle jsou velmi konkrétní stanovení toho, čeho má být dosaženo. Cíle by měly být jasné, měřitelné, ambiciózní, reálné a termínované. Cíle disertační práce jsou odvozeny ze stanovených hypotéz [15].

2.1 Hypotézy disertační práce

Základní východiska pro zpracování disertační práce je možné shrnout do těchto následujících hypotéz:

H1: Efektivně fungující informační systém ve veřejné správě zvyšuje spokojenost občanů.

Měření efektivnosti IS v podnicích je velmi složité, i přes vymezení kritických faktorů efektivnosti. Ve veřejné správě je to o to těžší, protože většinou tyto ukazatele nejsou hlídány. Jedním z měřítek ISVS by mohla být definována spokojenost samotných občanů.

H2: Úplné elektronizaci brání byrokratické úřední razítko.

Vychází se z hlavní zásady občanského práva platné pro státní organizace. Předpokládá se potvrzení dané hypotézy, protože veřejná správa se musí řídit platnými zákony České republiky.

H3: Neochota některých zaměstnanců úřadů učit se novým metodám brzdí rychlejší využití ISVS.

Předpokládá se, že každý informační systém je nepoužitelný, pokud jej nebudou plnohodnotně využívat pracovníci úřadů veřejné správy.

H4: ISVS stále vzbuzuje nedůvěru mezi lidmi. Obávají se většího zneužití osobních údajů.

Předpokládá se, že občané mají větší nedůvěru ze zneužití osobních údajů, pokud jsou poskytovány elektronicky, než klasickou „papírovou cestou“.

2.2 Cíle disertační práce

Hlavním cílem disertační práce je na základě teoretického a dotazníkového výzkumu poznat a zhodnotit současný stav informačních systémů ve veřejné správě.

Druhým hlavním cílem je zjištění kritických míst těchto informačních systémů veřejné správy.

Podpůrným cílem je zpracovat současný stav řešené problematiky a to se zaměřením na státní informační politiku ve srovnání s fungováním e-Governmentu v zahraničí.

K cílům zhodnocení stavu řešené problematiky patří rozbor konkrétních nástrojů aplikací, jako jsou:

- Czech POINT,
- možnosti elektronického podpisu,
- možnosti časového razítka.

Vedlejší cíle práce, které rozvíjejí oba hlavní cíle, jsou:

- jaký vliv mají ISVS na změnu komunikace mezi úřadem a občanem,
- identifikaci hlavních znalostí potřebných pro práci s ISVS,
- navržení vhodných metod pro sběr a vyhodnocení dat, navržení dotazníku,
- potvrdit či vyvrátit stanovené hypotézy,
- ukázat pracovníkům úřadů, že IS není nutné zlo, ale pokud jej člověk ovládá, je to dobrý pomocník při každodenní rutinní práci.

3 METODY A POSTUPY POUŽITÉ PŘI ZPRACOVÁNÍ DISERTAČNÍ PRÁCE

3.1 Stanovení typu výzkumu

Vzhledem k tomu, že výzkum efektivnosti informačních systémů ve veřejné správě je zaměřen na získání informací o postojích a subjektivních názorech respondentů, musí být předem vyřešena otázka typu výzkumu a použitých metod a technik k jeho provedení. Neméně důležitou je také otázka vyhodnocení získaných dat.

Hodnocení efektivnosti ISVS bude mít povahu jak kvantitativního, tak i kvalitativního výzkumu. Cílem je věnovat vyváženou pozornost oběma typům zkoumání, protože každý z nich vnáší do celkového pohledu specifické a potenciálně užitečné dimenze. Spojením obou typů zkoumání je možné adekvátně využít kvalitativní údaje k vyjasnění či ilustraci kvantitativně odvozených závěrů [14].

Výzkum uskutečněný za účelem splnění cílů disertační práce má povahu kombinace mapujícího a kauzálního výzkumu. Mapující výzkum má za úkol pomoci řešiteli zorientovat se v problematice a odhalit doposud nepříliš jasné souvislosti. Součástí mapujícího výzkumu je plošný výzkum na straně ministerstev, úřadů i občanů [12, 14].

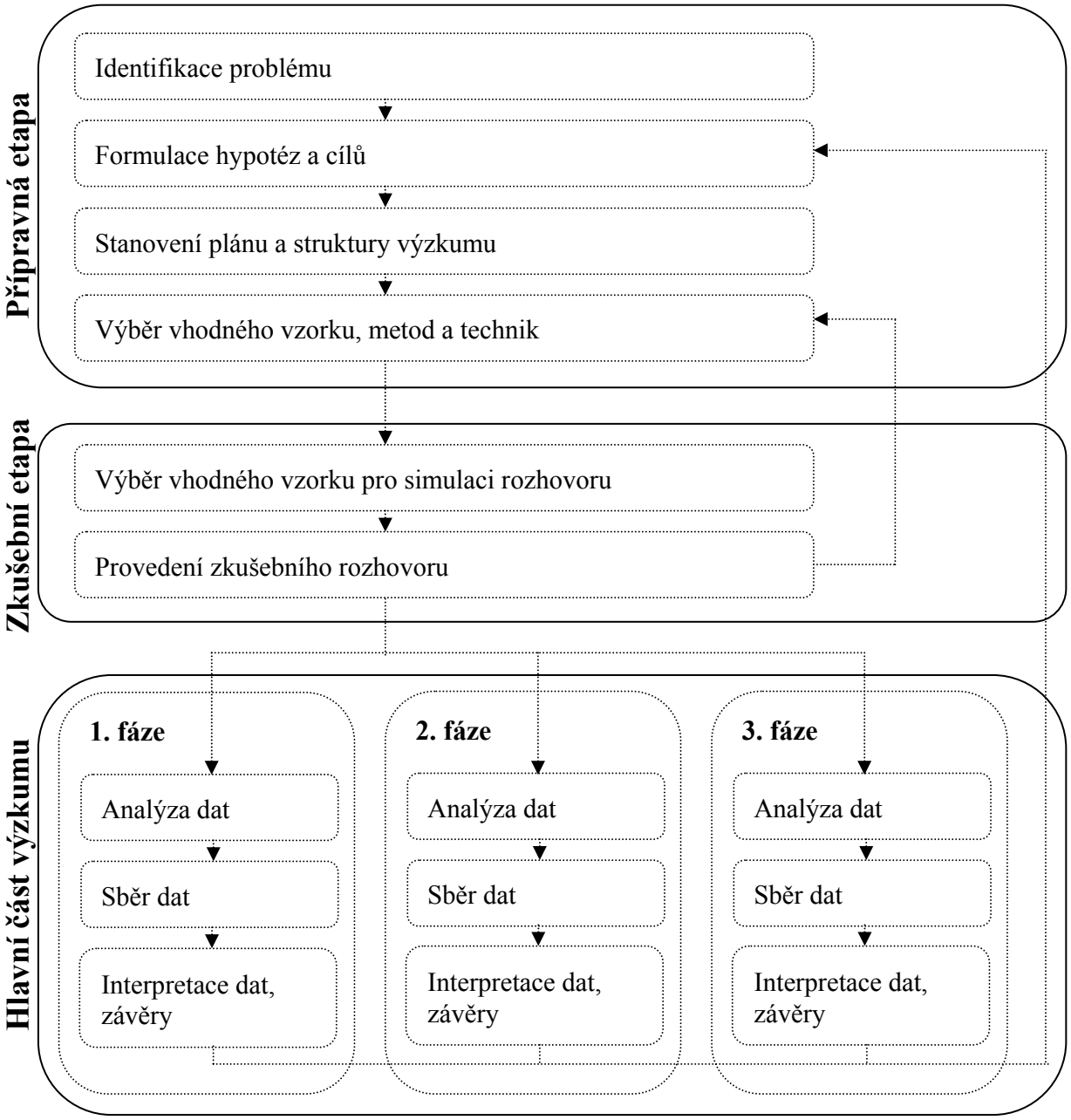
Kauzální část výzkumu má za úkol objasnit složitost vztahů a naznačit jaké CFE jsou rozhodující pro budoucí úspěch či neúspěch implementace ISVS. Při kauzálním výzkumu se často používá k ověření těchto vztahů experiment. Vzhledem k povaze a omezení prováděného výzkumu však není možné experiment seriózně provést, proto byly k posílení vypovídající schopnosti výzkumu uplatněny techniky kvalitativního dotazování.

3.2 Strategie a plán dílčího výzkumu zaměřeného na splnění cílů disertační práce

Dílčí výzkum určený pro zpracování disertační práce vychází ze stanovených cílů a byl rozložen do třech hlavních etap:

1. Přípravná etapa
2. Zkušební etapa
3. Etapa hlavního výzkumu (tři fáze):
   a) 1. fáze – strukturované rozhovory se zástupci jednotlivých ministerstev
   b) 2. fáze – dotazníkové šetření na vybraných úřadech Zlínského kraje

c) 3. fáze – dotazníkové šetření obyvatel Zlínského kraje týkající se služeb Czech POINTu



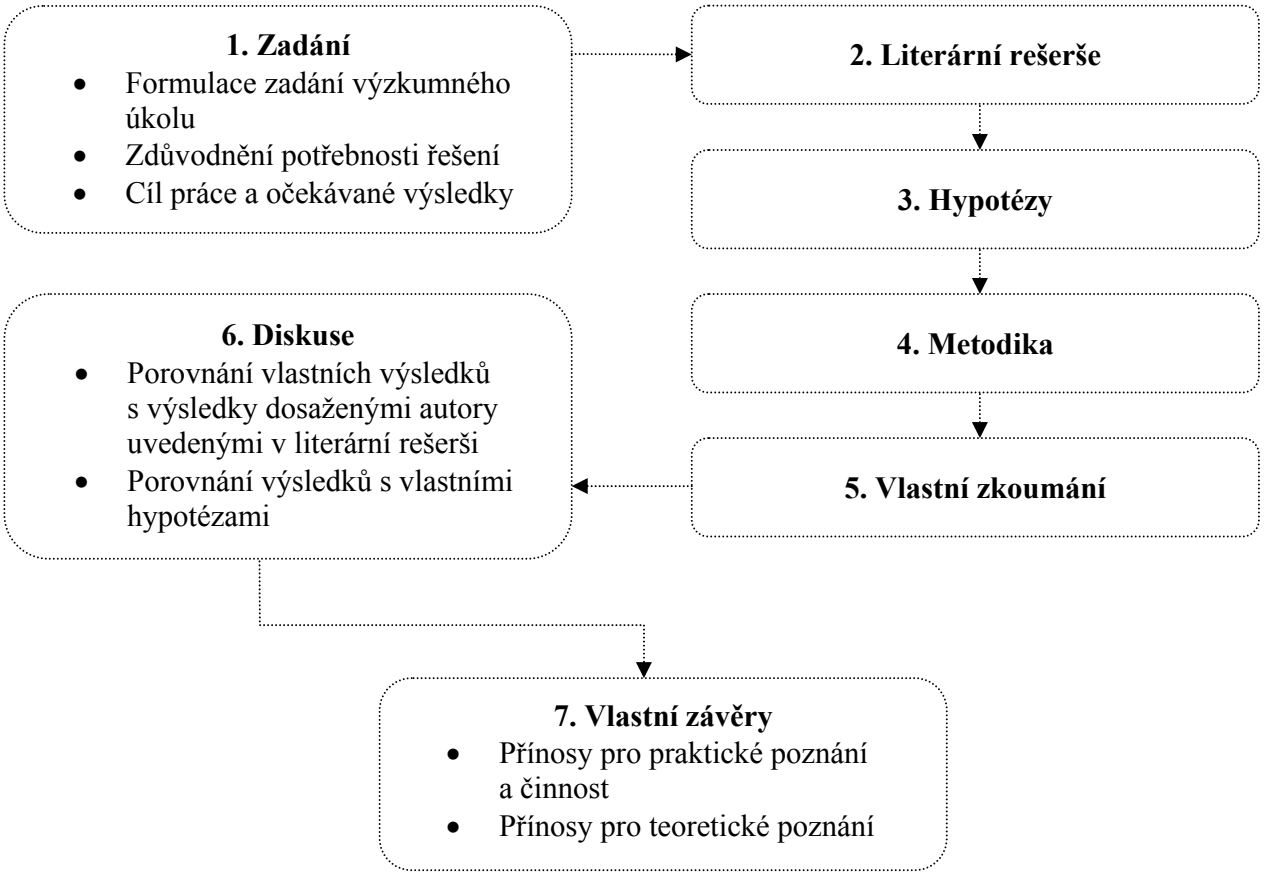
Obr. 10 - Plán výzkumu [vlastní zpracování]

3.3 Postupy použité při zpracování disertační práce

Komplexní postup zpracování disertační práce vychází z logické struktury a návaznosti výzkumné práce. V zásadě bude práce kopírovat strukturu vědecké práce, jak ji uvádí prof. Trnka (viz obr. 11)

Disertační práce má následující strukturu:

- úvod,
- současný stav řešené problematiky (tj. analýza a syntéza dostupných literárních pramenů),
- cíle a hypotézy práce,
- zvolené metody zpracování,
- hlavní výsledky práce a verifikace hypotéz,
- přínos pro vědu a praxi,
- závěr.



Obr. 11 - Struktura vědecké práce [vlastní zpracování]

3.4 Časový harmonogram výzkumu

K tomu, aby byly stanovené cíle dosaženy, je vhodné vytvořit si časový plán činností, které je potřeba vykonat.

1. Definování východisek disertační práce, stanovení hypotéz.
2. Stanovení hlavního cíle a vedlejších cílů práce.

3. Studium literatury, zpracování literární rešerše.
4. Tvorba dotazníku a uskutečnění 1. šetření na jednotlivých ministerstev (provedeno během března - května 2004).
5. Tvorba dotazníku a uskutečnění 2. šetření na jednotlivých úřadech Zlínského kraje (provedeno během února - dubna 2007).
6. Tvorba dotazníku a uskutečnění 3. (kvalitativního) výzkumu ISVS zaměřeno na Czech POINT (provedeno během dubna - května 2008).
7. Analýza, hodnocení a formulování výsledků.
8. Vyvození závěrů, konfrontace se stanovenými hypotézami.
9. Zhodnocení přínosů pro teoretické poznání a praxi.

3.5 Charakteristika zkoumaného vzorku

Hlavním metodologickým požadavkem na výzkum bylo vyřešení otázky výběru vzorku tak, aby reprezentoval základní soubor. Pouze za tohoto předpokladu je možno zjištěné závěry zobecnit na celý základní soubor. Ne vždy se však podaří tento problém vyřešit, proto je snaha vzorek ve zkoumaných charakteristikách alespoň co nejvíce přiblížit souboru základnímu.

Pro vytvoření vzorku u dotazníkového šetření na ministerstev a úřadech Zlínského kraje bylo použito techniky založené na nenáhodném výběru, tzv. záměrném výběru. Při tomto výběru se výzkumník řídí svými zkušenostmi, intuicí, představou a někdy též možnostmi. Do vzorku jsou zařazování jedinci, kteří se výzkumníkovi zdají vhodní pro výzkum. U závěrů je nutné poznamenat, že platí především pro daný výběr [5].

Pro vytvoření vzorku u dotazníkového šetření občanů Zlínského kraje bylo použito techniky založené na náhodném výběru. Při tomto výběru se výzkumník řídí svými zkušenostmi, intuicí, představou ale především možnostmi dané situace a okolí, kde se výzkumník nachází. Do vzorku jsou zařazování veškeří jedinci, kteří se pohybují v daný okamžik ve výzkumníkově teritoriu.

3.6 Systém zvolených metod a technik sběru dat

Ve výzkumné praxi je někdy těžké stanovit jednoznačnou hranici mezi kvalitativními a kvantitativními metodami. Jednou z hlavních příčin je skutečnost, že základní a výchozí výzkumné metody, za které lze označit pozorování a rozhovor, jsou rozvíjeny v rámci kvalitativní i kvantitativní metodologie, byť na odlišných principech. Příkladem by mohla být metoda

stojící na pomezí tzv. sémantického diferenciálu, která se orientuje na zjišťování postojů a zároveň však získané odpovědi kvantifikuje.

Podle Goodyeara se kvantitativní a kvalitativní výzkum liší čtyřmi důležitými způsoby:

1. Typem problému, který mohou řešit.
2. Metodami výběru.
3. Metodami a stylem sběru dat.
4. Přístup k analýze techniky analýzy [4].

Malý počet dotazovatelů a soustředění se na kvalitu dovoluje výzkumnému konzultantovi sbírat většinu dat osobně narozdíl od kvantitativních studií, kde je počet rozhovorů příliš vysoký na to, aby je uskutečnil jeden člověk. Jednou ze silných stránek kvalitativního výzkumu je schopnost výzkumníka informace kreativně proměnit ve výsledky. Navíc malý počet respondentů umožňuje otevřenější otázky než je tomu u kvantitativního výzkumu, navíc na odpovědi je možno reagovat dodatky. Takovéto otevřené vyptávání je cenným zdrojem informací [4].

3.6.1 Metody a techniky kvalitativního sběru dat

Metody a techniky kvalitativního výzkumu se používají k získání tzv. kvalitativních dat – tj. dat vyjadřujících smysl a význam (ne četnost) konkrétních lidských projevů. Součástí těchto výzkumných postupů bývají specifické způsoby analýzy a interpretace dat, obecně zaměřené na pochopení jednotlivce a jeho vnitřního světa.

Jak již bylo řečeno, základními metodami kvalitativního sběru dat jsou pozorování a rozhovor. Přitom se oba tyto postupy navzájem prolínají a doplňují tak, že mezi nimi nelze stanovit jednoznačnou hranici. Mezi základní techniky pozorování patří:

1. Zúčastněné pozorování
    a. Skryté pozorování – výzkumník v roli zaměstnance;
    b. Zjevné pozorování – výzkumník svou přítomnost nezatajuje;
    c. Přerušované pozorování - výzkumník svou přítomnost nezatajuje, avšak tráví v organizaci mnohem méně času.
2. Kvalitativní rozhovor

Výzkumný rozhovor je proces, jehož cílem je prostřednictvím záměrně vyvolané interakce mezi tzv. tazatelem a respondentem získat informace potřebné k pochopení určité problémové oblasti. Kvalitativní (nestandardizovaný, částečně strukturovaný) rozhovor probíhá volně, přičemž je na tazateli, jak jej předem naplánuje a připraví, jaké otázky a kdy v jeho průběhu položí [12].

3.6.2 Metody a techniky kvantitativního sběru dat

Kvantitativní výzkum představuje tradiční cestu poznání, chceme-li nalézt dostatek důkazů, které nám potvrdí naše předpoklady, hypotézy. Jak již bylo zmíněno, některé metody a techniky jsou společné či stojí na rozhraní i kvalitativního výzkumu, proto budou pouze vyjmenovány a dále již nerozebírány. Jedná se o tyto metody:

1. Standardizované pozorování.
2. Strukturovaný rozhovor.
3. Dotazník – jedná se o písemnou, více formalizovanou podobu metody dotazování. Podstata spočívá v písemném položení souboru otázek, na které respondent odpovídá. Konečný výsledek závisí na formulaci jednotlivých položek a konstrukci dotazníku.
4. Experiment – přesně popsaná výzkumná situace, ve které se sleduje kauzální vztah mezi dvěma či více proměnnými tak, že se záměrně vyvolá změna nezávislé proměnné a za kontroly nežádoucích proměnných se sleduje změna závislé proměnné [5, 12, 14].

3.6.3 Dotazník

Na základě použití jednotlivých metod, technik a připomínek získaných během zkušební fáze výzkumu byl navržen formát dotazníku.

Při sestavování pořadí otázek v dotazníku bylo nutno počítat s tím, že se neuplatňují izolovaně, ale ve vzájemném kontextu. Každá otázka tedy ovlivňuje nejen odpověď na sebe samu, ale i na otázky následující. V jejich řazení je proto třeba postupovat tak, aby neovlivňovaly odpovědi na jiné, následující otázky. V některých případech je možné využít tzv. „haló efekt“, kdy vhodně formulovaná otázka může usnadnit pochopení a smysl otázky následující.

Dotazník byl respondentům (občanům Zlínského kraje a pracovníkům ministerstva) poskytnut v tištěné podobě se slovním komentářem při samotném provádění rozhovoru. Dotazník určený pro úředníky Zlínského kraje byl zaslán elektronicky a byl cíleně zaměřen na pozici vykonávanou na úřadě.

Formulace otázek a konstrukce dotazníku

Formu jednotlivých otázek, které byly použity v dotazníku, lze charakterizovat následovně:

1. ***Uzavřené*** – poskytují dvě nebo více předem formulovaných odpovědí. Častá forma je dichotomní – výběr ANO/NE, Souhlasím/Nesouhlasím. U formy vícealternativní se nabízí respondentovi kontinuum od jednoho pólu k pólu opačnému se stejným důrazem na všechny alternativy (určitě ANO – spíše ANO – nevím – spíše NE – určitě NE).
2. ***Otevřené*** – nejsou dané žádné předem formulované odpovědi, respondent odpovídá podle svého uvážení. Umožňuje identifikovat postoje, názory a emoce. Předpokladem použití je dodatečné vytvoření kategorií k jejich vyhodnocení. Někdy se používá forma ***polootevřené***, kdy jsou dány možné odpovědi, ale zároveň je možno doplnit vlastní variantu.
3. ***Škálové*** – nejsou samostatné otázky, ale tvoří soubory zaměřené na různé okruhy. Umožňují na zkoumaný jev získat pohled z více úhlů.

Kromě těchto typů otázek používáme ještě tzv. otázky pomocné:

4. ***Identifikační*** – týkající se obecných informací o respondentech.
5. ***Kontrolní*** – sloužící k ověření validity i reliability odpovědí.
6. ***Kontaktní*** – určené ke zpětné vazbě na respondenta, pokud měl dotyčný zájem o výsledky daného průzkumu. Tyto otázky byly použity pouze u úředníků ministerstev a úřadů Zlínského kraje.

Formy jednotlivých otázek se přirozeně v dotazníku překrývaly. Důvodem byla snaha o efektivní formu vyjádření odpovědi s cílem snadného zpracování a vyhodnocení dat.

Specifickým rysem téměř všech otázek, vyplývajících z jeho provedení formou strukturovaného rozhovoru je možnost vlastního komentáře respondenta. Tak, aby respondent mohl vyjádřit vlastní názor, který ale lze převést do standardizované podoby vhodné k vyhodnocení [4, 12].

3.7 Systém zvolených metod a technik analýzy dat

3.7.1 Metody a techniky kvalitativní analýzy dat

Z povahy výzkumu vyplývá i způsob zpracování získaných dat. U kvalitativního výzkumu, jehož výsledků se nedosahuje pomocí statistických procedur nebo jiných způsobů kvantifikace, bude použito statistických metod

pouze k vyhodnocení dílčích částí dotazníkového šetření. Snaha o celkové statistické zpracování by mohla vést k nesprávné interpretaci získaných údajů, tudíž bude použito pouze slovního komentáře, který nejlépe souhrnně vystihne názory respondentů. Budou vyhledávány společné charakteristiky, na jejichž základě bude možné zobecnit výsledky výzkumu.

3.7.2 Metody a techniky kvantitativní analýzy dat

Základem kvantitativní analýzy dat je deduktivní přístup. Deduktivní usuzování naplňuje požadavek dospívání k pravdivým závěrům, existuje-li jako výchozí bod pravdivý předpoklad – statisticky správně vyhodnocený výzkum. Při zpracování výsledků výzkumu bude jako statistická metoda kvantitativní analýzy dat použit procentuální výpočet, absolutní a relativní četnost. K ověření validity výzkumu pak bude použita metoda hodnocení shody více pořadí – Kendallův koeficient konkordance.

3.7.3 Četnosti a vizualizace dat

Při zpracování zjištěných údajů, tj. třídění prvního stupně pomocí deskriptivní statistiky, bylo využito absolutní a relativní četnosti vybraných znaků. V případě tohoto třídění byly varianty sledovaného kvantitativního znaku seřazeny buď do rostoucí (klesající) posloupnosti, nebo do jiného logického uspořádání. Každé variantě znaku byly přiřazeny odpovídající počty příslušných statistických jednotek. Tyto počty jsou nazývány četnostmi a vzniklé tabulky tabulkami rozdělení četností. Označují-li se jednotlivé obměny nespojitého kvantitativního znaku symbolem x_i, kde i = 1, 2, …, k, a jim odpovídající absolutní četnosti n_i, kde i = 1, 2, …, k, lze rozdělení četností vyjádřit způsobem uvedeným v tabulce 3. Vzhledem k nutnosti porovnání různých rozdělení četností lišící se svým rozsahem byly absolutní četnosti převedeny na četnosti relativní. Relativní četnosti p_i byly získány jako podíl jednotlivých absolutních četností k celkovému rozsahu souboru:

$$p_i = \frac{n_i}{\sum_{i=1}^{k} n_i}$$

přičemž platí:

$$\sum_{i=1}^{k} p_i = \sum_{i=1}^{k} \frac{n_i}{n} = \frac{1}{n} \sum_{i=1}^{k} n_i = \frac{1}{n} n = 1$$

Tab. 3 - Rozdělení četností

Varianta znaků x_i	Četnost		Kumulativní četnost	
	absolutní	relativní	absolutní	relativní
x_1	n_1	p_1	n_1	p_1
x_2	n_2	p_2	n_1+n_2	p_1+p_2
…	…	…	…	…
x_k	n_k	p_k	$\sum_{i=1}^{k} n_i = n$	$\sum_{i=1}^{k} p_i = 1$
Součet	$\sum_{i=1}^{k} n_i = n$	$\sum_{i=1}^{k} p_i = 1$	X	X

K lepší přehlednosti prezentovaných výsledků bylo využito pruhových, sloupcových a výsečových grafů. Pořadí hodnocených znaků v grafech je určeno logickým řazením nebo jejich klesající posloupností.

4 HLAVNÍ VÝSLEDKY PRÁCE

4.1 Ministerstva České republiky

V roce 2004 se uskutečnil prostřednictvím strukturovaného rozhovoru společně s dotazníkovým šetřením průzkum na jednotlivých ministerstev a Českém úřadu zeměměřičském a katastrálním, pomocí kterého se zjišťoval tehdejší stav informačních systémů na těchto nejvyšších úřadech veřejné správy.

Hlavní kritéria pro výběr IS a jeho dodavatele

Jednotlivá ministerstva rozhodují o výběru, nasazení a správě informačního systému samostatně. Na základě ankety mezi vybranými rezorty byla shrnuta důležitá kritéria, která využívají pro konečné rozhodnutí při výběru dodavatele. Podle důležitosti jsou seřazeny takto:

- reference v oboru činnosti,
- jednotný integrovaný systém pokrývající potřeby ústředí i zahraničních pracovišť,
- operativní zpracování velkého množství převážně textových dokumentů v různých jazycích,
- automatizace administrativy a podpora řídící činnosti,
- ekonomická dostupnost (cena), optimální poměr cena/výkon,
- zkušenost, spolehlivost, pružnost a dlouhodobá stabilita dodavatele, široké pokrytí potřeb,
- systém musí plně vyhovovat metodickým požadavkům.

Hodnocení přínosu IS

Proč vlastně úřady daný systém implementují? Zástupci resortů vidí přínos využití informačních technologií ve zlepšení:

- dostupnosti informací pro pracovníky,
- produktivity, resp. snížení nákladů,
- integrace procesů uvnitř úřadu,
- řízení procesů uvnitř úřadu,
- standardizace IS/IT v úřadě,
- komunikace s právnickými osobami,
- vztahu k ostatním úřadům státní správy,

- komunikace s veřejností,
- podpory vrcholového rozhodování.

Tab. 4 - Využití IS

Úřad	Počet zaměstnanců	Počet uživatelů IS	Počet pracovníků SaÚ* IS	Poměr uživatelů k zaměst.	Poměr prac. SaÚ k uživat.	Počet IS
MZe	2 500	2 400	25	96,0%	1,04%	1 + 50
MŠMT	474	15	3	3,2%	20,00%	3
MV	-	-	-	-	-	4**
MI	160	150	6	93,8%	4,00%	0
MPSV	600	4 000***	30	-	-	2 + 6
MŽP	650	600	20	92,3%	3,33%	37
MPO	793	750	14	94,6%	1,87%	6 + 60
MZV	2 300	2 000	90	87,0%	4,50%	3 + 2
MSp	-	-	8	-	-	6
ČÚZK	5 650	5 000	-	88,5%	-	1 + 5

* SaÚ – správa a údržba

** IS Policie nejsou uvedeny z důvodu zákona o utajovaných informací

*** zahrnuje zejména pracoviště mimo MPSV, která využívají jejich IS (ČSSZ, úřady práce)

Tab. 4 znázorňuje procentuální využití informačních systémů zaměstnanci a vytížení pracovníků IT na správu a údržbu těchto systémů fungujících na jednotlivých úřadech. Poslední sloupec zobrazuje hlavní a podpůrné informační systémy. V následující tab. 5 mají uvedené údaje pouze informativní charakter, jde o odhady bez hlubší analýzy účetnictví.

