Návrh implementace bezpečnostní politiky v informačním systému veřejné správy

Bc. Michal Gerža

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal Gerža**
Osobní číslo:	**A13365**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh implementace bezpečnostní politiky v informačním systému veřejné správy**
Téma anglicky:	**The Design of the Implementation of a Security Policy in the Public Administration Information and Communication Systems Field**

Zásady pro vypracování:

1. **Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.**
2. **Proveďte analýzu legislativních požadavků na bezpečnost informačních a komunikačních systémů veřejné správy.**
3. **Vytvořte model informačního a komunikačního systému veřejné správy a popište zásady tvorby bezpečnostní politiky z hlediska komplexního způsobu zabezpečení – systémové, fyzické, personální, atd.**
4. **Analyzujte bezpečnostní rizika pro vnější a vnitřní prostředí a na základě této analýzy navrhněte implementaci bezpečnostní politiky.**
5. **Proveďte zobecnění/ doporučení pro postup při zvládání rizik – implementaci bezpečnostní politiky v objektech veřejné správy.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **JAŠEK, Roman: Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
2. **DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. Vyd. 1. Praha: Computer Press, 2001, xvi, 565 s. ISBN 807226513x.**
3. **MALANÍK, David: Význam fyzického zabezpečení IT systémů. Security Revue září 2010. ISSN 1336-9717.**
4. **NORTHCUTT, Stephen, et al. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.**
5. **THOMAS, M. : Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.**
6. **DOSEDĚL, Tomáš: Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno : Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 14. 5. 2015

.....
podpis diplomanta

ABSTRAKT

Diplomová práce mapuje využití a provázanost informačních technologií v oblasti veřejné správy. Zabývá se bezpečnostní politikou těchto informačních systémů v současném legislativním prostředí. Teoretická část rozebírá současný stav informačních a komunikačních systémů veřejné správy, jejich použití a provázanost s legislativními požadavky na jejich funkci. Jako referenční příklad je použit městský úřad, který díky rozsahu využití informačních systémů veřejné správy pokrývá velmi širokou oblast této problematiky.

Cílem praktické části práce je návrh postupu implementace bezpečnostní politiky s nastavením zabezpečení využívaných informačních systémů veřejné správy.

Klíčová slova: informační systém, veřejná správa, analýza rizik, bezpečnostní politika, systémové řízení bezpečnosti informací

ABSTRACT

The dissertation thesis conducts a survey of the application and interconnection of the information technology in the public administration. It is concerned with the security policy of these information systems in the current legislative environment. The theoretical part analyse the contemporary situation of the informative and communication systems of the public administration, its usage and interconnection with the legislative requirements for its function. As a reference example is used the municipality which thanks to the extent of information system usage of public administration covers a broad area of this issue.

The aim of the practical part is the design of the implementation of a security policy with the setting of usage of information system of public administration security.

Keywords: information system, public administration, risk analysis, security policy, information security management system

Děkuji panu doc. Ing. Jiřímu Gajdošíkovi, CSc. za odborné rady, vedení a konzultace při psaní mé diplomové práce.

OBSAH

ÚVOD

Vývoj a rozšíření výpočetní techniky mezi uživateli v posledních dvou desetiletích přispělo k integraci informačních technologií do běžného života populace. V současné době téměř každý obyvatel tohoto státu vlastní stolní počítač, či mobilní telefon s připojením na internet. Vzdálený přístup obyvatel k informačním systémům se tak stal naprosto samozřejmou skutečností.

Rozmach mobilních technologií vedl k tomu, že se dnes není problémem na většině území připojit k internetové síti. Vývoj přenosových technologií vede k neustálému zvyšování rychlosti a propustnosti datových sítí, ruku v ruce s tím jde zvyšování nároků uživatelů. Dříve byly prioritními nároky uživatelů spíše dostupnost, rychlost připojení a zvýšení limitů stažených dat. Dnes již tyto priority začaly být samozřejmostí, uživatelé zvyšují své nároky na služby, dostupnost potřebných informací či možnosti propojení na informační systémy soukromých organizací či veřejné správy.

Informační systémy prošly překotným vývojem, zvýšila se efektivita zpracování uchovávaných informací, která je hnána dopředu nutností zpracovávat neustále rostoucí množství ukládaných dat. Současná společnost se stala na informačních technologiích závislá ve všech oblastech. Postupný přesun informací z papírové podoby do digitální usnadňuje hromadné zpracování informací, zároveň však naši společnost vystavuje rizikům z poškození, ztráty či zneužití informací. Rozšíření dostupnosti přístupu k informačním systémům široké veřejnosti vyžaduje zvýšené úsilí o zajištění bezpečnosti. Vzhledem ke stále větší intenzitě snah o získání přístupu do cizích systémů s cílem jejich zneužití, je nezbytné využití bezpečnostní politiky pro informační systémy.

Veřejná správa je jedním z nejvýznamnějších správců a uživatelů informačních systémů. Na tyto systémy jsou kladeny obzvláště přísné nároky, které vyplývají z osobní povahy uchovávaných informací. Informačním systémům veřejné správy a vývoji jejich funkcionalit v návaznosti na legislativu je věnována teoretická část, ve které jsou též zahrnuty požadavky na bezpečnostní politiku informačních systémů veřejné správy.

V praktické části je navržen postup pro zpracování dokumentace informační strategie a informační koncepce organizace veřejné správy. Je zde také posouzeno zabezpečení využívaných informačních systémů a zpracována dokumentace bezpečnostní politiky s návrhem implementace bezpečnostní politiky v informačních systémech veřejné správy. Pro implementaci je použito reálné využití systémů při činnostech městského úřadu. V této

části stanovíme procesy a na jejich základě připravíme podklady pro dokumentaci k atestaci informačního systému. Závěrečná část je věnována budoucímu směřování informačních systémů veřejné správy s možnostmi v jejich zabezpečení.

I. TEORETICKÁ ČÁST

1 PŮSOBNOST VEŘEJNÉ SPRÁVY

Pod pojmem správa si vybavíme vedení, řízení či spravování záležitostí, majetku či organizace. Správa má blíže ke společenským procesům, kde zastupuje výkonnou část při procesech rozhodování. Správu lze dělit na soukromou a veřejnou. [1]

U soukromé správy je hlavním smyslem zajistit hospodaření a finanční výnosy ve prospěch soukromého subjektu. Správce v soukromém sektoru může pro správu uplatňovat téměř jakékoliv postupy a metody, které sám určuje, pokud je zákon nezakazuje, v tomto směru je vázán pouze mantinely platné legislativy. Téže volnosti se mu dostává při určování úkolů, které jsou závazné jen pro účastníky, kteří jsou k němu v určitém organizačním (zaměstnaneckém) vztahu. [1]

Veřejná správa je správou veřejných věcí, či záležitostí týkajících se veřejného zájmu. Veřejná správa se účastní na aplikaci a vytváření práva, může zavazovat občany k jeho dodržování. Je součástí procesu vyhotovení individuálních, nebo normativních závazných právních předpisů. Činnost veřejné správy je však možno provádět pouze na základě zákona a v mezích zákona. [1]

Veřejná správa zajišťuje výkon veřejných úkolů při čemž zároveň s jejich uskutečňováním připravuje podmínky potřebné pro jejich vyhotovení. Veřejnou správu můžeme charakterizovat ve funkčním, nebo organizačním pojetí. Pro funkční pojetí je důležitá náplň veřejné správy a povaha úkolů, které má plnit. Dle tohoto pojetí je souborem všech správních činností majících souvislost s poskytováním veřejné služby na místním a centrálním stupni. [2] Subjekty, které splňují podmínky existence působnosti, pravomoci, organizační samostatnosti a v vykonávají veřejnou správu jsou orgánem veřejného práva. Při organizačním pojetí jsou jen organizace vykonávající v rámci pravidelné a hlavní náplně veřejnou správu zahrnuty do veřejné správy. [1]

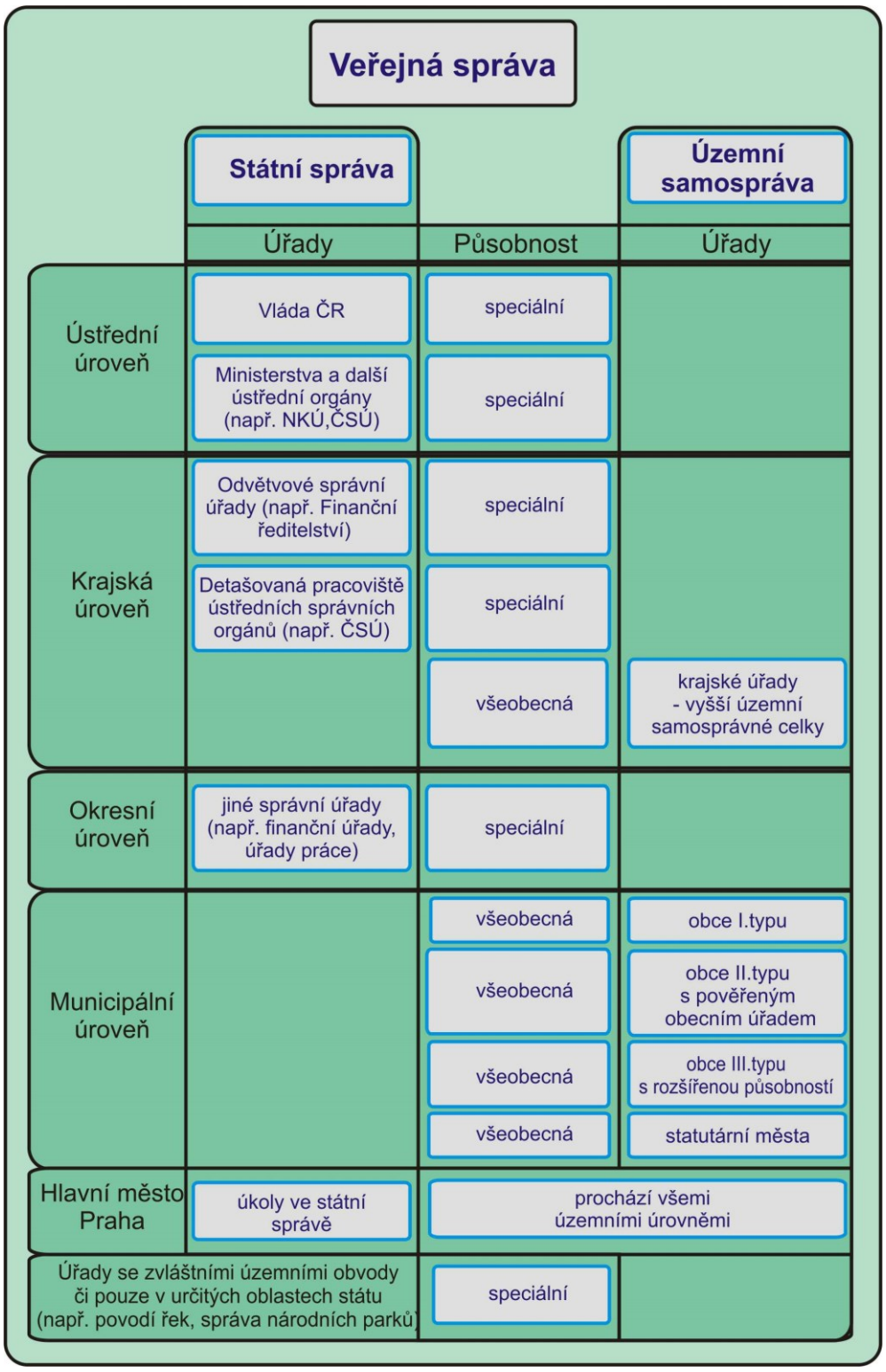
Veřejná správa (tabulka č.1) se dále dělí na státní správu a ostatní veřejnou správu, která zahrnuje veřejnou samosprávu (územní samospráva) a zbytkovou veřejnou správu. U zbytkové veřejné správy jde o organizace se specifickým postavením, vykonávající veřejnou správu, kterou neprovádí územní samospráva, nebo stát. Ostatní veřejná správa může být vykonávána též nesamosprávnými organizacemi zřízenými zákonem, které veřejnoprávní funkce plní zároveň se svou hlavní činností. Zde se jedná veřejné výzkumné instituce, veřejné ústavy, nadační fondy a jiné. [2]

Státní správa plní funkce výkonu a tvorby práva a uskutečňování státní politiky. Oproti tomu funkcí samosprávy je řízení záležitostí územně ohraničeného společenství, reprezentuje ho a snaží se prosazovat jeho zájmy, má omezenu možnost aplikace práva. Může mít jiný cíl než státní politika, protože prezentuje zájmy svého společenství. [1]

Územní samosprávu, jejíž základní jednotkou je obec stanovují právní předpisy:

- *„ústavní zákon České národní rady č. 1/1993 Sb. „Ústava České republiky“ ze dne 16. prosince 1992, ve znění Ústavních zákonů č. 347/1997 Sb., č. 448/2001 Sb., č. 395/2001 Sb., č. 300/2000 Sb., č. 515/2002 Sb., č. 319/2009 Sb., č. 71/2012 Sb. a č. 98/2013 Sb.,*
- *usnesení předsednictva České národní rady 2/1993 Sb. o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky ze dne 16. prosince 1992, ve znění ústavního zákona č. 162/1998 Sb.,*
- *zákon č. 128/2000 Sb., o obcích, ze dne 12. dubna 2000, ve znění pozdějších zákonů,*
- *zákon č. 129/2000 Sb., o krajích (krajské zřízení), ze dne 12. dubna 2000, ve znění pozdějších zákonů,*
- *zákon č. 131/2000 Sb., o hlavním městě Praze, ze dne 13. dubna 2000, ve znění pozdějších zákonů,*
- *zákon č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností, ze 13.června 2002, ve znění zákona č. 387/2004 Sb.“*

  [4]



Tabulka 1 Struktura a působnost veřejné správy [4]

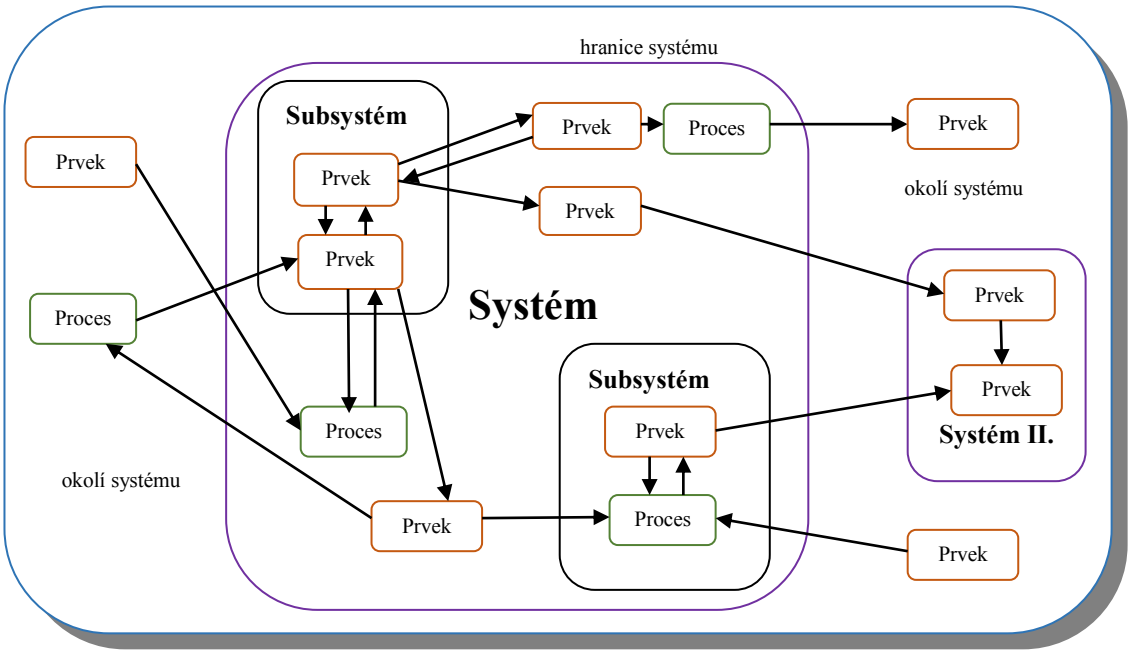
2 INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

2.1 Informační systémy

Informačním systémem můžeme rozumět souhrn technického a programového vybavení spolu s daty, nosiči pro uchování dat a také lidí udržujícími informace organizace a obsluhujícími ostatní části systému. [5] V rámci informačního systému shromažďujeme data, která ukládáme a pomocí analýz a procesů provádíme jejich třídění, vyhledání relevantních dat a zpracování do potřebného pro dané účely formátovaného výstupu. Výstupem může být forma srozumitelná pro uživatele, nebo souhrn dat určený pro řízení či zpracování jiným systémem.

Dle zakladatele kybernetiky, amerického matematika Norberta Wienara se systém (obrázek č. 1) dá definovat dle následujících charakteristik a zákonitostí, které jsou pro činnost každého systému nezbytné.

- Mezi subsystémy či prvky posuzovaného systému musí být definovány vazby (relace). Systém lze po analýze probíhajících procesů zobrazit jako uskupení fyzických objektů a uskupení, které jsou vzájemně propojeny zjištěnými vazbami,
- Nedělitelnými částmi každého systému jsou jeho jednotlivé prvky,
- Subsystémy tvoří seskupení prvků, lze je možné považovat za samostatný systém. Rozdělením systému na jednotlivé subsystémy můžeme po provedení jejich rozboru stanovit další rozhraní, kterými mezi sebou komunikují,
- V závislosti na zpětném ovlivnění vstupu prostředím reagujícím na výstup ze systému určujeme separabilitu systému, v případě separabilního subsystému by nemělo dojít k jeho ovlivnění ostatními subsystémy,
- Okolím systému, tj. prostředím rozumíme objekt, který odpovídá systému na přijaté výstupy ze systému. Jsou to prvky ležící mimo systém, ovlivňované či ovlivňující systém přes jeho vstupy a výstupy,
- Systém je od svého okolí, nebo jiných systémů oddělen hranicí systému,
- Dalšími charakteristikami jseu vstupy a výstupy systému, jeho chování, stav a stabilita. [6]



Obrázek 1 Součásti a vazby systému [6]

2.2 Vývoj informačních systémů ve veřejné správě

Veřejná správa je v současné době jedním z největších uživatelů informačních systémů v ČR. K tomuto stavu však vedla dlouhá cesta, při které bylo potřeba zvládnout stav, kdy výpočetní technika používaná před rokem 1990 začala být nahrazována moderní výpočetní technikou a nekoordinovaným vývojem informačních systémů.