Tab. 5 - Náklady na IS (v Kč)

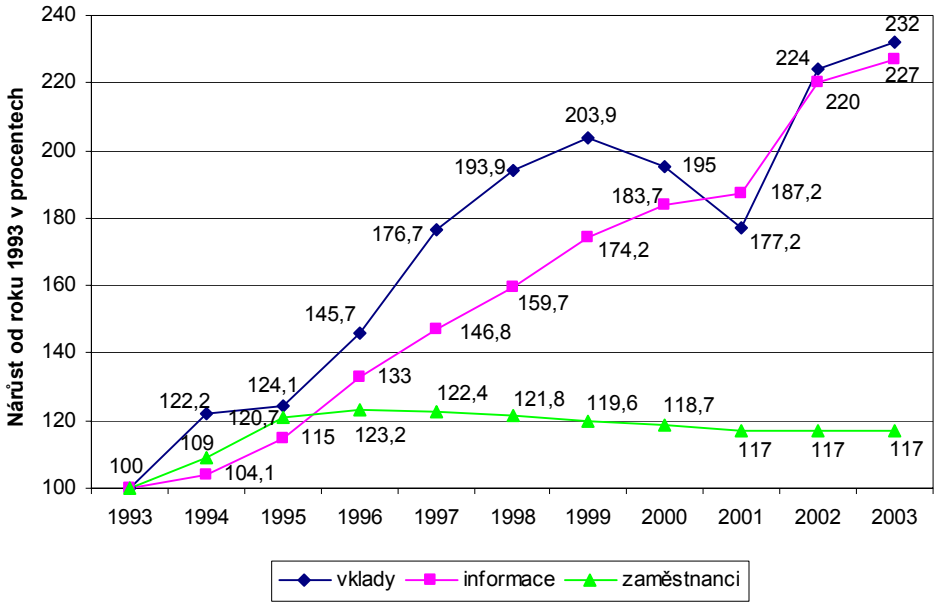
Úřad	Celkové náklady na pořízení systému	Celkové náklady na implementaci	Roční náklady na údržbu a provoz	Pořizovací náklady na 1 uživ.	Roční náklady na údržbu na 1 uživ.
MZe	300 000 000	200 000 000	120 000 000	208 333	50 000
MŠMT	775 240	975 240	135 135	116 699	9 009
MV	-	-	stovky mil.	-	-
MZV	100 000 000	300 000 000	200 000 000	200 000	100 000
ČÚZK	1 200 000 000	-	150 000 000	-	30 000

4.1.1 Český úřad zeměměřičský a katastrální

Český úřad zeměměřičský a katastrální (ČÚZK) používá vlastní IS (informační systém katastru nemovitostí) na 111 pracovištích, které jsou připojeny prostřednictvím WAN. V době, kdy tento systém vznikal, nebyla k dispozici dostatečná kapacita přenosových linek k tomu, aby mohl být celý systém založen na jedné centralizované databázi. Z tohoto důvodu disponuje každý katastrální úřad (KÚ) vlastní databází, která se v pravidelných intervalech (2 hodiny) aktualizuje s hlavní databází ČÚZK. V letošním roce se očekává zásadní změna tohoto systému.

Pro občana je důležité, že od ledna tohoto roku může nahlížet do online katastru nemovitostí na internetové adrese http://katastr.cuzk.cz. Dokumenty pořízené tímto způsobem z katastru nemovitostí jsou formálně i věcně naprosto shodné s dokumenty vydanými katastrálními úřady. Mají však výlučně informativní charakter a nelze je jako takové prozatím použít jako úředně platný výpis. ČÚZK o této možnosti uvažuje, svým klientům ji nabídne po schválení novely zákona o elektronickém podpisu, která v naše právním řádu zakotvuje institut časového razítka.

Pozitivní vliv využívání informačních systémů při práci na katastrálních úřadech je patrný z následujícího grafu. Doba na vyřízení žádosti se postupně zkracuje. Průměrná doba se dnes pohybuje okolo 1,7 měsíce na žádost, avšak na více než 50 pracovištích zvládnou vyřídit žádost do jednoho měsíce. Při stávajícím počtu zaměstnanců je možné vyřídit mnohem více žádostí za stejnou dobu. Z grafu je patrný nárůst ukazatelů od roku 1993 o 230 % při mírném nárůstu počtu zaměstnanců.



Obr. 12 - Výkonnost katastrálních úřadů [vlastní zpracování dle ČÚZK]

4.1.2 Ministerstvo životního prostředí

Na ministerstvu životního prostředí (MŽP) funguje přes 37 rozdílných informačních systémů a více než šest tisíc databází. V současnosti ministerstvo připravuje rozsáhlý projekt Integrovaný registr znečišťování (IRZ), který bude spojovat 7 ohlašovacích procesů do jednoho, který umožní splnit ohlašování povinnost znečišťovatelů v 7 zákonných oblastech. Tento systém by měl fungovat od roku 2005. Databáze, které dnes fungují osamoceně, se mají propojit jak po obsahové, tak po procesní stránce. Dochází totiž k tomu, že některé záznamy se v různých databázích duplují.

4.1.3 Ministerstvo práce a sociálních věcí

Ministerstvo práce a sociálních věcí (MPSV) provozuje dva hlavní informační systémy, které jsou propojeny online s finančními úřady:

- IS SSP – informační systém státní sociální podpory (262 instalací), který řeší příjem žádostí o státní sociální podporu a slouží jako podklad k rozhodování a výplatě dávek;
- IS SZ – informační systém služeb zaměstnanosti (400 instalací), který slouží k evidenci zájemců o zaměstnání a evidenci volných míst a zprostředkování zaměstnání.

V lednu 2002 MPSV zveřejnilo na své www adrese www.mpsv.cz formuláře žádostí o jednotlivé dávky státní sociální podpory a formulář hlášení změn. V první verzi programu byly tyto formuláře přístupné dvěma způsoby:

- pouze k vytištění, ručnímu vyplnění a podepsání,
- k elektronickému vyplnění (i částečnému), vytištění a ručnímu podepsání, od července 2002 je k dispozici i třetí způsob – úplná elektronická komunikace – formuláře je možné podat přímo, podepsané elektronicky pomocí zaručeného elektronického podpisu, vydaného akreditovaným poskytovatelem certifikačních služeb.

K dnešnímu datu je na stránkách ministerstva možné podávat 13 formulářů plně online. Na sedmdesáti kontaktních pracovištích jsou tzv. informační kiosky, ze kterých se občané mohou během několika sekund po internetu připojit k evidovaným údajům. Úřad eviduje přes 100 elektronicky podaných a elektronicky podepsaných žádostí. Ministerstvo zahájilo v roce 2001 projekt

pro využívání profesních a klientských čipových karet. K dnešnímu dni bylo vydáno na osm tisíc těchto čipových karet.

Profesní čipová karta je bezpečným nástrojem pro vytvoření elektronického podpisu a umožňuje jednoznačnou autentizaci. S pomocí profesních čipových karet a programového vybavení je zajištěno podstatně kvalitnější zabezpečení přenosu dat s využitím šifrování a elektronického podpisu, přístup k datům klientů na jejich čipových kartách a další možnosti.

Klientská čipová karta bude obsahovat elektronicky uložená identifikační data držitele, která umožní efektivnější práci s informačním systémem státní a sociální podpory a výhledově i v dalších informačních systémech veřejné správy.

S pomocí klientských čipových karet se bude možné přihlásit k informačnímu kiosku a zjistit údaje, které jsou uloženy na čipové kartě, a údaje, které jsou o držiteli čipové karty (klientovi) uloženy v databázi státní sociální podpory. Některé údaje bude moci dokonce držitel karty sám měnit, aniž bude muset čekat ve frontě u přepážky. Na úřadech práce bude v budoucnu možné na informačních kioscích vyhledávat volná místa vhodná pro držitele čipových karet.

4.1.4 Ministerstvo průmyslu a obchodu

Ministerstvo průmyslu a obchodu (MPO) využívá 6 hlavních informačních systémů a přibližně 60 dalších podpůrných systémů. Samotné ministerstvo vzniklo sloučením devíti původních ministerstev, takže na počátku stálo 364 autonomních systémů. V roce 2000 byly systémy z důvodů kompatibility sloučeny, avšak 200 z nich zůstalo. Po přechodu na operační systém MS Windows 2000 zůstalo dosavadních 65–70 systémů.

www.businessinfo.cz – je důkazem, že státní organizace jsou schopny se domluvit. MPO a CzechTrade spolu s dalšími partnery, organizacemi a institucemi státní správy (MZe, MZV, MPSV, MF a další), spustili projekt BusinessInfo.cz - Integrovaný systém pro podnikání a export, jehož cílem je vytvoření všeobecně dostupného jednotného on-line informačního místa na Internetu pro podnikatele, a to na základě koordinace vládních agentur a institucí i dalších organizací, které se zabývají poskytováním a vytvářením informací a dokumentů pro podnikatele.

4.1.5 Ministerstvo spravedlnosti

Ministerstvo spravedlnosti zastřešuje ve svém resortu tyto informační systémy:

- ISAS – informační systém pro okresní soudy,
- ISVKS – informační systém pro vrchní a krajské soudy,
- ISNS – informační systém pro nejvyšší soud,
- ISYZ – informační systém pro státní zastupitelstva – od okresních až po nejvyšší,
- Rejstřík trestů – databáze rejstříku trestů, která v současné době prochází inovací
- IRES – ekonomický a mzdový systém.

Jsou to evidenční systémy, kde jsou shromážděny spisy většiny soudních procesů. Celé spisy se však nepřevádí do digitální podoby. Pomocí informačního systému zjistíte pouze základní údaje o spisu, a kde se nachází. Systémy také umožňují generovat statistiky o funkčnosti soudů. Vzájemná vazba mezi jednotlivými systémy je možná, dosud však nerealizovaná.

4.1.6 Ministerstvo školství, mládeže a tělovýchovy

Ministerstvo školství, mládeže a tělovýchovy (MŠMT) provozuje tři informační systémy, z nichž jeden spravuje ve spolupráci s Masarykovou univerzitou v Brně (databáze studentů vysokých škol). Informační systémy slouží pro vedení agendy v oblasti personalistiky a zároveň pro evidenci základních a středních škol. Na ministerstvu školství probíhá příprava výběrového řízení na dodání informačního systému pro elektronickou výměnu dokumentů, který bude určen pro zaměstnance ministerstva formou outsourcingu.

4.1.7 Ministerstvo vnitra

Ministerstvo vnitra (MV) využívá čtyři informační systémy a několik desítek dalších systémů pro vedení menších agend.

SAP/R3 – implementován model personalistika a ekonomická agenda

IIS SDE – integrovaný informační systém správních a dopravně správních evidencí slouží k evidenci obyvatel, občanských průkazů, pasů, řidičských průkazů a technických průkazů. Tento systém využívají MPSV, MF, MS a územní soudy, připravuje se provázání s ČÚZK. Ostatní útvary mají pouze možnost nahlížet do systému, nemohou aktualizovat data.

Veškeré policejní a hasičské složky mají již dnes možnost zvyšovat svou kvalifikaci a informovanost formou E-learningu, který je dostupný na intranetu ministerstva.

4.1.8 Ministerstvo zemědělství

Ministerstvo zemědělství (MZe) zveřejnilo na svých webových stránkách formuláře, které se bohužel musí prozatím tisknout, vyplnit a poslat standardní papírovou formou. Převážně se jedná o formuláře na přímou dotaci a jiné finanční podpory.V budoucnu je plánován přechod na elektronickou formu.

Integrovaný administrativní a kontrolní systém (IACS) vícenásobné a křížové kontroly celkových podpor je velmi detailní systém kontroly soustavy zemědělských dotací. Podpory na zemědělskou činnost v Evropské unii jsou nenárokové a nezbytnou podmínkou jejich vyplácení v dané členské zemi je funkční IACS v součinnosti s platební agenturou. Jeho vytvoření bylo uloženou Radou EU v roce 1992 v souvislosti s požadavkem na účelnou administraci žádostí o podporu a zvýšení účinnosti kontrolních struktur pro vyplácení podpor z EAGGF (evropský záruční a garanční fond).

IACS výrazně zefektivňuje výkon kontroly, administraci žádostí, vyplácení podpor, udělování sankcí. Současně je využíván také jako informační zdroj pro realizaci dalších činností v sektoru zemědělství např. nastavení rozsahu podpor, výrobní kvóty, odhady úrody nebo z hlediska potřeb krizového řízení. Z hlediska kandidátských zemí systém IACS není možné obejít ani nahradit.

4.1.9 Ministerstvo informatiky

Ministerstvo informatiky bylo zákonem 110/2007 Sb., ze dne 19. dubna 2007 zrušeno a jeho kompetence byly převedeny Ministerstvu vnitra. Přesto MI do seznamu ministerstev zahrnuji, protože mělo svoji roli při budování e-Governmentu.

Mladé a relativně malé ministerstvo informatiky nemělo odbor informatiky. Jako jediné ministerstvo tehdy nedisponovalo žádným velkým uceleným informačním systémem. Ministerstvo informatiky zajišťovalo rozvoj, výstavbu a metodické řízení informačních systémů veřejné správy, realizovalo program intranetu veřejné správy jako jednotného a zabezpečeného komunikačního prostředí.

Prostřednictvím atestací informačních systémů a kontrolní činnosti realizovalo zpětnou vazbu na metodiky, best practices a standardy ISVS a jejich dodržování v praxi. Projektovým přístupem omezovalo vznik duplicit při provozování ISVS. Zabezpečovalo reálné požadavky na čerpání financí

z veřejných rozpočtů v oblasti informačních a komunikačních technologií. Připravovalo technické podmínky pro efektivnější výkon veřejné moci. Atestace mohou provádět pouze atestační střediska, nezávislé instituce, kterým Ministerstvo informatiky vydalo k výkonu atestací pověření.

Bílá kniha o elektronickém obchodu – je základním vládním dokumentem v oblasti podpory elektronického obchodu. Prezentuje vizi rozvoje elektronického obchodu v České republice a způsoby jeho podpory.

4.2 Vybrané úřady Zlínského kraje

Celý průzkum probíhal on-line přes webové rozhraní. Bylo osloveno na 320 úředníků ve Zlínském kraji, kterým byl zaslán email s odkazem na webový formulář. Byli osloveni úředníci z městských úřadů 2. a 3. typu, které reprezentuje města velikosti Zlína, Vsetína, Kroměříže, Rožnova a další, což odpovídá 13 městům Zlínského kraje.

Dotazník byl rozdělen do dvou částí. V první části byla zjišťována momentální situace o zavedených informačních systémech na jednotlivých úřadech, převážně pomocí uzavřených otázek. V druhé části byla pomocí otevřených otázek, snaha zjistit názory jednotlivých respondentů na zlepšení situace, kterou popisovali v první části tohoto dotazníku.

Po prvním rozeslání emailu s žádosti o vyplnění webového dotazníku jej vyplnilo 12% všech dotázaných. Zhruba po dvou týdnech byly osloveni stejní lidé, kteří však dotazník nevyplnili s novou žádostní o jeho vyplnění. Z celkového počtu oslovených úředníků nakonec odpovědělo 23%, informatiků 54%. Konečná návratnost vyplněných dotazníků činila 24,06%.

4.2.1 Stav zavádění IS na úřadech

Pouze 2 respondenti uvedli, že „*IS máme zaveden, ale zvažujeme změnu*“ jinak ostatní respondenti uvedli, že „*IS máme zaveden, jsme s ním spokojeni*“.

Tento ukazatel znamená, že výběr informačního systému jednotlivé úřady nijak nepodcenily a věnovaly mu dostatečný čas a prostor, vědomy si toho, že tyto systémy nejsou levné a hlavně, že budou muset se zakoupeným systémem pracovat a jejich rozpočet jim nedovolí, aby mohly tento systém jednoduše vyměnit.

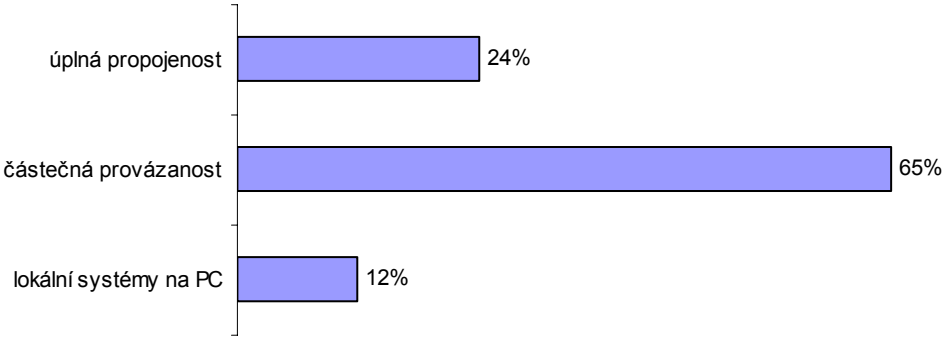
4.2.2 Celkový počet využívaných IS na úřadech

Na úřadech funguje vícero odborů, z toho se dalo předvídat, že budou mít nasazeno několik informačních systémů.

Odpovědi byly přímo závislé na velikosti úřadu, čím větší úřad, tím více informačních systémů. Z toho plyne myšlenka, proč se firmy, které vytváří tyto IS, nesnaží o vytvoření nějakého více modulového systému, jako to známe v klasickém soukromém sektoru, kde jsou nabízený ERP systémy, které dokáží pokrýt svojí modulovostí obrovský rozsah firemních procesů.

Pokud úřad využívá více informačních systémů, vyvstává otázka, zda jsou tyto systémy navzájem propojeny.

Získané odpovědi přesně popisují momentální stav informačních systémů ve veřejné správě. Úplnou propojenost má jen 24% dotázaných úřadů. Částečnou provázanost svých informačních systémů má 65% úřadů a zbylých 12% pracuje s nepropojenými „izolovanými“ informačními systémy. Z těchto 12% je ovšem řada systémů, které ani propojeny být nemůžou z legislativních důvodů (např. zákon o ochraně osobních údajů).



Obr. 13 - Stupeň integrace informačních systémů

4.2.3 Využití outsourcingu na úřadech

V soukromém sektoru začíná být běžnou situací, že firmy informační systémy nekupují, ale využívají služeb jiných společností, které nabízejí outsourcing. Z dotazníku usuzuji, že veřejný sektor sleduje, co se děje ve firmách, a zřejmě proto 62% dotázaných úřadů udržuje svůj informační systém částečně vlastními silami a částečně outsourcingem. 32% dotázaných outsourcingu nevěří a zabezpečují si svůj informační systém jen vlastními silami. Na druhou stranu úřadů plně využívající outsourcing je sice jen 5,5%, ale tyto mohou ukázat, zda se vydaly správnou cestou.

Přechod na outsourcing si v dnešní době dokáže již přestavit 56% dotázaných, kteří doposud zabezpečují informační systém vlastními silami

4.2.4 Propojenost jednotlivých počítačových stanic

V dnešní době si snad ani nedovedeme přestavit, že by úředníci měli pracovat na samostatných počítačových jednotkách a potom předávat kolegovi data přes disketu nebo za pomocí usb klíče. Otázkou jsem se chtěl ujistil, že opravdu jsou počítače zasíťované. Opět se potvrdily moje předpoklady a odpovědi byly vyplněny jednomyslně „*PC propojeny v rámci LAN*“.

4.2.5 Hlavní důvody zavedení daného IS

Nároky na práci jsou v dnešní době zvyšovány nejen v plně konkurenčním prostředí soukromého sektoru, ale také ve veřejné sféře. Od úředníků se očekává, že jejich práce bude rychlejší, přesnější a efektivnější. Odpovědi jsou seřazeny podle významnosti (1 – nejvýznamnější, 8 – nejméně významná).

Nemožnost zvládnutí agendy dosavadním způsobem	1,43
Efektivita práce	1,57
Zlepšení služeb občanům	1,88
Legislativa	2,51
Zrychlení služeb občanům	2,63
Vlastní rozhodnutí	3,44
Technická zaostalost (rozhodli se, že se zdokonalí)	3,97
Požadavek nadřízených orgánů	4,43
Požadavky ze strany občanů	4,74
Srovnání úrovně s jinými úřady	4,85

4.2.6 Duplicita – zbytečné několikanásobné ukládání stejných dat, kde k tomu nejčasněji dochází

Polovina dotázaných úředníků tvrdí, že k duplicitě údajů nedochází, zato druhá polovina je názoru, že se za současné situace duplicitě nevyhne. Jako hlavní důvod je použito tvrzení, že duplicita nastává v případech, kde zákon neumožňuje registry sloučit. Tento současný stav by měl odstranit zákon o základních registrech, kde by měla být data shromažďována pouze jednou. Z těchto registrů by čerpaly informace ostatní úřady, a tím by odpadla nutnost mít uložená data na každém úřadu zvlášť.

4.2.7 Rozložení výdajů na ICT na úřadě

Výsledná tabulka znázorňuje průměrné hodnoty rozložení jednotlivých výdajů v letech 2004 a 2007. Údaje v tab. 6 mají pouze informativní charakter, jedná se o odhady bez hlubší analýzy rozpočtů. Po kompletní implementaci informačních systémů by mělo dojít k vyššímu navýšení procent u technické podpory a opravy a údržbu.

Dále by mělo docházet k postupnému snižování procent u nákladů na hlasové a datové služby. Jedná se o využívání nových technologií a zvyšující se konkurenci na trhu poskytující datové a hlasové služby. Hlasové služby by měly být pomalu na ústupu a měly by být plně nahrazeny datovými. Nechci tím nijak popřít význam hlasových služeb, ale již dnes se využívá VoIP čili protokol pro přenos hlasu pomocí internetu, a ne klasickou telefonní linkou.

Tímto by mělo dojít ke spojení dat a hlasu. Připojení k internetu se stále zdokonaluje a hlavně zásadně klesá poměr cena/rychlost.

Tab. 6 - Porovnání výdajů na ICT v letech 2004 a 2007

Oblast	2004	2007
Neinvestiční pořizovací náklady HW	14 %	17 %
Neinvestiční pořizovací náklady SW	8 %	12 %
Náklady na hlasové a datové služby	19 %	13 %
Technická podpora	12 %	21 %
Opravy a udržování	12 %	13 %
Náklady související s GIS	6 %	6 %
Investiční náklady HW	15 %	10 %
Investiční náklady SW	14 %	8 %

V následující tabulce 7 jsou vypsány systémy, které používá daná oblast, či agenda ke své činnosti. Na základě získaných odpovědí byly zjištěny i základní nedostatky užívaných aplikací. Systémy byly hodnoceny podle těchto kritérií:

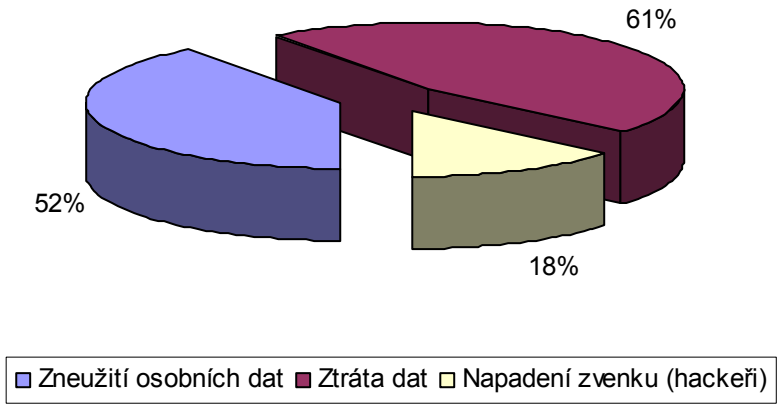
- funkcionalita,
- datová základna,
- uživatelské rozhraní,
- možnost integrace s jinými IS,
- dodavatelský servis.

Z hodnocení vyplývá, že systémy jsou z hlediska datové základny a funkcí plně dostačující. O něco hůře dopadli dodavatelé se svým servisem a uživatelské rozhraní. Nedostatkem se jeví možnost integrace s jinými aplikacemi.

Tab. 7 - Přehled nejčastěji využívaných SW dle oblastí činnosti (v %)

Ekonomická oblast		Kultura	
Ginis	52,1	Žádný SW	63,4
Fenix	17,3	CityWare	9,1
Radnice Vera	13,0	Ginis	9,1
Správa majetku		Radnice Vera	9,1
Munis	25,0	Stavební úřad	
Fenix	25,0	VITA	32,1
Radnice Vera	12,5	CityWare	9,4
Ginis	12,5	MISYS	9,4
Správní agendy		Microstation	7,6
IISSDSE-MV	24,0	MS Office	7,6
VITA	16,0	Radnice Vera	7,6
Munis	12,0	Spisová služba	
Radnice Vera	8,0	Munis	26,3
Registr živnost. podnikání	8,0	Ginis	21,1
Sociální služby		PVT SAS	21,1
OK-Nouze (MPSV)	48,2	Radnice Vera	15,8
CityWare	25,9	E-SPIS	5,3
Pors	7,4	Provozní IS	
Investiční oblast		Fenix	28,6
Žádný SW	45,4	Ginis	14,3
CityWare	9,1	Munis	14,3
Ginis	9,1	MS Office	14,3
GIS	9,1	CityWare	7,1
Munis	9,1	Radnice Vera	7,1
Radnice Vera	9,1	Mzdová a personální oblast	
Životní prostředí		FluxPam	37,5
Více drobných aplikací	12,9	DC SAM – DOC	12,5
T-Mapy	12,9	Cominfo	6,3
CityWare	6,5	DTG	6,3
Inisoft	6,5	Gordic	6,3
Kvasar	6,5	Kvasar	6,3
Vita	6,5	Munis	6,3
Yamaco	6,5	Rada a zastupitelstvo	
Školství		DZR	15,4
Fenix	30,8	MS Office	14,1
Žádný SW	23,1		
Ginis	15,4		
CityWare	7,7		
FluxPam	7,7		
Radnice Vera	7,7		

4.2.8 RIZIKA: Co považují úředníci za největší riziko provozu IS na úřadě



Obr. 14 - Největší rizika provozu IS na úřadě

Z tohoto grafu jsou překvapivá dvě čísla. První je celkem nízké procento napadení hackery. Úředníci tedy věří, že jejich systém je zabezpečený, nevěří však sami sobě. Budeme-li považovat malé procento získání a zneužití osobních dat u napadení zvenku, nezbývá, než že se musí jednat o získání těchto údajů uvnitř samotného úřadu. Zde to tedy není o IS jako takovém, ale hlavně změnit myšlení lidí a začít věřit sami sobě.

4.2.9 BARIÉRY: Co brání efektivnímu využití IS na úřadě

Doslova alarmující je zjištění, že se nejedná ani o to, že by úředníci nebyli dostatečně kvalifikování nebo nebylo dostatek financí na zakoupení lepšího informačního systému. Hlavní důvod, který na sebe uvedli úředníci, je neochota učit se nové věci. Tím se dostávám k jedné podstatné otázce. Má vůbec cenu investovat miliony korun do systémů a do školení, když sami úředníci nejsou ochotni tyto systémy pochopit a tím zjistit, zda jim opravdu jejich práci zjednoduší? Na druhou stranu si musíme říci, že informační systémy ve veřejné správě neslouží pouze pro úředníky samotné, ale i pro občany, kteří díky těmto systémům v budoucnu zvládnou vyřídit více záležitostí, a to právě bez oněch úředníků, kteří nemají snahu učit se novým věcem.

Pozn.: V rámci škály 1 - 5 vyjadřovali úředníci hlavní bariéry, které brání efektivnějšímu využívání jejich informačního systému. (1 - největší, 5 - nejmenší).

Neochota učit se nové věci	2,17
Nedostatek finančních prostředků	2,53
Nedostatečná kvalifikace pracovníků pro práci s IS/IT	2,61
Nevyhovující nabídka SW produktů na trhu	3,00

4.2.10 V čem spatřují zaměstnanci úřadů hlavní přínosy užívaného IS

V předchozí otázce jsem zjistil, že úředníci nejsou ochotni se učit novým věcem. Jak je tedy možné, že hlavní důvody uvádí skutečně racionální podněty, které jim daný informační systém nabízí?

Pozn.: V rámci škály 1 - 11 vyjadřovali úředníci hlavní přínosy (1 - největší, 11 - nejmenší)

Zvýšení dostupnosti informací pro zaměstnance	3,06
Zvýšení efektivity procesů, postupů	3,47
Rychlejší přístup k datům	4,53
Zabezpečení sdílení dat	4,69
Zlepšení podpory a koordinace činnosti jednotlivých úřadů	4,94
Zvýšení dostupnosti informací pro veřejnost	5,24
Zvýšení informační gramotnosti zaměstnanců	5,24
Zajištění bezpečnosti a ochrany dat	5,59
Standardizace IS/IT ve VS	6,13
Zvýš. produktivity resp. snížení nákladů	6,33
Snížení výdajů na IT	8,07

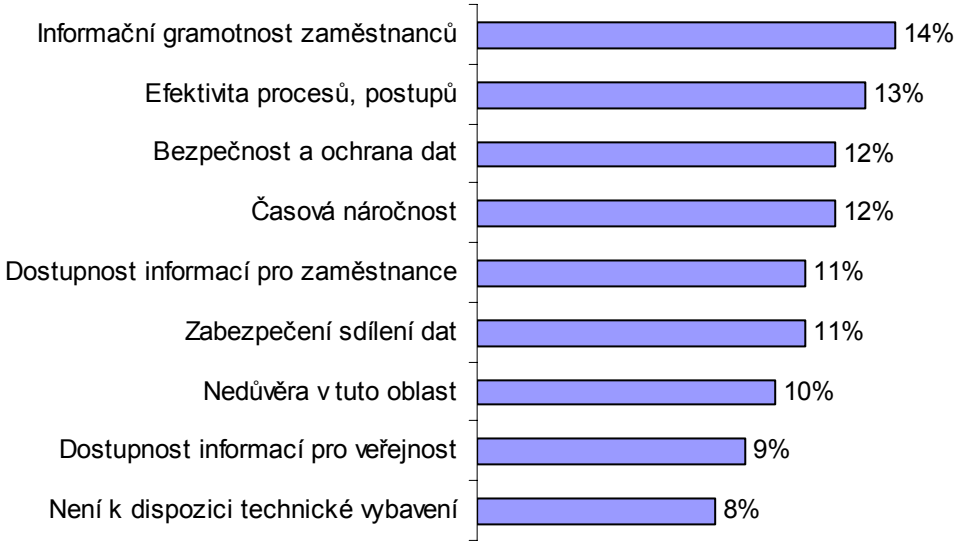
4.2.11 Největší těžkosti při práci s IT

Potvrzují předchozí zjištění. Jestliže se úředníci nejsou ochotni se učit novým věcem, tak potom musí být zákonitě na prvním místě největším problémem samotná IT gramotnost těchto lidi. Vše souvisí se vším, takže jestliže danému informačnímu systému nerozumí, vázne efektivita postupů a roste časová náročnost jejich práce.

Když na se to podíváme z jiného úhlu pohledu, a to, že pokud by byl samotný informační systém špatně navržen, tak by se bod 2 stal hlavním problémem

ISVS. I tak by bylo jednodušší napravit toto, než počítačovou gramotnost zaměstnanců a jejich neochotu učení se.

Jediným příznivým zjištěním zůstává, že technické vybavení už je na takové úrovni, že nezpůsobuje potíže pro samotnou elektronizaci procesů na úřadech.



Obr. 15 - Překážky pro práci s ICT

4.2.12 Školení

V odpovědích ohledně školení v IT oblasti si úředníci částečně protiřečí. Z předchozích odpovědí vyplývá, že není velká snaha učit se novým věcem, ale na druhou stranu považuje větší část úředníků jednotlivá školení za nedostatečná, proto by se mohla opakovat častěji, ale ve vyšší kvalitě.

Jsou dvě možnosti proč tomu tak je:

1. školení jsou opravdu nedostatečná, případně školitel nedokáže danou problematiku řádně vysvětlit nebo zaujmout,
2. školení jsou dostatečná, ale jak bylo řečeno, není snaha získávat nové poznatky a zaměstnanci tato školení chápou jako možnost relaxace v pracovní době.

4.2.13 Návrhy na zlepšení

Druhou částí dotazníkového šetření byly otevřené otázky, kde byl dán prostor samotným úředníkům, aby navrhli zlepšení, která by pomohla jejich práci zefektivnit a zjednodušit. Odpovědi jsou sesumarizovány a vybrány 3-4 nejčastěji se opakující, zároveň nejsou výroky úředníků jinak upravovány.

Na co je v současnosti kladen největší důraz na Vašem úřadě?

- péči o občany,
- efektivita chodu úřadu, finanční úspory, kvalitnější výkon správy (zrychlení, elektronizace postupů apod.),
- využití všech možností IS, propojení mezi jednotlivými procesy, bezpečnost,
- na zbytečnou byrokracii a lpění na dodržování některých zákonů, jejichž hodnota a přínos jsou minimální (např. zákon o kontrole apod.).

Domníváte se, že optimalizací procesů by mohlo dojít ke zkrácení času při plnění úkolů, na kterých spolupracuje více odborů Vašeho úřadu?

- drtivá většina napsala *Ano*,
- minimum napsalo *Spíše ne*,
- Bohužel zazněl i takovýto názor: „*Optimalizace procesů de facto jen přidává práci úředníkům o nadbytečné úkony, které nikdy plnit nemuseli, takže času naopak pochybí a úřednictvo se stává otrokem těchto systémů.*“

Jak by se tyto prostoje daly minimalizovat, případně odstranit?

- zjednodušením legislativy, standardizací postupů,
- centrálním propojením jednotlivých systémů VS, včetně legislativní provázanosti,
- zvýšením počítačové gramotnosti úředníků,
- efektivnějším využitím stávajících prostředků, lepší organizací práce
- a komentář, který to celé shrnuje: „*Těžko, pokud nebude systém jednodušší (lepší SW) a jednotný na všech úsecích a pokud možno i s ministerstvy na úsecích s centrálními registry apod., odpor úředníků zůstane, protože se přidává „zbytečná“ práce.*“

Co navrhujete ke zlepšení stávající situace?

- zrušení či zjednodušení některých zákonů, náprava legislativy,
- větší integritu IS,
- věnovat větší pozornost vnitřní komunikaci,
- zvýšit IT gramotnost zaměstnanců.

4.2.14 SWOT analýza stávajících informačních systémů na úřadech Zlínského kraje

Analýza SWOT hodnotí celkovou situaci využívání informačních systémů ve vybraných obecních úřadech Zlínského kraje. Zjištění mohou vést k využití silných stránek a příležitostí ke svému růstu, eliminaci slabých stránek a lepší připravenosti na potencionální ohrožení.

Silné stránky

- zvýšení dostupnosti informací pro zaměstnance,
- rychlejší přístup k datům,
- elektronická komunikace s občany,
- provádění školení a vzdělávání zaměstnanců,
- snaha o kvalitní výkon veřejné správy.

Slabé stránky

- neochota učit se nové věci,
- efektivita postupů, procesů,
- nedostatečná kvalifikace pracovníků pro práci s IS/IT,
- nedostatek času pro zapracování.

Příležitosti

- zvýšení efektivity postupů a procesů,
- zvýšení profesionality a kvality poskytování služeb občanům,
- zvýšení dostupnosti informací pro veřejnost,
- zlepšení podpory a koordinace činnosti jednotlivých úřadů.

Ohrožení

- pomalu rostoucí informační gramotnost zaměstnanců,
- nedostatečná propojenost informačních systémů veřejné správy,
- zneužití osobních dat, ztráta dat, napadení hackery,
- nedostatek finančních prostředků.

4.3 Občané

Poslední dotazníkové šetření bylo provedeno v první polovině letošního roku. Náhodně byli osloveni občané před několika úřady veřejné správy ve Zlíně.

Dotazník měl hlavní roztřiďovací otázku, která zjišťovala, zda dotazovaní znají nebo neznají Czech POINT. Na základě této roztřiďovací otázky byly následně modifikovány ostatní otázky.

Po vyhodnocení jednotlivých otázek byla udělána korelační analýza, aby se zjistilo, zda existuje závislost mezi jednotlivými otázkami. Výsledné dendrogramy jsou uvedeny v příloze E.

4.3.1 Úvodní informace

Celkově se průzkumu zúčastnilo 273 občanů Zlína. Na hlavní roztřiďovací otázku odpovědělo 126 lidí, že Czech POINT zná, a 147, že nikoliv. Z celkového počtu bylo 44,6% mužů a 56,4% žen. Věkovou hranici 18-35 let naplnilo 41,7%, 36-50 let 39,5%, 51-65 let 11,7% a nad 66 let mělo 7,1% lidí.

Následující dvě tabulky znázorňují nejvyšší dosažené vzdělání a pracovní zařazení dotazovaných osob. Jedna účastnice považovala tyto údaje za osobní, a proto je celkový počet 272.

Tab. 8 - Nejvyšší dosažené vzdělání dotazovaných osob

Vzdělání	Relativní četnost	Absolutní četnost
Základní	5,88 %	16
Vyučen/a	15,81 %	43
Středoškolské	51,84 %	141
Vysokoškolské	26,47 %	72

Tab. 9 - Pracovní zařazení dotazovaných osob

Pracovní zařazení	Relativní četnost	Absolutní četnost
Student	12,87 %	35
Zaměstnanec	48,90 %	133
Podnikatel, živnostník	16,17 %	44
Na mateřské dovolené	5,15 %	14
Nezaměstnaný	7,72 %	21
Důchodce	9,19 %	25

Oslovený vzorek respondentů je téměř rovnoměrně rozložen mezi muže a ženy. Z 81,2% se jedná o osoby do 50 let čili o produktivní skupinu obyvatel. Dosažené vzdělání (skoro 80% středoškolské a vysokoškolské vzdělání)

s pracovním zařazením (65% tvoří zaměstnaní lidé, ať již jako zaměstnanci, nebo jako podnikatelé) odpovídá běžnému vzorku obyvatel v naší republice.

4.3.2 Četnost vyřizování žádostí na úřadech

Největší skupinou návštěvníků úřadů veřejné správy jsou zaměstnanci (48,90%), kteří zavítají na úřad jednou ročně (13,60%), Další častější návštěvy u zaměstnanců jsou již vyrovnané, půlroční, měsíční a skoro denní se pohybují okolo 9%. Nejčastěji vyřizují různé poplatky, přídavky, daně či výpisy z KN. Studenti navštěvují úřady převážně jednou nebo dvakrát za rok. Podnikatelé jednají s úřady nejčastěji, proto jsou na úřadech skoro denně. Zajímavou skupinou jsou lidé v důchodovém věku, kteří chodí na úřady jednou měsíčně a z 90% zařizují podobné věci, jako jsou poplatky (pes, byt, komunální odpad).

Tab. 10 - Shrnuje pracovní zařazení, vzdělání a četnost návštěv úřadů (v %).

pracovní zařazení	vzdělání	1x ročně	1x za ½ roku	1x měsíčně	1x za 14 dní	1x týdně	skoro denně
student	SŠ	35,48	25,81	22,58	6,45	6,45	3,23
	VŠ	33,33	-	-	66,67	-	-
zaměstnanec	základní	16,67	33,33	16,67	16,67	16,67	-
	vyučen	37,50	16,67	29,17	12,50	4,17	-
	SŠ	30,00	17,14	15,71	8,57	8,57	20,00
	VŠ	18,18	24,24	18,18	9,09	3,03	27,27
podnikatel	vyučen	25,00	50,00	25,00	-	-	-
	SŠ	23,08	-	23,08	7,69	15,38	30,77
	VŠ	-	29,63	14,81	14,81	7,41	33,33
na mateřské	vyučen	50,00	-	50,00	-	-	-
	SŠ	16,67	33,33	16,67	33,33	-	-
	VŠ	-	16,67	16,67	66,67	-	-
nezaměstnaný	vyučen	12,50	37,50	25,00	12,50	-	12,50
	SŠ	7,69	7,69	23,08	38,46	23,08	-
důchodce	základní	11,11	-	88,89	-	-	-
	vyučen	20,00	-	80,00	-	-	-
	SŠ	25,00	12,50	37,50	12,50	12,50	-
	VŠ	-	-	33,33	66,67	-	-

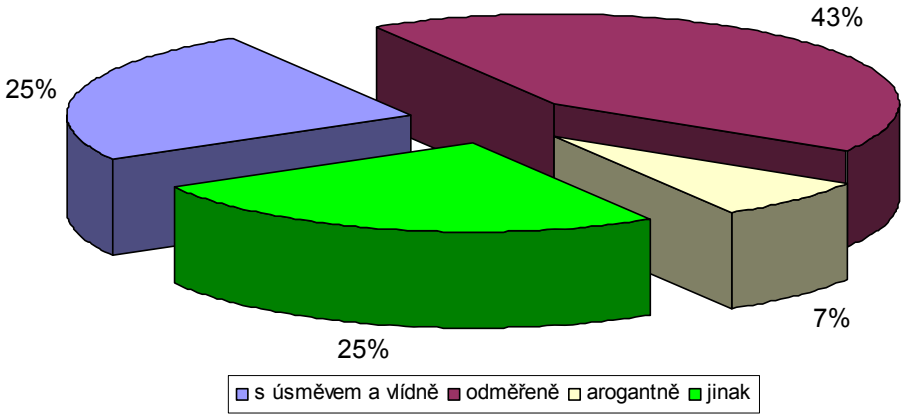
4.3.3 Jednání úředníků a doba vyřízení

Dalším dotazem se zkoumalo, jak lidé vnímají jednání úředníků a zda doba, kterou na úřadech stráví, je úměrná velikosti řešeného problému. Z následujícího grafu je patrné, že jsou úředníci vnímání spíše negativně. Celých 50% dotázaných uvedlo, že úředník za přepážkou působil odměřeně, až arogantně.

Na druhou stranu celá čtvrtina dotazovaných zažili jednání vlídné a s úsměvem. Posledních 25% osob by se dalo rozdělit na dvě poloviny, tito lidé označovali jednání úředníků částečně pozitivně i negativně zároveň. Jako nejčastější odpovědi byly:

- „Chování úředníka je závislé na tom, co potřebuji a kolik to zabere času,
- jak kdy, podle situace,
- úředně.“

Doba vyřízení byla z 55% hodnocena jako přiměřená. 34% lidi si myslelo, že doba byla zbytečně dlouhá a 11% dotazovaných bylo překvapeno při jednání rychlostí vyřízení záležitosti.

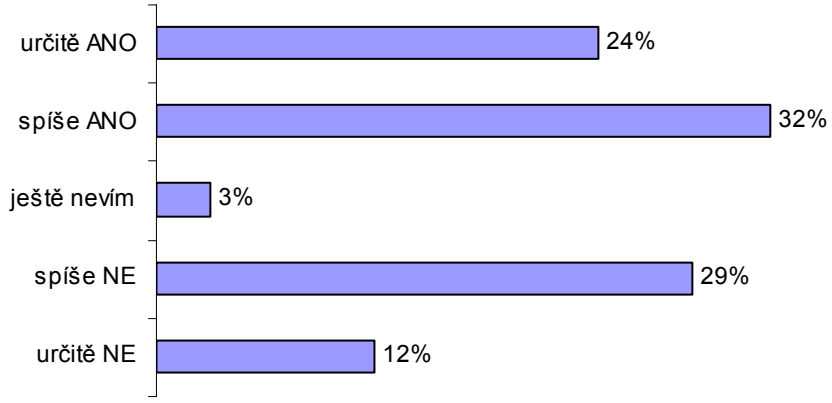


Obr. 16 - Chování úředníků při jednání

4.3.4 Důvody, které brání s Czech POINTem pracovat

Podle statistik počet výpisů pomocí Czech POINTu každým měsícem narůstá, ale nemohl by tento stav být přece jen o něco lepší? Co hlavně vadí lepšímu využívání Czech POINTu? Dotazovaní se téměř shodovali v jednom bodě. Výše poplatků, neosobní vztah či nedůvěra v IS zde nehraje příliš velkou roli. Tyto důvody totiž uvedlo okolo 8% všech dotázaných. Hlavním důvodem, proč lidé nevyužívají služeb Czech POINTu, je z 60% nedostatek informací. Jednoduše řečeno, občané ani nevědí, že něco takového existuje.

4.3.5 Budete využívat Czech POINT i nadále, případně vyzkoušíte tyto služby

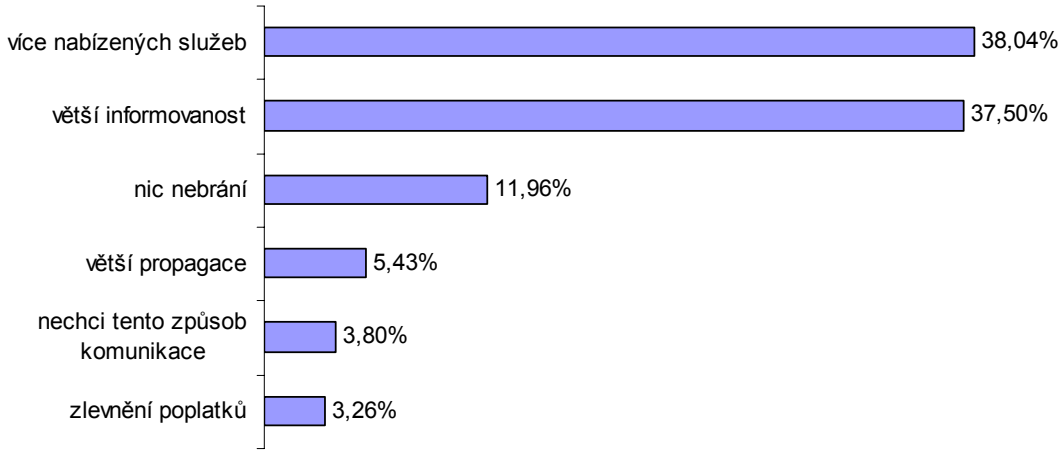


Obr. 17 - Opětovné využití služeb Czech POINTu

92% lidí, kteří s Czech POINTem pracovali, měli jednoznačnou odpověď, že hodlají i nadále tyto služby využívat. Pouze 8% nevědělo, zda tyto služby využijí. Trochu jiná situace byla u lidí, kteří ještě neměli možnost s Czech POINTem pracovat, a tak vlastně nevěděli, co jim tato služba přináší. Z této příčiny byly odpovědi rozděleny rovnoměrně. Celkové hodnocení lze vidět na obr. 17.

4.3.6 BARIÉRY: Co brání efektivnímu využití Czech POINTu

Negativní pohled na využívání Czech POINTu je minimální. Většinou ho mají starší občané, kteří se již nechtějí učit novým věcem. Ani cena Czech POINTu nebrání většímu využití. Hlavní dvě bariéry, které brzdí jeho širší využití, je malý rozsah služeb (38%) a malá informovanost mezi lidmi (37,5%).

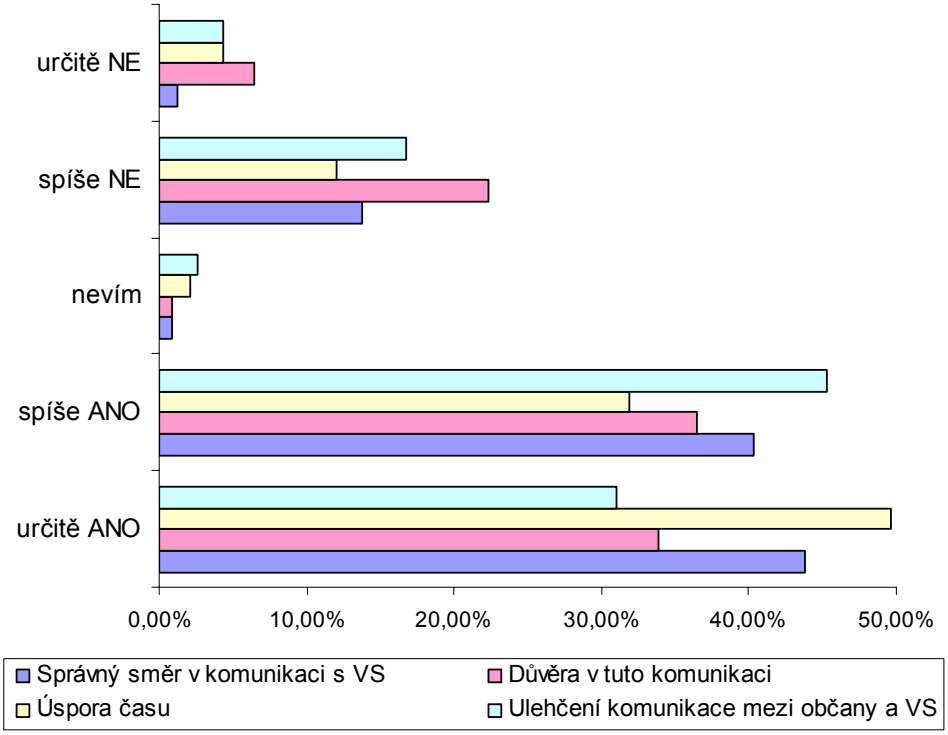


Obr. 18 - Bariéry efektivního využití Czech POINTu

V současné době lze pořídit z Czech POINTu 4 výpisy (z KN, z OR, z ŽR a z RT). Lidé by uvítali větší záběr nabízených služeb (Žádosti o pasy, výpis trestných bodů řidiče, aj.) Zároveň poukazují na velmi malou propagaci a tím pádem i neznalost tohoto systému. Většina lidí se o této možnosti dovídá až na úřadě, kde jim oznámí, že je tady možnost bez čekání si vyřídit některý ze 4 výpisů.

4.3.7 Komunikace, bezpečnost a úspora času

Díky rychle se rozvíjejí IT je celosvětovým trendem využívat tuto techniku ve všech oborech lidské činnosti. Díky IT nastala změna mimo jiné i v komunikaci. V soukromém sektoru se již běžně komunikuje pomocí ICT a nevyhnula se tomu ani veřejná správa. Jak tuto změnu přijímají občané ?



Obr. 19 - Komunikace, bezpečnost a úspora času (v %)

15% dotázaných se domnívá, že tento způsob komunikace s veřejnou správou nemůže fungovat. Vadí jim převážně neosobní vztah a nemožnost zeptat se přímo pracovníka úřadu. Toto stanovisko zaujímali zejména starší lidé a také ti, kteří byli momentálně bez práce bez ohledu na to, zda se Czech POINTem již setkali nebo ne. Necelé procento lidí nevědělo, na kterou stranu se přiklonit, ale zbylých 84% je přesvědčeno, že se jedná o krok správným směrem.

Tady dochází ke shodě s anketou, kterou realizoval v březnu 2008 časopis Egovernment ve spolupráci s Ministerstvem vnitra ČR, kde z došlých odpovědí

zjistili, že 92% občanů službu Czech POINT vítají. Z mého průzkumu vyšlo číslo 84%, což vzhledem k větší základně, která byla oslovena, může mít přesnější charakter. I tak se jedná o číslo velice povzbuvé do další práce na budování e-Governmentu jako celku.

Jestliže jsou lidé přesvědčeni, že se jedná o správný směr, měli by této formě komunikace i důvěřovat. Z výsledků vyplývá, že tomu tak skutečně je. Celých 70,5% dotázaných tuto důvěru má. Z bližšího zkoumání se dá odvodit, že lidé, kteří jsou pro tuto formu komunikace, jí následně i věří z 83,2%. Naopak občané, kterým se e-Government nezamlouvá, nedůvěřují této formě z 97% spíše NE a ze 3% určitě NE.

Při nasazování nových komunikačních prostředků má dojít k ulehčení práce, případně k časové úspoře. Při využívání ICT ve veřejné správě by se měly dostavit lepší výsledky u zmíněných ukazatelů. Podobného názoru jsou i občané, protože oběma hodnotám, tj. časové úspoře a ulehčení komunikace, věří z 80%.

V elektronickém světě je nezbytnou součástí jakéhokoliv systému jeho zabezpečení. Kvůli bezpečnosti IS a možnosti odcizení údajů jsou lidé více nedůvěřiví při jejich využívání. Ovšem z odpovědí na otázku, zda si myslí, že je Czech POINT dostatečně zabezpečen, lze vyvodit, že občané začínají těmto systémům věřit. Pouze 13% dotázaných, kteří se již s Czech POINTem seznámili, nepovažují tento systém za dostatečně zabezpečený. 15,5% dotazovaných nedokázalo odpovědět, protože neměli o zabezpečení Czech POINTu žádné informace. O to příjemnější je zjištění, že 71,5% lidí je názoru, že služby Czech POINTu jsou dostatečně bezpečné, a proto se mohou bez problémů využívat.

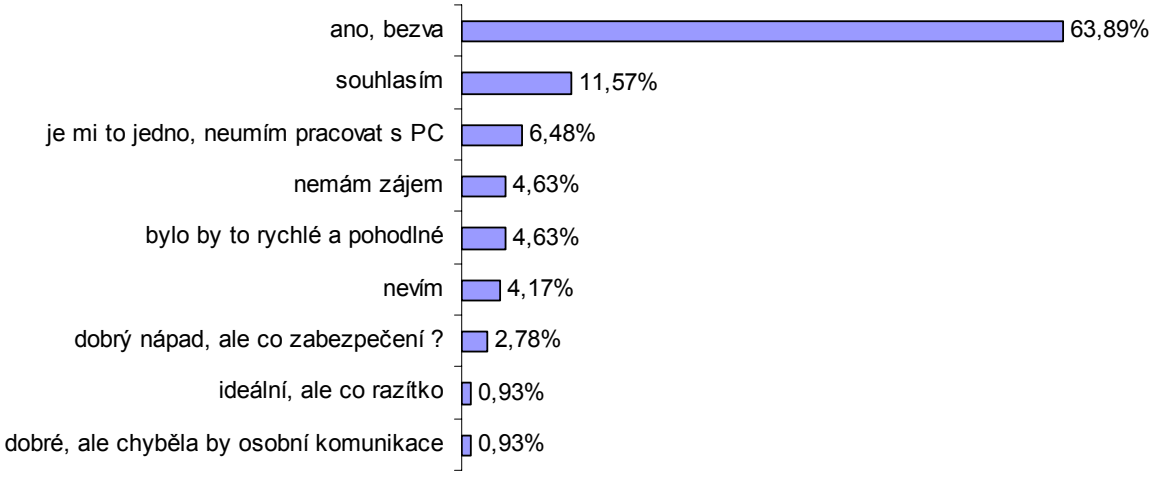
Tab. 11 - Shrnuje odpovědi na zadané otázky (v %)

Otázka	určitě ANO	spíše ANO	nevím	spíše NE	určitě NE
Myslíte si, že je správný směr v komunikaci s veřejnou správou ?	43,78	40,34	0,86	13,73	1,29
Máte důvěru v tento způsob komunikace ?	33,91	36,48	0,86	22,32	6,44
Myslíte si, že Vám Czech POINT ušetří čas ?	49,57	31,90	2,16	12,07	4,31
Myslíte si, že je Czech POINT dostatečně zabezpečen ? *	33,33	38,21	15,45	10,57	2,44
Myslíte si, že Czech POINT skutečně ulehčuje komunikaci mezi státem a občanem ?	31,03	45,26	2,59	16,81	4,31

* Otázka na zabezpečení Czech POINTu byla položena pouze jedincům, kteří již s tímto systémem pracovali.

4.3.8 Czech POINT do Vašich domovů

Návrhy zákonů, které by měly v nejbližší době projít vládou a potom senátem, začínají skutečně probouzet e-Government k reálnému životu. Absence jednoznačného bezvýznamového identifikátoru a následná autentizace znemožňuje využít ISVS z kteréhokoliv počítače, a proto musíme prozatím navštívit Czech POINTy na kontaktních místech. Avšak s příslušnou legislativou není vzdálená doba, kdy moci dělat většinu úkonů z pohodlí našeho domova. Při dotazování, jak by tuto skutečnost přijali občané, jsou reakce více než pozitivní. Od vyslovení mnoha superlativ se objevily i názory, které byly více konzervativnějšího postoje.



Obr. 20 - Názory na e-Government obsluhovaný z domova

4.4 Ověření hypotéz

H1: Efektivně fungující informační systém ve veřejné správě zvyšuje spokojenost občanů.

Připravovaným zákonem o e-Governmentu v návaznosti dalších zákonů vytýčila vláda základní směřování ke zkvalitňování efektivní veřejné správy a přátelské veřejné služby (Smart Administration).

Budování e-Governmentu a rozvoj služeb pro informační společnost není izolovaným úkolem. Úzce souvisí s racionalizací procesů a zaváděním moderních manažerských nástrojů ve veřejné správě stejně jako se zkvalitňováním tvorby politik a právního prostředí.

Úspěšným krokem bylo spuštění služby Czech POINT v březnu 2007, pomocí kterého mohou občané získat 4 typy výpisů. Služby budou postupně rozšiřovány, ale už tento pilotní projekt vzbudil u lidí značné nadšení.

Hypotéza byla potvrzena.

H2: Úplné elektronizaci brání byrokratické úřední razítko

Pro chování státních orgánů platí zásada : "*Vše je zakázáno, co není výslovně zákonem dovoleno*". Toto tvrzení je v dnešní době alfou a omegou celého problému informačních systémů ve veřejné správě. Několikrát se mi během dotazníkových šetření (2004 – dotazníkové šetření na ministerstvech; 2007 – dotazníkové šetření na úřadech Zlínského kraje) potvrdil názor, že pokud se nezmění příslušné zákony, nemohou být informační systémy ve veřejné správě nasazeny a využívány v plném rozsahu. I když to dnešní technologie zvládne, bez podpory zákonů, je k ničemu.

Hypotéza byla potvrzena.

H3: Neochota některých zaměstnanců úřadů učit se novým metodám, brzdí rychlejší využití ISVS.

Úředníci stále chápou využívání informačních systémů více jako nutné zlo, které musí využívat ve své každodenní práci než jako nástroj pro usnadnění své práce.

V průběhu šetření, které se uskutečnilo na úřadech ve Zlínském kraji, bylo doslova alarmující zjištění, že důležitou bariérou efektivního využívání ISVS není nedostatečná kvalifikaci úředníků nebo dostatek financí na zakoupení lepšího, přívětivějšího informačního systému. Hlavní důvod, který úředníci sami uvedli, je neochota učit se stále nové věci.

Citoval bych zde jeden názor zaměstnance úřadu: „*Pokud nebude systém jednodušší (lepší SW) a jednotný na všech úsecích a pokud možno i s ministerstvy na úsecích s centrálními registry apod., odpor úředníků zůstane, protože se přidává „zbytečná" práce.*"

Nezbývá než doufat, že nově přijatý zákon o e-Governmentu by měl výše zmiňovaný argument z větší části zrušit a úředníkům tím zefektivnit práci s informačními systémy,

Prozatím byla daná hypotéza také potvrzena.

H4: ISVS stále vzbuzuje nedůvěru mezi lidmi. Obávají se většího zneužití osobních údajů

Posledním šetřením, které jsem provedl v letošním roce, bylo vypozorováno, jak občané přijímají změny od osobní k elektronické komunikaci s veřejnou správou. Výsledky pozorování byly všeobecně shodné s průzkumy, které se provádějí pro zjišťování využívání IT ať doma, nebo v zaměstnání.

U občanů do 40 let bylo hodnocení přechodu od osobní komunikace ke komunikaci elektronické vnímáno převážně kladně a vítají tento způsob i do budoucna. Obavy ze zneužití dat nemají, případně jim připadá riziko zneužití zanedbatelné. U druhé skupiny starších občanů nebo občanů s nižším dosaženým vzděláním je tato forma méně oblíbená a raději volí možnost přímé komunikace s úředníky. Důvodem je neochota učit se novým technologiím, a z toho vyplývající strach z nepoznaných a neznámých věcí.

Hypotézu nelze jednoznačně potvrdit, ale ani úplně vyvrátit.