Roku 1991 byla v České a Slovenské Federativní Republice ustanovena Komise vlády ČR pro státní informační systém. Jedním z prvních úkolů komise bylo řídit zavedení jednotného státního informačního systému a zabezpečit zrušení nejednotnosti stávajících informačních systémů. Na zřízení komise navázalo usnesení vlády 26. června 1991 o řešení státního informačního systému ČR, kterým bylo schváleno řešení registrů pro veřejnou správu. Týkalo se registrů občanů, hospodářských subjektů, nemovitostí a také registru územně identifikačního. Ministerstvům byl zadán úkol předložit projekty informačních systémů do konce října 1991. Práce na projektech koordinovala Komise pro státní informační systém (SIS). Tímto nařízením byla v roce 1991 zřízena Informační agentura SIS ČR. Bylo stanoveno zaměření na otevřené systémy. [7]

V roce 1992 bylo vydáno usnesení vlády 78/1992 ke zprávě o výsledcích práce komise vlády ČR pro SIS. Pravomoci komise vlády ČR pro SIS byly později převedeny na ministerstvo hospodářství. To převzalo i závazek vypracovat návrh globální architektury

státní informační soustavy. Architektura měla být postavena na základních registrech a návrzích resortních IS, to vše do 31. ledna 1993. Pokud by orgány veřejné správy neměly ve svých rozpočtech dostatek finančních prostředků na vyhotovení SIS, měly předložit do konce května 1992 žádosti o potřebné prostředky vládě. Pozdější souhlas vlády se zprávou Výstavba SIS ČR v roce 1995 počítal s tím, že všechny ministerstva budou používat komunikační síť ministerstva financí, v provozu měly být registry obyvatel, sociálních dávek, zdravotního pojištění, nemovitostí a ekonomických subjektů. [7]

Úřad pro státní informační systém (ÚSIS) vznikl v roce 1996 na základě zákona č.272/1996 Sb. Díky jeho neadekvátnímu postavení nebyly názory úřadu ministerstvy dodržovány a k integraci systémů nedošlo. Proto byla v roce 1998 založena Rada vlády pro informační politiku, která byla poradním orgánem vlády a ta pokračovala v rozvíjení e-governmentu. Programové prohlášení vlády počítalo s návrhem zákona o kontrole IS, zákona o svobodném přístupu k informacím, chráněnými osobními údaji, systémem informací bytového fondu a dobudování SIS. Měly být stanovena pravidla pro financování ISVS a vypracován návrh materiálu Státní informační politika s koncepcí budování ISVS. [7]

Do roku 1999 byly snahy o budování informačních systémů omezeny pouze na komunikaci mezi finančními a daňovými správami, neřešila se elektronizace kompletní veřejné správy. Opravdu úplnou koncepci informační politiky přinesl až květen 1999, kdy byl přijat dokument Státní informační politika – cesta k informační společnosti (SIP). Vláda tak přijala dokument, jehož cíle jsou nadčasové. [8]

- Rozvoj ISVS, zřízení propojení oddělených informačních systémů do neveřejné sítě SIS. Řešení legislativy přijetím zákona o SIS, zákona o základních registrech, vybudování úřadu kontroly dodržení ochrany osobních dat, což bylo nutné pro realizaci komunikace ISVS, zřízení autentizace a použití elektronického podpisu.
- Informační gramotnost vyžadovala proškolit zaměstnance veřejné správy a občany.
- Komunikační infrastruktura informačních systémů veřejné správy (KI ISVS), vznik jednotného prostředí a systému pro komunikaci datovou a hlasovou, a aplikace ISVS. Zahrnutí stávajících datových linek do struktury KI ISVS. Během roku 2000 realizovat část infrastruktury spojující úřady veřejné správy a kontaktní

místa. Později, v roce 2005, došlo ke zkrácení názvu na Komunikační infrastruktura veřejné správy (KIVS), [9]

- Informatizovaná demokracie – realizace provádění zákona č.106/1999 o svobodném přístupu k informacím přes portál veřejné správy. Na úřadech měly být do začátku roku 2002 zřízeny informační místa, v knihovnách se plánoval vznik internetového přístupu pro veřejnost.
- Ochrana osobních údajů a zabezpečení IS, kdy se během roku 2001 měla realizovat dostupnost vlastních osobních údajů v registrech pro občany s ověřením přes elektronický podpis a elektronické identifikační prvky.
- Transparentnost prostředí v ekonomice měla být dosažena ve veřejné oblasti zveřejněním výběrových řízení, nakládání s rozpočty veřejné správy, v soukromé oblasti se jednalo o uveřejnění vlastnických a majetkových poměrech podniků, registr ekonomických subjektů přístupný pro veřejnost.
- Rozvoj elektronického obchodu – realizace legislativy při zapracování požadavků EU, zřízení centrální certifikační autority a elektronické služby veřejné správy pro podnikatele.
- Bezpečnost a stabilita informační společnosti spočívající v použití informačních a komunikačních technologií při obraně státu, podpoře krizového managementu a také při ochraně životního prostředí. [7]

Radě vlády pro SIP bylo uloženo vyhotovení Akčního plánu státní informační politiky. Pro realizaci úkolů bylo nutné připravit také koncepci budování ISVS spolu s koncepcí komunikační infrastruktury veřejné správy. Do systému ISVS měly být připojeny pouze systémy, které prošly atestací pro shodu referenčního rozhraní v souladu s předpisy EU. [7]

Po dokumentu Státní informační politiky byla schválena Koncepce budování ISVS, do níž byly zapracovány závěry z Koncepce reformy veřejné správy. Problémy vzniklé v návaznosti na nekoordinovanosti a živelného zavádění IS jednotlivými ministerstvy v dřívější době byly touto Koncepcí budování ISVS určeny a byla doporučena jejich náprava:

- vzhledem k možnostem informačních a komunikačních technologií (ICT) bylo jejich řešení ve veřejné správě nekoncepční,

- za nedostatku aktuálních informací, bez aplikace moderních postupů byly zavedeny rozhodovací, koncepční a kontrolní procesy,
- nebyly stanoveny závazná pravidla součinnosti IS v resortech a zásady pro datovou komunikaci a sdílení informací,
- veřejná kontrola je na nízké úrovni,
- procesy probíhající ve veřejné správě nebyly detailně určeny, v následku toho vznikla neprovázanost postupů mezi částmi veřejné správy, došlo ke zvýšení pracovního vytížení,
- každé ministerstvo si řešilo svůj IS, který byl určen jen pro shromažďování dat, IS byly oddělené od zbývající veřejné správy,
- pro použití moderních technologií nebyla zpracována legislativa,
- součinnost v organizacích veřejné správy, včetně komunikace ve všech směrech uvnitř veřejné správy, i k okolí byla na nízké úrovni
- chybí koncepční vzdělávání zaměstnanců veřejné správy pro použití moderních metod a technologií. [8]

Akční plán státní informační politiky počítající s dopracováním základních registrů veřejné správy propojených přes referenční rozhraní zároveň s komunikační infrastrukturou veřejné správy (KIVS) do roku 2002 byl schválen v roce 2000. Za nejdůležitější úkoly byly považovány realizace veřejné informační služby, realizace koncepce budování ISVS a umožnit provoz agend matričních úřadů, finančních úřadů a dalších věcí souvisejících s nutností elektronické identifikace osob v ISVS.

Předpoklad vyřešení koncepce budování ISVS pomocí jediného zákona však nebyl z důvodu rozdílů provozu každého registru reálný, což směřovalo ke zpracování několika zákonů pro vedení základních registrů. [7]

Mezi informační systémy veřejné správy patří podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy mimo informačních systémů státních úřadů a organizací také informační systémy obecních a městských úřadů. V průběhu používání dochází k jejich změnám s ohledem na změny legislativy a rychlý technologický rozvoj v prostředí informačních technologií. Důsledkem tohoto vývoje a různým finančním možnostem obcí a organizací patřících pod různá ministerstva byla velmi různorodá

základna používaného hardwarového a softwarového vybavení organizací státní správy a samosprávy. Z legislativy ČR týkající se oblasti informatiky je pro zavádění ISVS jedním z nejdůležitějších zákon č. 365/2000 Sb., o informačních systémech veřejné správy ve znění podle zákona č. 64/2014 Sb.

V roce 2002 byl novelizován Akční plán realizace SIP s ohledem na přijatý zákon č. 365/2000 Sb., pro období do roku 2003, předpokládající vytvoření všech registrů do 1. ledna 2006, s výjimkou registru obyvatel, který měl zahájit provoz v roce 2003. Měly být zjištěny znalosti zaměstnanců veřejné správy v ICT a provedeno zaškolení vedoucích pracovníků úřadů místní samosprávy. Během roku 2002 již byly dány do provozu realizované projekty aplikací pro daňová přiznání na internetu, zatím bez elektronického podpisu. Jednalo se o daň z nemovitostí, daň z přidané hodnoty, hlášení o vyplacených nezdaněných částkách a silniční daň, nebylo však provedeno potřebné dostatečné vyzkoušení ve zkušebním provozu, chyby byly opravovány až za ostrého provozu. Po půl roce se začalo se zkoušením podání se zaručeným elektronickým podpisem. [8]

V roce 2003 bylo zřízeno ministerstvo informatiky, kde se koncentrovaly všechny do té doby roztříštěné pravomoci napříč veřejnou správou a stalo se tak hlavní silou rozvoje e-governmentu. Zpracováním dokumentu Státní informační a komunikační politika e-Česko 2006, schválenému usnesením vlády č.265/2004 navázalo na předchozí vývoj a na politiku EU eEurope 2005. Největší roli e-governmentu měl hrát Portál veřejné správy se zachováním stávajících služeb pro občany a jejich rozšíření, zároveň však byla požadována úspora finančních nákladů na tyto služby. Portál pracoval ve zkušebním provozu pro veřejnost od podzimu 2003, do plného provozu přešel v říjnu 2004. Vznikl požadavek na další zřizování kontaktních míst veřejné správy na obcích a krajích a pobočkách České pošty.

Nový správní řád přijatý zákonem č.500/2004 Sb. v návaznosti na možnosti elektronického podání pojednával o e-podatelnách specifikovaných nařízením vlády č,495/2004 Sb. a úředních deskách zveřejněných na internetu. Elektronická úřední deska pro správní orgány se spolu s e-podatelnou pro veřejnou správu staly nezbytnými a pokud neměla organizace veřejné správy možnost poskytnout tuto službu, musela být uzavřena veřejnoprávní smlouva o poskytnutí těchto služeb obcí s rozšířenou působností. [8]

Veřejná správa dostala zákonem č. 499/2004 Sb., o archivnictví a spisové službě další impuls pro rozvoj ICT. Novela zákona č. 365/2000 Sb., o informačních systémech veřejné

správy zákonem č.81/2006 rozšířila možnost vydávání výstupů z ISVS dalším subjektům a dostupnost webových stránek veřejné správy. Veřejná správa dostala povinnost vypracování a dodržování informační koncepce a provozní dokumentace IS. [8]

V roce 2007 došlo zákonem č. 110/2007 Sb. ke zrušení ministerstva informatiky po změnách politické reprezentace v roce 2006. Došlo k převedení koordinační úlohy ICT na ministerstvo vnitra za pozdější asistence Rady vlády pro informační společnost. Bylo upřednostněno řešení dostupnosti všech služeb informačních systémů veřejné správy pro veřejnost na jednom místě. Z toho vznikl cíl vytvoření Czech POINTů v programovém prohlášení vlády, kde budou dostupné údaje ze všech registrů a půjde z nich provést podání veřejné správě. Usnesením vlády č.197/2007 přijatý Integrovaný operační program pro období 2007- 2013 měl návaznost na čerpání dotací ze strukturálních fondů Evropské unie. Efektivní veřejná správa a přátelské veřejné služby – Strategie realizace Smart Administration v období 2007 – 2015 byl dokumentem, který určil další úkoly pro rozvoj e-governmentu. Tyto úkoly v roce 2008 podrobněji rozebrala Strategie rozvoje služeb pro „informační společnost“. Zde se stanovovaly termíny zprovoznění služeb e-governmentu, pro rok 2009 byl předpokládán provoz Czech POINTů a datových schránek, zprovoznění centrálních registrů v roce 2010, infrastruktura pro ukládání a archivaci elektronických dokumentů, podsystémy pro sociální péči spolu se zajištěním správního, daňového a soudního řízení v roce 2012 a elektronizace datové základny a geografických dat s ukončením v roce 2015. [7]

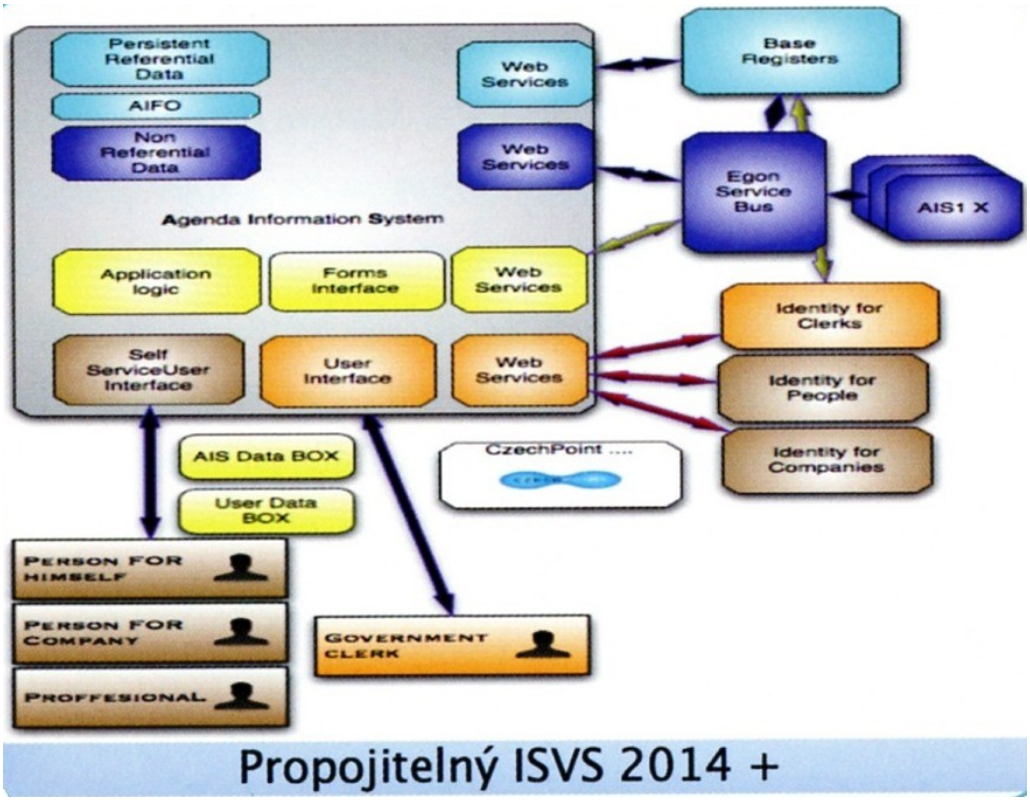
Symbolem e-Governmentu se stal v roce 2006 eGON, projekt elektonizace veřejné správy. V roce 2008 přijala vláda zákon 300/2008 Sb. zákona o elektronických úkonech a autorizované konverzi dokumentů, jež se stal základním právním předpisem pro systém datových schránek. Symbol eGONu má charakterizovat a spojovat služby Czech POINTU, Komunikační infrastruktury veřejné správy (KIVS), Základních registrů a to vše sdruženo okolo zákona o elektronických úkonech a autorizované konverzi dokumentů č.300/2008 Sb.

Klaudie přibyla k eGONu v roce 2011, kdy už bylo jasné, že nastoupený kurz pořizování kompletních nových řešení ISVS nebude možné s vyhrazenými finančními prostředky provozně pokrýt. Z tohoto důvodu byl opuštěn dosavadní způsob řešení výstavby každého ISVS na „zelené louce“, ale bylo rozhodnuto jít cestou orchestrovaného privátního cloudu veřejné správy, který bude ve správě ministerstva vnitra. Tyto centrálně

poskytované služby budou přístupné pomocí KIVSu přes přístupové body v krajích a okresech. [10]

Další z důležitých rozhodnutí bylo určeno pro zajištění ochrany ISVS a stalo se jím přijetí usnesení vlády ČR č. 781/2011, kterým bylo zřízeno Národní centrum kybernetické bezpečnosti (NCKB) a Rada pro kybernetickou bezpečnost. Hlavním úkolem NCKB působícím pod Národním bezpečnostním úřadem (NBÚ) bylo sepsání návrhu zákona o kybernetické bezpečnosti, který měl být odpovědí na neustále se zvyšující bezpečnostní hrozby. Zákon o kybernetické bezpečnosti č. 181/2014 byl přijat 23.července 2014 a jeho účinnost začala 1.ledna 2015, po jeho vydání následovalo vydání prováděcích vyhlášek č. 316/2014 a 317/2014. Dále bylo schváleno usnesení č. 105/2015 Sb., z 16. února 2015, k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020. [11]

Během další vývoje je možné také postupné otevření oddělených uzavřených agendových informačních systémů a jejich propojení za implementace bezpečnostních prvků, pro maximální snížení možných rizik plynoucích z propojené architektury (obrázek č. 2). [12]



Obrázek 2 Propojitelný ISVS 2014 + [12]

3 PROJEKTY E-GOVERNMENTU

3.1 Základní registry veřejné správy

Registry veřejné správy tvoří základ informačního obsahu ISVS. Po letech postupné integrace ISVS a snah o propojení vzájemně různorodých systémů ve správě jednotlivých ministerstev byl 26. března 2009 přijat zákon č. 111/2009 Sb., o základních registrech. Přijetí tohoto zákona si vyžádalo rozsáhlé změny v dosavadní legislativě. Postupně byly přijaty další novelizace a prováděcí vyhlášky, týkající se jednotlivých registrů.

- Zákon č. 227/2009 Sb., ze dne 17. června 2009, měnícím některé zákony v souvislosti s přijetím zákona o základních registrech,
- Zákon č. 100/2010 Sb. a zákon č. 424/2010 Sb., kterými se měnil zákon č. 111/2009 Sb., o základních registrech,
- Nařízení vlády č. 161/2011 Sb., ze dne 25.května 2011, o stanovení harmonogramu a technickém způsobu provedení opatření podle § 64 až 68 o základních registrech,
- Vyhláška 359/2011 Sb., ze dne 24. listopadu 2011, o základním registru územní identifikace, adres a nemovitostí,
- Usnesení vlády č. 244/2013 k průběžné zprávě z plnění úsporných opatření v oblasti zjednodušení agend a zrušení duplicit ve státní správě pro rok 2014,
- Usnesení vlády č. 585/2014, k postupu při procesním modelování agend a tvorby standardů agend veřejné správy pro jednotný a finančně měřitelný výkon veřejné správy,
- Usnesení vlády č. 6/2015, ze 7. ledna 2015 k průběžné zprávě o postupu procesního modelování a standardizace agend veřejné správy.

Z posledního usnesení vlády vyplývá, že dosud není dokončena počáteční analýza agend v základním registru agend, u které byl nově stanoven termín zpracování ministerstvem vnitra na konec června 2015. [3]

Registry zahrnuté do systému (obrázek č. 3):

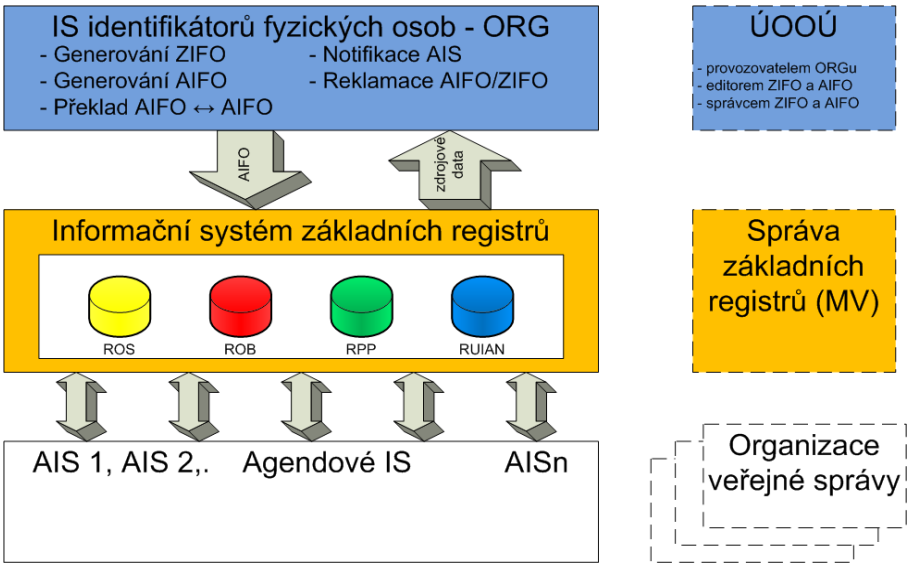
- **Registr obyvatel** (ROB) – obsahuje údaje o fyzických osobách, kteří jsou občany ČR , občanů cizích států s povolením pobytu na našem území, občanů cizích států, kterým byl udělen azyl či doplňková ochrana a jiných osob ze zákona

evidovaných v registru. Údaje zde vedené jsou považovány za referenční, jejich změna je zobrazena ve všech dalších agendách veřejné správy. Registr spravuje Ministerstvo vnitra ČR. [13]

- **Registr osob** (ROS) – jsou v něm vedeny právnické, podnikající fyzické a zahraniční osoby, státní organizace a mezinárodní organizace. Registr spravuje Český statistický úřad. Osoby a organizace vedené v rejstříku jsou opatřeny identifikátorem (IČ). [13]
- **Registr práv a povinností** (RPP) - má úlohu řízení přístupu uživatelů k datům ve všech registrech. Jsou v něm uloženy záznamy o přístupech k datům v základních registrech, které jsou zpětně dohledatelné a jsou dostupné dotčeným občanům. Jsou zde vedeny agendy orgánů veřejné moci, práva k přístupům k registrům. Registr spravuje Ministerstvo vnitra ČR.[13]
- **Registr územní identifikace, adres a nemovitostí** (RÚIAN) – jsou v něm evidovány adresy, územní prvky, účelové územní prvky, územně evidenční jednotky, umožňuje též získání informací z IS katastru nemovitostí. Ukládají se v něm také nereferenční údaje o budovách. Umožňuje dálkový přístup pro veřejnost přes rozhraní na webových stránkách Českého úřadu zeměměřického a katastrálního, který je také správcem registru. [13]

Systém základních registrů využívá pro výměnu informací s okolními IS tyto části:

- **Informační systém základních registrů** (ISZR) – zahrnuje vnitřní a vnější rozhraní pro přístup k registrům, udržuje jej Správa základních registrů.
- **ORG -** převodník identifikátorů fyzických osob byl zřízen Úřadem pro ochranu osobních údajů, vykonává identifikaci fyzických osob v základních registrech za nahrazení rodného čísla bezvýznamovým identifikátorem, který je pro každou agendu odlišný. V ORG jsou pro zajištění ochrany údajů uloženy pouze tyto identifikátory (obrázek č. 3).
  - Provádí určení zdrojového identifikátoru fyzickým osobám (ZIFO),
  - Cílovým agendám tvoří agendové identifikátory fyzických osob (AIFO),
  - Převádí AIFO v rámci systému základních registrů, přičemž pro každou agendu je pro stejný subjekt použito jiné AIFO. [13]