5 PŘÍNOSY DISERTAČNÍ PRÁCE

Disertační práce je zaměřena na oblast informačních systémů ve veřejné správě, z čehož vyplývají jednotlivé přínosy, které lze zvažovat jak v rovině teoretické, tak v rovině praktické.

Výsledky práce a souvisejícího výzkumu byly a budou publikovány v odborném tisku a prezentovány na odborných konferencích.

5.1 Přínosy pro vědu

Hlavním teoretickým přínosem disertační práce je vytvoření komplexního teoretického konceptu informačních systémů ve veřejné správě (jeho definování, popsání, přehled základních pojmů, způsob formování, rozvíjení, využívání a implementace v praxi).

Dalším významným teoretickým přínosem práce bude identifikace a analýza kritických faktorů efektivnosti pro moderní informační systémy ve veřejné správě.

Přínosem je rovněž sestavení uceleného přehledu základních pojmů spojených se zkoumanou problematikou.

Novým, doposud nepopsaným přínosem, bude odlišení pohledu úředníků a občanů na ICT ve veřejné správě.

5.2 Přínosy pro praxi

Využití výsledků disertační práce v praktické rovině lze předpokládat především u úřadů veřejné správy, které doposud nemají naimplementovaný ISVS, nebo u úřadů, kde s dosavadním systémem nejsou spokojeni a hledají řešení jak danou situací řešit. Dále budou přínosem i pro vedení dodavatelských firem zabývajících se vývojem informačních systémů do veřejné správy.

Zásadním přínosem je příspěvek ke zlepšení stavu řešení problematiky vytvořením praktických metodických základů pro ISVS.

Dalším přínosem je zjištění skutečného stavu využívání ISVS na úřadech veřejné správy a jejich možné další využití.

Posledním přínosem je zobecnění podrobných pravidel úspěšného využívání informačních systémů na základě nalezení souladu mezi pohledem úředníků a občanů.

6 ZÁVĚR

V roce 2000 byly přijaty mimo jiné zákony 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů a zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů a tím jsme se stali třetí zemí, která takovéto zákony přijala. Až v roce 2007 se opět začalo více diskutovat o e-Governmentu a situaci u nás. V ostatních zemích se tyto služby mezitím vyvinuly, o čemž svědčí diskuze, který model by bylo dobré přizpůsobit naším podmínkách. Dá se říci, že jsme těchto sedm let prospali.

Zákonem o e-Governmentu v návaznosti dalších zákonů vytyčila vláda základní směřování ke zkvalitňování efektivní veřejné správy a přátelské veřejné služby (Smart Administration). Budování e-Governmentu a rozvoj služeb pro informační společnost není izolovaným úkolem. Úzce souvisí s racionalizací procesů a zaváděním moderních manažerských nástrojů ve veřejné správě, stejně jako se zkvalitňováním tvorby politik a právního prostředí.

Viditelným krokem pro občany bylo spuštění služby Czech POINT v březnu 2007, pomocí kterého je možné získat 4 typy výpisů. Služby budou postupně rozšiřovány, ale už pilotní projekt vzbudil u lidí značné nadšení, které je s postupným rozšiřováním kontaktních míst stále výraznější.

I když byla naše země jedna z prvních, která zavedla elektronický podpis, jsme v oblasti e-Governmentu na samotném začátku. Bankám trval přechod z osobních návštěv poboček k elektronické komunikace pět až osm let. Domnívám se, že toto je minimální doba, než se dočkáme plnohodnotného e-Governmentu v České republice.

7 LITERATURA

Monografie:

[1] BAROŠ, L. et al.: *Reforma veřejné správy v České republice*. 1. vyd. Praha: MVČR 2003. 64 s. ISBN 80-239-0225-3.

[2] BRŮNA, M. et al.: *Veřejná správa v České republice*. 2. vyd. Praha: MVČR 2005. 118 s. ISBN 80-239-4709-5.

[3] FREJTICHOVÁ, J.: Elektronický stát. *Business World*, Praha: IDG Czech, 2004. č. 4.

[4] HAGUE, P. *Průzkum trhu : příprava, výběr metod, provedení, interpretace výsledků*. Brno : Computer Press, 2003. ISBN 80-7226-917-8.

[5] HINDLS, R., HRONOVÁ, S., NOVÁK, I. *Analýza dat v manažerském rozhodování.* Praha: Grada, 1999. ISBN 80-7169-255-7

[6] LIDINSKÝ, V.; ŠVARCOVÁ, I.; BUDIŠ, P.; LOEBL, Z.; PROCHÁZKOVÁ, B.: *Government bezpečně*. 1. vyd. Praha : Grada Publishing, 2008. ISBN 978-80-247-2462-1.

[7] LUKÁŠ, M.: *Informační management ve veřejné správě*. Dizertační práce. Praha: VŠE Praha, 2002.

[8] LUKÁŠ, M.: *Městský informační management*. 1. vyd. Praha: Grada Publishing, 2000. 320 s. ISBN 80- 7169-554-8.

[9] MATES, P.; MATULA, M.: *Kapitoly z dějin a teorie veřejné správy*. 1. vyd. Praha: VŠE Praha, 1998. 105 s. ISBN 80-7079-753-3.

[10] MATES, P.; WOKOUN, R.: *Malá encyklopedie regionalistiky a veřejné správy*. 1. vyd. Praha: Prospektrum, 2001. 200 s. ISBN 80-7175-100-6.

[11] MOLNÁR, Z.: *Efektivnost informačních systémů*. 1. vyd. Praha: Grada Publishing, 2000. 144 s. ISBN 80-7169-410-X.

[12] PAVLICA, K. a kol. *Sociální výzkum, podnik a management.* Praha: Ekopress, 2000. ISBN 80-86119-25-4

[13] SKLENÁK, V.: *Data, informace, znalosti a Internet*. 1. vyd. Praha: C. H. Beck, 2001. ISBN 80-7179-409-0.

[14] STRAUSS, A., CORBINOVÁ, J. *Základy kvalitativního výzkumu.* Boskovice: Nakladatelství Albert, 1999. ISBN 80-85834-60-X

[15] ŽID, N.; BENÁČANOVÁ, H.; KUNSTOVÁ, R.; SVOBODA, J.: *Orientace ve světě informatiky*. 1. vyd. Praha : Management Press, 1998. ISBN 80-85943-58-1.

Legislativní zdroje:

[16] Ústavní zákon ČNR č. 1/1993 Sb., Ústava České republiky

[17] Usnesení ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

[18] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

[19] Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Použité internetové zdroje:

[20] *Czech POINT* [online]. [cit. 2008-02-24]. Dostupný z WWW: <http://www.czechpoint.cz>.

[21] *Číselník obcí (CISOB)/ČSÚ* [online]. [cit. 2007-03-29]. Dostupný z WWW: <http://www.czso./csu/klasifik.nsf>.

[22] *Egovernment* [online]. [cit. 2008-04-15]. Dostupný z WWW: <http://www.egovernment.cz/archiv/default.htm>.

[23] *Egovernment The Best* [online]. [cit. 2008-07-30]. Dostupný z WWW: <http://www.egovernment.cz/best/best07.htm>.

[24] *ISSS 2008* [online]. [cit. 2008-07-23]. Dostupný z WWW: <http://www.isss.cz/>.

[25] *Lidské zdroje v informační společnosti: IT odborníci | ČSÚ* [online]. [cit. 2007-08-24]. Dostupný z WWW: <http://www.czso.cz/csu/redakce.nsf/i/lidske_zdroje_v_informacni_spolecnosti_it_odbornici>.

[26] *magazín Egovernment* [online]. [cit. 2008-07-04]. Dostupný z WWW: <http://www.egovernment.cz/czechpoint/>.

[27] *Ministerstvo informatiky ČR: Atestace ISVS podle zákona č. 365/2000 Sb.* [online]. [cit. 2007-03-29]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=486>.

[28] *Ministerstvo informatiky ČR: e-Government* [online]. [cit. 2007-03-30]. Dostupný z WWW: <http://www.micr.cz/egovernment/default.htm>.

[29] *Ministerstvo informatiky ČR: Pořizování informačních systémů veřejné správy* [online]. [cit. 2007-03-29]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=3764>.

[30] *Ministerstvo informatiky ČR: Sdílení dat a základní registry veřejné správy* [online]. [cit. 2007-04-01]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=3486>.

[31] *Ministerstvo informatiky České republiky: Státní informační a komunikační politika* [online]. [cit. 2007-03-27]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=275>.

[32] *Ministerstvo informatiky ČR: Zřizuje se rada vlády pro informační společnost* [online]. [cit. 2007-04-01]. Dostupný z WWW: <http://www.micr.cz/scripts/detail.php?id=3845>.

[33] *UNCITRAL* [online]. [cit. 2008-02-08]. Dostupný z WWW: <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

[34] *Úvodní stránka – Na úřad přes internet – Portál veřejné správy České republiky* [online]. [cit. 2007-03-31]. Dostupný z WWW: <http://www.portal.gov.cz/wps/portal/_s.155/6966/place>.

[35] *Vláda České republiky* [online]. [cit. 2008-08-12]. Dostupný z WWW: <http://www.vlada.cz/scripts/detail.php?id=33630>.

8 SEZNAM PUBLIKACÍ AUTORA

[1] SODOMKA, P., HABÁŇ, J., KLČOVÁ, H., TUREČEK, T. Výzkum efektivnosti ERP systémů v podnicích ČR. In TRNKA, F. *Výzkum konkurenční schopnosti českých průmyslových výrobců*. Výzkumný záměr UTB, FaME ve Zlíně. Zlín: 2002. MŠMT 265 300021.

[2] HABÁŇ, J., TUREČEK, T. V teple a bezpečí (Umíte chránit svá data?) *E-BIZ*, 2003, roč. 4, č. 3, s. 48-49. ISSN 1213-063X.

[3] HABÁŇ, J., TUREČEK, T. Učit se, učit se, učit se (Co nového v e-learningu?) *E-BIZ*, 2003, roč. 4, č. 4, s. 32-33. ISSN 1213-063X.

[4] TUREČEK, T. Satelitní sledování pohybu vozidel. In *Sborník Svět informačních systémů 2004* konané 8.-9. března 2004 ve Zlíně. Zlín, 2004, s. 299-304. ISBN 80-7318-166-5.

[5] TUREČEK, T., MEDEK, M. Vláda na baterky. Computer Press, a.s. *E-BIZ*, 2004, ročenka e-Government. ISSN 1213-063X.

[6] TUREČEK, T. Informační systémy ve veřejné správě. In *Sborník anotací z Internet a konkurenceschopnost podniku* konané 16. března 2005 ve Zlíně. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. s. 91. CD-ROM. ISBN 80-7318-269-6.

[7] TUREČEK, T., MEDEK, M. Komunikujte s orgány veřejné správy pomocí Internetu. In *Sborník příspěvků z I. Mezinárodní Baťovy doktorandské konference* konané 21. dubna 2005 ve Zlíně. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. s. 39. CD-ROM. ISBN 80-7318-257-2.

[8] TUREČEK, T. eGovernment - sen či realita?. In *Recenzovaný sborník příspěvků II. Mezinárodní Baťovy doktorandské konference* konané 27. dubna 2006 ve Zlíně. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. s. 237. CD-ROM. ISBN 80-7318-384-6.

[9] TUREČEK, T., VLČKOVÁ, I. Komunikace ve veřejných službách – věčný boj. In *Recenzovaný sborník abstraktů z konference studentů doktorského studia MendelNet 2006* konané 29. listopadu 2006 v Brně. Brno: Mendlova zemědělská a lesnická univerzita v Brně, 2006. CD-ROM. ISBN 80-86851-62-1.

[10] TUREČEK, T. Skutečně ulehčují úředníkům informační systémy nasazované do veřejné správy jejich práci?. In *Recenzovaný sborník příspěvků III. Mezinárodní Baťovy doktorandské konference* konané

12. dubna 2007 ve Zlíně. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. s. 315. CD-ROM. ISBN 978-80-7318-529-9.

[11] TUREČEK, T. eGON – pomůže lepší komunikaci veřejné správy s občanem. In *Recenzovaný sborník abstraktů z Mezinárodní Baťovy konference pro doktorandy a mladé vědecké pracovníky* konané 10. dubna 2008 ve Zlíně. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008. s. 194. CD-ROM. ISBN 978-80-7318-663-0.

9 CV AUTORA

Jména a příjmení: Ing. Tomáš TUREČEK
Datum narození: 6. únor 1978
Bydliště: Pod Skalkou 15, 741 01 Nový Jičín, Česká republika
E-mail: turecek@fame.utb.cz
Stav: svobodný

Dosažené vzdělání:

2002 – dosud Univerzita Tomáše Bati ve Zlíně, Česká republika
Fakulta Managementu a ekonomiky
Studijní obor: Management a ekonomie
Přijat na doktorandské studium.

2000 – 2002: Univerzita Tomáše Bati ve Zlíně, Česká republika
Fakulta Managementu a ekonomiky
Studijní obor: Management a ekonomie
Ukončeno získáním titulu Ing.

1997 – 2000: Vysoké učení technické v Brně, Česká republika
Fakulta Managementu a ekonomiky ve Zlíně (přestup z FT)
Studijní obor: Management a ekonomie
Ukončeno získáním titulu Bc.

1996 – 1997: Vysoké učení technické v Brně, Česká republika, Fakulta Technologická ve Zlíně
Studijní obor: Technologie a management.

1992 – 1996: Gymnázium, Nový Jičín
Maturita z českého a německého jazyka, matematiky a výpočetní techniky.

Odborné zaměření:
Informatika, informační systémy

Stáže a studijní pobyty:
07/2007 – 09/2007 3 měsíční studijní pobyt na Universität Duisburg-Essen
07/1999 – 09/1999 3 měsíční praxe v Mnichově

Jazykové znalosti:
Němčina – pokročilý
Angličtina – začátečník

Ve Zlíně dne 22. srpna 2008

PŘÍLOHY

Příloha A – Dotazník na jednotlivá ministerstva ČR

Příloha B – Dotazník pro úředníky Zlínského kraje

Příloha C – Dotazník pro občany na Czech POINT

Příloha D – Informace pro občany k dotazníku Czech POINT

Příloha E – Dendrogramy dotazníku Czech POINT

Příloha F – Harmonogram pilotního provozu Czech POINT

Příloha G – zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Příloha H – zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

Příloha I – Harmonogram přípravy základních zákonů e-Governmentu

PŘÍLOHA A – DOTAZNÍK NA JEDNOTLIVÁ MINISTERSTVA ČR

Dotazník k průzkumu IS ve státní správě
1. Údaje o organizaci a respondentovi (2004)

1.1 Název organizace:

1.2 Počet zaměstnanců celkem:

1.3 Počet uživatelů IS celkem:

1.4 Informace o respondentovi:

titul, jméno, příjmení	
pracovní zařazení	
telefon	
e-mail	
délka praxe s informačními technologiemi	let
délka praxe ve státní správě	let

1.5 Možnost ovlivnit výběr informačního systému ze strany respondenta:

minimální				maximální	
1	2	3	4	5	*(zaškrtněte)*

1.6 Počet pracovníků podílejících se na správě a údržbě IS:

2. Údaje o implementovaném informačním systému

2.1 Název informačního systému:

2.2 Jméno dodavatele:

2.3 Implementace IS:

Datum zahájení projektu		měsíc, rok
Datum ukončení projektu		měsíc, rok

Jednotlivé fáze projektu

Současná fáze projektu

	ze strany ministerstva	ze strany dodavatele	externí konzultanti
Počet pracovníků v implementačním týmu			
Počet pracovníků v řídící komisi projektu			

Celkové náklady na pořízení systému	
Celkové náklady na implementaci	
Roční náklady na údržbu a provoz systému	

2.4 Oblasti nasazení systému: *(zaškrtněte)*

účetní a ekonomická agenda	
personalistika a správa	
vzdělávání a školení zaměstnanců (e-learning)	
podpora vrcholového rozhodování (MIS)	
styk s veřejností (C2G)	
styk s právnickými osobami (B2G)	
styk s ostatními úřady státní správy (G2G)	
správa dokumentů (workflow)	
další klíčové oblasti *(prosíme, vyjmenujte)*	

2.5 Operační systém serveru:

2.6 Databázový systém:

2.7 Architektura systému:

Charakteristika serveru *(značka, kategorie apod.)*	
Charakteristika klienta *(tenký klient, terminály apod.)*	
Počet vrstev	
Online sdílení dat	
Distribuovaná varianta sdílení dat	

3. Hodnocení přínosů informačních systémů ve státní správě

3.1 Stručně charakterizujte hlavní kritéria pro výběr informačního systému a jeho dodavatele:

3.2 Hodnocení přínosů:

Přiřaďte bodové ohodnocení jednotlivým charakterizovaným přínosům podle priority
V případě, že daný přínos není sledován, ponechte bez hodnocení

	oček.	realizov.
Zlepšení dostupnosti informací pro pracovníky úřadu		
Zlepšení řízení procesů uvnitř úřadu		
Zlepšení integrace procesů uvnitř úřadu		
Zlepšení komunikace s veřejností		
Zlepšení komunikace s právnickými osobami		
Zlepšení vztahu k ostatním úřadům státní správy		
Zvýš. produktivity resp. snížení nákladů (vyšší produktivita se stejnými zdroji)		
Standardizace IS/IT ve úřadě		
Zlepšení podpory vrcholového rozhodování		
Jiný přínos, uveďte jaký a určete jeho prioritu:		

prosím o seřazení dle priority, žádné číslo se nesmí opakovat, známkujte od 1 (nejdůležitější) jako ve škole; v levém sloupci jsou přínosy, které jste očekávali před zavedením systému a v pravém sloupci přínosy, kterých jste dosáhli 1 rok po implementaci

4. Pohled státní správy na systémovou integraci

4.1 Jak vnímáte pojem **"systémová integrace"** ? *(zvolte pouze jednu variantu)*

1. Technické propojování heterogenních systémů na nejrůznějších úrovních (hardware, protokoly, databázové systémy atd.) ☐

2. Řešení jednoho konkrétního IS/IT projektu, přičemž systémovou integrací rozumíme optimální sladění projektového a právního přístupu tak, aby bylo dosaženo cílů projektu ☐

3. Dlouhodobý koordinovaný proces řešení IS/IT projektů vycházející ze strategického záměru zákazníka s cílem plnit jeho vyvíjející se požadavky na řízení procesů v organizaci ☐

4. Dlouhodobý koordinovaný proces řešení všech podnikových projektů (nejen IS/IT) s cílem naplňovat strategický záměr zákaznické organizace ☐

5. Nedokážu definovat ☐

6. Jiná definice, uveďte: ☐

4.2 Koho považujete za **Systémového integrátora** ?*(zvolte pouze jednu variantu)*

1. Jakoukoliv společnost dodávající informační technologie do podniků a organizací ☐

2. Společnost produkující aplikační software nebo jeho komplementy, není přitom nezbytně nutné, aby měla přímý vztah k zákaznickým organizacím (př.: Microsoft, Hewlett Packard) ☐

3. Společnost, která má přímý vztah k zákazníkům a je vždy spoluřešitelem IS/IT projektů u zákaznických organizací (př.: Varias, MSCBSP) ☐

4. Společnost, která má přímý vztah k zákazníkům, podílí se na řešení celé řady projektů (nejen IS/IT), čímž se na základě dlouhodobého partnerství spolupodílí na naplňování celopodnikové strategie u zákazníka (př.: Accenture, Deloitte) ☐

5. Nedokážu definovat ☐

6. Jiná definice, uveďte: ☐

PŘÍLOHA B – DOTAZNÍK PRO ÚŘEDNÍKY ZLÍNSKÉHO KRAJE

IDENTIFIKACE ORGANIZACE

Název úřadu

Pozice

E-mail

I. VNITŘNÍ INFORMAČNÍ SYSTÉM

1. **V jaké fázi zavádění IS se momentálně nacházíte?**
   - ☐ Nemáme žádný IS
   - ☐ Zvažujeme o jeho zavedení
   - ☐ Jsme ve fázi zavádění IS
   - ☐ Máme zaveden, jsme s ním spokojeni
   - ☐ Máme zaveden, ale zvažujeme změnu
2. **Kolik IS využíváte ?**

   Jsou mezi sebou vzájemně propojeny ?
   - ☐ Ano
   - ☐ Ne
   - ☐ Částečně
3. **IS spravujete vlastními silami nebo outsourcingem ?**

   Vlastními silami

   Částečně vlastními silami, částečně outsourcing

   Outsourcing
4. **Zvažujete případně v budoucnu přejít na outsourcing ?**

   Ano

   Ne
5. **Jakým způsobem jsou propojeny jednotlivé PC?**
   - ☐ Samostatné PC bez propojení
   - ☐ PC propojeny v rámci LAN
   - ☐ Propojení v rámci WAN

6. **Máte vybudovaný vnitřní systém pro zpřístupnění informací v rámci lokální sítě – Intranet?**

7. **Co Vás přimělo k zavedení daného IS?**
(očíslujte dle významnosti 1- nejvýznamnější, 8- nejméně významné)

Požadavek nadřízených orgánů

Srovnání úrovně s jinými úřady

Legislativa

Požadavky ze strany občanů

Zrychlení služeb občanům

Technická zaostalost *(rozhodli se, že se zdokonalí)*

Vlastní rozhodnutí

Jiný důvod

8. **V jakém stupni integrace je IS na Vašem úřadě?**

☐ Lokální agendy na PC

☐ Částečná integrace některých agend

☐ Plná integrace všech agend

9. **Používáte společné registry pro**

10. **Vyskytují se na Vašem úřadě duplicitní registry? Kde, podle Vašeho názoru, v rámci IS spatřujete duplicitu?**

11. **Jaký SW nástroj používáte ke zpracování jednotlivých oblastí Vaší činnosti?**
(vypište prosím)

Ekonomická oblast

Správa majetku

Správní agendy

Oblast sociálních služeb

Oblast investiční

Oblast život. prostředí

Oblast školství

Oblast kultury

Stavební úřad

Územní plánování

Spisová služba

Provozní IS

Mzdový a personální systém

Pro podporu zpracování materiálů do Rady a Zastupitelstva

---

12. V následující části prosím vypište do tabulky jednotlivé používané systémy. V rámci škály 1-5 vyjádřete svou spokojenost s IS v nastíněných oblastech.
(1 – nejlepší, 5 – nejhorší)

IS - inf. systém	**Spokojenost s:**				
	Funkcionalitou	**Datovou základnou**	**Uživatelským rozhraním**	**Možností integrace s jinými IS**	**Dodavatelským servisem**

13. Jak dlouho využíváte jádro (základ) Vašeho IS?

☐ Jiné, prosím upřesněte

14. Jaký kancelářský SW používáte?

☐ Microsoft Office %

☐ Win602/T602 %

☐ Open Office %

☐ Jiné, prosím upřesněte v %

15. Odhadněte rozložení výdajů na ICT na Vašem úřadě:

Neinvestiční pořizovací náklady HW	%
Neinvestiční pořizovací náklady SW	%
Náklady na hlasové a datové služby	%
Technická podpora	%
Opravy a udržování	%
Náklady související s GIS	%
Investiční náklady HW	%
Investiční náklady SW	%

16. Jak reagují dodavatelé Vašeho IS na legislativní změny?

- ☐ Okamžitě
- ☐ Musíme je upozorňovat
- ☐ Pomáháme jim s implementaci nové legislativy

17. RIZIKA: Co považujete za největší riziko provozu IS na Vašem úřadě?

- ☐ Zneužití osobních dat
- ☐ Ztráta dat
- ☐ Napadení zvenku (hackeři)
- ☐ Jiná, uveďte

18. BARIÉRY: Co brání efektivnímu využití IS na Vašem úřadě?
V rámci škály 1-5 vyjádřete hlavní bariéry (1 – největší, 5 – nejmenší)

- ☐ Nedostatek finančních prostředků
- ☐ Nedostatečná kvalifikace pracovníků pro práci s IS/IT
- ☐ Neochota učit se nové věci
- ☐ Nevyhovující nabídka SW produktů na trhu
- ☐ Jiný důvod, uveďte jaký

19. V čem spatřujete přínosy užívaného IS?
V rámci škály 1-11 vyjádřete hlavní přínosy (1 – největší, 11 – nejmenší)
V případě, že daný přínos není sledován, ponechte bez hodnocení

- ☐ Zvýšení dostupnosti informací pro zaměstnance
- ☐ Zvýšení dostupnosti informací pro veřejnost
- ☐ Zabezpečení sdílení dat
- ☐ Zvýšení efektivity procesů, postupů
- ☐ Zvýšení informační gramotnosti zaměstnanců
- ☐ Rychlejší přístup k datům
- ☐ Zajištění bezpečnosti a ochrany dat

- ☐ Zlepšení podpory a koordinace činnosti jednotlivých úřadů
- ☐ Zvýš. produktivity resp. snížení nákladů (vyšší produktivita se stejnými zdroji)
- ☐ Standardizace IS/IT ve VS
- ☐ Snížení výdajů na IT
- ☐ Jiný přínos, uveďte jaký a určete jeho prioritu

20. Co Vám přináší největší těžkosti pro práci s IT?
Přiřaďte bodové ohodnocení jednotlivým charakterizovaným těžkostem podle priority (1 – největší, 11 – nejmenší)

- ☐ Časová náročnost
- ☐ Nemáme k dispozici technické vybavení
- ☐ Nedůvěra v tuto oblast
- ☐ Dostupnost informací pro zaměstnance
- ☐ Dostupnosti informací pro veřejnost
- ☐ Zabezpečení sdílení dat
- ☐ Efektivita procesů, postupů
- ☐ Informační gramotnost zaměstnanců
- ☐ Zajištění bezpečnosti a ochrany dat
- ☐ Jiné, prosím uveďte

21. Proběhlo po spuštění IS případně nové aplikace vstupní školení ???

- ☐ Ano
- ☐ Ne
- ☐ Částečně

22. Jsou i postupem času pořádány průběžná školení ???

- ☐ Ano a jsou dostatečná
- ☐ Ano, ale mohly by být častěji
- ☐ Ne

23. Jakou metodu hodnocení efektivnosti preferujete pro hodnocení vašeho IS:
Přiřaďte bodové ohodnocení jednotlivým charakterizovaným přínosům podle priority (1 nejvíce – 7 nejméně).
Pokud se tato otázka netýká oblasti Vaší činnosti neodpovídejte.

Multikriteriální analýza

Čistá současná hodnota - NPV (Net Present Value)

Analýza náklady/přínosy (Cost/Benefit Analysis)

Diskontovaný Cash Flow

Vnitřní úroková míra - IRR (Internal Rate of Return)

Výnosnost investice - ROI (Return on Investment)

Návratnost investice (Payback Period)

Jiná metoda, uveďte jaká a určete její prioritu:

(pokud se provádí)

II. NÁVRHY NA ZLEPŠENÍ

1. **Na co je v současnosti kladen největší důraz na Vašem úřadě?**

   ☐ Jiné, prosím uveďte

2. **Domníváte se, že optimalizací procesů by mohlo dojít ke zkrácení času při plnění úkolů, na kterých spolupracuje více odborů Vašeho úřadu?**

3. **Jak by se tyto prostoje daly minimalizovat, případně odstranit?**

4. **Co navrhujete ke zlepšení stávající situace?**

5. **Máte ještě jiné připomínky, jež byste rádi uvedli, případně oblasti, o nichž jsme se nezmínili, které by nám pomohly porozumět komunikaci na Vašem úřadě?**

PŘÍLOHA C – DOTAZNÍK PRO OBČANY NA CZECH POINT

ANO

1) Co vyřizujete na úřadech nejčastěji ?

☐ občanku
☐ různé poplatky (pes, byt, komunál. odpad)
☐ výpis z trestního rejstříku
☐ jiné …….

2) Jak často chodíte něco vyřizovat na úřad ?

☐ 1x ročně
☐ 1x měsíčně
☐ 1x týdně
☐ 1x za ½ roku
☐ 1x za 14 dní
☐ skoro denně

3) Jak jednají úředníci ?

☐ s úsměvem a vlídně
☐ arogantně
☐ odměřeně
☐ jiné …….

4) Podařilo se Vám vyřídit to, kvůli čemu jste sem přišli ?

☐ běžnou „okýnkovou“ cestou
☐ pomocí CzechPOINTu

5) Zdála se Vám doba vyřízení :

☐ dlouhá
☐ krátká
☐ přiměřená
☐ jiná …….

6) Setkal jste se již s pojmem CzechPOINT ?

☐ ANO (***pokračuj na této stránce***)
☐ NE (***otoč list***)

7) Víte co všechno můžete přes CzechPOINT zařídit ?

☐ ANO (výpis – z KN, z OR, z ŽR, z RT), jiné……..
☐ NE

8) Využil jste již služeb CzechPOINT ?

☐ ANO (výpis – z KN, z OR, z ŽR, z RT), jiné……..
☐ NE (***přeskoč na ot. č. 12***)

---

9) Byly nějaké komplikace při využití CzechPOINT ?

☐ ANO, jaké …….
☐ NE

10) Ovládání CzechPOINT bylo:

☐ intuitivní
☐ složité, ale vyřídil jsem co jsem potřeboval
☐ musel jsem pořádat o pomoc úředníka
☐ uživatelsky přívětivé
☐ nedokázal jsem se zorientovat
☐ odešel jsem žádost vyřídit klasicky „k okýnku“

	určitě **ANO**	spíše **ANO**	ještě **nevím**	spíše **NE**	určitě **NE**
11) Budete i nadále používat CzechPOINT ?					

(***přeskoč na ot. č. 14***)

---

12) Co Vám brání s CzechPOINT pracovat ?