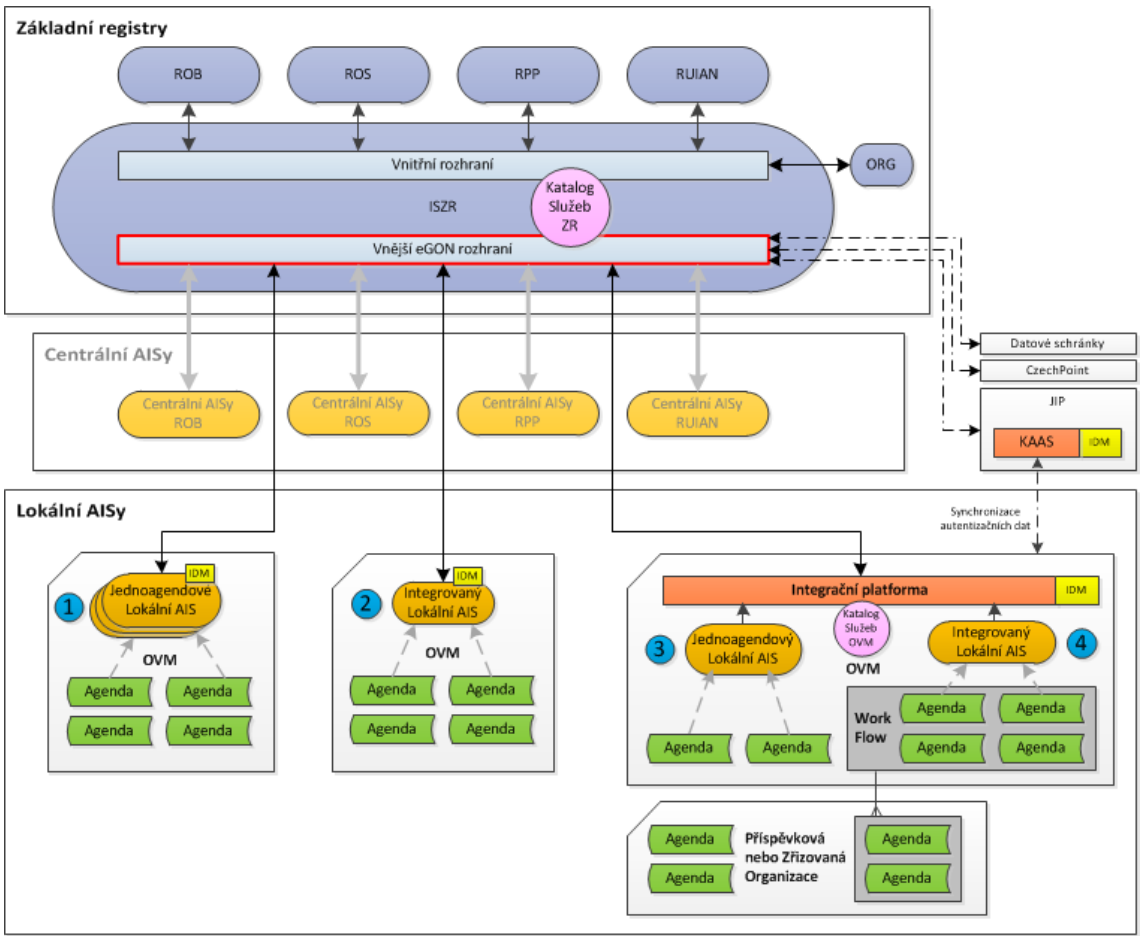
Obrázek 3 Role ORG v základních registrech [14]

V systému základních registrů se používají až na jedinou výjimku v RÚIANu pouze referenční údaje, pokládané za právně závazné, pokud není prokázán opak.

Do systému základních registrů je povolen přístup orgánům veřejné moci (OVM) pokud:

- Jsou registrovaným AIS z vnějšího eGON rozhraní ISZR,
- Jedná se o systém Czech POINT,
- Přistupují pomocí formuláře přes portál Datových schránek.

Informační systém základních registrů řídí zpracování všech služeb eGON rozhraním (obrázek č. 4), jenom ISZR umožňuje předání referenčních údajů. Pro provoz agendy je nutné, aby se OVM pro její provozování zaregistrovalo. Teprve poté zaměstnanci VM, kteří mají oprávnění k agendě, mohou začít službu používat. Přístup k agendám je možný přes centrální AISy, které využívají převážně portálového řešení a lokální AISy, využívané pro vlastní agendy OVM. Dovnitř OVM pak mohou být včleněny integrační platformy (ESB), které činí komunikaci mezi AISy a IS OVM efektivnější, protože dokáže propojit AIS OVM s ISZR bez toho, aby byl lokální AIS vybaven logovacím komunikačním rozhraním. [15]



Obrázek 4 Schéma propojení eGON rozhraní s lokálními AISy [15]

3.2 Identifikace v komunikační infrastruktuře veřejné správy

3.2.1 Certifikáty a elektronický podpis

Vznik zákona č. 227/2000 Sb., o elektronickém podpisu si vyžádala potřeba jednoznačné identifikace osob komunikujících uvnitř státní správy a samosprávy, stejně jako dalších subjektů a osob, které mají potřebu s OVM komunikovat elektronickou formou. Zákon rozlišuje a stanovuje vlastnosti některých druhů elektronických podpisů, certifikátů a poskytování certifikačních služeb. Dle tohoto zákona rozlišujme e-podpis a zaručený e-podpis. V případě zaručeného e-podpisu je vyžadováno jednoznačné propojení s podepisující osobou. [7]

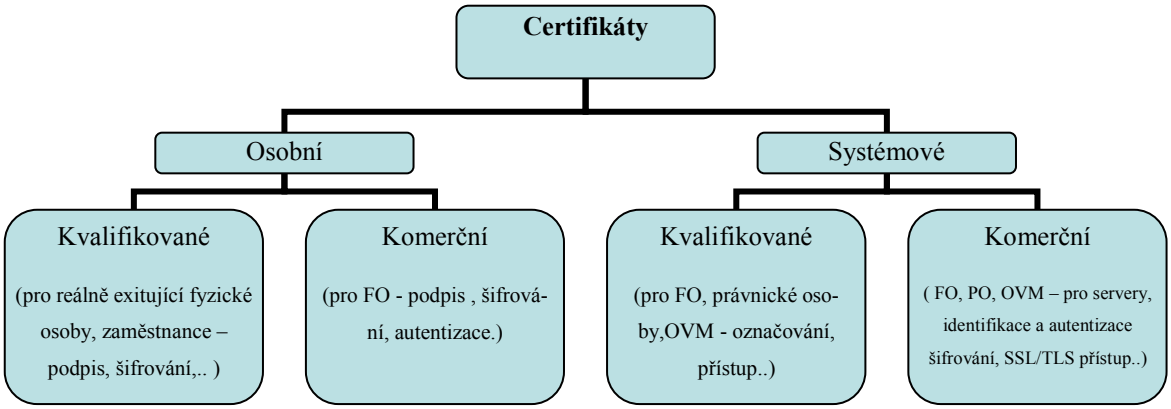
V počátcích používání elektronického podpisu bylo nutné řešit úpravy zákonů, které si odporovaly. Z tohoto důvodu musely být daňové přiznání podávány v elektronické i papírové variantě, protože elektroniký formulář používal formát xml bezelektronického podpisu. Ministerstvo práce a sociálních věcí umožňovalo nanejvýš elektronické vyplnění

formulářů, které se po vytištění musely ručně podepsat. Nařízení vlády č. 304/2001 Sb., z 25. července 2001, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu) uložilo OVM provozovat elektronické podatelny pro použití elektronických podání opatřených e-podpisem generovaným z kvalifikovaného certifikátu. Legislativa podrobněji specifikovala pravidla pro e-podatelnu až v roce 2004. [7]

Elektronický podpis umožňuje identifikaci podepsané osoby v datové zprávě. Manipulaci s elektronickým podpisem provádí pouze podepisující osoba, která ho tak má pod kontrolou. Připojení k elektronickému dokumentu je provedeno tak, že bez jeho porušení nemůže dojít k editaci zprávy. [7]

Pro elektronické podepisování dokumentů je k dispozici několik typů certifikátů, které se dělí dle různých kritérií (obrázek č. 5).

Zaručený elektronický podpis, založený na kvalifikovaném certifikátu obdrženého od akreditovaného poskytovatele certifikačních služeb obsahuje údaje, které podepisujícího identifikují pro komunikaci s OVM a zajišťuje neodmítnutelnou odpovědnost za podepsané dokumenty. [16]

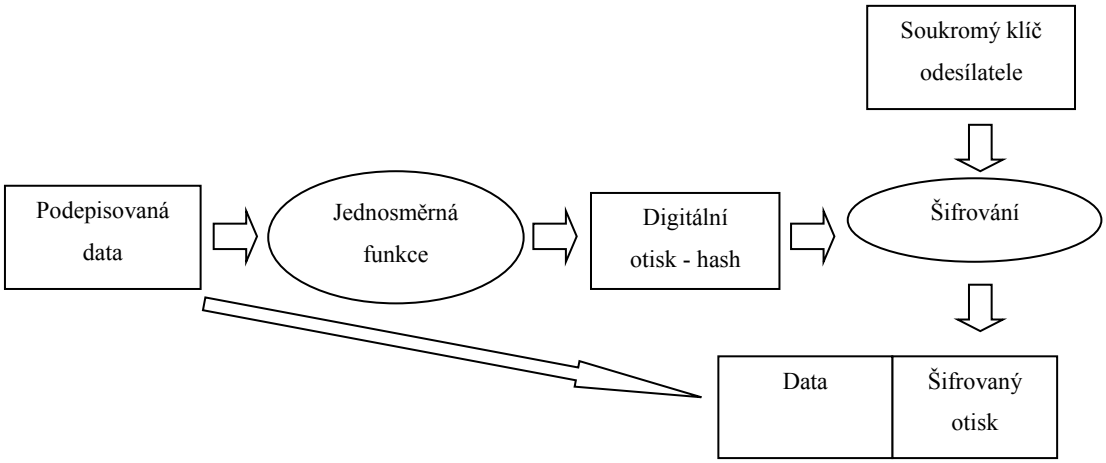


Obrázek 5 Rozdělení certifikátů [16]

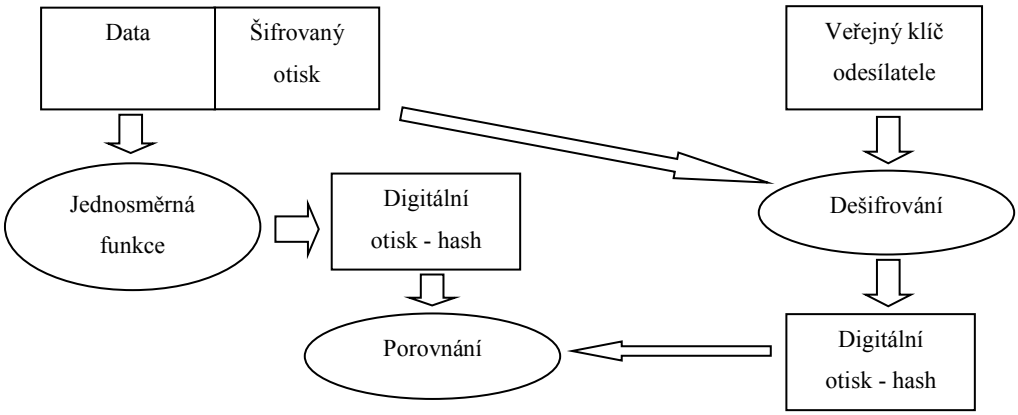
Dle zákona vydává certifikáty poskytovatel certifikačních služeb jinak nazývaný certifikační autorita. *Tuto činnost upravuje vyhláška č.378/2006 Sb, z 19. července 2006, o postupu kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb).*[3] Poskytovatel certifikačních služeb musí v případě, že chce poskytovat

kvalifikované certifikáty, požádat o udělení akreditace. Po prověření splnění zákonných povinností poskytovatelem je mu udělena akreditace a stane se z něho akreditovaný poskytovatel certifikačních služeb (akreditovaná certifikační autorita). V České republice působí tři autorizované certifikační autority, jsou to PostSignum, eIdentity a I. CA (První certifikační autorita). Tyto CA jsou vnitřně rozčleněny na kořenové certifikační autority vydávající certifikát svým podřízeným autoritám a podřízené (zprostředkující) autority vydávají certifikáty zákazníkům. [16] [17]

Tvorba elektronického podpisu (obrázek č. 6) probíhá u odesílatele soukromým klíčem asymetrickou kryptografií, jeho platnost je poté na straně adresáta ověřována (obrázek č. 7) veřejným klíčem. Vzhledem k náročnosti na výpočetní výkon, je z podepisovaného dokumentu vypočítán hashovací funkcí digitální otisk (hash), jehož velikost je natolik malá, že jej není problém zašifrovat soukromým klíčem. Nejznámějšími algoritmy pro hashovací funkci jsou algoritmy MD4, MD5, SHA-1, SHA-2 a SHA-256. [18]



Obrázek 6 – Schéma tvorby elektronického podpisu [18]



Obrázek 7 – Schéma ověření elektronického podpisu [18]

Pro zaručený elektronický podpis se dříve používal algoritmus SHA-1. Používání algoritmu SHA-1 bylo k 31.12.2009 ukončeno u autorizovaných certifikačních autorit, pro elektronický podpis jej bylo možné využívat do konce roku 2010. V současné době jsou pro zaručený elektronický podpis vydávány certifikáty s délkou klíče 2048 bitů, používají se hashovací funkce SHA-256 v kombinaci s atgoritmem RSA. [19]

Certifikáty jsou vydávány uživatelům na základě osobně odevzdané písemné žádosti s ověřením totožnosti, na počítači musí vygenerovat žádost, která se odešle certifikační autoritě. Vydaný certifikát se poté páruje s údaji o žádosti v daném počítači. Kvalifikovaný i komerční certifikát je certifikační autoritou vydáván s roční platností, před ukončením platnosti musí uživatel odeslat žádost o vystavení následného certifikátu, podepsanou ještě platným certifikátem. Poskytovatel certifikačních služeb poskytuje služby certifikační a validační (ověřovací). [20]

3.2.2 Časová razítka

Z důvodu, že platnost elektronického podpisu je závislá na době platnosti vydaného certifikátu, opatřuje se ještě podepsaný dokument elektronickým razítkem s časovým údajem. Časové razítko tvoří další samostatnou elektronickou značku s časovým údajem, která je vytvořena přímo poskytovatelem důvěryhodného časového údaje. Časové razítko má delší dobu platnosti a určuje nám, že k připojení elektronického podpisu došlo před časem připojení časového razítka. Tím je zaručena možnost ověření, že tvůrce dokumentu jej podepsal elektronickým podpisem v době jeho platnosti. V případě, že u dokumentu hrozí termín ukončení platnosti certifikátu časového razítka, musíme ještě v době jeho platnosti provést přerazítkování novým časovým razítkem. Časová razítka u nás poskytují kvalifikovaní poskytovatelé certifikačních služeb. [20]

3.2.3 Elektronická značka

Elektronickou značkou dle zákona č. 440/2004 Sb.. z 24.června 2004, kterým se mění zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění dalších předpisů, rozumíme elektronický podpis vytvořený technickým zařízením, např. informačním systémem, tvoří ho údaje připojené k datové zprávě. Elektronická značka musí splňovat umožnění ověření, že datovou zprávu označila osoba identifikovatelná prostřednictvím certifikátu. Dále se předpokládá, že označení zprávy probíhá s vědomím označující osoby, i když se tak děje

automaticky. Rozdílné s použitím elektronického podpisu je to, že při podepisování e- podpisem se předpokládá, že podepisující se s písemností seznámil, u elektronické značky se předpokládá, že označující osoba nemusí být seznámena s obsahem dokumentu. [20]

3.3 Veřejná dostupnost služeb – CzechPoint

Odpovědí na požadavek přiblížení úřadů státní správy směrem k uživatelům byla myšlenka na systém, který by byl dostupný prostřednictvím zaměstnanců obecních úřadů. Vzhledem k absenci státem vlastněné komunikační sítě bylo rozhodnuto o použití veřejného internetového připojení. Zabezpečení přístupu mělo být zajištěno vícestupňovou autentizací zaměstnanců úřadů. Zkušebního provozu projektu CzechPOINT se zůčastnilo 35 úřadů, byl zahájen 28.3.2007, skončit měl na konci června 2007. V roce 2008 byl zahájen plný provoz projektu. Zpočátku bylo počítáno s povinnou účastí obcí s matričními úřady, ovšem obce projevily přes Svaz měst a obcí nesouhlas s tímto řešením. Proto bylo odstoupeno od tohoto řešení a propříště měla být účast obcí na projektu dobrovolná. Náklady na vybudování pracovišť Czech POINTU byly částečně dotovány v rámci integrovaného operačního programu na pořízení a provoz pracovišť Czech POINT, jehož podmínky se však v průběhu realizace několikrát změnily. Za služby poskytované prostřednictvím Czech POINTU byly stanoveny poplatky, které mimo úhrad jiným organizacím zůstávaly obci. Pracoviště Czech POINTU byla zřízena na obecních úřadech a pobočkách České Pošty. Novela zákona rozšířila možnost zřízení pracovišť Czech POINTu na obecní, matriční a krajské úřady, úřady městských částí a obvodů statutárních měst, městské části Prahy, notáře, zastupitelské úřady, Hospodářskou komoru a držitele poštovní licence (obrázek č. 8). Upřesňující údaje obsahuje vyhláška č. 364/2009 Sb., z 15.října 2009, o seznamu obecních úřadů a zastupitelských úřadů, které jsou kontaktními místy veřejné správy (vyhláška o kontaktních místech veřejné správy). Dalšími institucemi, které mohou zřídit pracoviště CzechPOINTu se po roce 2011 staly banky. [7]

Funkcionality služby Czech POINT jsou přidávány neustále od zahájení provozu. Výhodou pro občany kromě toho, to že všechny žádosti vyřídí na jednom místě je i to, že nemusí mít elektronický podpis, ani zřízenou datovou schránku.

Funkcionality Služby Czech POINT, s rokem zprovoznění:

- Výpis z bodového hodnocení řidiče, (2009),

- Výpis z insolvenčního rejstříku, (2009),
- Úplný, nebo částečný výpis z Katastru nemovitostí, (2007),
- Výpis z veřejného rejstříku – obchodní, spolkový a nadační rejstřík, rejstřík společenství vlastníků, rejstřík ústavů, rejstřík obecně prospěšných společností, (2007),
- Výpis nebo opis z Rejstříku trestů, (2008-2009),
- Výpis z rejstříku trestů právnických osob, (2008-2009),
- Seznam kvalifikovaných dodavatelů, (2009),
- Živnostenský rejstřík, (2007),
- Autorizovaná konverze z elektronické podoby na listinnou a naopak, (2009),
- Ověření provedení autorizované konverze, (2009),
- Výpis údajů z registru obyvatel, (2010),
- Výpis údajů z registru osob, (2010),
- Žádost o změnu údajů v registru obyvatel, (2010),
- Žádost o změnu údajů v rejstříku osob, (2010),
- Žádost o vydání seznamu voličů, (2010),
- Agendy ISDS – žádost o zřízení datové schránky (DS), zneplatnění přístupových údajů a vydání nových, přidání pověřené osoby pro přístup do DS, zneplatnění přístupových údajů pověřené osoby, znepřístupnění DS zřízené na žádost, opětovné zpřístupnění DS zřízené na žádost, žádost o plnění či neplnění funkce OVM pro datovou schránku, (2009),
- Czech POINT@office - Základní registry – výpis údajů z registru obyvatel, výpisy údajů registru osob, veřejný z registru osob, o využití údajů z registru obyvatel, záznam o využívání údajů v registru osob, žádost o změnu údajů v registru obyvatel, žádost o změnu údajů v registru osob, žádost o poskytnutí údajů třetí osobě, (2012),
- Czech POINT@office – obchodní rejstřík, (2012),
- Czech POINT@office – konverze dokumentů, (2012),

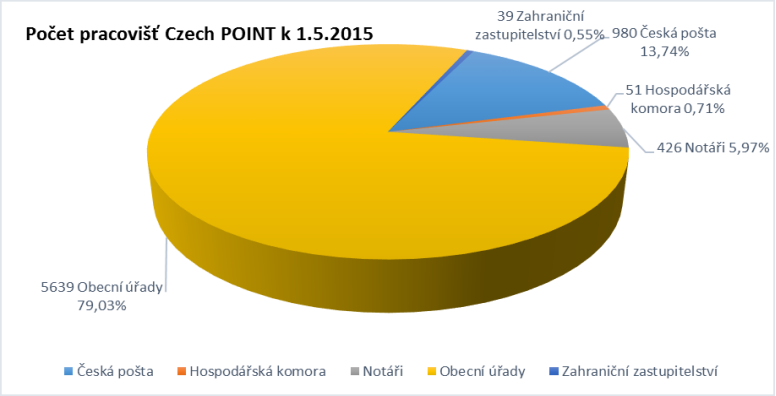
- Agendy matriky – narození, manželství, úmrtí a ostatní,
- Agendy ohlašovny. [8]

V plánu bylo zřízení dalších služeb Czech POINTu, nebyly ale zatím uskutečněny, zde jsou některé z nich s původně plánovaným rokem spuštění:

- Podání podnětu soudu, (2008),
- Info soud – výpisy, (2009),
- Potvrzení o bezdlužnosti za zdravotní pojištění, (2009),
- Potvrzení o bezdlužnosti za sociální pojištění, (2009). [8]

V roce 2009 bylo podepsáno memorandum mezi ministerstvem vnitra a Českou televizí, o zprostředkování služeb Czech POINTu v televizi. Dále mělo být z domácností dostupné portálové řešení Czech POINT@home, s vyřizováním životních událostí pomocí elektronických formulářů, zajištění rezervace pro jednání na úřadech, sledování stavu podané žádosti a dalších služeb. [7]

Nevýhodou pro domácí použití se může jevit využití formulářového řešení Software602 Form Filler systémem Czech POINT, které vyžaduje instalaci objemného programu třetí strany na počítači klienta s poměrně častou nutností aktualizací. V současné době je vyvíjena pouze varianta pro operační systém MS Windows, pro operační systémy Linux a Mac OS X jsou k dispozici na stránkách výrobce pouze archivní verze programu pro použití se zprávami datových schránek. [22]



Obrázek 8 - Počet pracovišť Czech POINT k 1.5.2015 [21]

3.4 Portál územních samospráv

Původním záměrem vzniku portálu územních samospráv bylo zřízení databáze s kontakty obecních a městských úřadů, jaké dřív spravovaly okresní úřady. V té době Svaz měst a obcí hledal podobnou aplikaci s databází stejných kontaktních dat. Při vyhledávání způsobu provedení se pak spojil s ministerstvem vnitra a za spoluúčasti Asociace krajů a Portálu města a obce online začali s realizací projektu. První pilotní projekty proběhly v kraji Vysočina a v Plzeňském kraji. Po vyhodnocení řešení byly stanoveny pravidla a funkce, které by mělo řešení obsahovat a v roce 2003 vznikla ePUSA verze 1.0, později představená jako univerzální řešení pro kraje. Postupně se do projektu zapojovaly další obce. Tehdy vznikla potřeba využít tohoto informačního systému jako zdrojového systému dat s kontakty obcí pro informační zdroje veřejné správy. Další verze již obsahovala adresářové služby s určením role pro zaměstnance obecních, městských a krajských úřadů. Při přihlášení do jednoho z propojených systémů povolí ostatní systémy autorizovaný přístup k informacím, ke kterým je oprávněn vzhledem k přidělené roli. Tento portál je propojen s registrem adres a územně identifikačním registrem ministerstva práce a sociálních věcí, rozpočty obcí ministerstva financí a Českým statistickým úřadem.