☐ nedostatek informaci
☐ nedůvěra v IS
☐ neosobní vztah
☐ výše poplatků
☐ jiné……

	určitě **ANO**	spíše **ANO**	spíše **NE**	určitě **NE**
13) Hodláte v budoucnu vyzkoušet služby CzechPOINT ?				

---

14) Co by pomohlo k většímu využití CzechPOINT u Vás ?

	určitě **ANO**	spíše **ANO**	spíše **NE**	určitě **NE**
15) Myslíte si, že je to správný směr v komunikaci s veřejnou správou ?				
16) Máte důvěru v tento způsob komunikace ?				
17) Myslíte si, že Vám CzechPOINT ušetří čas ?				
18) Myslíte si, že díky CzechPOINT dojde k urychlení vyřízení Vašeho požadavku ?				
19) Myslíte si, že je CzechPOINT dostatečně zabezpečen ?				
20) Myslíte si, že CzechPOINT skutečně ulehčuje komunikaci mezi státem a občanem ?				

21) Je výše poplatků za výpisy z CzechPOINT :

☐ vysoké
☐ přiměřené
☐ nízké
☐ jiné ……..

22) Co říkáte na to, že by jste tyto záležitosti mohl řešit díky CzechPOINT v budoucnu z domova přes svůj PC ?

IDENTIFIKAČNÍ OTÁZKY

Pohlaví

☐ Muž
☐ Žena

Věk

☐ 18-35 let
☐ 51-65 let
☐ 36-50 let
☐ 66-více let

Nejvyšší dosažené vzdělání

☐ základní
☐ středoškolské
☐ vyučen/a
☐ vysokoškolské

Pracovní zařazení

☐ student
☐ na mateřské dovolené
☐ zaměstnanec
☐ nezaměstnaný
☐ podnikatel, živnostník
☐ důchodce

NE

1) Co vyřizujete na úřadech nejčastěji ?

☐ občanku
☐ různé poplatky (pes, byt, komunál. odpad)
☐ výpis z trestního rejstříku
☐ jiné …….

2) Jak často chodíte něco vyřizovat na úřad ?

☐ 1x ročně
☐ 1x měsíčně
☐ 1x týdně
☐ 1x za ½ roku
☐ 1x za 14 dní
☐ skoro denně

3) Jak jednají úředníci ?

☐ s úsměvem a vlídně
☐ arogantně
☐ odměřeně
☐ jiné …….

4) Podařilo se Vám vyřídit to, kvůli čemu jste sem přišli ?

☐ běžnou „okýnkovou“ cestou
☐ pomocí CzechPOINTu

5) Zdála se Vám doba vyřízení :

☐ dlouhá
☐ krátká
☐ přiměřená
☐ jiná …….

6) Setkal jste se již s pojmem CzechPOINT ?

☐ ANO (***otoč list***)
☐ NE (***pokračuj na této stránce***)

7) Měl by jste zájem dozvědět se více o této možnosti komunikace s veřejnou správou ?

☐ ANO (***předej info letáček***)
☐ NE (***zkus dokončit otázky***)

8) Co Vám brání s CzechPOINT pracovat ?

☐ nedostatek informaci
☐ neosobní vztah
☐ jiné……
☐ nedůvěra v IS
☐ výše poplatků

	určitě **ANO**	spíše **ANO**	spíše **NE**	určitě **NE**
9) Hodláte v budoucnu vyzkoušet služby CzechPOINT ?				

10) Co by pomohlo k většímu využití CzechPOINT u Vás ?

	určitě **ANO**	spíše **ANO**	spíše **NE**	určitě **NE**
11) Myslíte si, že je to správný směr v komunikaci s veřejnou správou ?				
12) Máte důvěru v tento způsob komunikace ?				
13) Myslíte si, že by Vám CzechPOINT ušetřil čas ?				
14) Myslíte si, že by díky CzechPOINTu došlo k urychlení vyřízení Vašeho požadavku ?				
15) Myslíte si, že CzechPOINT skutečně ulehčuje komunikaci mezi státem a občanem ?				

16) Co říkáte na to, že by jste tyto záležitosti mohl řešit díky CzechPOINT v budoucnu z domova přes svůj PC ?

IDENTIFIKAČNÍ OTÁZKY

Pohlaví

☐ Muž ☐ Žena

Věk

☐ 18-35 let ☐ 51-65 let
☐ 36-50 let ☐ 66-více let

Nejvyšší dosažené vzdělání

☐ základní ☐ středoškolské
☐ vyučen/a ☐ vysokoškolské

Pracovní zařazení

☐ student ☐ na mateřské dovolené
☐ zaměstnanec ☐ nezaměstnaný
☐ podnikatel, živnostník ☐ důchodce

PŘÍLOHA D – INFORMACE PRO OBČANY K DOTAZNÍKU CZECH POINT

Český Podací Ověřovací Informační Národní Terminál, tedy Czech POINT je projektem, který by měl zredukovat přílišnou byrokracii ve vztahu občan – veřejná správa. V současnosti musí občan navštívit několik úřadů k vyřízení jednoho problému. Czech POINT bude sloužit jako asistované místo výkonu veřejné správy, umožňující komunikaci se státem prostřednictvím jednoho místa tak, aby „*obíhala data ne občan*“.
Jednoduše řečeno jedná se o počítač na obecním či městském úřadě, české poště, případně v kancelářích hospodářských komor, který je napojen pomocí internetu do jednotlivých resortu veřejné správy. V konečné fázi projektu by občan mohl své záležitosti vyřizovat i z domova prostřednictvím internetu.

Co poskytuje Czech POINT

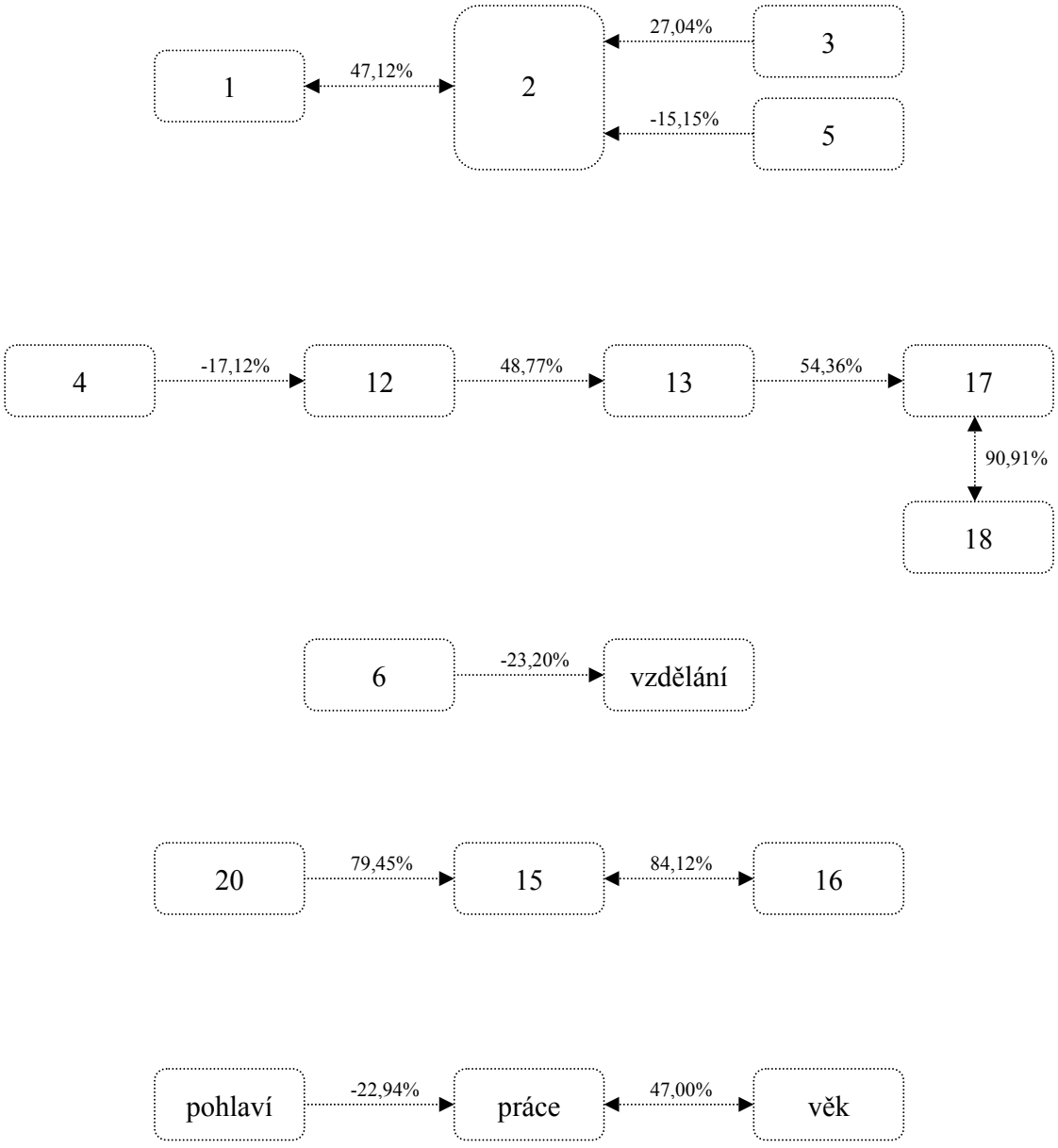
Czech POINT v současné době poskytuje čtyři druhy výstupů. To znamená, že každý, kdo zaplatí příslušný poplatek na místě Czech POINT, může požádat o následující:

- ✓ Výpis z Katastru nemovitostí
- ✓ Výpis z Obchodního rejstříku
- ✓ Výpis z Živnostenského rejstříku
- ✓ Výpis z Rejstříku trestů

Kolik tyto výpisy občana stojí?

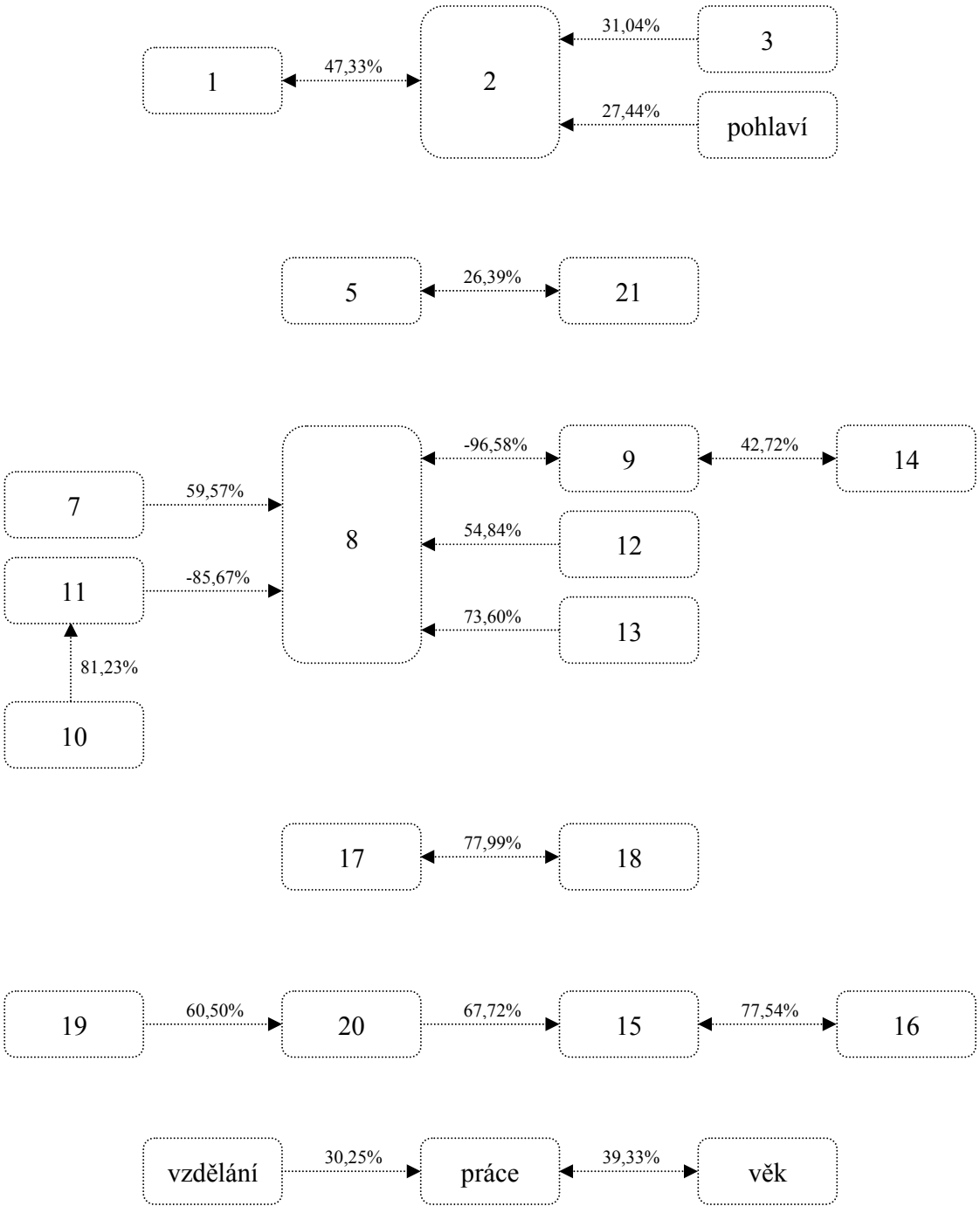
Cena jako taková je závislá na počtu stran, které jsou pomocí Czech POINTu vydány. Vydání první strany výpisu je zpoplatněno částkou, jejíž maximální výše je zákonem omezena na **100,- Kč**; každá další strana výpisu je zpoplatněna částkou, jejíž maximální výše je zákonem omezena na **50,- Kč**. Prozatím jedinou výjimkou je výpis z rejstříku trestů, kde je částka stanovena na **50,- Kč** za tento výpis.

PŘÍLOHA E – DENDROGRAMY – VŠECH OBČANŮ, KTEŘÍ SE ZÚČASTNILI PRŮZKUMU



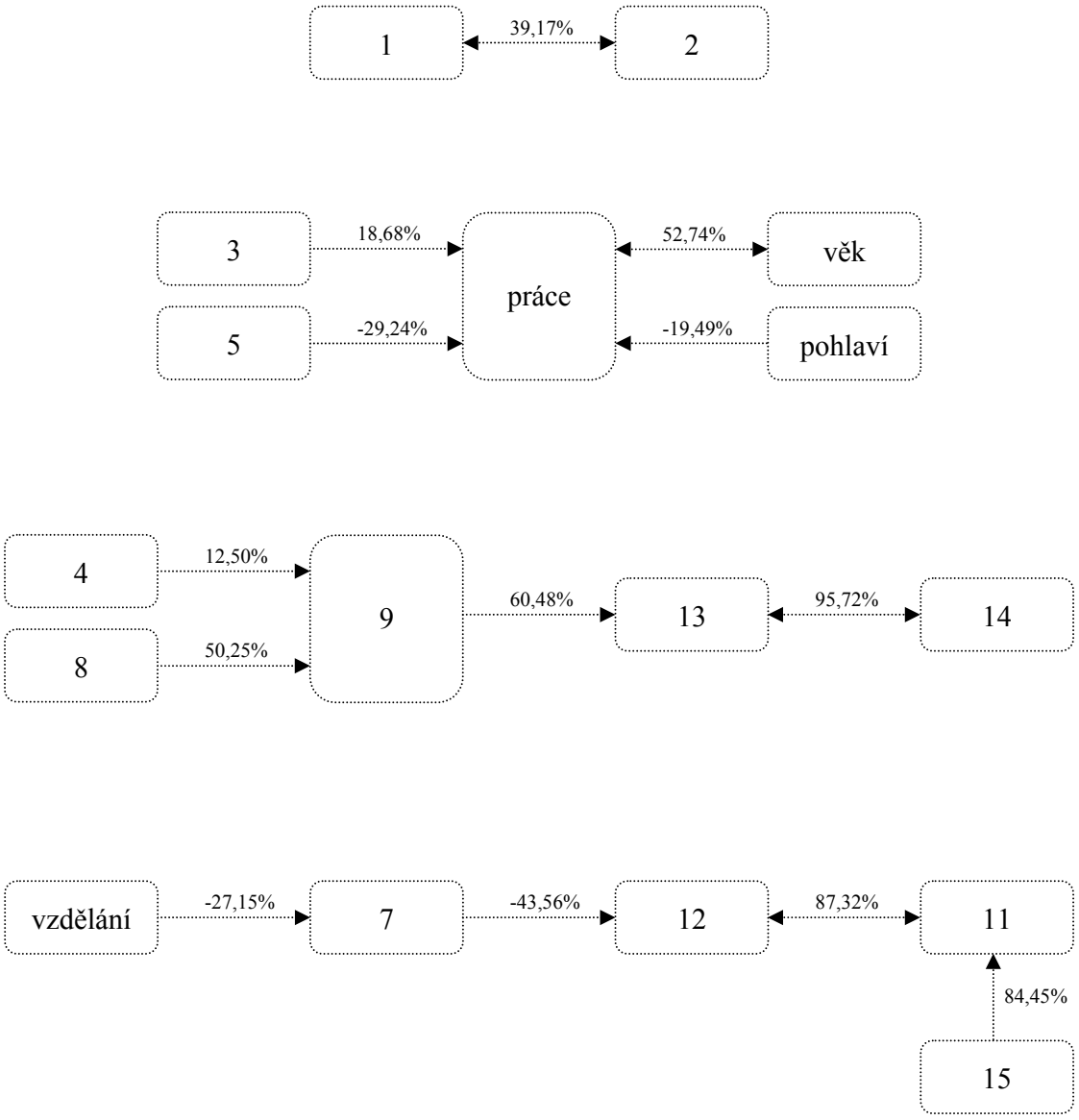
Pozn.: čísla označují jednotlivé otázky v dotazníku z přílohy C

PŘÍLOHA E – DENDROGRAMY – OBČANŮ, KTEŘÍ ZNALI SLUŽBY CZECH POINTU



Pozn.: čísla označují jednotlivé otázky v dotazníku z přílohy C

PŘÍLOHA E – DENDROGRAMY – OBČANŮ, KTEŘÍ NEZNALI SLUŽBY CZECH POINTU



Pozn.: čísla označují jednotlivé otázky v dotazníku z přílohy C

PŘÍLOHA F – HARMONOGRAM PILOTNÍHO PROVOZU CZECH POINT

<table>
<tr><th colspan="2">Týden</th><th rowspan="2">Pracovní tým Czech POINT</th><th rowspan="2">Pilotní obce</th></tr>
<tr><th>od</th><th>do</th></tr>
<tr><td>1.1.2007</td><td>7.1.2007</td><td rowspan="5">Analýza</td><td></td></tr>
<tr><td>8.1.2007</td><td>14.1.2007</td><td></td></tr>
<tr><td>15.1.2007</td><td>21.1.2007</td><td></td></tr>
<tr><td>22.1.2007</td><td>28.1.2007</td><td></td></tr>
<tr><td>29.1.2007</td><td>4.2.2007</td><td></td></tr>
<tr><td>5.2.2007</td><td>11.2.2007</td><td rowspan="6">Příprava centrály Czech POINT</td><td></td></tr>
<tr><td>12.2.2007</td><td>18.2.2007</td><td></td></tr>
<tr><td>19.2.2007</td><td>25.2.2007</td><td></td></tr>
<tr><td>26.2.2007</td><td>4.3.2007</td><td></td></tr>
<tr><td>5.3.2007</td><td>11.3.2007</td><td></td></tr>
<tr><td>12.3.2007</td><td>18.3.2007</td><td>Pracovní setkání pilotních obcí</td></tr>
<tr><td>19.3.2007</td><td>25.3.2007</td><td></td><td></td></tr>
<tr><td>26.3.2007</td><td>1.4.2007</td><td></td><td>První pracoviště Czech POINTU</td></tr>
<tr><td>2.4.2007</td><td>8.4.2007</td><td></td><td></td></tr>
<tr><td>9.4.2007</td><td>15.4.2007</td><td></td><td>Školení pilotních obcí</td></tr>
<tr><td>16.4.2007</td><td>22.4.2007</td><td></td><td rowspan="4">Hlavní vlna implementace na pilotních obcích</td></tr>
<tr><td>23.4.2007</td><td>29.4.2007</td><td></td></tr>
<tr><td>30.4.2007</td><td>6.5.2007</td><td></td></tr>
<tr><td>7.5.2007</td><td>13.5.2007</td><td></td></tr>
<tr><td>14.5.2007</td><td>20.5.2007</td><td></td><td></td></tr>
<tr><td>21.5.2007</td><td>27.5.2007</td><td></td><td></td></tr>
<tr><td>28.5.2007</td><td>3.6.2007</td><td></td><td></td></tr>
<tr><td>4.6.2007</td><td>10.6.2007</td><td></td><td></td></tr>
<tr><td>11.6.2007</td><td>17.6.2007</td><td></td><td></td></tr>
<tr><td>18.6.2007</td><td>24.6.2007</td><td></td><td>Anketa spokojenosti</td></tr>
<tr><td>25.6.2007</td><td>1.7.2007</td><td></td><td>Pracovní setkání pilotních obcí</td></tr>
<tr><td>2.7.2007</td><td>8.7.2007</td><td></td><td></td></tr>
<tr><td>9.7.2007</td><td>15.7.2007</td><td></td><td></td></tr>
<tr><td>16.7.2007</td><td>22.7.2007</td><td></td><td></td></tr>
<tr><td>23.7.2007</td><td>29.7.2007</td><td></td><td></td></tr>
<tr><td>30.7.2007</td><td>5.8.2007</td><td rowspan="8">Úprava centrály Czech POINT</td><td rowspan="8">Vyhodnocení pilotního provozu</td><td></td></tr>
<tr><td>6.8.2007</td><td>12.8.2007</td><td></td></tr>
<tr><td>13.8.2007</td><td>19.8.2007</td><td></td></tr>
<tr><td>20.8.2007</td><td>26.8.2007</td><td></td></tr>
<tr><td>27.8.2007</td><td>2.9.2007</td><td></td></tr>
<tr><td>3.9.2007</td><td>9.9.2007</td><td></td></tr>
<tr><td>10.9.2007</td><td>16.9.2007</td><td></td></tr>
<tr><td>17.9.2007</td><td>23.9.2007</td><td rowspan="2">Testování</td><td>Pracovní setkání pilotních obcí</td></tr>
<tr><td>24.9.2007</td><td>30.9.2007</td><td></td></tr>
<tr><td>1.10.2007</td><td></td><td colspan="2">Spuštění ostrého provozu</td></tr>
</table>

Zdroj: www.czechpoint.cz

PŘÍLOHA G – ZÁKON Č. 365/2000 SB.

365/2000 Sb.

ZÁKON

ze dne 14. září 2000

o informačních systémech veřejné správy a o změně některých dalších zákonů

Změna: 517/2002 Sb.

Změna: 413/2005 Sb., 444/2005 Sb.

Změna: 81/2006 Sb. (část)

Změna: 70/2006 Sb.

Změna: 81/2006 Sb.

Změna: 110/2007 Sb.

Změna: 81/2006 Sb. (část), 269/2007 Sb.

Změna: 130/2008 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

§ 1

Předmět úpravy

Tento zákon stanoví práva a povinnosti, které souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.

§ 2

Vymezení pojmů

Pro účely tohoto zákona se rozumí

a) informační činností získávání a poskytování informací, reprezentace informací daty, shromažďování, vyhodnocování a ukládání dat na hmotné nosiče a uchovávání, vyhledávání, úprava nebo pozměňování dat, jejich předávání, šíření, zpřístupňování, výměna, třídění nebo kombinování, blokování a likvidace dat ukládaných na hmotných nosičích. Informační činnost je prováděna správci, provozovateli a uživateli informačních systémů prostřednictvím technických a programových prostředků;

b) informačním systémem funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, a dále nástroje umožňující výkon informačních činností;

c) správcem informačního systému veřejné správy subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá;

d) provozovatelem informačního systému veřejné správy subjekt, který provádí alespoň některé informační činnosti související s informačním systémem. Provozováním informačního systému veřejné správy může správce pověřit jiné subjekty, pokud to jiný zákon nevylučuje;

e) vytvářením informačních systémů veřejné správy proces zavádění informačních a komunikačních technologií, včetně jeho právního, organizačního, znalostního a technického zajištění;

f) datovým prvkem jednotka dat, která je v daném kontextu dále považována za nedělitelnou a je jednoznačně definována;

g) službou činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému;

h) číselníkem seznam přípustných hodnot datového prvku obvykle ve formě dvojic, to znamená kódovaného údaje a hodnoty jeho kódu;

i) referenčním, sdíleným a bezpečným rozhraním informačních systémů veřejné správy (dále jen "referenční rozhraní") souhrn právních, technických, organizačních a jiných opatření vytvářejících jednotné integrační prostředí informačních systémů veřejné správy, které poskytuje kvalitní soustavu společných služeb, včetně služeb výměny oprávněně vyžadovaných informací mezi jednotlivými informačními systémy orgánů veřejné správy a dalšími subjekty, a to i se systémy mimo Českou republiku;

j) atestacemi stanovení shody

   1. způsobilosti k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní, nebo

   2. dlouhodobého řízení informačních systémů veřejné správy s požadavky tohoto zákona a prováděcích právních předpisů k tomuto zákonu;

k) produktem souhrnný název pro technické vybavení, programové vybavení, dokumentaci informačních systémů nebo služby nebo jejich kombinaci;

l) atestem doklad osvědčující kladný výsledek atestace;

m) atestačním střediskem právnická nebo fyzická osoba, kteří jsou podnikateli, provádějící atestace;

n) dálkovým přístupem přístup do informačního systému prostřednictvím sítě nebo služby elektronických komunikací (například s využitím internetu);

o) správcem datového prvku právní subjekt, který nové datové prvky předkládá, navrhuje jejich změnu nebo zrušení;

p) správcem číselníku právní subjekt odpovědný za tvorbu a distribuci číselníku;

q) portálem veřejné správy informační systém vytvořený a provozovaný se záměrem usnadnit veřejnosti dálkový přístup k pro ni potřebným informacím z veřejné správy a komunikaci s ní;

r) sdílením dat umožnění přístupu (tj. poskytování příslušné služby) k daným datům prostřednictvím referenčního rozhraní více subjektům současně;

s) vazbou mezi informačními systémy veřejné správy vzájemné nebo jednostranné poskytování služeb a informací, například sdílení dat;

t) veřejným informačním systémem informační systém vedený správci uvedenými v § 3 odst. 2 nebo jiný informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy;

u) provozním informačním systémem informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy;

v) atestačními podmínkami obchodní podmínky vydané atestačním střediskem, obsahující zejména vymezení předmětu atestace a postupy atestačního střediska při provádění atestací schválené Ministerstvem vnitra (dále jen "ministerstvo"),

w) akreditací postup, na jehož základě se vydává osvědčení o tom, že právnické nebo fyzické osoby, které jsou podnikateli, splňují ve vymezeném rozsahu technické, organizační, ekonomické a personální předpoklady k provádění atestací,

x) provozní dokumentací dokumentace informačního systému veřejné správy, která popisuje funkční a technické vlastnosti informačního systému.

§ 3

Informační systémy veřejné správy

(1) Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů.[1])

(2) Správci informačních systémů veřejné správy jsou ministerstva, jiné správní úřady a územní samosprávné celky (dále jen "orgány veřejné správy").

(3) Zákon se nevztahuje na informační systémy veřejné správy vedené

a) zpravodajskými službami;[2])

b) Policií České republiky při plnění jejích úkolů;[3])

c) orgány činnými v trestním řízení v souvislosti s trestním řízením[3a]), s výjimkou evidence Rejstříku trestů[3b]),

d) Policií České republiky a Vězeňskou službou České republiky při poskytování zvláštní ochrany a pomoci ohroženým osobám podle zvláštního právního předpisu[3c]),

e) Ministerstvem financí v rámci činnosti podle zvláštního právního předpisu o boji proti legalizaci výnosů z trestné činnosti nebo zvláštního právního předpisu o provádění mezinárodních sankcí za účelem udržování mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu;[4]

f) Národním bezpečnostním úřadem, zpravodajskou službou nebo Ministerstvem vnitra při provádění bezpečnostního řízení a vedení evidencí podle zvláštního zákona[5]),

g) v působnosti Ministerstva obrany, při činnostech vykonávaných podle zvláštních právních předpisů[6]),

h) Ministerstvem vnitra,Ministerstvem financí a Ministerstvem spravedlnosti při zpracování osobních údajů příslušníků bezpečnostních sborů podle zvláštního právního předpisu[6a]),

i) správními úřady a orgány územních samosprávných celků v přenesené působnosti při činnostech souvise-

[1] Například zákon č. 89/1995 Sb., o státní statistické službě, ve znění zákona č. 356/1999 Sb., zákon č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, zákon č. 48/1997 Sb., o veřejném zdra-votním pojištění, ve znění pozdějších předpisů, zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů, zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

[2] Zákon č. 153/1994 Sb., o zpravodajských službách, ve znění zákona č. 118/1995 Sb.

[3] § 42d zákona č. 283/1991 Sb., o Policii České republiky, ve znění zákona č. 60/2001 Sb.

[3a] § 12 odst. 1 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

[3b] Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění zákona č. 126/2003 Sb.

[3c] Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

[4] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

[5] Zákon č. 218/1999 Sb., o rozsahu branné povinnosti a o vojenských správních úřadech (branný zákon), ve znění pozdějších předpisů.