Výměna dat mezi Portálem veřejné správy, Portálem MOOL a ePUSA zaručuje, že kontakty udržované zaměstnanci samosprávy budou na ostatních místech aktuální. Portál je také využíván ke zveřejňování povinně zveřejňovaných informací. ePUSA slouží také pro automatizované zasílání informací na adresy pracovníků majících ve správě činnost dle zařazení uvedeného v systému.

Elektronický portál územních samospráv má implementováno několik způsobů funkčnosti, dle přistupujícího uživatele. Veřejnosti jsou dostupná data územně správních obvodů krajů, měst a obcí s kontakty na potřebné činnosti hledaného úřadu, včetně informací o provozní době a dalších, rozhraní je dostupné na adrese www.epusa.cz. Po autorizaci je možný přístup k editaci informací a vyhledání podrobných informací a kontaktů na zaměstnance úřadů. Díky umístění kontaktních informací pouze na tomto místě se snížila náročnost jejich udržování v aktuálním stavu. V tomto rozhraní se také nastavují informace pro propojení spisové služby s agendami Czech POINTu a další. [23]

3.5 Seznam orgánů veřejné moci

Seznam orgánů veřejné moci (Seznam OVM) vznikl na základě zákona č. 300/2008 Sb., ze 17. července 2008, o elektronických úkonech a autorizované konverzi dokumentů, díky dlouhodobé snaze o centralizaci nesourodých datových zdrojů s přívětivým rozhraním. Tvoří centrální referenční zdroj obsahující informace o organizacích státní správy a samosprávy. Agenda obsahuje detailní popis příslušného OVM, správu uživatelů organizace, adresu a provozní dobu pracovišť, adresy datových schránek, seznam registrovaných agendových informačních systémů, krizové řízení, zřizované organizace a správu agend a rolí příslušících OVM.

Součásti portálu:

- Rozhraní portálu pro veřejnost, s informacemi o orgánu veřejné moci včetně kontaktních osob, přístup přes http://www.seznamovm.cz,
- Administrace obsahu, rozhraní pro správu lokálními administrátory, přístup přes https://www.seznamovm.cz/spravadat/,
- Elektronické formulářové rozhraní umožňující změny údajů a správu lokálních administrátorů.

Veřejná část portálu umožňuje uživatelům anonymní získání potřebných informací o OVM, přehled struktury organizace, výpis kontaktních osob určených za OVM s možností vyhledání potřebných údajů.

Administrační část portálu je jedním z centrálních rozhraní, provázaným s administračním portálem ePUSA a agendovým informačním systémem Registru práv a povinností působnostní. Pro všechna tato rozhraní se používají společné přihlašovací údaje. Funkce dříve provozovaného portálu Administrace uživatelů Czech POINTu byly přesunuty na portál Seznam OVM. Seznam OVM sdílí údaje správy uživatelů pro Czech POINT, informace o orgánech veřejné moci s portálem datových schránek a je také řídícím zdrojem informací pro systém datových schránek (obrázek č. 9). [24]

V ISVS Seznamu orgánů veřejné moci jsou stanoveny následující role a práva uživatelů:

- Statutární zástupce (např. starosta), případně pověřená osoba, která má oprávnění k datové schránce, pomocí elektronických formulářů a komunikací přes datovou schránku provádí správu lokálních administrátorů a úpravu informací o OVM,

- Lokální administrátor má oprávnění správy uživatelů a osob vedených pod příslušným OVM, přidělení a správu agendových rolí pro zaměstnance OVM, správu pracovišť, agendových informačních systémů, organizací zřizovaných OVM (např. školy, příspěvkové organizace), export dat,
- Administrátor krizového řízení má oprávnění spravovat údaje o krizovém řízení OVM.

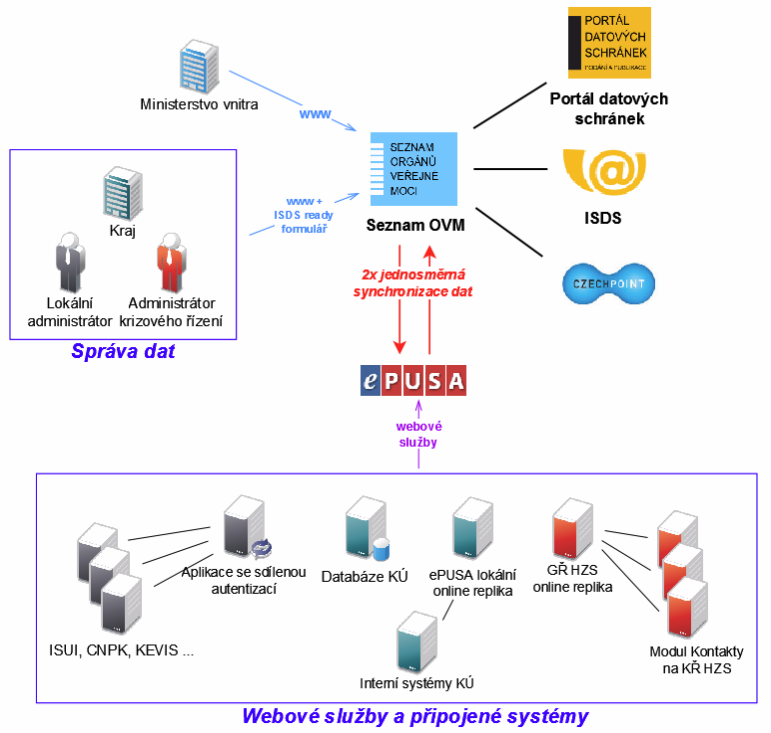
Lokální administrátor má možnost provádět úpravy následujících oblastí:

- Správa všech uživatelů v OVM,
- Určení statutárního zástupce OVM s návazností na přístup k datovým schránkám,
- Správa oprávnění k Registru práv a povinností působnostní, Czech POINTu a dalších systémů,
- Registrace certifikátů uživatelů v OVM pro přístup k jiným ISVS,
- Správa agendových informačních systémů používaných OVM,
- Určení oprávnění k činnostním rolím používaných zaměstnanci pro umožnění jejich přístupu k základním registrům,
- Editace informací o pracovištích OVM, jejich adrese a úředních hodinách,
- Oblast krizové řízení s určením složek krizového řízení OVM s kontaktními údaji a osobami určenými pro krizové řízení, registruje administátora pro krizové řízení OVM. [24]

Administrátor pro krizové řízení

- Má přístup ke správě krizového řízení OVM a všech podřízených organizací
- Udržuje strukturu krizového řízení OVM a přiřazuje kontaktní osoby krizového řízení ze seznamu všech uživatelů OVM

Pro komunikaci lokálního administrátora slouží elektronické formuláře Seznamu OVM. Jedná se o formulář pro registraci lokálního správce OVM a editaci jeho údajů, formulář editace údajů o OVM dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. Potvrzení schválení žádosti o úpravu údajů probíhá prostřednictvím systému datových schránek. [24]



Obrázek 9 – Vazby Seznamu OVM na ostatní IS [24]

3.6 Datové schránky

Počáteční legislativní specifikaci datové schránky pro komunikaci mezi občany, právními subjekty, orgány veřejné moci stanovil zákon č.300/2008 Sb., který rozšířil možnosti zasílání podání a dokumentace o elektronickou formu komunikace.

Datová schránka (DS) je prostorem pro ukládání elektronických dat (elektronické úložiště), do kterého jsou OVM zasílány datové zprávy, jsou jejím prostřednictvím uskutečňována podání orgánům veřejné moci a slouží k zasílání elektronických dokumentů fyzických, právnických a podnikajících fyzických osob. [20]

Datová zpráva má povahu elektronických dat doručovaných datovými komunikačními prostředky, lze ji uchovávat a přenášet na záznamových médiích. Datová zpráva je tvořena obsahem (hlavní zprávou a případnými přílohami) a obálkou datové zprávy. Datová zpráva umožňuje přenos elektronických podpisů a časových razítek. [25]

Výhodou tohoto systému se stala fikce doručení, kdy písemnost je považována za doručenou v okamžiku uplynutí deseti dnů od doručení do datové schránky adresáta

dostupné z adresy www.mojedatovaschranka.cz a od toho okamžiku běží zákonné lhůty pro odvolání a nabytí právní moci. Jinak je písemnost považována za doručenou v okamžiku přihlášení adresáta do datové schránky. Na adresátovi leží povinnost pravidelně kontrolovat, zda neobdržel do datové schránky nějakou písemnost. Systémem je umožněno nastavení zaslání SMS upozornění adresátovi v případě přijetí datové zprávy, ovšem tato služba je zpoplatněna. Doručené datové zprávy zůstávají v úložišti 90 dnů, které se počítají od přihlášení osoby oprávněné k obdržení zprávy. Datové zprávy doručené způsobem fikce doručení jsou uloženy na neomezeně dlouhou dobu, po uplynutí lhůty devadesáti dnů však můžou být přemístěny do off-line úložiště, odkud mohou být zase vráceny do datové schránky na žádost adresáta. Uživatelé datových schránek mají k dispozici placenou službu „Datový trezor“ kde lze datové zprávy uložit, aniž by byly smazány. [25]

Ze zákona byly datové schránky zřízeny pro právnické osoby uvedené v obchodním rejstříku či založené ze zákona a orgány veřejné moci, ostatní uživatelé z řad fyzických či právnických osob si mohli datovou schránku bezplatně aktivovat na vlastní žádost. Do roku 2012 měli dobrovolnost v užívání datových schránek notáři, insolvenční správci, exekutoři, advokáti, také daňoví poradci, poté jim byla zřízena povinně. Komunikace přes datové schránky je pro OVM povinná, v případě zaslání písemnosti adresátovi majícímu zřízenu datovou schránku standardním listinným postupem, může být považováno za neplatné. Tato povinnost má výjimku pouze v případě, že povaha zasílaných dokumentů neumožňuje použití datové schránky, což se může stát v případě např. projektové dokumentace a rozsáhlých spisů, nebo jsou předány na místě, případně doručeny veřejnou vyhláškou. [7]

Dle §11 zákona 300/2008 Sb., lze na požádání osoby, administrátora či OVM datovou schránku, která byla zřízena na žádost, znepřístupnit. Znepřístupnění a obnovení znepřístupněné datové schránky je provedeno do tří dnů od obdržení žádosti, kterou lze podat také přes pracoviště Czech POINTu. Znepřístupnění je možné s tím omezením, že pokud uživatel provede znepřístupnění dvakrát za rok, může ji znovu zpřístupnit až po uplynutí jednoho roku. Datové schránky, které byly zřízeny automaticky ministerstvem vnitra, nebo které jsou pro subjekt povinné ze zákona znepřístupnit nelze. [3]

Vyhláška č.194/2009 Sb., z 23.června 2009, o stanovení podrobností užívání, provozování informačního systému datových schránek, ve znění vyhlášky č. 422/2010Sb., určuje velikost příloh datové zprávy na maximálně 10 MB a povolené

přípony příloh. Novela vyhlášky z roku 2010 podstatně rozšířila seznam povolených příloh o nové verze a formáty projekčních kreslících programů. Elektronickou konverzi upravuje vyhláška 193/2009 Sb., ze 17. června 2009, stanovuje detaily způsobu provádění autorizované konverze dokumentů. [3]

3.7 Služby pro informační systémy veřejné správy ČR

Webový portál na adrese www.sluzby-isvs.cz spravovaný Ministerstvem vnitra ČR je určen pro přístup k informačním systémům, které jsou páteří infrastruktury pro komunikaci uvnitř veřejné správy. Patří k nim „Informační systém o informačních systémech veřejné správy“, (IS o ISVS) a „Informační systém o datových prvcích“ (IS DP). Na provoz systémů se vztahuje vyhláška č.469/2006 Sb., ze 3. října 2006, vyhláška o informačním systému a datových prvcích, vyhláška č.528/2006 Sb., z 23. listopadu 2006, o informačním systému o informačních systémech veřejné správy. Tyto systémy jsou veřejné, každý uživatel má možnost anonymního prohlížení zde uložených dat. Pro editaci vyžaduje přihlášení kvalifikovaným certifikátem.

IS o ISVS je určen pro sběr informací o ISVS a jejich dostupnosti a poskytování těchto informací. Zprovozněn byl 24.6.2008. Poskytuje přehled ISVS, jejich správců, kategorií IS, identifikátoru a data zprovoznění. Je v něm možné vyhledávat a tisknout sestavy řazené dle různých kritérií, například sestavy přehledů, nákladů ISVS, nebo tyto data exportovat.

Informačního systém o datových prvcích, který byl zprovozněn 13.4.2006, je určen pro vyhlášení datových prvků, uveřejnění číselníků a sdělení informace o datových prvcích ISVS, které jsou závazné pro provoz IS orgánů veřejné moci. Umožňuje vyhledání jednoduchých (JeDP) a složených datových prvků (SLDP) a jejich číselníků. [26]

3.8 Informační systém o státní službě

Informační systém o státní službě (ISoSS) vznikl na základě zákona 234/2014Sb., z 1.října 2014, o státní službě.

Funkčnosti ISoSS:

- Rejstřík státních zaměstnanců dle § 181 zákona 234/2014Sb.,
- Evidence obsazení služebních míst ve státní službě,
- Přihlášení k úřednické zkoušce,

- Evidence proběhlých úřednických zkoušek.

V současné době je ISoSS ve stadiu realizace projektu s probíhajícím ověřováním funkčnosti, k zahájení provozu rejstříku by mělo dojít 1.7.2015 s plnou funkčností do konce září 2015. [27]

3.9 Portál o veřejných zakázkách a koncesích

Tvůrcem portálu je ministerstvo pro místní rozvoj. Portál na adrese www.portal-vz.cz sdružuje informační systémy zabývající se výběrovými řízeními OVM a koncesemi.

Informační systémy dostupné z portálu:

- Informační systém o veřejných zakázkách (IS VZ),
- Národní infrastruktura pro elektronické zadávání veřejných zakázek (NIPEZ),
- Elektronické tržiště veřejné správy. [28]

3.9.1 Informační systém o veřejných zakázkách

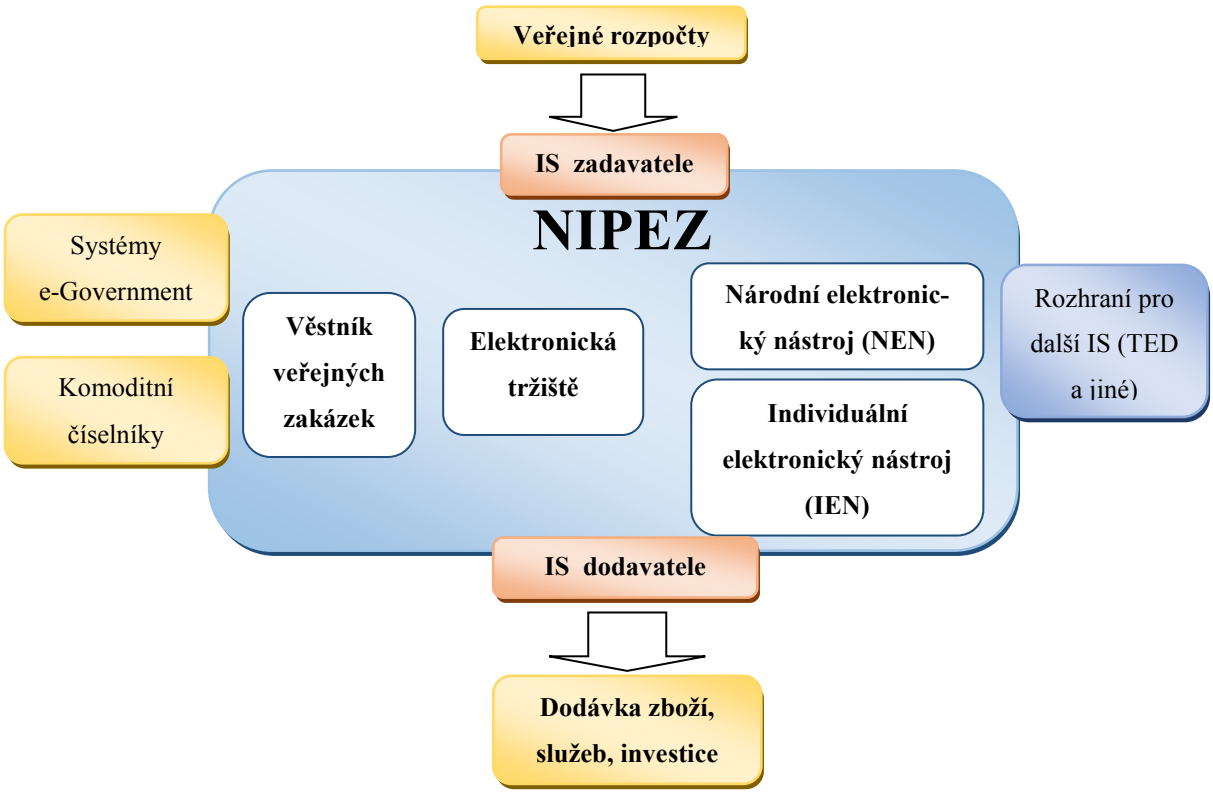
Správcem tohoto systému je Ministerstvo pro místní rozvoj. Informační systém o veřejných zakázkách (IS VZ) je provozován v souladu se zákony č.137/2006 Sb. o veřejných zakázkách a zákona č. 139/2006 Sb. o koncesních smlouvách a koncesním řízení (koncesní zákon). [3]

Tento IS VZ na adrese www.portal-vz.cz je nástupcem bývalého Informačního systému o zadávání veřejných zakázek a uveřejňování dat VZ na Centrální adrese. IS VZ zajišťuje vedení seznamu kvalifikovaných dodavatelů, věstník veřejných zakázek, seznam systémů certifikovaných dodavatelů, číselníky a klasifikace, statistické výstupy z veřejných zakázek a rejstřík koncesních smluv. Dále také obsahuje rejstříky osob se zákazy plnění veřejných zakázek, či koncesních smluv. [28]

3.9.2 Národní infrastruktura pro elektronické zadávání veřejných zakázek

V letech 2009 až 2010 vznikl návrh funkčnosti projektu národní infrastruktury pro elektronické zadávání veřejných zakázek (NIPEZ). V rámci jeho přípravy byly provedeny analýzy procesů a studie proveditelnosti, na základě které bylo rozhodnuto o realizaci projektu. Realizace probíhá v rámci „Elektronizace služeb veřejné správy“. [29]

NIZEP má za úkol zpřístupnit zadávání veřejných zakázek bez stávajícího rozšířeného najímání konzultantských firem a poradců, v současné době nezbytného pro většinu firem a úřadů, které chtějí čerpat dotace pro své projekty. Elektronickým zadáváním dojde k úsporám pro zadavatele veřejné zakázky a dodavatele. Dojde ke zvětšení transparentnosti při vypisování, zadávání a realizaci veřejných zakázek. [30]



Obrázek 10 Schéma národní infrastruktury pro elektronické zadávání veřejných zakázek [31]

Nová infrastruktura by dle předpokladu měla zajistit, aby všichni zadavatelé měli do konce roku 2015 možnost použít elektronický nástroj, který obsáhne celou délku trvání veřejné zakázky. NIPEZ (obrázek č. 10) je modulárně řešenou soustavou více informačních systémů, která obsahuje:

- Jednotný uveřejňovací systém v podobě Věstníku veřejných zakázek,
- Elektronické tržiště,
- Elektronický nástroj – Národní elektronický nástroj (NEN),
  – Individuální elektronické nástroje (IEN),
- Rozhraní pro interní IS zadavatele a dodavatele.