[6] Zákon č. 218/1999 Sb., o rozsahu branné povinnosti a o vojenských správních úřadech (branný zákon), ve znění pozdějších předpisů.
Zákon č. 219/1999 Sb., o ozbrojených silách České republiky, ve znění pozdějších předpisů.
Zákon č. 220/1999 Sb., o průběhu základní nebo náhradní služby a vojenských cvičeních a o některých právních poměrech vojáků v záloze, ve znění zákona č. 128/2002 Sb.
Zákon č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů.
Zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění zákona č. 320/2002 Sb.

[6a] Zákon č.361/2003Sb.,o služebním poměru příslušníků bezpečnostních sborů, ve znění zákona č. 186/2004 Sb.

jících se zajišťováním obrany státu podle zvláštního právního předpisu[6b]),

j) orgány veřejné správy a právnickými osobami, pokud jsou používané výlučně k podpoře krizového řízení [6c]).

(4) Mají-li informační systémy uvedené v odstavci 3 písm. b) až j) vazby na jiné informační systémy veřejné správy realizované prostřednictvím informačních činností, vztahuje se na ně zákon pouze v rozsahu těchto vazeb, nestanoví-li zvláštní právní předpisy jinak.

(5) Zákon se nevztahuje na provozní informační systémy správců informačních systémů veřejné správy, s výjimkou vazeb provozních informačních systémů na informační systémy veřejné správy.

(6) Zákon se rovněž nevztahuje na informační systémy veřejné správy nakládající s utajovanými informacemi[5]).

(7) Práva a povinnosti správců a provozovatelů informačních systémů při zpracovávání informací v informačních systémech stanovené zvláštními zákony[7]) nejsou tímto zákonem dotčeny.

(8) Provozovatel je povinen při provozování informačního systému [§ 2 písm.d)]zajišťovat ochranu a bezpečnost informací v rámci provozovaného informačního systému.

§ 4

Ministerstvo vnitra

(1) Ministerstvo ve spolupráci s orgány veřejné správy

a) vyhledává, zpracovává, ukládá a vytváří nové informace, které jsou znalostní základnou pro kvalitní vytváření a rozvoj informačních systémů veřejné správy;

b) zpracovává návrhy strategických dokumentů v oblasti informačních systémů veřejné správy, a to i z hlediska bezpečnosti těchto systémů, a předkládá tyto dokumenty vládě, sleduje a analyzuje informační potřeby veřejné správy a stav informačních systémů veřejné správy;

c) připravuje nebo koordinuje přípravu záměrů pro budování nebo přetváření informačních systémů veřejné správy vyvolané společnou potřebou více správců informačních systémů veřejné správy;

d) připravuje nebo koordinuje přípravu záměrů pro budování nebo přetváření informačních systémů veřejné správy vyvolané potřebou spolupráce a koordinace na mezinárodní úrovni;

e) vyjadřuje se k návrhům dokumentací programů obsahujících pořízení, obnovu a provozování informačních a komunikačních technologií vypracovaných podle zvláštního právního předpisu[7a]). Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele dokumentace programu a k potřebám zajištění řádného výkonu veřejné správy,

f) zajišťuje tvorbu metodických pokynů pro výkon odborných činností spojených s vytvářením, rozvojem a využíváním informačních systémů veřejné správy;

g) stanoví a spravuje referenční rozhraní a stanoví prováděcím právním předpisem technické a funkční náležitosti uskutečňování vazeb mezi informačními systémy prostřednictvím referenčního rozhraní;

h) vytváří a spravuje veřejný informační systém, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy;

i) vytváří a spravuje veřejný informační systém o datových prvcích, jeho prostřednictvím vyhlašuje datové prvky, a stanoví prováděcím právním předpisem formu a technické náležitosti předávání údajů do něj;

j) vytváří a spravuje portál veřejné správy;

k) koordinuje a vytváří podmínky pro podporu rozvoje elektronického obchodu;

l) koordinuje a vytváří podmínky pro činnost veřejné správy prostřednictvím veřejných informačních systémů, včetně dálkového přístupu,

m) koordinuje a vytváří podmínky pro činnost kontaktních míst veřejné správy.

(2) Ministerstvo

a) kontroluje u orgánů veřejné správy dodržování povinností stanovených tímto zákonem. Při kontrole postupuje podle zvláštního zákona;[8])

b) se vyjadřuje k investičním záměrům akcí pořízení, obnovy a provozování informačních a komunikačních technologií,jejichž registrace v Informačním systému financování reprodukce majetku, zadání jejich realizace a změna jejich závazně stanovených parametrů se provádí pouze se souhlasem Ministerstva financí podle zvláštního právního předpisu7a).Ministerstvo přitom přihlíží zejména k oprávněným zájmům předkladatele investičních záměrů a akcí a k potřebám zajištění řádného výkonu veřejné správy;

c) vykonává působnost stanovenou tímto zákonem v oblasti akreditace a atestací;

[6b] Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.

[6c] § 26 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění zákona č. 320/2002 Sb.

[7] Například zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, zákon č. 337/1992 Sb., ve znění pozdějších předpisů, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 101/2000 Sb., zákon č. 158/1999 Sb., o sčítání lidu, domů a bytů v roce 2001.

[7a] Zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů.

[8] Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

d) stanoví pravidla pro sdílení dat a služby mezi jednotlivými informačními systémy veřejné správy prostřednictvím referenčního rozhraní a pravidla pro zápis datových prvků do informačního systému o datových prvcích. Postupy ministerstva a orgánů veřejné správy při vedení a zápisu datových prvků do informačního systému o datových prvcích, včetně postupů ministerstva při vyhlašování datových prvků, stanoví prováděcí právní předpis;

e) ukládá sankce za správní delikty podle § 7;

f) ukládá opatření směřující k nápravě nedostatků;

g) vyjadřuje se k projektům informačních systémů veřejné správy;

h) vydává Věstník, v němž uveřejňuje metodické pokyny [odstavec 1 písm.f)], seznam atestačních středisek, udělení osvědčení o akreditaci a udělení atestů a další dokumenty vztahující se k informačním systémům veřejné správy. Vydávání Věstníku zabezpečuje ministerstvo prostřednictvím portálu veřejné správy;

i) konzultuje návrhy metodických pokynů zejména s dotčenými subjekty formou veřejné konzultace, jejímž cílem je získání stanovisek a připomínek dotčených subjektů k předmětnému návrhu, a za tímto účelem zřídí a spravuje informační systém, kde způsobem umožňujícím dálkový přístup uveřejňuje návrhy metodických pokynů, umožňuje předkládání připomínek a uveřejňuje výsledek konzultace.

§ 5

Orgány veřejné správy

(1) Orgány veřejné správy v rozsahu své zákonné působnosti provádějí výběr technických a programových prostředků a dalších produktů pro provoz jimi vytvářených a spravovaných informačních systémů.

(2) Orgány veřejné správy jsou v rámci informačních systémů veřejné správy povinny

a) spolupracovat s ministerstvem při plnění jeho úkolů podle § 4 odst. 1, včetně kontroly na místě podle § 4 odst. 2 prováděné ministerstvem;

b) předložit ministerstvu k vyjádření návrhy dokumentací programů obsahující pořízení, obnovu a provozování informačních a komunikačních technologií vypracovaných podle zvláštního právního předpisu[7a]) a investiční záměry akcí pořízení, obnovy a provozování informačních a komunikačních technologií, jejichž registrace v Informačním systému financování reprodukce majetku, zadání jejich realizace a změna jejich závazně stanovených parametrů se provádí pouze se souhlasem Ministerstva financí podle zvláštního právního předpisu[7a]). Náležitosti dokumentací programů a investičních záměrů stanoví zvláštní právní předpis[8a]);

c) uveřejňovat číselníky, pokud jsou správci těchto číselníků a není zákonem stanoveno jinak, a to i způsobem umožňujícím dálkový přístup a předávat ministerstvu údaje do informačního systému o datových prvcích v elektronické podobě,ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem;

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. Způsobilost informačního systému k realizaci těchto vazeb jsou povinny prokázat atestem. Toto ustanovení se nevztahuje na vazby mezi jimi provozovanými informačními systémy a informačními systémy vedenými zpravodajskými službami;

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 informačním systému podle § 4 odst. 1 písm. h) a i), pokud zvláštní zákon nestanoví jinak,[9]);

f) postupovat při uveřejňování informací způsobem umožňujícím dálkový přístup tak, aby byly informace související s výkonem veřejné správy uveřejňovány ve formě, která umožňuje, aby se s těmito informacemi v nezbytném rozsahu mohly seznámit i osoby se zdravotním postižením. Formu uveřejnění informací stanoví prováděcí právní předpis;

g) odstranit zjištěné nedostatky ve lhůtě stanovené ministerstvem.

(3) Ústřední správní úřady zveřejňují věstníky vydávané ve své působnosti na portálu veřejné správy.

§ 5a

Dlouhodobé řízení informačních systémů veřejné správy

(1) Orgány veřejné správy vytvářejí a vydávají informační koncepci, uplatňují ji v praxi a vyhodnocují její dodržování. V informační koncepci orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných informačních systémů veřejné správy a vymezí obecné principy pořizování, vytváření a provozování informačních systémů veřejné správy. Obsah a strukturu informační koncepce, jakož i postupy orgánů veřejné správy při jejím vytváření, vydávání a při vyhodnocování jejího dodržování a požadavky na řízení bezpečnosti a kvality informačních systémů veřejné správy stanoví prováděcí právní předpis.

[8a] Vyhláška č. 231/2005 Sb., o účasti státního rozpočtu na financování programů pořízení a reprodukce majetku, ve znění vyhlášky č. 269/2005 Sb.

[9] Například zákon č. 148/1998 Sb., ve znění pozdějších předpisů, zákon č. 337/1992 Sb., ve znění pozdějších předpisů, zákon č. 89/1995 Sb., ve znění zákona č. 356/1999 Sb., zákon č. 106/1999 Sb., ve znění zákona č. 101/2000 Sb., zákon č. 101/2000 Sb.

(2) Na základě vydané informační koncepce orgány veřejné správy vytvářejí a vydávají provozní dokumentaci k jednotlivým informačním systémům veřejné správy, uplatňují ji v praxi a vyhodnocují její dodržování. Obsah a strukturu provozní dokumentace stanoví prováděcí právní předpis.

(3) Orgány veřejné správy si zajistí atestaci dlouhodobého řízení informačních systémů veřejné správy a prokáží splnění povinností podle odstavců 1 a 2 atestem dlouhodobého řízení informačních systémů veřejné správy. Rozsah provozní dokumentace předkládané při atestaci stanoví prováděcí právní předpis. Povinnost podle věty první se nevztahuje na obce,které vykonávají přenesenou působnost pouze v základním rozsahu[9a]).

§ 5b

Orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.

§ 5c

Kontrola dodržování povinností orgánů veřejné správy

(1) Zjistí-li ministerstvo při kontrole podle § 4 odst. 2 písm. a) u orgánu veřejné správy nedostatky, vyzve orgán veřejné správy, aby přijal opatření k nápravě těchto nedostatků.

(2) Ve výzvě podle odstavce 1 ministerstvo specifikuje zjištěné nedostatky a stanoví opatření, která mají být orgánem veřejné správy přijata k nápravě těchto nedostatků, a určí orgánu veřejné správy přiměřenou lhůtu k přijetí těchto opatření. Tato lhůta nesmí přesáhnout 6 měsíců.

§ 6

Pověření k provádění akreditace

(1) Akreditaci provádí právnická osoba, která je členem mezinárodních sdružení zabývajících se akreditací a určených ministerstvem podle odstavce 6 a která byla na základě žádosti o pověření k provádění akreditace rozhodnutím ministerstva k provádění akreditace pověřena (dále jen "akreditující osoba"). Pověření k provádění akreditace je nepřevoditelné.

(2) K žádosti o pověření právnické osoby k provádění akreditace žadatel přikládá

a) zakladatelský dokument,

b) doklad o věcných, personálních a organizačních předpokladech pro činnost akreditující osoby,

c) doklad o členství v mezinárodních sdruženích zabývajících se akreditací a určených ministerstvem podle odstavce 6 a způsob a rozsah plnění povinností z členství vyplývajících,

d) doklad o zajištění zdrojů potřebných pro výkon činností akreditující osoby,

e) podmínky a postupy posuzování žadatelů o akreditaci (dále jen"akreditační pravidla"),které musí být v souladu s pravidly mezinárodních sdružení zabývajících se akreditací určených ministerstvem podle odstavce 6.

(3) Splňuje-li žadatel všechny podmínky předepsané tímto zákonem pro pověření k provádění akreditace, vydá ministerstvo rozhodnutí, jímž jej prováděním akreditace pověří. V opačném případě žádost o pověření k provádění akreditace zamítne. V rozhodnutí, kterým ministerstvo pověřuje akreditující osobu prováděním akreditace, vysloví ministerstvo souhlas s akreditačními pravidly.

(4) Akreditující osoba je povinna

a) postupovat při provádění akreditace v souladu s akreditačními pravidly, s nimiž ministerstvo vyslovilo souhlas,

b) plnit povinnosti vyplývající z členství v mezinárodních sdruženích zabývajících se akreditací určených ministerstvem podle odstavce 6,

c) mít zajištěné zdroje potřebné pro výkon svých činností,

d) personálně zajišťovat své činnosti osobami, které mají odborné znalosti, zkušenosti a kvalifikaci nezbytnou pro provádění akreditací a které jsou obeznámeny s akreditačními pravidly,

e) jednat v průběhu akreditace nestranně a nepodjatě, zejména se zdržet všeho, co by mohlo ohrozit důvěru v její nestrannost,

f) ohlásit bezodkladně ministerstvu, že není schopna po dobu delší než 3 měsíce plnit povinnosti podle písmene c).

(5) Neplní-li akreditující osoba povinnosti stanovené v tomto zákoně a

a) byla jí v uplynulém kalendářním roce nejméně dvakrát ministerstvem uložena pokuta podle § 7, nebo

b) porušení zákona je natolik závažné, že již nelze očekávat nápravu závadného stavu a řádné plnění povinností akreditující osoby, rozhodne ministerstvo o odnětí pověření k provádění akreditace. Ministerstvo vždy rozhodne o odnětí pověření k provádění akreditace, pokud o to akreditující osoba písemně požádá.

(6) Seznam určených mezinárodních sdružení zabývajících se akreditací, rozhodnutí o pověření akreditující osoby k provádění akreditace a rozhodnutí o odnětí pověřeník provádění akreditace uveřejní ministerstvo ve Věstníku.

[9a] § 61 odst. 1 písm. a) zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.

(7) Dozor nad akreditující osobou při plnění povinností vyplývajících z tohoto zákona vykonává ministerstvo. Při dozoru se postupuje podle zvláštního zákona[8]).

§ 6a

Osvědčení o akreditaci

(1) Akreditaci zahájí akreditující osoba na žádost právnické nebo fyzické osoby, pokud jsou podnikateli. Akreditace se provádí za úplatu. Cena se sjednává podle zvláštního právního předpisu[10]).

(2) Na základě provedené akreditace vydá akreditující osoba osvědčení o akreditaci, pokud má žadatel o akreditaci oprávnění podnikat v oblasti atestací a splňuje podmínky akreditačních pravidel. Osvědčení o akreditaci vymezuje předmět, rozsah a podmínky zabezpečení předpokladů podle věty první a dobu, na kterou bylo vydáno.

(3) Akreditující osoba předá v elektronické podobě ministerstvu informace o vydaném osvědčení o akreditaci ve lhůtě 7 pracovních dnů ode dne jeho vydání.

(4) Akreditující osoba dohlíží u atestačních středisek nad dodržováním podmínek v akreditačních pravidlech. Zjistí-li nedostatky v jejich plnění, podle závažnosti nedostatků v souladu s akreditačními pravidly, osvědčení o akreditaci odejme. Tuto skutečnost akreditující osoba bezodkladně sdělí ministerstvu v elektronické podobě.

§ 6b

Pověření k provádění atestací

(1) Atestace provádí atestační středisko podle § 2 písm. o), které bylo na základě žádosti o pověření k provádění atestací rozhodnutím ministerstva pověřeno k provádění atestací.

(2) Ministerstvo vydá rozhodnutí o pověření atestačního střediska k provádění atestací, pokud k žádosti o pověření k provádění atestací předloží

c) návrh atestačních podmínek, jež obsahují náležitosti podle § 2 písm.v),

d) osvědčení o akreditaci podle § 6a a

e) potvrzení příslušných orgánů, že nemá splatný nedoplatek na pojistném na veřejné zdravotní pojištění, na pojistném na sociální zabezpečení, na příspěvku na státní politiku zaměstnanosti a nemá v evidenci daní zachyceny daňové nedoplatky.

(3) V pověření k provádění atestací ministerstvo stanoví období, na které se pověření uděluje, a schválí postupy atestačního střediska při provádění atestací obsažené v atestačních podmínkách, které žadatel o pověření k provádění atestací předložil.

(4) Pověření k provádění atestací nelze bez souhlasu ministerstva převést na jinou osobu. Pověření k provádění atestací se uděluje na období nejvýše 5 let.

§ 6c

(1) Ministerstvo odejme pověření k provádění atestací, jestliže atestační středisko

a) pozbylo osvědčení o akreditaci, na jehož základě mu bylo pověření k provádění atestací uděleno,

b) pozbylo oprávnění k podnikání, na základě kterého bylo oprávněno podnikat v oblasti atestací,

c) neplní povinnosti stanovené tímto zákonem, nepostupuje podle atestačních podmínek, nebo nedodržuje ustanovení prováděcích právních předpisů k tomuto zákonu, ačkoliv bylo na možnost odnětí pověření k provádění atestací z těchto důvodů ministerstvem písemně upozorněno a nápravu nezjednalo ani v přiměřené lhůtě stanovené ministerstvem, nebo

d) ve stanovené lhůtě nepředložilo ministerstvu upravené znění atestačních podmínek podle odstavce 4.

(2) Ministerstvo odejme pověření k provádění atestací, jestliže o to atestační středisko písemně požádá.

(3) Ministerstvo může z vlastního podnětu zrušit rozhodnutí o schválení postupů atestačního střediska podle § 6b odst. 3,

a) dojde-li k ohrožení nebo omezení provozu informačních systémů veřejné správy,

b) je-li to nezbytné k dodržení mezinárodních smluv, jimiž je Česká republika vázána.

(4) Jestliže ministerstvo zruší rozhodnutí o schválení postupů atestačního střediska při provádění atestací, sdělí atestačnímu středisku důvody, proč bylo rozhodnutí zrušeno, a vyzve ho, aby ve stanovené přiměřené lhůtě předložilo ministerstvu upravené znění atestačních podmínek ke schválení postupů atestačního střediska při provádění atestací.

(5) Ministerstvo schvaluje postupy atestačního střediska při provádění atestací, jestliže atestační středisko předloží návrh jejich nového znění.

§ 6d

Provádění atestací

(1) Atestační střediska jsou při provádění atestací povinna

a) postupovat podle atestačních podmínek a

b) provádět posuzování dlouhodobého řízení informačních systémů veřejné správy a způsobilosti k realizaci vazeb informačních systémů veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní v souladu s tímto zákonem a uděleným pověřením postupy stanovenými prováděcím právním předpisem.

(2) Atestační středisko není oprávněno provádět atestace dlouhodobého řízení informačních systémů veřejné správy a atestace způsobilosti k realizaci vazeb informačních systémů veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní, na jejichž vývoji, přípravě, výrobě nebo na obchodu se

jakkoliv podílelo samo nebo s ním ekonomicky nebo personálně spojená osoba, kdy

a) ekonomicky nebo personálně spojenými osobami se pro účely tohoto zákona rozumí, jestliže se jedna osoba podílí přímo nebo nepřímo na vedení, kontrole nebo jmění druhé osoby nebo jestliže se shodné právnické nebo fyzické osoby přímo nebo nepřímo podílejí na vedení, kontrole nebo jmění obou osob anebo fyzické osoby blízké[11]),

b) účastí na kontrole nebo jmění se pro účely tohoto zákona rozumí jakýkoli podíl na základním kapitálu nebo podíl s hlasovacím právem.

(3) Atestační středisko provádí atestace na základě smlouvy uzavřené s žadatelem o atestaci za úplatu. Cena se sjednává podle zvláštního právního předpisu[10]).

(4) Atestační středisko vydá žadateli o atestaci protokol o provedené zkoušce ve lhůtě 7 pracovních dnů ode dne ukončení této zkoušky. Atestační středisko vydá o kladném výsledku atestace žadateli atest. Atest musí obsahovat podmínky platnosti atestu.

(5) Atest se vydává na dobu nejvýše 5 let.

(6) Atestační středisko, které vystavilo atest, může na základě žádosti držitele atestu před uplynutím platnosti atestu prodloužit jeho platnost o 2 roky, a to i opakovaně. Žadatel i atestační středisko při prodlužování platnosti atestu postupují obdobně jako při provádění atestací.

(7) Atestační středisko předá v elektronické podobě prostřednictvím automatizovaného ohlašovacího procesu přístupného dálkovým přístupem na elektronické adrese,kterou ministerstvo uveřejní ve Věstníku, ministerstvu informace o provedené atestaci ve lhůtě 7 pracovních dnů ode dne jejího provedení. Informaci o vydání atestu ministerstvo uveřejní ve Věstníku.

(8) Dozor nad atestačními středisky při plnění povinností vyplývajících z tohoto zákona vykonává ministerstvo. Při dozoru se postupuje podle zvláštního zákona[8]).

§ 6e

Uzavření smlouvy o provedení atestace

(1) Atestační středisko zveřejní atestační podmínky, každou jejich změnu, odejmutí pověření k provádění atestací (§ 6c odst. 1 a 2) nebo zrušení rozhodnutí o schválení postupů atestačního střediska (§ 6c odst. 3) ve své provozovně a způsobem umožňujícím dálkový přístup do 7 pracovních dnů od vydání příslušného rozhodnutí ministerstva.

(2) Atestační středisko navrhne uzavření smlouvy a provedení atestace každému, kdo jej způsobem stanoveným v atestačních podmínkách vyzve k uzavření smlouvy podle zveřejněných atestačních podmínek.

(3) Odchylky od atestačních podmínek lze pro jednotlivý případ sjednat jen tehdy, jestliže to atestační podmínky připouštějí a jestliže se těmito změnami nemění povaha nabízené atestační služby.

(4) Atestačnímu středisku nevzniká povinnost navrhnout uzavření smlouvy o provedení atestace, jestliže jejím obsahem mají být také odchylky od atestačních podmínek podle odstavce 3.

§ 6f

Dodání datové zprávy orgánu veřejné moci prostřednictvím portálu veřejné správy

(1) Správce portálu veřejné správy (dále jen "správce portálu") zajišťuje podle podmínek stanovených tímto zákonem dodání datové zprávy orgánu veřejné moci, pokud tak stanoví zvláštní právní předpis.

(2) Každý je oprávněn využít služby dodání datové zprávy orgánu veřejné moci (dále jen "dodání") prostřednictvím portálu veřejné správy (dále jen"portál") za podmínek stanovených tímto zákonem, zvláštními právními předpisy[11a]) a provozním řádem portálu pro dodávání datových zpráv orgánům veřejné moci prostřednictvím portálu (dále jen "provozní řád").

(3) Převzetím datové zprávy vzniká správci portálu povinnost bez zbytečného prodlení a za podmínek stanovených tímto zákonem dodat datovou zprávu orgánu veřejné moci, kterého odesílatel datové zprávy označil jako příjemce (dále jen "příjemce"). Datová zpráva je převzata portálem v okamžiku, kdy je mu dostupná a je způsobilá k dalšímu zpracování za účelem dodání.

(4) Převzetí datové zprávy potvrzuje správce portálu neprodleně odesílateli datovou zprávou, která je označena elektronickou značkou[11b]) správce portálu a obsahuje datum a čas převzetí.

(5) Správce portálu dodává datovou zprávu příjemci doplněnou o údaje data a času, kdy datovou zprávu převzal.

(6) Dodání potvrzuje příjemce bez zbytečného prodlení správci portálu datovou zprávou, která je označena elektronickou značkou[11b]) příjemce a obsahuje datum a čas dodání příjemci. Datová zpráva je dodána příjemci v okamžiku, kdy je dostupná elektronické podatelně orgánu veřejné moci.

(7) Dodání datové zprávy příjemci potvrzuje příjemce prostřednictvím portálu bez zbytečného prodlení odesílateli datovou zprávou, která je označena elektronickou značkou[11b]) příjemce a obsahuje datum a čas dodání příjemci.

[11] § 116 a násl. občanského zákoníku.

[10] § 21 až 24 zákona č. 89/1995 Sb., ve znění zákona č. 356/1999 Sb.

[11a] Zákon č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, ve znění pozdějších předpisů.

[11b] Zákon o elektronickém podpisu.

§ 6g

Provozní řád

(1) Provozní řád pro dodávání datových zpráv orgánu veřejné moci prostřednictvím portálu veřejné správy vydává ministerstvo a zveřejňuje jej ve Věstníku.

(2) Provozní řád obsahuje vymezení

a) způsobu předání datové zprávy odesílatelem portálu, včetně stanovení technických parametrů datových zpráv,

b) způsobu dodání portálem příjemci, včetně nejvyšší možné doby, která může uplynout od převzetí do dodání,

c) orgánů veřejné moci, kterým je podle zvláštního právního předpisu možné prostřednictvím portálu datové zprávy dodávat, a typů podání, která je podle zvláštního právního předpisu možné prostřednictvím portálu dodávat,

d) provozní doby přístupnosti portálu.

§ 6h

Povinnost zachovávat mlčenlivost

(1) Správce portálu a fyzické osoby podílející se na straně správce portálu na poskytování služby dodání mají povinnost zachovávat mlčenlivost o obsahu datových zpráv, u kterých zajišťují dodání. Odesílatel nebo příjemce, případně jejich zástupci nebo právní nástupci mohou osoby podle věty první povinnosti mlčenlivosti zprostit.

(2) Správce portálu a fyzické osoby podílející se na straně správce portálu na poskytování služby dodání mají povinnost zachovávat mlčenlivost o skutečnostech týkajících se služby dodání datové zprávy orgánu veřejné moci prostřednictvím portálu, které se při své činnosti dozvěděli. Znalosti těchto skutečností smějí využívat jen pro potřeby poskytování služby dodání; nesmějí umožnit, aby se s nimi neoprávněně seznámila jiná osoba. Odesílatel nebo příjemce, případně jejich zástupci nebo právní nástupci mohou osoby podle věty první povinnosti mlčenlivosti zprostit.

(3) Povinnost mlčenlivosti podle odstavce 2 se nevztahuje na údaje, ze kterých nevyplývá, kdo byl odesílatelem, ani kdo byl příjemcem.

(4) Porušením povinnosti mlčenlivosti podle odstavce 2 není, pokud správce portálu a osoby podílející se na straně správce portálu na poskytování služby dodání sdělí údaje podle odstavce 2 odesílateli nebo příjemci, popřípadě jejich zástupci, právnímu nástupci nebo jiným osobám, které s vědomím odesílatele nebo příjemce jednají v jeho prospěch.

(5) Povinnost zachovávat mlčenlivost se nevztahuje na případ, kdy má správce portálu podle zvláštního právního předpisu[11d]) povinnost

a) sdělit osobám a orgánům oprávněným podle zvláštního právního předpisu[11d]) informace o poskytovaném nebo poskytnutém dodání, nebo jim umožnit, aby tyto informace získaly,

b) vydat osobám a orgánům oprávněným podle zvláštního právního předpisu[11d]) záznam o zpracování datové zprávy, která je předmětem dodání, nebo

c) učinit nebo umožnit jiná opatření.

§ 6i

Práva a povinnosti správce portálu

(1) Správce portálu je oprávněn zjišťovat obsah datové zprávy pouze v rozsahu údajů nezbytných pro splnění povinností stanovených tímto zákonem. Technické parametry datové zprávy, která je předmětem dodání, je správce portálu oprávněn zjišťovat za účelem ověření, zda odpovídají podmínkám stanoveným provozním řádem.

(2) Právo nakládat s datovou zprávou mají až do jejího dodání jen správce portálu a odesílatel.

(3) Správce portálu není oprávněn datové zprávy, které převzal za účelem dodání, kopírovat nebo uchovávat.

(4) Správce portálu vede evidenci datových zpráv, které převzal za účelem dodání, v rozsahu nutném k naplnění povinností stanovených tímto zákonem. V evidenci vede zejména

a) datum a čas převzetí datové zprávy, která je předmětem dodání, potvrzení o jejím převzetí,

b) datum a čas dodání datové zprávy, která je předmětem dodání, potvrzení o jejím dodání,

c) informace nezbytné k určení odesílatele a příjemce datové zprávy.

(5) Informace podle odstavce 4 je správce portálu povinen uchovávat po dobu 3 let od okamžiku jejich vzniku.

(6) Správce portálu je oprávněn datovou zprávu zničit, jestliže

a) jde o datovou zprávu, kterou nelze dodat příjemci ani vrátit odesílateli, nebo

b) je to nezbytné pro zabránění vzniku škody.

§ 7

Správní delikty právnických osob

(1) Akreditující osobě, která

a) neprovádí akreditaci podle akreditačních pravidel, s nimiž ministerstvo vyslovilo souhlas [§ 6 odst. 4 písm. a)],

[11d] Například § 7 až 12 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, § 11 až 16 zákona č. 67/1992 Sb., o Vojenském obranném zpravodajství, ve znění zákona č. 153/1994 Sb. a zákona č. 88/1995 Sb.

b) vydá osvědčení o akreditaci, aniž by splňovala personální požadavky [§ 6 odst. 4 písm. d)],

c) neohlásí bezodkladně ministerstvu, že nemá po dobu delší než 3 měsíce zajištěné zdroje potřebné pro výkon svých činností [§ 6 odst. 4 písm. f)],

d) nepostupuje při provádění akreditace nestranně [§ 6 odst. 4 písm. e)], nebo

e) nesplní ve stanovené lhůtě povinnost předání informací ministerstvu (§ 6a odst. 3), se uloží pokuta do 100 000 Kč.