Rozhraní pro další IS – poskytuje propojení k jiným systémům, jedním z nich je systém Tendered Electronic Daily (TED), který je určen pro veřejné zakázky z Evropské unie a je skrze něho bezplatně zprostředkován přístup k těmto zakázkám.[31]

Národní elektronický nástroj (NEN)

Národní elektronický nástroj byl navržen pro zadavatele, kteří nemají k dispozici vlastní elektronický nástroj pro zadávání veřejných zakázek do systému *„Národní infrastruktury pro elektronické zadávání veřejných zakázek“*. Je využitelný též pro špatně standardizovatelné komodity, které by bylo problematické zadávat přes elektronická tržiště. [32]

Elektronické tržiště veřejné správy

Systém je určen pro elektronické zadání veřejných zakázek, které obsahovalo pět e-tržišť, od 6. ledna 2015 jsou zde v provozu pouze tři e-tržiště. Provoz je legislativně řešen vyhláškou č.343/ 2010 Sb., z 10.května 2010, k používání elektronických tržišť subjekty veřejné správy při vynakládání finančních prostředků ve znění usnesení vlády č. 451/2011, č. 933/2011, č. 222/2012 a č. 981/2013. [30]

3.10 Monitorovací systém evropských fondů

Monitorovací systém evropských fondů (https://mseu-sandbox.mssf.cz/index.aspx) má nahradit stávající tři systémy různých ministerstev. Zadávání žádostí o dotace přes Monitorovací systém MS2014+ bude jednodušší a poskytne stejné rozhraní místo dosud různých systémů. [33]

V dubnu 2015 bylo Ministerstvem pro místní rozvoj oznámeno, že systém je připraven k provozu, od roku 2014 již probíhá školení uživatelů veřejné správy a zájemců o dotace.

[34]

3.11 i - Server

Veřejný informační server www.i-server.cz je projektem, jehož realizace probíhala od 1.10.2008 do 30.9.2011 za finanční spoluúčasti Evropské unie. Na tomto serveru jsou dostupné informační zdroje veřejné správy s popisnými daty. Došlo zde k aplikaci výstupu z výzkumného programu, který prováděla Akademie věd České republiky *„Informační společnost“, "Výzkum procesů získávání, přenosu, uchovávání a využívání elektronických zdrojů, jednotný systém elektronické dokumentace zdrojů veřejné správy“*. [35]

3.12 Web státní správa

V roce 2000 ministr vlády vybízel při realizování státní informační politiky k větší spolupráci mezi státní správou s podnikatelskou veřejností. Jako odpověď společnosti European Business Enterprise, s.r.o. na žádost předsedy Rady vlády pro státní informační politiku byl na konci roku 2000 uveden do provozu server www.statnisprava.cz. Tento server je založen na technologii serveru www.i-server.cz.[36]

Na tomto webu je využíván CMS systém pro správu obsahu v reálném čase. Je tvořen moduly těchto aplikací: Agendy veřejné správy, zakázky v ČR, adresář veřejné správy, redakční systém, číselníky druhů úřadů a území, vyhledávání, volná místa v ČR, měření návštěvnosti, insolvence v ČR a monitoring uživatelů. [37]

3.13 Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti (NCKB) slouží pro koordinaci při návrzích postupů a nápravě konfliktů, nebo aktuálních útoků na informační infrastrukturu. Bylo zřízeno usnesením č. 781/2011 Sb., z 19. října 2011, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast, ve znění usnesení vlády č. 364/2012. Jedná se o organizační složku NBU.

NCKB má za úkol spravovat vládní CERT ČR (na adrese govcert.cz), spolupracovat s národními a mezinárodními týmy CERT a CSIRT. Pro organizace v rámci státu chystá bezpečnostní standardy, v kybernetické bezpečnosti se stará o vzdělávání a osvětu odborné veřejnosti, výzkum a vývoj nových bezpečnostních postupů.

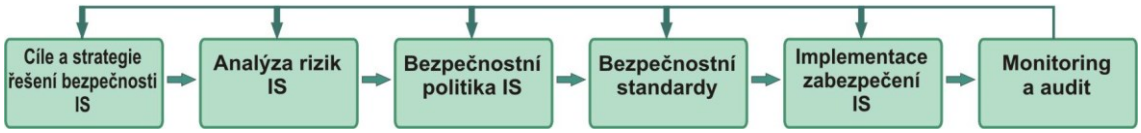
Web NCKB slouží pro veřejnost jako zdroj legislativních opatření, informační servis o aktuálních bezpečnostních hrozbách, podání informací a registraci systémů spadajících mezi kritickou informační infrastrukturu a významné informační systémy dle zákona o kybernetické bezpečnosti č. 181/2014 a nařízení vlády č. 432/2010 Sb., z 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury. [11]

4 ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Pojem bezpečnost informací v organizaci veřejné správy znamená dodržení pravidel dostupnosti informace, která musí být k dispozici autorizovaným uživatelům, důvěrnosti informace přístupné jen oprávněným uživatelům a integrity tj. úplnosti a zabezpečení verifikace informace. [20]

Bezpečný IS je ten, ve kterém jsou informace v průběhu doručení, přípravy, zpracování,vyhodnocení, uložení, tj. v průběhu všech operací, kdy je s nimi nakládáno zabezpečeny před neoprávněným přístupem. [18]

Bezpečnost informačních systémů sestává z informační bezpečnosti (obrázekč. 11), fyzického zabezpečení informačních systémů, dostatečné ochrany pomocí šifrování, zamezení možnosti odposlechu elektronických signálů, organizačních opatření, personální bezpečnosti. [38]



Obrázek 11 Schéma informační bezpečnosti [5]

4.1 Kybernetický zákon

Při řízení bezpečnosti informací se ve veřejné správě, i kdekoliv jinde řídíme platnou legislativou. Stěžejními předpisy jsou vyhlášky č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy (ISVS), zákon č. 365/2000 Sb. o informačních systémech veřejné správy (v aktuálním znění), zákon č. 181/2014 Sb, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a vyhlášky 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, vyhláškou přímo jmenované systémy jsou v příloze P III. [5]

Práva a povinnosti OVM a osob dle zákona č. 181/2014 o kybernetické bezpečnosti					
Subjekty OVM mající ve správě	**Povinnosti**				
	Nahlášení kontaktních údajů	**Detekce bezpečnostních událostí IS**	**Nahlásit bezpečnostní incidenty IS**	**Zpracovat bezpečnostní dokumentaci a zavést bezpečnostní opatření**	**Provést opatření vydané NBÚ**
Elektronické komunikace	X				
	X				X
Významné sítě	X	X	X		
	X	X	X		X
Informační systémy kritické informační infrastruktury	X	X	X	X	X
	X	X	X	X	X
Komunikační systémy kritické informační infrastruktury	X	X	X	X	X
	X	X	X	X	X
Významné IS	X	X	X	X	X
	X	X	X	X	X

Vysvětlivky: Standardní stav, stav kybernetického nebezpečí

Tabulka 2 Práva a povinnosti OVM a osob dle zákona č. 181/2014 [39]

Dalším faktorem je vztah zákona č. 240/2000 Sb., o krizovém řízení k IS provozovaných organizací dle nařízení č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení č. 315/2014. Zde je nutné posoudit, zda informační systémy provozované organizací nespadají do kategorie kritické infrastruktury, a na jejich provoz (tabulka č. 2) se nevztahují výše uvedené právní předpisy. [3] Provozovatelé informačních systémů, které spadají do kategorie významných informačních systémů mají povinnost tento systém registrovat na stránkách Národního centra kybernetické bezpečnosti (http://www.govcert.cz/cs/kii--vis/formulare/).

4.2 Normy ISVS

Bezpečnost ICT řeší též české technické normy, v oblasti řízení (managementu) bezpečnosti informací jsou to normy řady ČSN ISO/IEC 27000 – 27006 a další, uvedené v příloze P II „Technické normy pro ISVS“.[40] [41]

4.3 Systém řízení bezpečnosti

Pro řízení bezpečnosti informací můžeme využít systém řízení bezpečnosti (ISMS), který vychází z norem ČSN ISO/IEC 27001a ČSN ISO/IEC 27002. Tento systém umožňuje procesním přístupem vycházejícím z Demingova cyklu PDCA, plánuj, dělej, kontroluj a jednej, aktivně řídit rizika buď v systému řízení, nebo samostatně (příloha P IV PCDA model ISMS). [42] [43]

4.4 Cíle a strategie bezpečnosti

Určíme cíle, které potřebujeme zabezpečit vzhledem k potřebám organizace. Navrhneme tyto cíle spolu s provedením dalších fází chystané bezpečnostní politiky. Vypracujeme z nich dokument s celkovou bezpečnostní politikou organizace a rozhodnutím managementu o vypracování řízení bezpečnosti informací, která může také sloužit jako zadání na vypracování dokumentace řízení bezpečnosti informací externí organizací.

4.5 Analýza rizik IS

Úplným začátkem při tvorbě bezpečnostní politiky je provedení analýzy rizik. Je třeba zjistit, která aktiva máme chránit, a proti jakým hrozbám. Analýzou prověříme stávající úroveň bezpečnosti. Jde nám o zjištění všech slabých míst a nalezení opatření, které nám rizika pomohou snížit na přijatelnou mez. Při analýze se musíme zabývat nejenom informačním systémem a hardwarem, ale také lidským faktorem, který může být neprávem zlehčován. Výsledkem provedené analýzy je detailní zdokumentování bezpečnostní situace v organizaci. [5]

Provedení analýzy rizik by mělo objasnit:

- Následky toho, nebude-li dostatečně zajištěna bezpečnost.
- Jakým způsobem může být bezpečnost porušena.
- Jaká je pravděpodobnost vzniku této situace. [19]

Můžeme postupovat například dle prováděcí vyhlášky 316/2014 Sb., kybernetického zákona dle toho, která z částí vyhlášky je pro naši organizaci určena. Touto vyhláškou jsou dána pravidla, které informační systémy patří mezi významné informační systémy kritické infrastruktury, a obsahuje seznam IS, které byly mezi mezi významné informační systémy vyhláškou přímo zařazeny, viz příloha P III „Významné informační systémy dle přílohy č.1 vyhlášky č. 317/2014 Sb.“. [3]

- Určíme hranici systému řízení bezpečnosti informací, například jestli se bude týkat všech částí organizace, nebo jen některých poboček,
- Stanovíme použitou metodiku pro určení aktiv a rizik, hodnocení aktiv, rizik a určíme podmínky přijatelnosti rizik,
- Provedeme identifikaci aktiv, vyhodnotíme jejich důležitost a hodnotu,
- Provedeme identifikaci rizika, vezmeme v potaz zranitelnost a hrozby.Poté zvážíme jaké mohou mít dopad na aktiva, vyhodnotíme rizika (riziko = dopad x hrozba x zranitelnost), stanovíme výši přijatelného rizika a schválí jej, vypracuje dokument o vyhodnocení aktiv a rizik IS,
- Vypracujeme dle vyhodnocení rizik a bezpečnostních potřeb prohlášení o proveditelnosti, ve kterém budou uvedeny vybrané a uskutečněné bezpečnostní opatření,
- Vypracuje a zavedeme plán na zvládnutí rizik, ve kterém budou obsaženy cíle klady bezpečnostních opatření na zvládání rizika. Je třeba určit osobu která bude dbát na implementaci bezpečnostních opatření na zvádnutí rizik, termíny jejich nasazení, popíše provázanost mezi riziky a bezpečnostními opatřeními, zajišťující potřebné technické, finanční, informační a lidské zdroje,
- Zapracuje bez odkládání ochranné a reaktivní opatření, které vydá NBÚ v hodnocení rizik. Doplní plán zvládání rizik v situaci, při které překročí hodnocení rizik doplněné o nové zranitelnosti ve spojení s realizací ochranného či reaktivního opatření stanovenou výši přijatelnosti rizika. [3]

Některé z metod stanovení rizik:

- Safety Audit – bezpečnostní kontrola,
- Check List – kontrolní seznam,

- Metoda Monte Carlo – smulační metoda s využitím posloupnosti náhodných čísel,
- What – If Analysis - co se stane když,
- Preliminary Hazard Analysis (PHA) – předběžná analýza ohrožení, patří sem také:
  - HAZOP (Hazard Operation Process) – analýza ohrožení a provozuschopnosti,
  - FMEA (Failure Mode and Effect Analysis) – identifikace závažnosti a četnosti poruch,
- Stromové diagramy,
- Příčinkové diagramy,
- Ishikawův diagram,
- QRA (Process Quantitative Risk Analysis – analýza kvantitativních rizik procesu,
- UMRA (Universal Matrix of Risk Analysis) – univerzální matice rizikové analýzy,
- SWOT (Strengths, Weaknesses, Oportunities, Threats) – silné, slabé stránky, příležitosti a hrozby. [19]

Pro analýzu rizik a řízení bezpečnostní politiky je vhodné použít softwarové nástroje, které významnou měrou urychlí vypracování potřebné dokumentace, jsou to například:

- CRAMM – nástroj metodiky pro provádění systému řízení bezpečnosti informací, analýzu rizik IS a certifikaci. Podpora normy BS7799-2, ISO/IEC 27001:2005, má českou jazykovou verzi, [43]
- RAMSES – nástroj pro řízení bezpečnosti informací, podporuje normy ISO/IEC 22301, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, umožňuje import analýz z CRAMM, [43]
- CYBERWATCH dostupný na adrese www.riskwatch.com,
- COBRA dostupný na adrese www.riskworld.net, podpora ISO 17799,
- NETRECON,
- RISKPAC dostupný na adrese www.csciweb.com
- @RISK dostupný z adresy www.palisade.com [5]

Programy většinou disponují organizace, jejich náplní je provádění bezpečnostní analýzy a bezpečnostní politiky ostatních firem, či OVM, nálady na pořízení programu jen pro své vlastní využití mohou být pro malou firmu, či OVM neúnosné. V takových případech je výhodnější na základě výběrového řízení vybrat externí organizaci, která bezpečnostní politiku organizace zpracuje, včetně potřebné dokumentace a případně též provede, nebo zajistí provedení auditu bezpečnosti informací organizace.

Výhodami kvalitně provedené bezpečnostní analýzy jsou:

- Uchránění dobré pověsti organizace před možností zveřejnění úniku citlivých dat,
- Zvýšená důvěryhodnost organizace,
- Ochrana vývoje před konkurencí,
- Chrání stabilitu organizace,
- Chrání organizaci před vnějším průnikem do IS,
- Ochrana informací,
- Umožní rozpoznat podezřelé situace v IS,
- Je vypracován postup pro případ závady HW, SW, či jiných zařízení. [5]

4.6 Bezpečnostní politika

Bezpečnostní politika informačního systému organizací veřejné správy je dokument obsahující souhrn bezpečnostních zásad, pravidel, cílů, potřeb, opatření, povinností a práv provázaných s řízením bezpečnosti informací. Tento dokument je po schválení managementem organizace závazný.

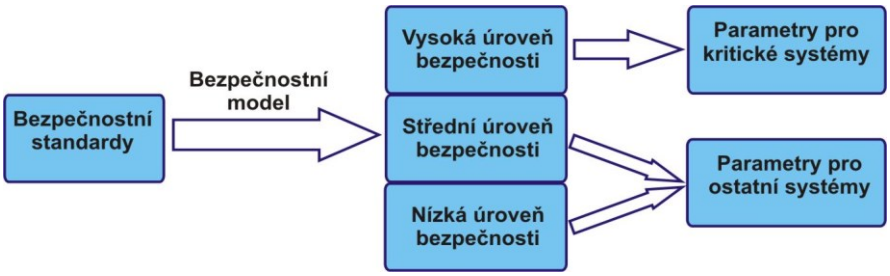
- Organizace stanoví hlavní cíle ochrany informací,
- Určí možnosti řešení bezpečnosti IS,
- Stanoví pravomoci a odpovědnosti dotčených osob. [5]

4.7 Bezpečnostní standardy

Bezpečnostní standardy tvoří závazné interní dokumenty organizace. Jsou v nich do detailů rozebrány a specifikovány postupy a pravidla vyplývající z dokumentace bezpečnostní politiky ISVS. Měly by zde být zachyceny všechny stránky organizace ovlivňující bezpečnost. Bezpečnostní politika na rozdíl od bezpečnostních standardů tvoří dokument se stálejším charakterem. Bezpečnostní standardy naproti tomu procházejí úpravami, aby byly schopny zachytit vývoj bezpečnostních hrozeb a rizik. Reagují také na změny právních předpisů, které v oblasti informačních systémů veřejné správy procházejí neustálým vývojem.

Pro zajištění ochrany aktiv způsobem odpovídajícímu míře rizika a tomu adekvátnímu vynaložení prostředků je vhodné vytvoření bezpečnostního modelu (obrázek č. 12). Pro každé aktivum je vyhotoveno ohodnocení důležitosti, zhodnocení hrozby a její pravděpodobnosti a posouzení jak jsou uživateli aktiva používána a chráněna. Získáme tak rozdělení hrozeb se zřetelem na jejich důležitost pro organizaci. Díky tomu budeme moci nastavit bezpečnostní kontrolní zajištění dle důležitosti a kritičnosti. Důležité je správné nastavení odpovědnosti, můžeme stanovit tři uživatelské skupiny: uživatele, operátory a administrátory, nebo z jiného hlediska vlastníky, správce a uživatele informací.

Mezi standardy je nutné zahrnout také technické standardy pro všechny platformy: monitoring, audit a logování událostí, provoz a údržba systémů, konfigurace systémů, přístup k technice, vzdálený přístup, zálohování, obnova, používání hesel, řízení práv, administrace bezpečnosti. Vypracované standardy a směrnice jsou pro organizaci závazné.



Obrázek 12 Aplikace bezpečnostního modelu [38]

4.8 Implementace bezpečnosti

Pro implementaci bezpečnosti je potřeba zabezpečit s podporou managementu zahájení bezpečnostních projektů, kterými uvedeme do užívání bezpečnostní standardy, postupy a směrnice. Provádíme je formou bezpečnostního vzdělávání a havarijního plánování v organizaci, spolu se zodpovědností za jejich dodržování. [38]

4.9 Monitorování a audit

Pro správnou implementaci bezpečnostní politiky je nutné monitorovat a zajistit dodržení bezpečnostních standardů a směrnic. Je třeba mít zpětnou vazbu, která umožní při případných změnách či odchylkách od schválených směrnic a postupů zahrnout tyto změny do dokumentace a řízení bezpečnosti. Pravidelné zapracovávání změn do stávajících směrnic je nezbytné, v opačném případě dojde ke zvýšení rizik a později by jsme byli nuceni začít celý proces od počátku. [5]

V případě, že se na naši organizaci vztahuje zákon o kybernetické bezpečnosti č. 181/2014 Sb., z důvodu provozu významného informačního systému, jsme povinní zajistit nejméně jednou ročně provedení auditu kybernetické bezpečnosti. Audit je v případech, kdy je vyžadováno podání výsledků třetí straně vhodné nechat vypracovat externí společností. U ní je zajištěno nestranné posouzení informační bezpečnosti. [5]

Pro vlastní účely zprávy pro vedení organizace můžeme provést vnitřní audit organizace, kdy se zaměříme na tyto oblasti:

- Postup budování bezpečnosti,
- Vývoj systémů a změny programů.
- Kontrola a komentáře k bezpečnostní politice, předpisům a standardům,
- Zabezpečení sítí a vzdáleného přístupu do sítě. [45]
- Kontroly operačních systémů. [5]

4.10 Informační strategie

Obsahuje definici koncepce rozvoje ISVS v příštích letech, tak aby byly zabezpečeny procesy potřebné pro chod organizace a její cíle v příštích obdobích. Informační analýza se skládá z:

- Analýzy výchozího stavu IS,
- Cílového stavu IS,
- Postupu rozvoje do cílového stavu.

Informační strategie tvoří základní nástroj pro systémovou integraci. Navazuje na ni analytická, projektová a realizační dokumentace jednotlivých projektů. [5]

4.11 Informační koncepce

Informační koncepce je dokumentací, v níž jsou stanoveny dlouhodobé cíle organizace v oblastech řízení informačních systémů. Její obsah je dán vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy a komentářem k této vyhlášce. V informační koncepci jsou zahrnuty všechny organizací spravované ISVS, pro které jsou určeny dlouhodobé cíle v dosažení bezpečnosti a řízení kvality, pravidla pro nákup, vývoje a provozu.

- Obsahuje základní údaje organizace,
- Základní údaje o informační koncepci,
- Údaje o dřívějších verzích,
- Zdroje a východiska – přehled zdrojových dokumentů pro tvorbu informační koncepce,
- Legislativní rámec,
- Seznam využívaných ISVS a provozních agend propojených s ISVS,
- Plány na pořízení ISVS,
- Řízení kvality ISVS,
- Řízení bezpečnosti ISVS,
- Vyhodnocení dodržování informační koncepce,

- Postupy při zavádění změn
- Financování IS
- Odpovědnost za dodržování informační koncepce. [5]

4.12 Provozní dokumentace

Provozní dokumentace se skládá ze systémové příručky, příručky uživatele a bezpečnostní dokumentace. Dále ji tvoří bezpečnostní směrnice a v případě vazby na ISVS jiné organizace bezpečnostní politika ISVS. Provozní dokumentace je většinou vypracovávána pro každý ISVS samostatně. Skladba je určena vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy a komentářem k této vyhlášce. [26][44]

Jsou v ní uvedeny realizované bezpečnostní opatření a dokumentace bezpečnostních mechanizmů. [5]

Skladba provozní dokumentace:

- Bezpečnostní dokumentace informačního systému veřejné správy – směrnice činností bezpečnostního správce IS a bezpečnostní politika,
- Systémová příručka – funkce pro administraci ISVS, popis ISVS, definice uživatelů, oprávnění uživatelů a pravidel pro administraci ISVS.
- Uživatelská příručka – funkce ISVS pro uživale, popis ISVS, oprávnění uživatelů a kategorií uživatelů a pravidel pro používání ISVS. [44]

4.13 Atestace ISVS

Orgány veřejné správy mají dle zákona č. 365/2000. Sb. povinnost zpracovat informační koncepci, provádět ji a sledovat a průběžně hodnotit její plnění. Další nutnou dokumentací pro získání atestu je provozní dokumentace. Atestace se skládají z částí „Atest dlouhodobého řízení ISVS“ a „Referenční rozhraní“.

Dodržování této zákonné povinnosti se prokazuje v atestačním řízení, po jehož proběhnutí organizace obdrží Atest dlouhodobého řízení ISVS od akreditovaného atestačního střediska s pětiletou platností. Tento atest je dle zákona nutný pro OVM a obce II. A III.

typu, obce I. typu s přenesenou působností nemusí mít atest, ale musí mít vypracovánu informační koncepci. [46]

Atestace dlouhodobého řízení je získána po kontrole kompletnosti provozní dokumentace a informační koncepce, posouzení jejich srozumitelnosti, přehlednosti a logické skladbě, jejich kvality, monitoringu plnění a zpětné vazby přijímáním nápravných opatření.

Atestace referenčního rozhraní znamená kontrolu kompatibility s jinými IS ohledně možností komunikace pomocí referenčního rozhraní. Posuzuje se shoda provedení vazby s dokumentací a funkcí služby, dostupnost ISVS do IS o ISVS, soulad prvků při komunikaci a zabezpečení služby s rozsahem oprávnění k přístupu. [47]

II. PRAKTICKÁ ČÁST

5 INFORMAČNÍ STRATEGIE

Tato dokumentace informační strategie byla zpracována na příkladu stávajícího skutečného IS městského úřadu, se zapracováním údajů týkajících se provozních systémů. Některé z těchto údajů však byly v nezbytné míře pozměněny z důvodu zachování bezpečnosti provozovaných informačních systémů a agendového informačního systému.

Prvotním materiálem pro definování Informační strategie je stanovení, jaké jsou cíle města. Cíle jsou formulovány v programu rozvoje města schválenému zastupitelstvem a jsou zároveň s výkonem základních činností MěÚ v oblastech státní správy v přenesené působnosti a samosprávy ohraničením činnosti úřadu v nejbližší budoucnosti, většinou se jedná o časový horizont volebního období. Ze základních cílů jsou určeny ty, u kterých je možné pomoci k jejich splnění prostředky IS, a ty jsou ve strategii dále přiblíženy a rozpracovány. Potřeby jednotlivých odborů MěÚ jsou převedeny na požadavky, které jsou zapracovány do informační strategie, stejně jako konkrétní požadavky z kontrol aktuálního stavu IS a splnění starších strategických dokumentů.

Významnými přínosy vypracování Informační strategie je považováno:

- Stanovení rámce a požadavků pro informační systémy,
- Zjištění stávajícího stavu, zvlášť parametrů všech ICT projektů,
- Stanovení cílového stavu v segmentu informačních systémů,
- Určení přesného postupu přeměny do cílového stavu.

Možnosti začlenění hlavních ICT projektů lze určit dle vytvořeného přehledu organizačních částí a procesů, datových skupin, projektů a jejich následného zpracování pro definování celkové architektury IS s integraci jednotlivých subsystémů.

Tato dokumentace je postavena na skutečném provozovaném informačním systému Městského úřadu.

Smyslem dokumentu studie „Informační strategie„ je definice způsobu a směru, kterým by se měly výhledově rozvíjet a používat informační technologie v Městském úřadu (dále jen MěÚ) v letech 2015 – 2020, aby bylo možné v plné míře podpořit cíle a s nimi související procesy MěÚ.

Hlavní součástí dokumentu jsou informace obsažené v částech:

- Výchozí stav, analýza IS MěÚ,

- Cílový stav,
- Přeměna do cílového stavu.

Dokument „Informační strategie“ plní též další funkce, jsou to:

- Hlavní prostředek systémové integrace,
- Dokument, který bude podkladem pro analytické, implementační a projektové dokumentace projektů.

5.1 Zdroje a východiska

5.1.1 Přehled zdrojů použitých pro Informační strategii

Informační systém Městského úřadu (dále jen MěÚ) náleží dle zákona č.365/200 Sb., o ISVS, mezi informační systémy veřejné správy. IS je v současnosti ve stádiu provozu, správy a dalšího vývoje. Vznikal od roku 2001, od té doby byl a je vyvíjen dle aktuálních právních předpisů, potřeb a požadavků jednotlivých odborů a vedení úřadu. Změny IS jsou prováděny také s ohledy na technologický rozvoj v informačních technologiích a se zřetelem na finanční možnosti rozpočtu města.

Ze základních právních předpisů ČR v je pro provoz ISVS nejdůležitějším zákon č. 365/ 2000 Sb., o informačních systémech veřejné správy, ve znění dalších zákonů, následují právní předpisy, jejichž podrobný seznam je v příloze P I „Právní předpisy pro ISVS“.

Důležitými dokumenty a projekty z celostátního měřítka jsou:

- Státní informační a komunikační politika,
- Národní program počítačoví gramotnosti,
- Národní strategie informační bezpečnosti ČR,
- Program informatizace územních orgánů místní samosprávy,
- Základní registry veřejné správy,
- Komunikační infrastruktura veřejné správy,
- Portál veřejné správy,
- Czech POINT,

- Portál územních samospráv
- Seznam orgánů veřejné moci,
- Národní centrum kybernetické bezpečnosti.

Informační strategie má brát ohled na informační strategie a strategické dokumenty vyšších organizačních celků. Dalšími dokumenty, které je třeba brát v úvahu jsou strategické dokumenty EU, které se týkají informačních technologií. Tato dokumenty mohou být důležité při realizaci projektů, z hlediska získání finančního zajištění dotacemi, nebo metodikami pro zřizování informačních systémů.

Informační strategie vychází především z dokumentů:

- Program rozvoje města + Strategický plán rozvoje města 2009 - 2016
- Strategický plán rozvoje města 2015 – 2020

5.2 Charakteristika a cíle informační strategie MěÚ

Zadáním informační strategie ukázání výhledu, hodnoty a cílů budoucnosti IS a informačních technologií MěÚ, najít řešení realizace, stanovit přechod ze stávajícího řešení k plánovanému IS a informačním technologiím. Informační strategie vyhodnocuje stávající situaci v oblasti IT a navrhuje možnosti pro další rozvoj v této oblasti.

Informační strategie má za cíl:

- Navrhnout postup realizace koncepce budování IS, která napomůže MěÚ efektivně dosahovat cílů pomocí IS,
- zajištění souvislého a bezproblémového chodu IS za pomoci jednotných postupů, práv a povinností danými interními směrnicemi MěÚ,
- navrhnout pracovní činnosti a agendy převeditelné na počítačové zpracování, pravidla rozvoje a realizace informační podpory s ohledem na současné a příští možnosti informačních technologií.

Informační strategie je ve shodě s platnými právními předpisy, bere ohled na finanční možnosti a technologický rozvoj v oblasti IT. Základním podkladem pro informační strategii je stanovení cílů města. Cíle jsou většinou formulovány v programu rozvoje města schváleného zastupitelstvem a jsou s výkonem základních činností MěÚ v oblasti státní

správy v přenesené působnosti a samosprávy hranicemi pro činnost MěÚ v dalších letech. Z těchto cílů jsou poté vybrány ty, jejichž splnění lze podpořit prostředky IS, a tyto jsou v informační strategii jmenovány a rozvíjeny, cíle informační strategie také počítají s konkrétními požadavky a potřebami odborů úřadu.

5.3 Závěr globální strategie, poslání a cíle

Informační strategie je pokračováním globální strategie, která obsahuje smysl a cíl všech činností MěÚ. Počítá s legislativou vymezující oblasti výkonu státní správy a samosprávy.

Poslání úřadu

Je formulací objasnění důvodu existence MěÚ, vysvětluje jeho hlavní smysl. Poslání by mělo být podporováno všemi zaměstnanci a pro jeho naplnění by měli věnovat veškerou činnost. Poslání MěÚ je:

- Podpora činnosti místní samosprávy zahrnující správu a rozvoj města,
- Výkon státní správy v přenesené působnosti v určeném správním obvodu.

Cíle MěÚ

- Zkvalitnění služeb poskytovaných občanům,
- Zvýšení efektivnosti a produktivity MěÚ,
- Urychlení komunikace mezi MěÚ a OVM,
- Zlepšení stavu v oblasti bezpečnosti a pořádku, dopravy, životního prostředí, bydlení, územního rozvoje, školství a volnočasových aktivit.

Faktory ovlivňující naplnění poslání MěÚ

- Lidský kapitál, pracovníci úřadu,
- Kvalita řízení MěÚ, efektivita a odpovědnost,
- Transformace vytyčených cílů do měřitelných úkolů na dané období,
- Stabilizovaná finanční situace, finanční prostředky na investice,
- Přístupnost ke změnám,
- Legislativní podmínky,
- Kvalita IS pro podporu dosažení cílů,

- Bariéry mezi MěÚ a občany.

5.4 Legislativní rámec ISVS

Vývoj informačních systémů pro oblast veřejné správy musí respektovat několik hlavních souborů požadavků či doporučení, které pocházejí z různých zdrojů. Některé z nich jsou určeny legislativními předpisy a další dokumenty mají jen povahu doporučení, avšak potřebnost a autorita z nich většinou vytvořily standardy, jejichž dodržování při tvorbě IS je doporučeno z následujících důvodů:

- Zvýší se zhodnocení IS,
- Vytvoří kladný obraz informačního systému,
- Zvětší využitelnost těchto IS,
- Sníží finanční náklady na provoz systému a podporu uživatelů.

Všechnu legislativu, postupy či doporučení pro zřízení informačních systémů ve veřejné správě můžeme rozdělit na:

- Legislativní předpisy (zákony, jejichž dodržení je nařízeno právním předpisem),
- Metodické pokyny a všeobecně uznávané standardy,
- Doporučení konsorcia W3C (standard WWW aplikací),
- Přístupnost pro handikepované (standard WWW aplikací).

Legislativa ČR v oblasti informatiky pro provozování ISVS v oblasti státní správy a samosprávy:

Zákon č. 365/2000 Sb., ze 14. září 2000, o informačních systémech veřejné správy ve znění dalších zákonů,

Zákon č. 148/1998 Sb., z 11. července 1998, o ochraně utajovaných skutečností, ve znění dalších zákonů,

Zákon 181/2014 Sb., z 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů. [3]

Přehled všech relevantních právních předpisů je uveden v příloze P I „Právní předpisy pro ISVS“.

Bezpečnost ICT řeší též české technické normy, v oblasti řízení (managementu) bezpečnosti informací jsou to normy řady **ČSN ISO/IEC 27000 – ČSN ISO/IEC 27006** a další. Přehled všech relevantních norem je uveden v příloze P II „Technické normy pro ISVS“.

5.5 Metodické pokyny

Katalog datových prvků ISVS

V katalogu datových prvků ISVS je uložen sumář obsahující jednoduché a složené datové prvky katalogizované v ISVS. Využití datových typů v ISVS ve shodě s katalogem zajišťuje, že i v budoucnu bude provozovatel IS schopen komunikace s dalšími ISVS. Doporučení kontroly a provedení případné nápravy.

5.6 Doporučení konsorcia W3C

Činnost konsorcia W3C spočívá ve správě standardů webu a řešení k tomu patřících technických problémů. Dokumenty W3C jsou pouze doporučeními, ale autorita a respekt z nich činí standard. Dodržení standardů W3C doporučujeme, tvůrci webu tak mohou předejít budoucím problémům. Kvalitní kód zvyšuje užitnou hodnotu webu, zajistí korektní a rychlé zobrazení stránky.

5.7 Přístupnost pro handikepované – Blind friendly

Podle odhadů žije v ČR kolem 100 000 občanů s těžkým zrakovým postižením, kteří jsou odkázáni při práci s výpočetní technikou používat speciální zařízení jako SW lupy, nebo zařízení s hlasovým či hmatovým výstupem. Z tohoto důvodu by měli autoři webových stránek s tímto omezením počítat a respektovat pravidla Blind friendly V ČR se této problematice věnuje občanské sdružení SONS (Sjednocená organizace nevidomých a slabozrakých). Tato organizace provozuje projekt Blind friendly web (http://www.blindfriendly.cz), na kterém jsou publikována základní pravidla přístupnosti. Pravidla jsou rozdělena dle priority nutnosti použití.

5.8 Výchozí stav, analýza IS

5.8.1 Přehled podpory ICT dle organizačních jednotek

Předmět	**Počet**	
Celkový počet zaměstnanců	30	
Celkový počet odborů	7	
Celkový počet PC a NB	42	
Celkový počer serverů, včetně virtualizovaných	7	
Odbor	**Zaměstnanci**	**PC a NB**
VED	2	2
OHS	5	6
OKŠCRS	6	13 (z toho 7 pro veřejnost)
OSMŽP	4	5
OFI	5	6
OIÚP	4	5
SÚ	2	2
MP	2	3
Poměr PC a NB kpočtu zaměstnanců	1,17 PC nebo NB na 1 zaměstnance (při zahrnutí PC pro veřejnost je poměr 1,4 PC nebo NB na 1 zaměstnance)	
Poměr PC a NB k počtu serverů	6 PC na jeden server	

Tabulka 3 Přehled podpory ICT dle organizačních jednotek [Zdroj:vlastní]

5.8.2 Globální architektura IS

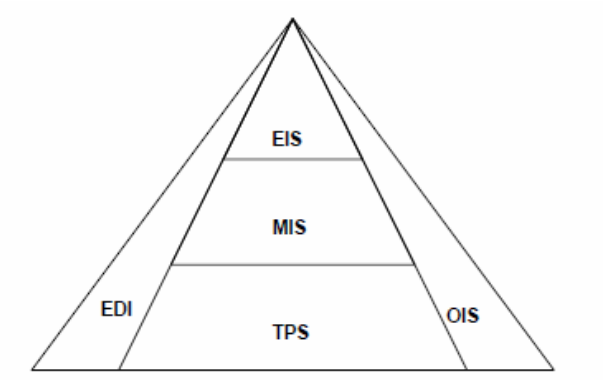
TPS – podpora hlavní činnosti úřadu na operativní úrovni (odbory operativního řízení a provozu)

MIS – řízení na taktické úrovni (ekonomické, obchodní a organizační hledisko)

EIS – strategické řízení (informace se získávají z ostatních vrstev, výstup má roli v rozhodování)

OIS – podpora kancelářských prací a týmové práce

EDI – zajištění komunikace s okolím



Obrázek 13 Globální architektura IS

[Zdroj:vlastní]

Dle globální architektury (obrázek č.13) je budován informační systém MěÚ. Přehled SW náležícího ke globální architektuře IS je uveden v kapitole Informační koncepce MěÚ.

5.8.3 Servery a klienti v ISVS MěÚ

Seznam všech serverů úřadu a jejich stručná charakteristika

Název serveru	**INT**
Účel, funkce	Poštovní a internetový server
Operační systém	OS Debian GNU Linux
SW	Webmail, antivir, antispam, vzdálený přístup
HDD	80 GB
CPU	Intel Core Duo 2GHz
RAM	512 MB

Tabulka 4 Popis serveru INT [Zdroj:vlastní]

Název serveru	**DATA**
Účel, funkce	Datové úložiště MěÚ
Operační systém	Virtualizovaný OS Debian GNU Linux
SW	Proxmox, Codexis, Mysis, Genero (IS VERA)
HDD	RAID 10 4x 300GB
CPU	Intel Xeon 5050 3GHz/667MHz/4MB
RAM	10 GB

Tabulka 5 Popis serveru DATA [Zdroj:vlastní]

Zbývající tabulky jsou uvedeny v příloze P V Servery ISVS a jejich charakteristika.

Charakteristika a počty klientů na MěÚ

Tenký klient (terminál) - počet	0
Tlustý klient (standardní PC/NB) - počet	42
Převažující operační systém	MS Windows 7 Professional
Termín pořízení	2004-2015
Minimální HW konfigurace	Intel Celeron, 2GHz, 1GB RAM, 80GB HDD
Maximální HW konfigurace	Intel Core i5-4590 CPU 3.30GHz, 8GB RAM, 120 GB SSD, 1TB HDD
Nejčastější HW konfigurace	Intel Core 2, 2,5 GHz, 4GB RAM 500 GB HDD

Tabulka 6 Charakteristika a počet klientů na MěÚ [Zdroj:vlastní]

5.8.4 Topologie sítě

Ve schématu sítě jsou vyznačeny jednotlivé budovy úřadu, jejich adresa, vyznačeny komunikační kanály, všechny vstupy a výstupy mimo úřad, jsou zde zakresleny základní síťové prvky, jejich propojení a základní technické parametry. U schématu sítě MěÚ v příloze P VI jsou z důvodu zabezpečení skryty IP adresy.

5.8.5 Stávající významné ICT projekty a jejich charakteristika

1) **Projekt :** Rekonstrukce objektu Kulturního domu

   Dodavatel: CGM, a.s.

   Zahájen / dokončen: Zahájeno 2.pololetí 2011/ Dokončeno 1.pololetí 2015

   Fáze projektu: Probíhá dokončovací fáze projektu

   Popis: V rámci projektu se řeší připojení historické budovy, na vysokorychlostní internetovou konektivitu o dostatečné kapacitě. Propojení bude realizováno optickými kabely, zároveň bude realizací zajištěno připojení odloučených pracovišť MěÚ k počítačové síti a informačním systémům MěÚ.

   Základní vlastnosti: Optická kabeláž mezi budovami, aktivní prvky, převodníky 1000MBit WDM

2) **Projekt:** Veřejné informační služby knihoven – informační centra veřejných knihoven

Dodavatel: AutoCont, a.s.

Zahájen / Dokončen: Přípravné práce zahájeny ve 2. pololetí roku 2013, dokončeno 12.2014

Fáze projektu: Dokončeno.

Popis: Nové HW a SW vybavení poslouží k plynulému přístupu ke knihovnickému systému Clavius pro čtenáře v knihovně a uživatele webového rozhraní knihovny. Byly zřízeny 4 nově vybavené pracoviště veřejného internetu o rychlosti 20MB/s. Zároveň s realizací byl pořízen přípojný WiFi bod pro přístup k internetu a knihovním službám v prostorách budovy v pásmech 2,4 a 5 GHz a knihovna vybavena multifunkčním kopírovacím zařízením formátu A3 připojeným na datovou síť.

Základní vlastnosti: Rozšíření pracovišť veřejného internetu a připojení ke knihovním službám v nových prostorách knihovny.