(2) Atestační středisko se dopustí správního deliktu tím, že

a) neprovádí atestaci podle postupů atestačního střediska schválených ministerstvem (§ 6b odst. 3),

b) vyhodnotilo způsobilost žadatele o atestaci (§ 6b) k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní nebo způsob dlouhodobého řízení informačních systémů veřejné správy v rozporu s osvědčením o akreditaci (§ 6a) nebo tímto zákonem,

c) vydá atest na způsobilost k realizaci vazeb informačního systému veřejné správy s jinými informačními systémy prostřednictvím referenčního rozhraní nebo na dlouhodobé řízení informačních systémů veřejné správy, na jejichž vývoji, přípravě, výrobě nebo na obchodu se jakkoliv podílelo samo nebo s ním ekonomicky nebo personálně spojená osoba (§ 6d odst. 2),

d) nesplní ve stanovené lhůtě povinnost vydání protokolu o provedené zkoušce (§ 6d odst. 4),

e) nesplní ve stanovené lhůtě povinnost předání informací ministerstvu (§ 6d odst. 7), nebo

f) nesplní ve stanovené lhůtě povinnost zveřejnění atestačních podmínek (§ 6e odst. 1).

(3) Za správní delikt podle odstavce 2 písm. a) až c) se uloží pokuta do 1 000 000 Kč, za správní delikt podle odstavce 2 písm. d) až f) se uloží pokuta do 100 000 Kč.

§ 7a

Společná ustanovení

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při určení výše pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Správní delikty podle tohoto zákona projednává ministerstvo.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby[12]) nebo v přímé souvislosti s ním, se vztahují ustanovení tohoto zákona o odpovědnosti a postihu právnické osoby.

(6) Pokuty vybírá ministerstvo a vymáhá celní úřad. Příjem z pokut je příjmem státního rozpočtu.

(7) Při vybírání a vymáhání uložených pokut se postupuje podle zvláštního právního předpisu[12a]).

§ 8

(1) Účastníkem řízení o udělení pověření k provádění akreditace je žadatel o pověření k provádění akreditace. Účastníkem řízení o odnětí pověření k provádění akreditace je akreditující osoba, které má být rozhodnutím pověření odňato.

(2) Účastníkem řízení o udělení pověření k provádění atestací je žadatel o pověření k provádění atestací. Účastníkem řízení o odnětí pověření k provádění atestací je atestační středisko, kterému má být rozhodnutím pověření odňato.

(3) Účastníkem řízení o vyslovení souhlasu se změnou postupů atestačního střediska a o zrušení rozhodnutí o schválení postupů atestačního střediska je atestační středisko, jehož postupů se řízení týká.

Kontaktní místa veřejné správy

§ 8a

(1) Podání správním orgánům lze činit v rozsahu a za podmínek stanovených jinými právními předpisy prostřednictvím kontaktního místa veřejné správy (Českého podacího ověřovacího informačního národního terminálu – Czech POINT).

(2) Kontaktními místy veřejné správy jsou

a) notáři,

b) krajské úřady,

c) matriční úřady,

d) obecní úřady, úřady městských částí nebo městských obvodů územně členěných statutárních měst a úřady městských částí hlavního města Prahy, jejichž seznam stanoví prováděcí právní předpis,

e) zastupitelské úřady stanovené prováděcím právním předpisem,

f) držitel poštovní licence[15]) a Hospodářská komora České republiky.

---

[12] § 2 obchodního zákoníku.

[12a] Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

[15] Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.

(3) Držitel poštovní licence a Hospodářská komora České republiky mohou za provedení správního úkonu kontaktního místa veřejné správy požadovat poplatek,jehož výše nesmí přesáhnout sazbu správního poplatku stanovenou pro tento správní úkon v zákoně o správních poplatcích.

(4) Nestanoví-li tento zákon nebo jiný právní předpis jinak, je působnost kontaktního místa veřejné správy výkonem přenesené působnosti krajských a obecních úřadů.

(5) Označení Český podací ověřovací informační národní terminál nebo Czech POINT lze užít jen pro kontaktní místo veřejné správy.

(6) Systém kontaktních míst veřejné správy (Český podací ověřovací informační národní terminál – Czech POINT) provozuje ministerstvo.

Vydávání ověřených výstupů z informačních systémů veřejné správy

§ 9

(1) Z informačních systémů veřejné správy nebo jejich částí, které jsou veřejnými evidencemi, rejstříky nebo seznamy, vydávají orgány veřejné správy, které jsou správci nebo provozovateli těchto systémů (dále jen "správci"), na požádání úplný nebo částečný výpis ze zápisu vedeného v elektronické podobě v tomto informačním systému. Z informačních systémů veřejné správy nebo jejich částí, které jsou neveřejnými evidencemi, rejstříky nebo seznamy, vydávají správci, pokud tak stanoví zvláštní právní předpis, na požádání úplný nebo částečný výpis ze zápisu vedeného v elektronické podobě v tomto informačním systému osobě, které se zápis přímo týká, nebo osobě, která je podle zvláštního právního předpisu oprávněna žádat informaci uvedenou v zápisu, a to v rozsahu tímto zvláštním právním předpisem stanoveném.

(2) Stanoví-li tak zvláštní právní předpis, výpis podle odstavce 1 (dále jen „výpis“) nebo potvrzení o tom, že určitý údaj v informačním systému veřejné správy není v elektronické podobě označené elektronickou značkou11b) správce (dále jen „výstup z informačního systému veřejné správy“), ověřují a ověřené výstupy z informačních systémů veřejné správy na žádost vydávají kontaktní místa veřejné správy. S přihlédnutím k současným technickým podmínkám mohou kontaktní místa veřejné správy vydávat ověřené výstupy i z ostatních registrů veřejné správy, které jsou veřejnými evidencemi, rejstříky nebo seznamy.

(3) Ověřeným výstupem z informačního systému veřejné správy (dále jen "ověřený výstup") se rozumí listina, která vznikla úplným převodem výstupu z informačního systému veřejné správy z elektronické do listinné podoby(§ 9a).

(4) Výpis v listinné podobě a ověřený výstup podle odstavce 3 jsou veřejnými listinami.

§ 9a

(1) Ověřením výstupu z informačního systému veřejné správy se rozumí ověření té skutečnosti, že listina vznikla převedením výstupu z informačního systému veřejné správy z elektronické do listinné podoby. Ověření se provede ověřovací doložkou, která obsahuje

a) údaj o ověření toho, že ověřený výstup odpovídá výstupu z informačního systému veřejné správy,

b) údaj o tom, z kolika listů se skládá ověřený výstup,

c) údaj o tom, že ověřený výstup obsahuje částečný výpis z informačního systému veřejné správy, pokud neobsahuje výstup úplný,

d) místo a datum vyhotovení doložky o ověření,

e) pořadové číslo, pod kterým je ověření vedeno v evidenci ověření výstupu z informačního systému veřejné správy,

f) otisk úředního razítka a podpis ověřujícího.

(2) Ověřovací doložku vyhotoví ověřující na listině, která vznikla převedením výstupu z informačního systému veřejné správy z elektronické do listinné podoby, nebo ověřovací doložku vyhotoví zvlášť a s touto listinou ji pevně spojí. Listina, která vznikla převedením výstupu z informačního systému veřejné správy z elektronické do listinné podoby, a na ní vyhotovená nebo s ní pevně spojená ověřovací doložka, se považují za jednu listinu.

§ 9b

Povinnosti ověřujícího

(1) Ti, kteří vydávají ověřené výstupy (dále jen "ověřující"), jsou povinni při ověřování výstupu z informačního systému veřejné správy používat pouze takové technické zařízení, které výstup z informačního systému veřejné správy, který má být ověřen, zobrazí do formy, v níž je jeho obsah pro fyzickou osobu čitelný tak, aby jeho interpretace odpovídala zápisu v informačním systému veřejné správy.

(2) Ověřující je povinen provést veškeré úkony potřebné k tomu, aby ověřil tu skutečnost, že výstup z informačního systému veřejné správy je označen elektronickou značkou[11b]) správce, že tato elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn a výstup z informačního systému veřejné správy nebyl následně změněn.

(3) Při vydávání ověřených výstupů na základě výpisů podle § 9 odst. 1 věty druhé je ověřující povinen prověřit oprávnění žadatele a zjistit jeho totožnost. Jde-li o právnickou osobu, zjišťuje její existenci a totožnost osob jednajících jejím jménem.

(4) Ověřující je povinen vést evidenci vydaných ověřených výstupů. Evidence obsahuje alespoň tyto údaje:

a) pořadové číslo, pod kterým je ověření vedeno v evidenci ověření výstupu z informačního systému veřejné správy,

b) datum vyhotovení doložky o ověření,

c) je-li žadatelem fyzická osoba jméno, příjmení, adresu místa trvalého pobytu, nemá-li trvalý pobyt, adresu bydliště, rodné číslo, nemá-li rodné číslo, datum narození osoby, jejíž totožnost byla pro účely vydání ověřeného výstupu ověřena, včetně druhu a čísla průkazu, jímž byla totožnost zjištěna, je-li ověření totožnosti předepsáno; je-li žadatelem právnická osoba, její obchodní firmu nebo název, adresu sídla, identifikační číslo, je-li přiděleno, a jméno, příjmení, rodné číslo, nemá-li rodné číslo, datum narození, a adresu místa trvalého pobytu,nemá-li trvalý pobyt, adresu bydliště osoby nebo osob, jednajících jménem této právnické osoby, nebo osoby jednající za právnickou osobu jejím jménem na základě zastoupení,

d) číslo kvalifikovaného systémového certifikátu, na němž je založena elektronická značka, kterou je výstup z informačního systému veřejné správy označen, unikátní u daného akreditovaného poskytovatele certifikačních služeb, a obchodní firmu akreditovaného poskytovatele certifikačních služeb, který tento kvalifikovaný systémový certifikát vydal.

§ 9c

Povinnosti orgánů veřejné správy, které jsou správci nebo provozovateli informačních systémů veřejné správy

(1) Správci jsou povinni předat ověřující osobě na požádání bezodkladně výstup z informačního systému veřejné správy a opatřený datem a časem s uvedením hodiny, minuty a sekundy, kdy byl výstup vytvořen, a datem a časem s uvedením hodiny, minuty a sekundy okamžiku, ke kterému správce odpovídá za soulad výstupu se stavem zápisu v informačním systému veřejné správy (dále jen "okamžik platnosti údajů"), a označený elektronickou značkou[11b]).

(2) Správci odpovídají za soulad výpisu, který vydávají podle § 9, nebo výstupu z informačního systému veřejné správy se stavem zápisu v informačním systému veřejné správy k okamžiku platnosti údajů.

(3) Správci jsou povinni uvědomit neprodleně ověřující osoby o tom, že hrozí nebezpečí zneužití dat pro vytváření elektronické značky[11b]) správce.

(4) Správci informačních systémů veřejné správy, které jsou neveřejnými evidencemi, rejstříky nebo seznamy, jsou povinni předat ověřující osobě výstup z informačního systému veřejné správy tak, aby byl tento výstup z informačního systému veřejné správy v průběhu předání odpovídajícím způsobem skryt před třetími osobami.

§ 9d

Zpoplatnění ověřování výstupu z informačního systému veřejné správy

(1) Správce je oprávněn požadovat za poskytnutí výstupu z informačního systému veřejné správy ověřujícímu úplatu, a to za každý poskytnutý výstup z informačního systému veřejné správy částku, která je stanovena zvláštním právním předpisem jako poplatek za vydání výpisu z předmětného záznamu, jenž má jednu stránku [16]).

(2) Správní poplatek za vydání ověřeného výstupu vydaného ověřujícím podle § 8a odst. 2 písm. b) až e) stanoví zvláštní právní předpis[16]).

(3) Odměnu notáře za vydávání ověřených výstupů stanoví zvláštní právní předpis[17]).

§ 10

Přechodná ustanovení

(1) Informační systémy, které orgány veřejné správy ke dni účinnosti tohoto zákona již spravují, provozují nebo budují, musí orgány veřejné správy nejpozději do 2 let ode dne účinnosti tohoto zákona uvést do souladu s tímto zákonem nebo ukončit jejich činnost.

(2) V případě informačních systémů veřejné správy, jejichž správci jsou orgány územní samosprávy, které nevykonávají státní správu v přenesené působnosti, se na tyto správce povinnosti uvedené v § 5 odst. 2 písm. c), f), g) a h) vztahují po uplynutí doby 2 let ode dne nabytí účinnosti těchto ustanovení zákona.

§ 11

Zrušení Úřadu pro státní informační systém

(1) Úřad pro státní informační systém se zrušuje.

(2) Dosavadní působnost Úřadu pro státní informační systém stanovená zvláštními zákony[13]) přechází na Úřad.

(3) Práva a povinnosti z pracovněprávních a jiných právních vztahů přecházejí z Úřadu pro státní informační systém na Úřad.

Zmocňovací ustanovení

§ 12

(1) Ministerstvo stanoví vyhláškou

a) Technické a funkční náležitosti uskutečňování vazeb mezi informačními systémy veřejné správy prostřednictvím referenčního rozhraní podle § 4 odst. 1 písm. g),

b) formu a technické náležitosti předávání údajů do informačního systému podle § 4 odst. 1 písm. h) a i),

c) postupy ministerstva a orgánů veřejné správy při vedení, zápisu a vyhlašování datových prvků v informačním systému o datových prvcích podle § 4 odst. 2 písm. d),

---

[16] Zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů.

[17] Vyhláška č. 196/2001 Sb., o odměnách a náhradách notářů a správců dědictví, ve znění vyhlášky č. 42/2002 Sb.

[13] § 64d zákona č. 199/1994 Sb., o zadávání veřejných zakázek, ve znění zákona č. 28/2000 Sb. § 62 zákona č. 26/2000 Sb., o veřejných dražbách.

d) formu uveřejňování informací, která zajistí, aby se s informacemi souvisejícími s výkonem veřejné správy uveřejňovanými způsobem umožňujícím dálkový přístup mohly v nezbytném rozsahu seznámit i osoby se zdravotním postižením podle § 5 odst. 2 písm. f),

e) požadavky na strukturu a obsah informační koncepce, postupy orgánů veřejné správy při jejím vytváření, vydávání, při vyhodnocování jejího dodržování a požadavky na řízení bezpečnosti a kvality informačních systémů veřejné správy podle § 5a odst. 1,

f) požadavky na strukturu a obsah provozní dokumentace podle § 5a odst. 2 a na rozsah provozní dokumentace předkládané při atestaci podle § 5a odst. 3,

g) postupy atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy podle § 6d odst. 1 písm. b),

h) postupy atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní podle § 6d odst. 1 písm. b),

i) seznam obecních úřadů, úřadů městských částí nebo městských obvodů územně členěných statutárních měst a úřadů městských částí hlavního města Prahy podle § 8a odst. 2 písm. d).

(2) Ministerstvo v dohodě s Ministerstvem zahraničních věcí vydá vyhlášku k provedení § 8a odst. 2 písm. e).

§ 12a

zrušen

ČÁST DRUHÁ

Změna zákona o správních poplatcích

§ 12

1. V sazebníku správních poplatků uvedeném v příloze k zákonu č.368/1992 Sb., o správních poplatcích, ve znění zákona č. 10/1993 Sb., zákona č. 85/1994 Sb., zákona č. 273/1994 Sb., zákona č. 36/1995 Sb., zákona č. 301/1995 Sb., zákona č. 305/1997 Sb., zákona č. 149/1998 Sb., zákona č. 157/1998 Sb., zákona č. 167/1998 Sb., zákona č. 63/1999 Sb., zákona č. 166/1999 Sb., zákona č. 167/1999 Sb., zákona č. 326/1999 Sb., zákona č. 352/1999 Sb., zákona č. 357/1999 Sb., zákona č. 360/1999 Sb., zákona č. 363/1999 Sb., zákona č. 62/2000 Sb., zákona č. 117/2000 Sb., zákona č. 133/2000 Sb., zákona č. 151/2000 Sb., zákona č. 153/2000 Sb., zákona č. 154/2000 Sb., zákona č. 156/2000 Sb., zákona č. 158/2000 Sb., zákona č. 227/2000 Sb., zákona č. 241/2000 Sb., zákona č. 242/2000 Sb. a zákona č. 307/2000 Sb., se doplňuje část XIV, která zní:

ČÁST XIV

Řízení podle zákona o informačních systémech veřejné správy a o změně některých dalších zákonů Položka 164

Podání žádosti o udělení statutu atestačního střediskaKč100 000".

2. REJSTŘÍK K SAZEBNÍKU se doplňuje o část XIV, která zní:

ČÁST XIV

Řízení podle zákona o informačních systémech veřejné správy a o změně některých dalších zákonů 164".

3. Tečka za částí XIII se zrušuje.

ČÁST TŘETÍ

Změna zákona o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky

§ 13

V § 2 odst. 1 bodu 6 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění zákona č. 272/1996 Sb., se slova "Úřad pro státní informační systém" nahrazují slovy "Úřad pro veřejné informační systémy".

ČÁST ČTVRTÁ

ÚČINNOST

§ 14

Tento zákon nabývá účinnosti dnem vyhlášení, s výjimkou ustanovení

a) § 5 odst. 2 písm. c), které nabývá účinnosti dnem 1. července 2001;

b) § 5 odst. 2 písm. f), které nabývá účinnosti dnem 1. ledna 2001;

c) § 5 odst. 2 písm. g), které nabývá účinnosti dnem 1. ledna 2002;

d) § 5 odst. 2 písm. h), které nabývá účinnosti dnem 1. ledna 2001 a pro zveřejňování informací dálkovým přístupem nabývá účinnosti dnem 1. ledna 2002;

e) § 6, které nabývá účinnosti dnem 1. července 2001.

Klaus v. r.

Havel v. r.

Zeman v. r.

PŘÍLOHA H – ZÁKON Č. 227/2000 SB.

227/2000 Sb.

ZÁKON

ze dne 29. června 2000

o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)

Změna: 226/2002 Sb.

Změna: 517/2002 Sb.

Změna: 440/2004 Sb.

Změna: 635/2004 Sb.

Změna: 501/2004 Sb., 444/2005 Sb.

Změna: 110/2007 Sb.

Změna: 124/2008 Sb.

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

ELEKTRONICKÝ PODPIS

§ 1

Účel zákona

Tento zákon upravuje v souladu s právem Evropských společenství[1]) používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

§ 2

Vymezení některých pojmů

Pro účely tohoto zákona se rozumí

a) elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě,

b) zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky

   1. je jednoznačně spojen s podepisující osobou,

   2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

   3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

   4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,

c) elektronickou značkou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky

   1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,

   2. byly vytvořeny a připojeny k datové zprávě pomocí prostředků pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,

   3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat,

d) datovou zprávou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou,

e) podepisující osobou fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby,

f) označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou,

g) držitelem certifikátu fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu pro sebe nebo pro podepisující nebo označující osobu a které byl certifikát vydán,

h) poskytovatelem certifikačních služeb fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy,

i) kvalifikovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systé-

[1] Směrnice Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy.

mové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen "kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,

j) akreditovaným poskytovatelem certifikačních služeb poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,

k) certifikátem datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,

l) kvalifikovaným certifikátem certifikát, který má náležitosti podle §12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

m) kvalifikovaným systémovým certifikátem certifikát, který má náležitosti podle § 12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

n) daty pro vytváření elektronických podpisů jedinečná data, která podepisující osoba používá k vytváření elektronického podpisu,

o) daty pro ověřování elektronických podpisů jedinečná data, která se používají pro ověření elektronického podpisu,

p) daty pro vytváření elektronických značek jedinečná data, která označující osoba používá k vytváření elektronických značek,

q) daty pro ověřování elektronických značek jedinečná data, která se používají pro ověření elektronických značek,

r) kvalifikovaným časovým razítkem datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem,

s) prostředkem pro vytváření elektronických podpisů technické zařízení nebo programové vybavení, které se používá k vytváření elektronických podpisů,

t) prostředkem pro ověřování elektronických podpisů technické zařízení nebo programové vybavení, které se používá k ověřování elektronických podpisů,

u) prostředkem pro bezpečné vytváření elektronických podpisů prostředek pro vytváření elektronického podpisu, který splňuje požadavky stanovené tímto zákonem,

v) prostředkem pro bezpečné ověřování elektronických podpisů prostředek pro ověřování podpisu, který splňuje požadavky stanovené tímto zákonem,

w) nástrojem elektronického podpisu technické zařízení nebo programové vybavení, nebo jejich součásti, používané pro zajištění certifikačních služeb nebo pro vytváření nebo ověřování elektronických podpisů,

x) prostředkem pro vytváření elektronických značek zařízení, které používá označující osoba pro vytváření elektronických značek a které splňuje další náležitosti stanovené tímto zákonem,

y) elektronickou podatelnou pracoviště orgánu veřejné moci určené pro příjem a odesílání datových zpráv,

z) akreditací osvědčení, že poskytovatel certifikačních služeb splňuje podmínky stanovené tímto zákonem pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

§ 3

Soulad s požadavky na podpis

(1) Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.

(2) Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.

§ 3a

(1) Použití elektronické značky založené na kvalifikovaném systémovém certifikátu a vytvořené pomocí prostředku pro vytváření elektronických značek umožňuje ověřit, že datovou zprávu označila touto elektronickou značkou označující osoba.

(2) Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli.

§ 4

Soulad s originálem

Použití zaručeného elektronického podpisu nebo elektronické značky zaručuje, že dojde-li k porušení obsahu datové zprávy od okamžiku, kdy byla podepsána nebo označena, toto porušení bude možno zjistit.

§ 5

Povinnosti podepisující osoby

(1) Podepisující osoba je povinna

a) zacházet s prostředky, jakož i s daty pro vytváření zaručeného elektronického podpisu s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření zaručeného elektronického podpisu.

(2) Za škodu způsobenou porušením povinností podle odstavce 1 odpovídá podepisující osoba podle

zvláštních právních předpisů.[1a]) Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že zaručený elektronický podpis je platný a jeho kvalifikovaný certifikát nebyl zneplatněn.

§ 5a

Povinnosti označující osoby

(1) Označující osoba je povinna

a) zacházet s prostředkem, jakož i s daty pro vytváření elektronických značek s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití,

b) uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný systémový certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření elektronických značek.

(2) Označující osoba je povinna zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené tímto zákonem.

(3) Za škodu způsobenou porušením povinnosti podle odstavce 1 odpovídá označující osoba, i když škodu nezavinila, podle zvláštních právních předpisů,[1a]) odpovědnost za vady podle zvláštních předpisů tím není dotčena.[1a]) Odpovědnosti se však zprostí, pokud prokáže, že ten, komu vznikla škoda, neprovedl veškeré úkony potřebné k tomu, aby si ověřil, že elektronická značka je platná a její kvalifikovaný systémový certifikát nebyl zneplatněn.

§ 5b

Povinnosti držitele certifikátu

Držitel certifikátu je povinen bez zbytečného odkladu podávat přesné, pravdivé a úplné informace poskytovateli certifikačních služeb ve vztahu ke kvalifikovanému certifikátu a ve vztahu ke kvalifikovanému systémovému certifikátu.

§ 6

Kvalifikovaný poskytovatel certifikačních služeb

(1) Kvalifikovaný poskytovatel certifikačních služeb je povinen

a) zajistit, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu, na jehož základě označuje vydané kvalifikované certifikáty nebo kvalifikované systémové certifikáty a seznamy certifikátů, které byly zneplatněny, nebo kvalifikovaná časová razítka,

b) zajistit, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnou pro poskytování kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) používat bezpečné systémy a bezpečné nástroje elektronického podpisu, zajistit dostatečnou bezpečnost postupů, které tyto systémy a nástroje podporují, a zajistit dostatečnou kryptografickou bezpečnost těchto nástrojů; systémy a nástroje jsou považovány za bezpečné, pokud odpovídají požadavkům stanoveným tímto zákonem a prováděcí vyhláškou, nebo pokud splňují požadavky technických norem uvedených v rozhodnutí Komise vydaném na základě článku 3 (5) směrnice 99/93/ES,

d) používat bezpečné systémy pro uchovávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů nebo kvalifikovaných časových razítek v ověřitelné podobě takovým způsobem, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny porušující tyto bezpečnostní požadavky byly zjevné,

e) mít po celou dobu své činnosti k dispozici dostatečné finanční zdroje nebo jiné finanční zajištění na provoz v souladu s požadavky uvedenými v tomto zákoně a s ohledem na riziko vzniku odpovědnosti za škodu,

f) před uzavřením smlouvy o poskytování kvalifikovaných certifikačních služeb s osobou, která žádá o poskytování služeb podle tohoto zákona, informovat tuto osobu písemně o přesných podmínkách pro využívání kvalifikovaných certifikačních služeb, včetně případných omezení pro jejich použití, o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je, či není akreditován Ministerstvem vnitra (dále jen "ministerstvo") podle § 10; tyto informace lze předat elektronicky.

(2) Není-li poskytovatel certifikačních služeb akreditován ministerstvem, je povinen ohlásit ministerstvu nejméně 30 dnů před zahájením poskytování kvalifikované certifikační služby, že ji bude poskytovat, a okamžik, kdy její poskytování zahájí. Zároveň předá ministerstvu k ověření svůj kvalifikovaný systémový certifikát uvedený v odstavci 1 písm. a).

(3) Pokud byla kvalifikovanému poskytovateli certifikačních služeb, který získal akreditaci podle § 10 tohoto zákona, akreditace ministerstvem odňata, je povinen bez prodlení informovat o této skutečnosti subjekty, kterým poskytuje své kvalifikované certifikační služby, a další dotčené osoby.

(4) Kvalifikovaný poskytovatel certifikačních služeb poskytuje služby podle tohoto zákona na základě smlouvy. Smlouva musí být písemná.

(5) Kvalifikovaný poskytovatel certifikačních služeb uchovává informace a dokumentaci související s poskytovanými kvalifikovanými certifikačními službami podle tohoto zákona, zejména

a) smlouvu o poskytování kvalifikované certifikační služby, včetně žádosti o poskytování služby,

[1a] Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

b) vydaný kvalifikovaný certifikát, vydaný kvalifikovaný systémový certifikát nebo vydané kvalifikované časové razítko,

c) kopie předložených osobních dokladů podepisující osoby nebo dokladů, na jejichž základě byla ověřena identita označující osoby,

d) potvrzení o převzetí kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu držitelem, případně jeho souhlas se zveřejněním kvalifikovaného certifikátu v seznamu vydaných kvalifikovaných certifikátů,

e) prohlášení držitele certifikátu o tom, že mu byly poskytnuty informace podle odstavce 1 písm. f),

f) dokumenty a záznamy související s životním cyklem vydaného kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu, jejichž náležitosti upřesní prováděcí vyhláška.

(6) Veškeré informace a dokumentaci o poskytovaných službách podle tohoto zákona uchovává kvalifikovaný poskytovatel certifikačních služeb po dobu nejméně 10 let. Kvalifikovaný poskytovatel je povinen zajistit uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením za podmínek, které upřesní prováděcí vyhláška. Informace a dokumentaci podle věty první může kvalifikovaný poskytovatel certifikačních služeb pořizovat a uchovávat v elektronické podobě. Pokud tento zákon nestanoví jinak, postupuje se při nakládání s informacemi a dokumentací podle zvláštního právního předpisu.[2])

(7) Zaměstnanci kvalifikovaného poskytovatele certifikačních služeb, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji a daty pro vytváření elektronických podpisů podepisujících osob a elektronických značek označujících osob, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací; uvedené osoby může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

§ 6a

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných certifikátů a kvalifikovaných systémových certifikátů

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty (dále jen "certifikáty vydané jako kvalifikované"), je povinen

a) zajistit, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby údaje uvedené v certifikátech jím vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) před vydáním certifikátu jako kvalifikovaného bezpečně ověřit odpovídajícími prostředky identitu podepisující osoby nebo identitu označující osoby, případně i její zvláštní znaky, vyžaduje-li to účel takového certifikátu,

d) zjistit, zda v okamžiku podání žádosti o vydání certifikátu jako kvalifikovaného měla podepisující osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo označující osoba data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek, která obsahuje žádost o vydání certifikátu,

e) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, k jejichž zveřejnění dal držitel certifikátu souhlas v souladu s § 6 odst. 5 písm. d), a zajistit dostupnost tohoto seznamu i dálkovým přístupem a údaje v seznamu obsažené při každé změně bez zbytečného odkladu aktualizovat,

f) zajistit provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) zajistit, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) přijmout odpovídající opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované,

i) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání certifikátů vydaných jako kvalifikované, včetně omezení pro jejich použití, a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Pokud kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty jako kvalifikované, vytváří pro podepisující osobu data pro vytváření elektronických podpisů nebo pro označující osobu data pro vytváření elektronických značek,

a) musí zajistit utajení těchto dat před jejich předáním, nesmí tato data kopírovat a uchovávat je déle, než je nezbytné,

b) musí zaručit, že tato data odpovídají datům pro ověřování elektronických podpisů nebo datům pro ověřování elektronických značek.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává certifikáty jako kvalifikované, musí neprodleně zneplatnit certifikát, pokud o to držitel, podepisující osoba nebo označující osoba požádá, nebo pokud ho uvědomí, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů nebo elektro-

[2] Zákon č. 97/1974 Sb., o archivnictví, ve znění pozdějších předpisů.

nických značek, nebo v případě, že byl certifikát vydán na základě nepravdivých nebo chybných údajů.