5.9 Ekonomická rozvaha

Rozpočty (v tis.Kč)

Rok	Provozní náklady na ICT	Investiční náklady na ICT	Celkem náklady na ICT	Rozpočet města (jedná se o upravený rozpočet vždy na konci roku)
2010	543,74	1444,53	1988,27	171 174,00
2011	540,24	1343,90	1884,14	74 562,80
2012	435,80	715,96	1151,76	66 631,40
2013	472,51	698,86	1171,37	73,742,00
2014	476,50	524,38	1000,88	125,542,52
2015	469,12	861,11	1330,22	

Tabulka 7 Rozpočty ICT [Zdroj:vlastní]

Významné dotace do rozpočtu, které by mohly zkreslit průměrné hodnoty

Rok	Provozní náklady	Investiční náklady	Celkem
2010	0	98,77	98,77
2011	0	0	0
2012	0	0	0
2013	0	0	0
2014	0	16,84	19,84
2015	0	24,00	24,00

Tabulka 8 Významné dotace do rozpočtu [Zdroj:vlastní]

5.9.1 SWOT analýza

SWOT analýza (tabulka č. 9) identifikuje hlavní vlivy na vybudování a provoz IS, jsou pomocí ní určeny silné (Strenghs) a slabé (Strengths) faktory IS, příležitosti (Oportunities) a hrozby (Threats) IS MěÚ. Výsledky této analýzy jsou použity na upřesnění kritických oblastí IS.

Zaměstnanci provedli posouzení důležitosti a určení silných a slabých stránek faktorů uvnitř MěÚ.

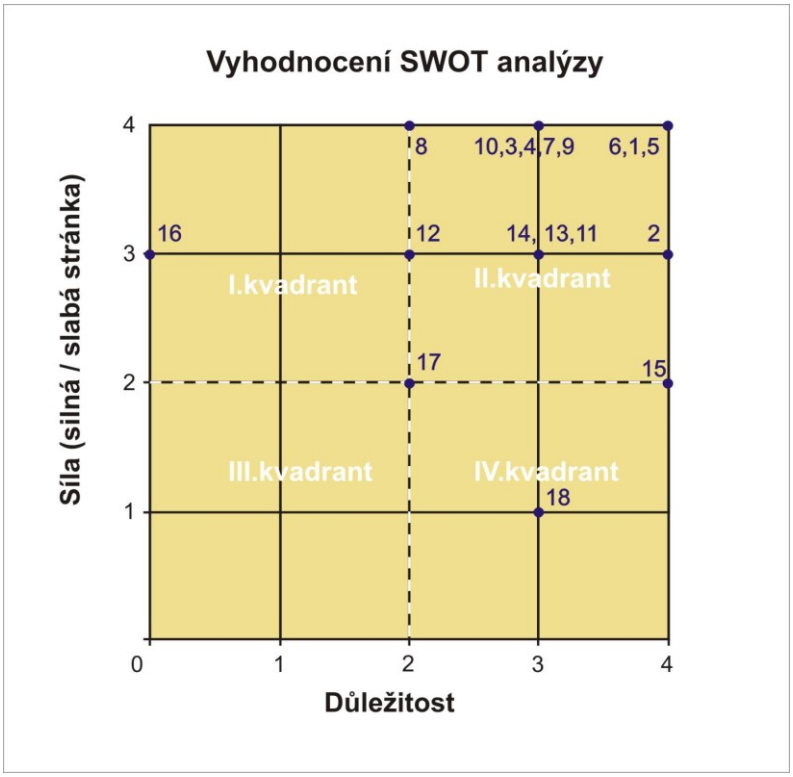
SWOT analýza		
Interní faktory s možností ovlivnění	**Silné stránky (+)**	**Slabé stránky (-)**
	• podpora rozvoje ICT od vedení MěÚ • dobrý základ infrastruktury sítí • velký počet PC na zaměstnance MěÚ • použití stejného kancelářského SW (MS Office) • zaměstnanci vyškolení v IT • vysoké využití IT v činnostech MěÚ • definice základních pravidel v IT • internetové stránky jako prostředek komunikace • vlastní provoz a rozvoj IS • koordinované řízení rozvoje informatiky (globální strategie města, informační strategie úřadu) • malý podíl agendového přístupu v aplikacích IS (nízká duplicita a nekonzistence dat) • projektové řízení • komunikace mezi odbory MěÚ • systém školení uživatelů IT	• nedostatek finančních prostředků pro rozvoj IT • absence metadat (dat o datech) – nepřehlednost dat používaných na MěÚ • různorodost aplikačního SW • omezené možnosti odměňování zaměstnanců v oblasti IT ve srovnání s komerční sférou

Externí faktory bez možnosti ovlivnění	Příležitosti (+)	Hrozby (-)
	• existence celostátních projektů se snahou o koncepční řešení ISVS • snaha o minimalizaci legislativních a koncepčních nedostatků v ISVS v celostátním měřítku • rozšířená nabídka nových IT • vysoká nabídka široké škály komunikačních kanálů	• pomalá a nejasná realizace celostátních projektů v IT • protichůdná a nekonzistentní legislativa • nemožnost konkurence v nabídce pracovních míst v IT komerční sféře • nejednoznačná odpovědnost a kompetence OVM v oblast správy dat a IT

Tabulka 9 SWOT analýza [Zdroj:vlastní]

V tabulkách přílohy P VII jsou faktory seřazeny podle důležitosti, poté následuje seřazení dle síly faktoru. Hodnoty faktorů pro důležitost jsou zadány od 0 do 4, kde 0 označuje nejméně a 4 nejvíce důležitý faktor pro rozvíjení a provoz IS. U hodnoty pro sílu faktoru 0 znamená velmi slabou stránku současného IS, 4 nejsilnější stránku.

Po zanesení faktorů do grafu dostaneme vyhodnocení SWOT analýzy, na faktory kvadrantu IV je potřeba se v budoucnosti zaměřit, protože jsou důležité a zároveň jsou slabou stránkou. Faktory kvadrantu II jsou v pořádku, ty je třeba udržet, faktory v kvadrantu I zvážíme a ty v kvadrantu III můžeme pokládat za málo významné.



Tabulka 10 Vyhodnocení SWOT analýzy [Zdroj:vlastní]

Faktory, které zasluhují pozornost jsou:

č.15 nedostatek finančních prostředků pro rozvoj IT,

č.18 omezené možnosti odměňování zaměstnanců v oblasti IT ve srovnání s komerční sférou.

Faktory, které je nutné udržet:

č.2 dobrý základ infrastruktury sítí,

č.6 vysoké využití IT v činnostech MěÚ,

č.1 podpora rozvoje ICT od vedení MěÚ,

č.5 zaměstnanci vyškolení v IT,

č.14 systém školení uživatelů IT,

č.13 komunikace mezi odbory MěÚ,

č.11 malý podíl agendového přístupu v aplikacích IS,

č.10 koordinované řízení rozvoje informatiky,

č.3 velký počet PC na zaměstnance MěÚ,

č.4 použití stejného kancelářského SW (MS Office),

č.7 definice základních pravidel v IT,

č.9 vlastní provoz a rozvoj IS.

5.10 Cílový stav

5.10.1 Vize a cíle IS

Informační strategie počítá s tím, které činnosti MěÚ vykonává, určuje priority při řešení problémů a navrhuje postupy. Hlavním účelem IS je podpora správy a provozu MěÚ, dalšího růstu města a výkonu státní správy v přenesené působnosti a samosprávy.

Základním významem IS je:

- podpora správy MěÚ,

- podpora činností MěÚ,
- podpora činnosti státní správy v přenesené působnosti,
- podpora funkčnosti místní samosprávy,
- podpora komunikace mezi MěÚ a občany,
- podpora spolupráce mezi organizacemi zřízenými MěÚ,
- podpora spolupráce mezi MěÚ a OVM.

5.10.2 Základní požadavky na IS

MěÚ má umožněno implementovat libovolný vhodný IS a není v tomto ohledu nijak významně limitován nadřízenými subjekty. Stejný předpoklad je i v budoucnosti, zatím není reálný vznik nějakého jednotného IS pro všechny OVM. Dnes je pro MěÚ povinnost zajištění kompatibility svého IS s okolními ISVS po stránce funkční (např. přístup k registrům VS), technologické a komunikační, všechno v rámci platné legislativy. MěÚ by měl nejdříve udělat procesní optimalizaci, případně reorganizaci s ohledem na informační toky a teprve na jejím základě vybudovat IS dle potřeb s ohledem na místní finanční možnosti. V případě, že by nedošlo k počáteční procesní optimalizaci, je nebezpečí, že dojde k zachování procesů se všemi neoptimalizovanými procesy a nebude možné plně využít možností růstu efektivity. Z důvodu že neexistuje ideální řešení je třeba, aby procesní reorganizace byla realizována citlivě a ve spolupráci s implementací IS.

Nároky z hlediska strategického a taktického řízení

Z hlediska posílení strategického a taktického řízení je po IS MěÚ vyžadováno, aby:

- podporoval dosahování strategických cílů a také naplnění poslání,
- dlouhodobě snižoval náklady na provoz MěÚ,
- přínosy ze zavedení a provozu IS v krátkém období byly prokazatelně zřejmé, hodnota se dá měřit způsoby, např. zrychlením úředních úkonů, nebo finančním ziskem zvyšováním efektivity výběru poplatků atd.,
- umožňoval zpětný monitoring potřebných hodnot (např. doby vyřizování podání, účinnosti bezpečnostních opatření, sledování finančních nákladů atd.).

Požadavky z hlediska koncových uživatelů

Koncový uživatel, tj. zaměstnanec MěÚ, člen rady města, zastupitelstva, nebo občan klade na IS požadavky, aby:

- byl schopen zajistit potřebné služby pro občany,
- disponoval infrastrukturou, která umožní on-line přístup k datům celému MěÚ v souladu s platnými právními předpisy, s informacemi k dispozici zaměstnancům i vedení MěÚ,
- všechny budovy MěÚ byly propojeny do společné sítě,
- byl jednoduchý a srozumitelný pro uživatele při zachování potřebných funkcionalit IS.

Požadavky z hlediska informačních technologií

Z hlediska IT jsou na IS kladeny nároky, aby:

- umožňoval snadnou administraci,
- dokázal zabezpečit ochranu informací va vysoké úrovni,
- byl komplexním IS. Tím je míněn takový IS, který by vyhovoval potřebám celého MěÚ. Všichni uživatelé mohou pracovat nad společnými daty a využívají programy, které mohou vzájemně komunikovat,
- nedocházelo k duplicitě a nekonzistenci dat v IS,
- byl co nejvíce nezávislý na použité platformě operačního systému a mohl tak být snadno používán na jiném zařízení a umožnil budoucí rozvoj a rychlou reakci na změny,
- byla dostupná HW infrastruktura, která umožní implementaci libovolného SW vybavení, které bude ve shodě s potřebou, plánem a koncepcí strategie rozvoje IS.

5.10.3 Strategické projekty a kritéria hodnocení

Strategické cíle:

- zvýšení efektivity řízení a organizace MěÚ,
- optimalizace komunikace s OVM s působností pro město,

- tvorba organizačních a technických podmínek pro růst produktivity MěÚ,
- rozvoj komunikace mezi MěÚ a občany.

Aby bylo možno dosáhnout výše uvedených strategických cílů, budou vybrány vzájemně související projekty:

Procesní organizace a řízení MěÚ

Informační technologie pro MěÚ

Regionální informační a poradenský servis

Kritéria hodnocení dosahování strategických cílů

Každý z projektů bude mít stanoveny úkoly na období 2016-2020.

Úkoly bude připravovat tajemník MěÚ s informatikem MěÚ ve spolupráci v vedoucími odborů. Realizace a hodnocení etap projektů, ustanovení a splnění úkolů, harmonogram, finanční náklady, bude schvalovat komise pro informatiku, strategické projekty schválí rada města.

5.10.4 Architektura IS

Je zde doplněna aktuální architektura IS MěÚ, jsou stanovena doporučení, aby doplnila dříve uvedené strategické cíle MěÚ.

Doporučení pro globální architekturu:

TPS – implementovat aplikace, které zaručí zajištění rozhraní do úrovně MIS případně EIS.

MIS - rozšíření a implementace nové nadstavby nad databázi dat společných pro aplikace z TPS. V souvislosti se zaváděním nového SW modernizovat SW zajišťující konzistenci dat mezi aplikacemi TPS, SW podporující řízení a manažerské nadstavby.

EIS - zřídit datový sklad (Data Warehouse) s celkovými statistikami, agregací, sumarizace a výběr důležitých dat z MIS a TPS.

OIS - sjednotit verze kancelářský SW v rámci MěÚ.

EDI – pokračovat v budování mechanizmů pro komunikaci s okolím úřadu prostřednictvím rozhraní. Technologické bezpečnostní mechanizmy pro ochranu vnitřní sítě úřadu jsou na špičkové úrovni, pro budoucnost je nutné dosažený standard udržet.

Návrhy pro technologickou architekturu:

- Na úrovni TPS použít technologie klient – server, technologii WWW,
- Na úrovních MIS a EIS používat hlavně technologie WWW,
- Pro servery vybudovat bezpečnou demilitarizovanou zónu,
- Prosazovat třívrstvou architekturu (klient/aplikační server/datový server).

Návrhy pro SW architekturu:

- Pro úsporu finančních nákladů využívat free SW a open source SW tam kde to lze, hlavně na serverech,
- Pro jednodušší implementaci a usnadnění provozu provést sjednocení verzí SW u klientů a zřídit jednotnou konfiguraci,
- Zřídit centrální správu SW, monitoring požadavků od zaměstnanců a bezpečnostních incidentů.

Návrhy pro HW architekturu

- Hromadné pořizování hardware pro uživatele s jednotnou HW konfigurací vždy pokud to bude realizovatelné,
- Dbát na bezpečnost a potřebnou kvalitu komunikační infrastruktury, nakupovat aktivní síťové prvky umožňující SW správu na úrovni Layer 3 s virtuálními sítěmi.

5.10.5 Organizační předpoklady

Účinnost nasazení IT je závislá na radě města, schvalující finančně náročnější etapy pořizování IT. Pro rozhodování rady města jsou klíčovými tajemník MěÚ a informatik, zpracovávající podklady pro rozhodnutí, která posléze realizují. Tajemník spravuje MěÚ a tím zajišťuje jeho provoz, informatik má za úkol zajišťovat vše informačními technologiemi. Společně mohou dosáhnout zlepšení v oblastech řízení a chodu MěÚ. Vedení úřadu dbá ma personální a materiální zabezpečení odboru, který má na starost rozvoj a správu IS. Pracovníci IT musí v rámci rozvoje a provozu IS zajišťovat nebo koordinovat:

- Sestavit rozpočet kapitoly informatiky, zajišťovat správu financí informatiky a administrativní činnosti,
- Spravovat evidenci IS, dokumentaci, provozní deník, udržovat administrátorskou a uživatelskou dokumentaci IS,
- Projektovou a analytickou činnost,
- Vzdělávání uživatelů,
- Administrátorské, provozní a servisní práce,
- Opravy a servis výpočetní techniky na pracovištích,
- Podporu uživatelů při zpracování dat mimo běžných činností.

Pracovníci IT by měli být informováni o důležitých jednáních a rozhodování relevantních pro IT, nebo se přímo účastnit jednání, pokud má mít důsledky pro IT:

- Rady a zastupitelstva,
- Komisí rady města a výborů zastupitelstva,
- Vedení MěÚ,
- Tajemníka MěÚ a vedoucích odborů,
- Pracovních týmů.

Zásadní rozhodnutí uvnitř MěÚ by neměly být činěny bez předběžného stanoviska informatika. Pracovníkovi IT by měl být umožněn kariérový růst. Pro pracovníka IT by mělo být zajištěno profesní vzdělávání, např. školení.

5.10.6 Legislativní předpoklady

Rozvoj a provoz informačního systému by měl být určen vnitřními směrnicemi a dokumenty:

- Provozní řád IS,
- Plán realizace informační strategie,
- Plán realizace bezpečnostní politiky,
- Spisový řád (obsahující spisový plán),
- Systematické vzdělávání uživatelů v oboru ICT,

- Směrnice pro sledování a řešení požadavků uživatelů,
- Evidence poruch a mimořádných událostí,
- Provozní bezpečnostní dokumentace,
- Provozní deník IS.

5.11 Transformace do cílového stavu

5.11.1 Obecné požadavky

Státní informační a komunikační politika

Přeměna do cílového stavu musí brát ohled na vývoj ve strategických dokumentech jako Státní informační a komunikační politika. V současnosti lze říci, že zřizování IS je prováděno v rámci těchto dokumentů.

Způsoby řízení vývoje IS

IS bude řízen a modernizován dle požadavků:

- vycházejících vyplývajících z platné legislativy,
- vycházejících z potřeb pro dosahování strategických cílů,
- vycházejících z provozních potřeb MěÚ.

5.11.2 Specifikace projektů a harmonogram realizace

Zde se popisuje provádění hlavních projektů a podprojektů pro dosáhnutí strategických cílů, přičemž realizaci hlavních projektů je nutno provádět současně.

Procesní organizace MěÚ

Výsledkem projektu je optimalizace a automatizace procesů MěÚ, jimiž MěÚ provádí své činnosti a optimalizace organizační struktury MěÚ.

Důležité je zefektivnit komunikaci a výměnu informací, správná koordinace mezi MěÚ a zřízenými organizacemi, s ostatními OVM a jinými důležitými subjekty působícími v katastru města. Tím je stanoven způsob řízení a provozu MěÚ a budování informačního systému pro MěÚ. Hlavním cílem je dosáhnout vyšší efektivity činnosti MěÚ.

Informační technologie MěÚ

Cílem projektu je realizace komplexního IS, umožňujícího mimo činností běžných agend MěÚ, také provoz agend souvisejících se správou a řízením samotného MěÚ pro vedoucí pracovníky MěÚ a volených zástupců. Informační systém, který je takto koncipován, je jedním z rozhodujících činitelů pro zvýšení efektivity úřadu.

Úkoly pro období 2015 - 2020

Kontrola dokumentace k IS:

- Vytvoření evidence aktuální dokumentace IS.

Aktualizace dokumentů:

- Provozní řád IS,
- Sledování požadavků uživatelů IS a jejich aktualizace požadavků uživatelů,
- Evidence poruch a mimořádných událostí.

Vytvoření dokumentace:

- Plánu realizace informační strategie,
- Plánu realizace bezpečnostní politiky,
- Průběžné a neustálé zvyšování vzdělání uživatelů v IT.

Vytvoření potřebného materiálu:

- Architektura IS.

Sjednocení SW projektů:

- Slaďování realizace důležitých projektů.

Datová základna:

- Dále postupovat ve tvorbě základny pro společná data,
- Zřizovat referenční rozhraní pro úrovně MIS a TPS.

6 INFORMAČNÍ KONCEPCE

Informační koncepce je dokumentací v níž jsou stanoveny dlouhodobé cíle organizace v oblastech řízení informačních systémů. Její obsah je dán vyhláškou č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy a komentářem k této vyhlášce. V informační koncepci jsou zahrnuty všechny organizací spravované ISVS, pro které jsou určeny dlouhodobé cíle v dosažení bezpečnosti a řízení kvality, pravidla pro nákup, vývoje a provozu. V této informační koncepci nejsou uvedeny identifikační údaje subjektu, na základě kterého byla informační koncepce zpracována.

Základní údaje organizace

Zde by měl být uveden název MěÚ, IČ, adresa, telefon, fax, e-mail, web a kontaktní osoba.

Základní údaje o Informační koncepci

Uvádí se název dokumentu „Informační koncepce MěÚ ...“, datum jejího schválení, způsob schválení, dobu platnosti, která je standardně 5 let a aktuální verzi dokumentu.

Údaje o předchozích verzích

V této kapitole jsou uvedeny všechny změny provedené v dokumentu, tak jak byly po jeho schválení postupem času prováděny. Změny dokumentu jsou prováděny především po provedení zásadních změn v IS MěÚ nebo po provedení pravidelného vyhodnocení dodržování Informační koncepce. Změny provedené oproti každé předchozí verzi jsou vždy uvedeny v příslušné tabulce.

Aktuální verze

Uvádí se označení verze a datum jejího vytvoření. Dále následuje datum schválení, způsob schválení „Schváleno dne .... Radou města .....“, „Schváleno dne .... tajemníkem úřadu...“. Je uvedena platnost, do kdy verze platí, umístění dokumentu, počet stran, příloh a jsou vypsány provedené změny.

6.1 Zdroje a legislativa

Souhrn pramenů použitých pro vytváření Informační koncepce

Jsou zde uváděny zdroje organizace, dokumenty strategické, tak dokumenty zaznamenávající stav IS k danému datu a další záměry, např.

- Strategický plán rozvoje města v letech 2015 – 2020

- Program rozvoje města

Vzhledem k členství ČR v EU, je třeba zahrnout také strategické dokumenty EU z oblasti IT. Informační koncepce musí brát v potaz informační strategie, globální strategie a další strategické dokumenty vyšších OVM, tak úřadu samotného.

Nejdůležitějšími dokumenty a projekty mohou být celostátně považovány:

- Státní informační a komunikační politika,
- Koncepce budování informačních systémů veřejné správy,
- Program informatizace územních orgánů veřejné správy,
- Akční plán realizace státní informační politiky.

6.1.1 Legislativní rámec

Zde jsou uvedeny právní předpisy ČR pro provozování ISVS, viz příloha P I „Právní předpisy pro ISVS“.