(4) Kvalifikovaný poskytovatel certifikačních služeb musí rovněž neprodleně zneplatnit certifikát vydaný jako kvalifikovaný, dozví-li se prokazatelně, že podepisující nebo označující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil,[2a]) nebo pokud údaje, na jejichž základě byl certifikát vydán, pozbyly pravdivosti.

§ 6b

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při vydávání kvalifikovaných časových razítek

(1) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, je povinen

a) zajistit, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené tímto zákonem,

b) zajistit, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) zajistit, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, jednoznačně odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) přijmout odpovídající opatření proti padělání kvalifikovaných časových razítek,

e) poskytovat na vyžádání třetím osobám podstatné informace o podmínkách pro využívání kvalifikovaných časových razítek, včetně omezení pro jejich použití a informace o tom, zda je, či není akreditován ministerstvem; tyto informace lze poskytovat elektronicky.

(2) Kvalifikovaný poskytovatel certifikačních služeb vydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

§ 7

Odpovědnost za škodu

(1) Za škodu způsobenou porušením povinností stanovených tímto zákonem odpovídá kvalifikovaný poskytovatel certifikačních služeb podle zvláštních právních předpisů.[1a])

(2) Kvalifikovaný poskytovatel certifikačních služeb neodpovídá za škodu vyplývající z použití certifikátu vydaného jako kvalifikovaný, která vznikla v důsledku nedodržení omezení pro jeho použití podle § 12 odst. 1 písm. i) a j) a § 12a písm. h).

§ 8

Ochrana osobních údajů

Ochrana osobních údajů se řídí zvláštním právním předpisem.[3])

§ 9

Akreditace a dozor

(1) Udělování akreditací k působení jako akreditovaný poskytovatel certifikačních služeb, jakož i dozor nad dodržováním tohoto zákona náleží ministerstvu.

(2) Ministerstvo

a) uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb subjektům působícím na území České republiky,

b) vykonává dozor nad činností akreditovaných poskytovatelů certifikačních služeb a kvalifikovaných poskytovatelů certifikačních služeb, ukládá jim opatření k nápravě a pokuty za porušení povinností podle tohoto zákona,

c) vede evidenci udělených akreditací a jejich změn a evidenci kvalifikovaných poskytovatelů certifikačních služeb,

d) vede evidenci vydaných kvalifikovaných systémových certifikátů, které používá kvalifikovaný poskytovatel certifikačních služeb podle § 6 odst. 1 písm. a) a které byly podle § 6 odst. 2 ověřeny ministerstvem,

e) průběžně uveřejňuje přehled udělených akreditací, přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb a kvalifikované systémové certifikáty podle písmena d), a to i způsobem umožňujícím dálkový přístup,

f) vyhodnocuje shodu nástrojů elektronického podpisu s požadavky stanovenými tímto zákonem a prováděcí vyhláškou,

g) plní další povinnosti stanovené tímto zákonem.

(3) Za účelem výkonu dozoru je akreditovaný poskytovatel certifikačních služeb a kvalifikovaný poskytovatel certifikačních služeb povinen pověřeným zaměstnancům ministerstva umožnit v nezbytně nutném rozsahu vstup do obchodních a provozních prostor, na požádání předložit veškerou dokumentaci, záznamy, doklady, písemnosti a jiné podklady související s jeho činností, umožnit jim v nezbytně nutné míře přístup do svého informačního systému a poskytnout informace a veškerou potřebnou součinnost.

(4) Není-li tímto zákonem stanoveno jinak, postupuje ministerstvo při výkonu dozoru podle zvláštního právního předpisu.[4])

[2a] § 10 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

[3] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[4] Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

(5) Kvalifikovanému poskytovateli certifikačních služeb, který nesplnil povinnost součinnosti podle odstavce 3, lze uložit pořádkovou pokutu do výše 1 000 000 Kč.

§ 10

Podmínky udělení akreditace pro poskytování certifikačních služeb

(1) Každý poskytovatel certifikačních služeb může požádat ministerstvo o udělení akreditace pro výkon činnosti akreditovaného poskytovatele certifikačních služeb.

(2) V žádosti o akreditaci podle odstavce 1 musí žadatel doložit

a) v případě právnické osoby obchodní firmu nebo název, sídlo, popřípadě adresu organizační složky zahraniční osoby na území České republiky, a identifikační číslo žadatele, bylo-li přiděleno; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, místo usazení, místo podnikání, pokud je odlišné od místa usazení, a identifikační číslo žadatele, bylo-li přiděleno,

b) doklad o oprávnění k podnikatelské činnosti a u osoby zapsané do obchodního rejstříku také výpis z obchodního rejstříku ne starší než 3 měsíce,

c) věcné, personální a organizační předpoklady pro činnost kvalifikovaného poskytovatele certifikačních služeb podle § 6, 6a a 6b tohoto zákona,

d) údaj o tom, které kvalifikované certifikační služby hodlá žadatel poskytovat.

(3) Jestliže žádost neobsahuje všechny požadované údaje, ministerstvo řízení přeruší a vyzve žadatele, aby ji ve stanovené lhůtě doplnil. Jestliže tak žadatel v této lhůtě neučiní, ministerstvo řízení zastaví.

(4) Splňuje-li žadatel všechny podmínky předepsané tímto zákonem pro udělení akreditace, vydá ministerstvo rozhodnutí, jímž mu akreditaci udělí. V opačném případě žádost o udělení akreditace zamítne.

§ 10a

Podmínky pro rozšíření služeb akreditovaného poskytovatele certifikačních služeb

(1) Akreditovaný poskytovatel certifikačních služeb může rozšířit poskytování kvalifikovaných certifikačních služeb o vydávání kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek nebo o vydávání prostředků pro bezpečné vytváření elektronických podpisů podle tohoto zákona (dále jen "rozšiřované služby").

(2) Akreditovaný poskytovatel certifikačních služeb je povinen rozšíření podle odstavce 1 oznámit ministerstvu tak, aby ministerstvo oznámení obdrželo alespoň 4 měsíce před zahájením poskytování služby.

(3) V oznámení musí akreditovaný poskytovatel certifikačních služeb doložit věcné, personální a organizační předpoklady pro zajištění rozšiřovaných služeb.

(4) Nedoloží-li akreditovaný poskytovatel certifikačních služeb skutečnosti podle odstavce 3, anebo jsou-li tyto skutečnosti neúplné nebo nepřesné, ministerstvo na to akreditovaného poskytovatele certifikačních služeb upozorní s tím, že nebudou-li tyto vady ve lhůtě, kterou k tomu určí, odstraněny, rozhodnutím rozšiřování služeb zakáže.

(5) Ministerstvo oznámené rozšíření zakáže, pokud akreditovaný poskytovatel certifikačních služeb nesplnil všechny podmínky předepsané tímto zákonem pro poskytování rozšiřovaných služeb.

(6) O zákazu rozšíření poskytování kvalifikovaných certifikačních služeb vydá ministerstvo rozhodnutí nejpozději do 90 dnů od okamžiku, kdy obdrželo oznámení.

§ 11

(1) V oblasti orgánů veřejné moci je možné za účelem podpisu používat pouze zaručené elektronické podpisy a kvalifikované certifikáty vydávané akreditovanými poskytovateli certifikačních služeb (dále jen "uznávaný elektronický podpis"). To platí i pro výkon veřejné moci vůči fyzickým a právnickým osobám. Pokud je uznávaný elektronický podpis užíván v oblasti orgánů veřejné moci, musí kvalifikovaný certifikát obsahovat takové údaje, aby osoba byla jednoznačně identifikovatelná. Strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, stanoví ministerstvo prováděcím právním předpisem.

(2) Písemnosti orgánů veřejné moci v elektronické podobě označené elektronickou značkou založenou na kvalifikovaném systémovém certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb nebo podepsané uznávaným elektronickým podpisem mají stejné právní účinky jako veřejné listiny vydané těmito orgány.

(3) Orgán veřejné moci přijímá a odesílá datové zprávy podle odstavce 1 prostřednictvím elektronické podatelny.

§ 12

Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jméno, popřípadě jména, a příjmení podepisující osoby nebo její pseudonym s příslušným označením, že se jedná o pseudonym,

d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,

e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,

f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,

h) počátek a konec platnosti kvalifikovaného certifikátu,

i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,

j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám.

(3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

§ 12a

Náležitosti kvalifikovaného systémového certifikátu

Kvalifikovaný systémový certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,

b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek,

d) data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,

e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,

f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

g) počátek a konec platnosti kvalifikovaného systémového certifikátu,

h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.

§ 12b

Náležitosti kvalifikovaného časového razítka

Kvalifikované časové razítko musí obsahovat

a) číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,

b) označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,

c) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,

d) hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,

e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,

f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

§ 13

Povinnosti kvalifikovaného poskytovatele certifikačních služeb při ukončení činnosti

(1) Kvalifikovaný poskytovatel certifikačních služeb musí záměr ukončit svou činnost ohlásit ministerstvu nejméně 3 měsíce před plánovaným datem ukončení činnosti a musí vynaložit veškeré možné úsilí k tomu, aby evidence vedená podle § 6 odst. 5 byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb. Kvalifikovaný poskytovatel certifikačních služeb dále musí prokazatelně informovat každou podepisující osobu, označující osobu a držitele, kterým poskytuje své certifikační služby, o svém záměru ukončit svoji činnost nejméně 2 měsíce před plánovaným datem ukončení činnosti.

(2) Nemůže-li kvalifikovaný poskytovatel certifikačních služeb zajistit, aby evidenci vedenou podle § 6 odst. 5 převzal jiný kvalifikovaný poskytovatel certifikačních služeb, je povinen to nejpozději 30 dnů před plánovaným datem ukončení činnosti ministerstvu ohlásit. V takovém případě ministerstvo převezme evidenci a oznámí to dotčeným subjektům.

(3) Ustanovení odstavců 1 a 2 se použijí přiměřeně také v případě, když kvalifikovaný poskytovatel certifikačních služeb zanikne, zemře nebo přestane vykonávat svoji činnost, aniž splní ohlašovací povinnost podle odstavce 1.

§ 14

Opatření k nápravě

(1) Zjistí-li ministerstvo, že akreditovaný poskytovatel certifikačních služeb nebo kvalifikovaný poskyto-

vatel certifikačních služeb porušuje povinnosti stanovené tímto zákonem, uloží mu, aby ve stanovené lhůtě zjednal nápravu, a případně určí, jaká opatření k odstranění nedostatků je tento poskytovatel certifikačních služeb povinen přijmout.

(2) V případě, že se akreditovaný poskytovatel certifikačních služeb dopustí závažnějšího porušení povinností stanovených tímto zákonem nebo ve stanovené lhůtě neodstraní nedostatky zjištěné ministerstvem, je ministerstvo oprávněno mu udělenou akreditaci odejmout.

(3) Rozhodne-li ministerstvo o odnětí akreditace, může současně rozhodnout o zneplatnění certifikátů vydaných jako kvalifikované poskytovatelem certifikačních služeb v době platnosti akreditace.

§ 15

Zrušení kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu

Ministerstvo může nařídit kvalifikovanému poskytovateli certifikačních služeb jako předběžné opatření[7]) zneplatnění certifikátu vydaného jako kvalifikovaný, pokud existuje důvodné podezření, že certifikát byl padělán, nebo pokud byl vydán na základě nepravdivých údajů. Rozhodnutí o zneplatnění certifikátu vydaného jako kvalifikovaný může být vydáno také v případě, kdy bylo zjištěno, že podepisující nebo označující osoba používá prostředek pro vytváření podpisu nebo prostředek pro vytváření elektronických značek, který vykazuje bezpečnostní nedostatky, které by umožnily padělání zaručených elektronických podpisů nebo elektronických značek nebo změnu podepisovaných nebo označovaných údajů.

§ 16

Uznávání zahraničních kvalifikovaných certifikátů

(1) Certifikát, který je vydán poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie jako kvalifikovaný, je kvalifikovaným certifikátem ve smyslu tohoto zákona.

(2) Certifikát, který je vydán jako kvalifikovaný ve smyslu tohoto zákona v jiném než členském státu Evropské unie, je kvalifikovaným certifikátem ve smyslu tohoto zákona, pokud

a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství[1]) a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie,

b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, který splňuje podmínky práva Evropských společenství,[1]) převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů,

c) to vyplývá z mezinárodní smlouvy.

§ 17

Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

(1) Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že

a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,

b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,

c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

(2) Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.

(3) Prostředky pro bezpečné vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána.

(4) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby

a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,

b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,

d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,

e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,

f) bylo jasně uvedeno použití pseudonymu,

g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§ 17a

Prostředky pro vytváření elektronických značek

(1) Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že

a) data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,

[7]) § 43 zákona č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů.

b) označující osoba je informována, že zahajuje používání tohoto prostředku.

(2) Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.

(3) Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

§ 18

Správní delikty právnických osob

(1) Kvalifikovanému poskytovateli certifikačních služeb, který

a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a d), ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6, se uloží pokuta do výše 10 000 000 Kč.

(2) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty a který

a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4, se uloží pokuta do výše 10 000 000 Kč.

(3) Kvalifikovanému poskytovateli certifikačních služeb, který vydává kvalifikovaná časová razítka a který

a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání,se uloží pokuta do výše 10 000 000 Kč.

(4) Kvalifikovanému poskytovateli certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů a který

a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3,se uloží pokuta do výše 10 000 000 Kč.

(5) Akreditovanému poskytovateli certifikačních služeb, který nesplní oznamovací povinnost podle § 10a odst. 2, se uloží pokuta do výše 10 000 000 Kč.

(6) Akreditovanému poskytovateli certifikačních služeb, který poruší zákaz vydaný ministerstvem podle § 10a odst. 5, se uloží pokuta do výše 10 000 000 Kč.

§ 18a

Přestupky

(1) Kvalifikovaný poskytovatel certifikačních služeb se dopustí přestupku tím, že

a) nezajistí, aby se každý mohl ujistit o jeho identitě a jeho kvalifikovaném systémovém certifikátu podle § 6 odst. 1 písm. a),

b) nezajistí, aby poskytování kvalifikovaných certifikačních služeb vykonávaly osoby s odbornými znalostmi a kvalifikací nezbytnými pro poskytované kvalifikované certifikační služby a obeznámené s příslušnými bezpečnostními postupy,

c) nezajištěním dostatečné bezpečnosti používaných systémů a nástrojů elektronického podpisu a postupů, které tyto systémy a nástroje podporují podle § 6 odst. 1 písm. c) a písm. d), ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

d) nedisponuje dostatečnými finančními zdroji nebo jiným finančním zajištěním na provoz podle § 6 odst. 1 písm. e), a tím ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6 odst. 1 písm. f), § 6 odst. 3 nebo § 13 odst. 1,

f) nesplní ohlašovací povinnost podle § 6 odst. 2, včetně předání kvalifikovaného systémového certifikátu k ověření nebo podle § 13 odst. 1 nebo 2,

g) poskytne certifikační služby na základě jiné než písemné smlouvy,

h) neuchovává informace a dokumentaci podle § 6 odst. 5,

i) neuchovává veškeré informace a dokumentaci podle § 6 odst. 6 po dobu nejméně 10 let, nebo

j) nezajistí uchovávané informace a dokumentaci před ztrátou, zneužitím, zničením nebo poškozením podle § 6 odst. 6.

(2) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty, se dopustí přestupku tím, že

a) nezajistí, aby certifikáty jím vydané jako kvalifikované obsahovaly všechny náležitosti stanovené tímto zákonem,

b) nezajistí, aby údaje uvedené v certifikátech vydaných jako kvalifikované byly přesné, pravdivé a úplné,

c) neověří identitu osoby podle § 6a odst. 1 písm. c),

d) nezajistí soulad dat podle § 6a odst. 1 písm. d),

e) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované a nezajistí jeho dostupnost a aktualizaci podle § 6a odst. 1 písm. e),

f) nezajistí provozování bezpečného a veřejně přístupného seznamu certifikátů vydaných jako kvalifikované, které byly zneplatněny, a to i dálkovým přístupem,

g) nezajistí, aby datum a čas s uvedením hodiny, minuty a sekundy, kdy je certifikát vydaný jako kvalifikovaný vydán nebo zneplatněn, mohly být přesně určeny,

h) nepřijetím odpovídajících opatření proti zneužití a padělání certifikátů vydaných jako kvalifikované ohrozí bezpečnost poskytovaných kvalifikovaných certifikačních služeb,

i) nesplní informační povinnost podle § 6a odst. 1 písm. i),

j) nezajistí soulad a utajení dat podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří,

k) kopíruje a uchovává data podle § 6a odst. 2, pokud tato data pro podepisující nebo označující osobu vytváří, nebo

l) nezneplatní certifikát podle § 6a odst. 3 a 4.

(3) Kvalifikovaný poskytovatel certifikačních služeb, který vydává kvalifikovaná časová razítka, se dopustí přestupku tím, že

a) nezajistí, aby časová razítka jím vydávaná jako kvalifikovaná obsahovala všechny náležitosti stanovené v § 12b,

b) nezajistí, aby časový údaj vložený do kvalifikovaného časového razítka odpovídal hodnotě koordinovaného světového času při vytváření kvalifikovaného časového razítka,

c) nezajistí, aby data v elektronické podobě, která jsou předmětem žádosti o vydání kvalifikovaného časového razítka, odpovídala datům v elektronické podobě obsaženým ve vydaném kvalifikovaném časovém razítku,

d) nepřijme odpovídající opatření proti padělání kvalifikovaných časových razítek, a tím ohrozí bezpeč-

nost poskytovaných kvalifikovaných certifikačních služeb,

e) nesplní informační povinnost podle § 6b odst. 1 písm. e), nebo

f) nevydá kvalifikované časové razítko neprodleně po přijetí žádosti o jeho vydání.

(4) Kvalifikovaný poskytovatel certifikačních služeb, který vydává prostředky pro bezpečné vytváření elektronických podpisů, se dopustí přestupku tím, že

a) nevydá prostředky pro bezpečné vytváření elektronických podpisů bezpečně podle § 17 odst. 3, nebo

b) nevytvoří v těchto prostředcích nebo nepřidá do těchto prostředků data pro vytváření elektronických podpisů důvěryhodným způsobem podle § 17 odst. 3.

(5) Fyzická osoba se dopustí přestupku tím, že poruší povinnost mlčenlivosti podle § 6 odst. 7.

(6) Za přestupky podle odstavců 1 až 4 lze uložit pokutu do výše 10 000 000 Kč.

(7) Za přestupek podle odstavce 5 lze uložit pokutu do výše 250 000 Kč.

§ 19

Společná ustanovení

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž bylo spácháno.

(3) Odpovědnost právnické osoby za správní delikt zaniká, jestliže správní orgán o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl spáchán.

(4) Správní delikty podle tohoto zákona v prvním stupni projednává ministerstvo.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby[8]) nebo v přímé souvislosti s ním, se vztahují ustanovení zákona o odpovědnosti a postihu právnické osoby.

(6) Pokuty vybírá a vymáhá místně příslušný celní úřad. Výnos z pokut je příjmem státního rozpočtu.

§ 20

Zmocňovací ustanovení

(1) Ministerstvo stanoví prováděcím právním předpisem způsob splnění informační povinnosti podle § 6 odst. 1 písm. a) a f) a odst. 3, kvalifikační požadavky podle § 6 odst. 1 písm. b), požadavky na bezpečné systémy a bezpečné nástroje podle § 6 odst. 1 písm. c) a d), způsob uchovávání informací a dokumentace podle § 6 odst. 5 a 6 a způsob, jakým se splnění těchto požadavků dokládá.

(2) Ministerstvo stanoví prováděcím právním předpisem způsob ověření souladu dat podle § 6a odst. 1 písm. d), způsob zajištění bezpečnosti seznamů podle § 6a odst. 1 písm. e) a f), určení data a času podle § 6a odst. 1 písm. g), náležitosti opatření podle § 6a odst. 1 písm. h), způsob splnění informační povinnosti podle § 6a odst. 1 písm. i), způsob ochrany a zajištění souladu dat podle § 6a odst. 2, způsob zneplatnění certifikátů podle § 6a odst. 3 a 4 a způsob, jakým se splnění těchto požadavků dokládá.

(3) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění přesnosti času při vytváření kvalifikovaného časového razítka podle § 6b odst. 1 písm. b), způsob zajištění souladu dat podle § 6b odst. 1 písm. c), náležitosti opatření podle § 6b odst. 1 písm. d), způsob splnění informační povinnosti podle § 6b odst. 1 písm. e) a způsob,jakým se splnění těchto požadavků dokládá.

(4) Ministerstvo stanoví prováděcím právním předpisem strukturu údajů, na základě kterých je možné osobu jednoznačně identifikovat, a postupy orgánů veřejné moci uplatňované při přijímání a odesílání datových zpráv prostřednictvím elektronické podatelny podle § 11 odst. 3.

(5) Ministerstvo stanoví prováděcím právním předpisem způsob zajištění postupů, které musí podporovat prostředky pro bezpečné vytváření a ověřování elektronických podpisů při ochraně dat pro vytváření elektronických podpisů podle § 17 a prostředky pro vytváření elektronických značek při ochraně dat pro vytváření elektronických značek podle § 17a, a způsob, jakým se splnění těchto požadavků dokládá.

ČÁST DRUHÁ

Změna občanského zákoníku

§ 21

Zákon č. 40/1964 Sb., občanský zákoník, ve znění zákona č. 58/1969 Sb., zákona č. 131/1982 Sb., zákona č. 94/1988 Sb., zákona č. 188/1988 Sb., zákona č. 87/1990 Sb., zákona č. 105/1990 Sb., zákona č. 116/1990 Sb., zákona č. 87/1991 Sb., zákona č. 509/1991 Sb., zákona č. 264/1992 Sb., zákona č. 267/1994 Sb., zákona č. 104/1995 Sb., zákona č. 118/1995 Sb., zákona č. 89/1996 Sb., zákona č. 94/1996 Sb., zákona č. 227/1997 Sb., zákona č. 91/1998 Sb., zákona č. 165/1998 Sb., zákona č. 159/1999 Sb., zákona č. 363/1999 Sb., zákona č. 27/2000 Sb. a zákona č. 103/2000 Sb., se mění takto:

V § 40 odst. 3 se doplňuje tato věta:

[8] § 2 odst. 2 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.

„Je-li právní úkon učiněn elektronickými prostředky, může být podepsán elektronicky podle zvláštních předpisů.“.

ČÁST TŘETÍ

Změna zákona č. 337/1992 Sb., o správě daní a poplatků

§ 22

Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění zákona č. 35/1993 Sb., zákona č. 157/1993 Sb., zákona č. 302/1993 Sb., zákona č. 315/1993 Sb., zákona č. 323/1993 Sb., zákona č. 85/1994 Sb., zákona č. 255/1994 Sb., zákona č. 59/1995 Sb., zákona č. 118/1995 Sb., zákona č. 323/1996 Sb., zákona č. 61/1997 Sb., zákona č. 242/1997 Sb., zákona č. 91/1998 Sb., zákona č. 168/1998 Sb., zákona č. 29/2000 Sb., zákona č. 159/2000 Sb. a zákona č. 218/2000 Sb., se mění takto:

V § 21 odstavce 2 a 3 znějí:

„(2) Stanoví-li tak tento nebo zvláštní zákon, podávají daňové subjekty o své daňové povinnosti příslušnému správci daně přiznání, hlášení a vyúčtování na předepsaných tiskopisech. Tiskopisy zveřejněné v elektronické podobě lze podepsat elektronicky podle zvláštních předpisů.

(3) Jiná podání v daňových věcech, jako jsou oznámení, žádosti, návrhy, námitky, odvolání apod., lze učinit buď písemně nebo ústně do protokolu nebo elektronicky podepsané podle zvláštních předpisů či za použití jiných přenosových technik (dálnopis, telefax apod.).“.

ČÁST ČTVRTÁ

zrušena

§ 23

zrušen

ČÁST PÁTÁ

Změna občanského soudního řádu

§ 24

Zákon č. 99/1963 Sb., občanský soudní řád, ve znění zákona č. 36/1967 Sb., zákona č. 158/1969 Sb., zákona č. 49/1973 Sb., zákona č. 20/1975 Sb., zákona č. 133/1982 Sb., zákona č. 180/1990 Sb., zákona č. 328/1991 Sb., zákona č. 519/1991 Sb., zákona č. 263/1992 Sb., zákona č. 24/1993 Sb., zákona č. 171/1993 Sb., zákona č. 117/1994 Sb., zákona č. 152/1994 Sb., zákona č. 216/1994 Sb., zákona č. 84/1995 Sb., zákona č. 118/1995 Sb., zákona č. 160/1995 Sb., zákona č. 238/1995 Sb., zákona č. 247/1995 Sb., nálezu Ústavního soudu č. 31/1996 Sb., zákona č. 142/1996 Sb., nálezu Ústavního soudu č. 269/1996 Sb., zákona č. 202/1997 Sb., zákona č. 227/1997 Sb., zákona č. 15/1998 Sb., zákona č. 91/1998 Sb., zákona č. 165/1998 Sb., zákona č. 326/1999 Sb., zákona č. 360/1999 Sb., nálezu Ústavního soudu č. 2/2000 Sb., zákona č. 27/2000 Sb., zákona č. 30/2000 Sb., zákona č. 46/2000 Sb., zákona č. 105/2000 Sb., zákona č. 130/2000 Sb., zákona č. 155/2000 Sb. a zákona č. 220/2000 Sb., se mění takto:

V § 42 odst. 1 věta první zní:

„Podání je možno učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky nebo telefaxem.“.

ČÁST ŠESTÁ

Změna trestního řádu

§ 25

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění zákona č. 57/1965 Sb., zákona č. 58/1969 Sb., zákona č. 149/1969 Sb., zákona č. 48/1973 Sb., zákona č. 29/1978 Sb., zákona č. 43/1980 Sb., zákona č. 159/1989 Sb., zákona č. 178/1990 Sb., zákona č. 303/1990 Sb., zákona č. 558/1991 Sb., zákona č. 25/1993 Sb., zákona č. 115/1993 Sb., zákona č. 292/1993 Sb., zákona č. 154/1994 Sb., nálezu Ústavního soudu č. 214/1994 Sb., nálezu Ústavního soudu č. 8/1995 Sb., zákona č. 152/1995 Sb., zákona č. 150/1997 Sb., zákona č. 209/1997 Sb., zákona č. 148/1998 Sb., zákona č. 166/1998 Sb., zákona č. 191/1999 Sb., zákona č. 29/2000 Sb. a zákona č. 30/2000 Sb., se mění takto:

V § 59 odstavec 1 zní:

„(1) Podání se posuzuje vždy podle svého obsahu, i když je nesprávně označeno. Lze je učinit písemně, ústně do protokolu, v elektronické podobě podepsané elektronicky podle zvláštních předpisů, telegraficky, telefaxem nebo dálnopisem.“.

ČÁST SEDMÁ

Změna zákona o ochraně osobních údajů

§ 26

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, se mění takto:

V § 29 se doplňuje odstavec 4, který zní:

„(4) Úřad uděluje a odnímá akreditace k působení jako akreditovaný poskytovatel certifikačních služeb a provádí dozor nad dodržováním povinností stanovených zákonem o elektronickém podpisu.“.

ČÁST OSMÁ

Změna zákona o správních poplatcích

§ 27

Zákon č. 368/1992 Sb., o správních poplatcích, ve znění zákona č. 10/1993 Sb., zákona č. 72/1994 Sb., zákona č. 85/1994 Sb., zákona č. 273/1994 Sb., zákona č. 36/1995 Sb., zákona č. 118/1995 Sb., zákona č.

160/1995 Sb., zákona č. 301/1995 Sb., zákona č. 151/1997 Sb., zákona č. 305/1997 Sb., zákona č. 149/1998 Sb., zákona č. 157/1998 Sb., zákona č. 167/1998 Sb., zákona č. 63/1999 Sb., zákona č. 166/1999 Sb., zákona č. 167/1999 Sb., zákona č. 223/1999 Sb., zákona č. 326/1999 Sb., zákona č. 352/1999 Sb., zákona č. 357/1999 Sb., zákona č. 360/1999 Sb., zákona č. 363/1999 Sb., zákona č. 46/2000 Sb., zákona č. 62/2000 Sb., zákona č. 117/2000 Sb., zákona č. 133/2000 Sb., zákona č. 151/2000 Sb., zákona č. 153/2000 Sb., zákona č. 154/2000 Sb., zákona č. 156/2000 Sb. a zákona č. 158/2000 Sb., se mění takto:

1. V příloze k zákonu (Sazebník správních poplatků) se doplňuje nová část XII, která zní:

„ČÁST XII

ŘÍZENÍ PODLE ZÁKONA O ELEKTRONICKÉM PODPISU

Položka 162

a) podání žádosti o akreditaci poskytovatele certifikačních služeb Kč 100 000,-

b) podání žádosti o vyhodnocení shody nástrojů elektronického podpisu s požadavky Kč 10 000,-.“.

2. REJSTŘÍK K SAZEBNÍKU se doplňuje o část XII, která zní:

„ČÁST XII

Řízení podle zákona o elektronickém podpisu 162.“.

3. Tečka za částí XI se vypouští.

ČÁST DEVÁTÁ

ÚČINNOST

§ 28

Tento zákon nabývá účinnosti prvním dnem třetího kalendářního měsíce po dni jeho vyhlášení.

Klaus v. r.

Havel v. r.

Zeman v. r.

PŘÍLOHA I – HARMONOGRAM PŘÍPRAVY ZÁKLADNÍCH ZÁKONŮ E-GOVERNMENTU

Zdroj: Strategie rozvoje služeb pro informační společnost. www.egovernment.cz