6.2 Přehled ISVS a agend provázaných s ISVS

Zde je uveden seznam všech informačních systémů a agend využívaných MěÚ, které splňují podmínky ISVS a spadají pod dlouhodobé řízení ISVS.

Podmínky pro uvedení ISVS:

- Správcem ISVS je MěÚ (byl jím zakoupen),
- Provozní agenda je provázána s jiným ISVS.

U provozovaného ISVS a agend jsou uvedeny tyto atributy:

- Kompletní název agendy,
- Zkratka názvu agendy,
- Související právní předpis,
- Odbor zajišťující provoz ISVS,
- Vlastnosti ISVS, nebo agendy,
- HW a SW prostředí ISVS,
- Zpracovávaná data,

- Stávající stav,
- Popis vazby na ISVS (jen agendy),
- Plánované změny a úpravy (pouze ISVS).

6.2.1 Informační systémy veřejné správy

Úplný název ISVS:	IS Radnice – Registry
Zkratka názvu:	REG
Právní předpisy:	Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech, zákon č. 128/2000 Sb., o obcích, zákon č. 36/1960 Sb., o územním členění státu, zákon č. 256/2013 Sb., o katastru nemovitostí
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Evidence obyvatel, vedení agendy ohlašovny. Popis správního území z hlediska členění na katastry, sídelní jednotky a jejich částí, evidence a správa číselníků katastrů, obcí a jejich částí, ulic, čísel popisných a evidenčních Evidence majetkoprávních vztahů ve spravovaném území, generování a tisk sestav pozemků, budov, bytových jednotek a jejich vlastníků
Zpracovávaná data:	Údaje o osobách, jejich partnerech, rodičích, dětech a trvalém pobytu. Názvy, kódy, vzájemné vazby a doplňující informativní údaje katastrů, obcí, částí obcí, ulic, čísel popisných. a evidenčních Geografické a popisné údaje o pozemcích, budovách, bytových jednotkách, atd.
Technické a programové prostředí:	Server MeU
Současný stav:	ISVS je v běžném provozu.
Předpokládané změny:	Pro ISVS nejsou plánovány žádné změny.

Tabulka 11 IS Radnice – Registry [Zdroj:vlastní]

Tímto způsobem (tabulka č. 11) jsou zpracovány ISVS, viz. příloha P VIII. Mezi další ISVS, které je třeba tímto způsobem rozepsat patří: Pozemky, Registr střetu zájmů, IS Radnice – Doprava a komunikace, Evidence psů, Hrací automaty, Komunální odpad, Městská policie, Občanské průkazy a pasy, Organizace voleb, Přestupkové řízení, Stavební úřad, Volební agenda.

6.2.2 Provozní agendy s vazbou na ISVS

Úplný název ISVS:	IS Radnice – Rozpočtové účetnictví
Zkratka názvu:	ROU
Právní předpisy:	Zákon č. 563/1991 Sb., o účetnictví
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Účetní agenda, výkaznictví
Současný stav:	V běžném provozu.
Vazba na ISVS:	Předávání finančních výkazů krajskému úřadu.

Tabulka 12 IS Radnice – rozpočtové účetnictví [Zdroj:vlastní]

Tímto způsobem (tabulka č. 12) jsou zpracovány všechny agendy ISVS, viz. příloha P IX.

6.3 Plán zřízení nových ISVS

MěÚ neplánuje zakoupení, nebo zřízení nového ISVS

6.3.1 Pravidla pro zřízení ISVS

Před zahájením jednání o pořízení nového ISVS musí být formulován záměr pro pořízení ISVS v písemné, nebo elektronické podobě se základními charakteristikami a důvodu pořízení ISVS. Záměr na pořízení vypracuje odbor MěÚ na základě požadavku.

Záměr by měl obsahovat tyto položky:

- Název ISVS,
- Související právní předpisy,
- Data, která budou zpracovávána a služby, které bude ISVS poskytovat,
- Důvod pořízení,
- Náklady na pořízení a náklady na provoz,
- Požadavek na zaměstnance,
- Termín realizace a termín spuštění do plného provozu.

O schválení, nebo zamítnutí rozhoduje pracovní skupina ve složení, které se může měnit dle typu ISVS:

- Tajemník MěÚ,
- Vedoucí dotčeného odboru MěÚ,
- Informatik MěÚ.

V případě schválení realizace ISVS, je pořízení dále řešeno formou samostatného projektu, jehož realizátorem je informatik MěÚ, většinou způsobem dodávky externí organizací.

Informatik odpovídá za splnění podmínek:

- Dodávka musí obsahovat kompletní dokumentaci k administraci a pro uživatele,
- Firma zajistí provádění aktualizací ISVS dle aktuální legislativy,
- Je provedeno zaškolení uživatelů ISVS.

Plnění podmínek kontroluje tajemník MěÚ.

6.3.2 Řízení změn v ISVS

Odpovědnost za průběh řízení změn v ISVS má informatik MěÚ. Zodpovídá za:

- Dodávku aktualizované dokumentace k ISVS,
- Zálohování dat a konverzi dat,
- Řádné testování a provoz nových verzí,
- Proškolení uživatelů.

Pokud dojde ke zrušení ISVS, vypracuje harmonogram ukončení, je odpovědný za další manipulaci s daty (archivace) a SW. Plnění podmínek kontroluje tajemník MěÚ.

6.4 Řízení kvality ISVS

6.4.1 Určení dlouhodobých cílů

ISVS MěÚ obsluhuje 30 uživatelů pracujících v 57 agendách, což znamená vysokou náročnost pro HW, infrastrukturu, SW a dlouhodobé řízení IS. Pro ISVS musí platit:

- Vysoké zabezpečení a spolehlivost,
- Vysoká kvalita poskytovaných služeb,
- Dokumentace všech provedených úkonů,

- Dodržení všech právních předpisů.

6.4.2 Požadavky na kvalitu

Při změnách stávajícího, případně pořízení nového ISVS je potřebné určit požadavky na kvalitu, které se určují dle charakteru plánovaného projektu. Určení požadavků je na zodpovědnosti informatika, případně tajemníka MěÚ. Zavádění kvalitativních požadavků ve spolupráci s dodavateli provádí informatik MěÚ. Mezi standardní požadavky patří:

- Stanovení způsobu identifikace uživatelů,
- Záruka včasné aktualizace dat,
- Určení způsobu testování ISVS,
- Stanovení rozsahu dokumentace k provozu a zavádění ISVS,
- Vypracování organizační směrnice pro provoz ISVS

6.4.3 Funkce a odpovědnost

Je důležité určit osoby, které budou v organizaci zodpovědné za řízení kvality ISVS.

Zde jsou zodpovědnými osobami informatik MěÚ a tajemník. Informatik MěÚ odpovídá za zavádění požadavků na kvalitu, dodržování určeného stupně kvality dodavateli, vede dokumentaci kontrol kvality a jejich vyhodnocování, toto vyhodnocování provádí pravidelně a je odpovědný za kompletnost dokumentace o řízení kvality. Tajemník MěÚ stanovuje dlouhodobé cíle v řízení kvality a jejich dodržení při provozu a instalaci ISVS kontroluje.

6.4.4 Vyhodnocení řízení kvality ISVS

Součástí vyhodnocování řízení kvality je přezkoumání cílů v oblasti kvality a poté jejich aktualizování, které je třeba provádět alespoň jednou ročně se zadokumentovaným zápisem v provozní dokumentaci ISVS. Může být proveden také na příkaz starosty či tajemníka MěÚ. Provádí jej informatik, poté jej kontroluje tajemník MěÚ.

Informatik také provádí pravidelné kontroly toho, zda jsou dodržovány předsevzaté cíle dodržování kvality za provozu ISVS. Je udržován seznam požadavků kvality, které jsou odpovídající pro provoz stanovené při zřizování ISVS.

6.5 Řízení bezpečnosti

Pro řízení bezpečnosti je důležitý dokument „Bezpečnostní politika ISVS“, který zahrnuje bezpečnostní předpisy a pravidla upřesňující zabezpečení ISVS. Bezpečnostní politikou určujeme postupy důležité pro bezpečný provoz, řízení přístupů, celistvost dat a oprávnění uživatelů. Bezpečnostní politika stanovuje pravidla, právní předpisy a normy, kterými určuje, jak mají být chráněny, spravovány, používány a distribuovány citlivé informace a informační zdroje v organizaci, v tomto případě MěÚ.

6.5.1 Dlouhodobé cíle a základní požadavky bezpečnosti

Nejdůležitějšími bezpečnostními cíli je zaručení činností a stavů:

- Ochrana dat, HW a SW prostředků ISVS,
    - Zajištění fyzické bezpečnosti HW a SW prostředků MěÚ,
    - Personální bezpečnost,
    - Systém celkové ochrany před škodlivým SW,
    - Bezpečností pravidla proti napadení zevnitř,
    - Ochrana ISVS MěÚ před nebezpečím z vnějších sítí, zabezpečující vnitřní síť před průnikem
    - Stanovit správce ISVS,
- Zajištění bezpečné komunikace,
    - Použití bezpečných komunikačních sítí a cest,
    - Bezpečná komunikace mezi MěÚ a OVM,
    - Prostředky šifrování dat.
- Kvalitní a dlouhodobé zajištění dostupnosti, integrity a důvěrnosti s autentizací dat,
    - Identifikace a autorizace uživatele,
    - Zabezpečení soukromí uživatele,
    - Systematické zálohování dat a jejich archivace,
    - Řízení provozu a monitorování sítě,
    - Plán obnovy IS po havárii.

6.5.2 Role a odpovědnosti

Bezpečnost ISVS MěÚ patří do provozní části úřadu, z tohoto důvodu provádí tajemník MěÚ schvalování a vyhlášení provádění bezpečnostní politiky, s personálním obsazením a stanovením role a odpovědnosti v oblasti bezpečnosti.

Na zajištění bezpečnosti jsou určena tato organizační opatření:

- Určení bezpečnostní komise, jejich pravomocí a odpovědnosti,
- Určení bezpečnostního správce, jeho pravomocí a odpovědnosti,
- Určení povinností a odpovědnosti uživatelů ISVS MěÚ.

Bezpečnostní komise

Bezpečnostní komise se skládá z:

- Informatika MěÚ
- Tajemníka MěÚ,
- Tajemníka krizového štábu.

Bezpečnostní komise:

- Stanovuje pravidla bezpečnostní politiky
- Koordinuje zavádění bezpečnostních opatření ISVS MěÚ,
- Má zodpovědnost za řízení přístupu k informačním aktivům a ISVS,
- Má zodpovědnost za monitorování a kontrolu fungování implementovaných bezpečnostních opatření,
- Stará se, aby podpora bezpečnostní politiky od vedení MěÚ byla dostatečně viditelná,
- Navrhuje důležité opatření směřující ke zvýšení bezpečnosti dat, HW a SW prostředků,
- Navrhuje a prosazuje iniciativy k bezpečnosti IS MěÚ,
- Navrhuje role a odpovědnost v oblasti bezpečnosti ISVS,
- Kontroluje, zda byla bezpečnost součástí plánování ISVS,
- Snaží se o zvyšování bezpečnostní vzdělanosti uživatelů ISVS MěÚ,

- Navrhuje postupy a metody bezpečnosti,
- Stanovuje požadavky na znalosti a na finanční náklady,
- Vyhodnocuje úroveň a účinnost bezpečnostní politiky,
- Má na starosti řešení disciplinárních prohřešků vůči bezpečnosti.

Bezpečnostní správce

- Spolupracuje s bezpečnostní komisí a správcem ISVS MěÚ,
- Má zodpovědnost za dodržování bezpečnosti ISVS,
- Zodpovídá za integraci bezpečnostní politiky do plánování v ICT,
- Monitoruje incidenty v bezpečnosti a spolehlivost bezpečnostní politiky,
- Kontroluje bezpečnostní opatření, navrhuje postupy zvýšení bezpečnosti a řídí jejich zavádění,
- Navrhuje role, odpovědnost, metody a postupy v bezpečnosti IS MěÚ,
- Dohlíží na dodavatele IT služeb, aby dodržovali bezpečnostní politiku MěÚ.

6.5.3 Požadavky na bezpečnost

Plnění bezpečnostních požadavků má na zodpovědnosti informatik, který je administrátorem ISVS. Stará se, aby při provozu IS byly dodrženy postupy předepsané pro splnění bezpečnostních požadavků ISVS.

Mezi tyto postupy patří:

- Zákonné normy,
- Interní směrnice MěÚ – bezpečnostní politika, provozní řád, spisový řád atd.
- Pravidla a doporučení dodavatele ISVS.

Při zavádění nového ISVS je řízení bezpečnosti neoddělitelnou součástí procesu, kdy za plnění bezpečnostních požadavků je odpovědný tajemník MěÚ, jejich realizaci provádí informatik MěÚ.

6.5.4 Vyhodnocování požadavků

Provádí se pomocí testů a prověrek, které řídí bezpečnostní správce spolupracující s administrátorem ISVS. Provádí se alespoň jedenkrát ročně, na žádost bezpečnostního správce, nebo může být mimořádná na pokyn bezpečnostního správce, či bezpečnostní komise. Provádí se kontroly logovacích souborů, provozních deníků, dodržování směrnic, přístupových práv, pokusy o průnik do IS a uložení nesprávných dat a další. Po ukončení testů a prověrek se uskuteční zápis do provozní dokumentace IS MěÚ.

6.6 Vyhodnocení dodržování informační koncepce

Pro plnění dlouhodobých cílů MěÚ je důležité pravidelné sledování a vyhodnocování dodržení zásad určených informační koncepcí. Vyhodnocení dodržování informační koncepce se provádí jedenkrát ročně a o jejím výsledku se vyhotovuje zápis, který se stane součástí dokumentace IS MěÚ. Vyhodnocením dodržování je pověřena skupina, kterou tvoří tajemník MěÚ a informatik. Může být rozšířena o odborníky v rámci MěÚ, nebo externí specialisty. Z průběhu vyhodnocení se pořizuje zápis, který obsahuje odpovědné osoby a termíny nápravy zjištěných závad a schválena všemi zúčastněnými osobami. Pracovní skupina vyhodnocuje následující oblasti jestli:

- Stávající verze informační koncepce obsahuje aktuální a pravdivý popis všech ISVS a provozních systémů s vazbou na ISVS i s plánovanými změnami,
- Požadavky na bezpečnost a kvalitu jsou u agend dodržovány a plněny,
- Stávající verze informační koncepce obsahuje všechny záměry na pořízení nových ISVS,
- Postupy stanovené v informační koncepci nejsou v rozporu s dalšími vnitřními směrnicemi vztahujícími se k IS MěÚ,
- Plnění požadavků na kvalitu a bezpečnost kladně ovlivňuje plnění dlouhodobých cílů,
- Při pořizování a změnách ISVS jsou uplatňovány postupy uvedené v informační koncepci,
- Zásady a postupy z informační koncepce jsou opravdu dodržovány,
- Dodržují se zásady financování IS MěÚ uvedené v informační koncepci,

- Jsou dodržovány zásady provádění aktualizací informační koncepce,
- S aktuálním zněním informační koncepce jsou seznámeni všichni zaměstnanci MěÚ,
- Byly odstraněny všechny nedostatky zjištěné při posledním vyhodnocení.

6.7 Způsob změny informační koncepce

Ke změně informační koncepce může dojít z důvodu změny právních předpisů, změn technických či organizačních. Kontrolu informační koncepce provádí tajemník MěÚ, který navrhuje postup k nápravě. Informatik, který má přehled o ISVS a provozních systémů s vazbami na ISVS, odpovídá za dodržování informační koncepce a způsob prováděných změn s archivováním dokumentace informační koncepce. Změna informační koncepce je vždy zdokumentována.

Kdy dochází ke změnám informační koncepce:

- Při pořízení ISVS, nebo systému s vazbou na ISVS,
- Změna v ISVS, je rozuměna změna funkčnosti, poskytovaných služeb, nebo rozsahu zpracovávaných dat. Změny jsou zdokumentovány a stanou se součástí dokumentace ISVS,
- Ukončení provozu ISVS, v tomto případě se stanoví časový harmonogram ukončení provozu a způsob naložení s daty ISVS, SW, HW a provozní dokumentací, stanoví se lhůty pro skartaci dat, datových nosičů a dokumentace. Informatik zodpovídá za dodržení lhůt a postupů,
- Změna organizační struktury MěÚ, kdy dojde k přesunu pravomocí, činností atd. mezi odbory MěÚ. Za provedení zodpovídá informatik.

6.8 Financování IS MěÚ

Hlavním finančním zdrojem pro IS MěÚ je zastupitelstvem schválený rozpočet města. Provoz a rozvoj IS musí dodržovat rozpočtová pravidla. Souhrnný rozpočet ICT je součtem investičních a provozních nákladů za kalendářní rok. Za přípravu rozpočtu ICT MěÚ je odpovědný informatik, který zahrne potřebné výdaje do návrhu rozpočtu. Pro financování se také používají dotační tituly, kdy získaná částka je zařazena změnou rozpočtu do rozpočtu města.

6.9 Odpovědnost za dodržení informační koncepce

Za naplnění dlouhodobých cílů v informatice, provozu ISVS a provozních systémů s vazbou na ISVS, odstraňování nedostatků , dodržování metodik určených v informační koncepci zodpovídá informatik.

Tajemník MěÚ zodpovídá za splnění právních předpisů při dodržování informační koncepce.

7 BEZPEČNOSTNÍ POLITIKA

Informační systémy veřejné správy prochází v současné době procesem centralizace datových zdrojů. Další snahou je zajištění dostupnosti těchto dat pro všechny aplikace využívané veřejnou správou. Dostupnost dat však vyžaduje striktní dodržování bezpečnostní politiky v informačních systémech veřejné správy.

Základní údaje organizace

Zde by měl být uveden název MěÚ, IČ, adresa, telefon, fax, e-mail, web a kontaktní osoba.

Základní údaje o Bezpečnostní politice

Uvádí se název dokumentu „Bezpečnostní politika MěÚ ...“, datum jejího schválení, způsob schválení, dobu platnosti, která je standardně 5 let a aktuální verzi dokumentu.

Údaje o předchozích verzích

V této kapitole jsou uvedeny všechny změny provedené v dokumentu, tak jak byly po jeho schválení postupem času prováděny. Změny dokumentu jsou prováděny především po provedení zásadních změn v IS úřadu nebo po provedení pravidelného vyhodnocení dodržování Informační koncepce. Změny provedené oproti každé předchozí verzi jsou vždy uvedeny v příslušné tabulce.

Aktuální verze

Uvádí se označení verze a datum jejího vytvoření. Dále následuje datum schválení, způsob schválení „Schváleno dne .... Radou města .....“, „Schváleno dne .... tajemníkem úřadu...“. Je uvedena platnost, do kdy verze platí, umístění dokumentu, počet stran, příloh a jsou vypsány provedené změny.

7.1 Zdroje a legislativa

Pro vytvoření Bezpečnostní politiky použijeme dokumenty strategické a dokumentaci zachycující stávající stav IS. Zdrojem mohou být také materiály a informace Ministerstva vnitra ČR. Ministerstvo vnitra ze zákona č. 365/2000 Sb. ve spolupráci s orgány veřejné správy zpracovává a ukládá informace, které mohou být využity pro kvalitní vytváření a rozvoj ISVS, zpracovává návrhy strategických dokumentů pro ISVS, také z hlediska bezpečnosti systémů, předkládá dokumenty vládě, analyzuje potřeby veřejné správy z oblasti informatiky a stav ISVS, zajišťuje tvorbu metodiky činností spojených s vytvářením, vývojem a využíváním ISVS.

Podle zákona č. 365/2000 Sb., Ministerstvo vnitra vydává Věstník, v němž uveřejňuje metodické pokyny a další dokumenty vztahující se k ISVS. Bezpečnostní politika Městského úřadu souhlasí s Informační koncepcí Městského úřadu.

Právní předpisy z legislativy ČR pro provozování ISVS, jsou umístěny v příloze P I „Právní předpisy pro ISVS“. Normy ČSN jsou umístěny v příloze P II „Technické normy pro ISVS“.

7.2 Terminologie pro bezpečnostní politiku

Terminologie pro bezpečnostní politiku je uvedena v příloze P X.

7.3 Obsah a účel bezpečnostní politiky

Bezpečnostní politika informačního systému organizací veřejné správy je souhrnem bezpečnostních zásad, opatření, předpisů, pravidel a procedur definujících způsob zabezpečení provozu IS MěÚ, který zajišťuje bezpečnost IS na požadované úrovni, s přihlédnutím k efektivně vynaloženým prostředkům.

Informační bezpečnost je na MěÚ prosazována v souladu s deklarovanými cíli. Za její prosazování jsou obecně odpovědní vedoucí zaměstnanci jednotlivých organizačních odborů MěÚ. Základem prosazení informační bezpečnosti je implementace stejného systému řízení informační bezpečnosti ve všech oborech činnosti MěÚ. Bezpečnostní politika ISVS je důležitou součástí provozní dokumentace ISVS MěÚ v souladu s požadavky vyhlášky č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy, zákona č. 365/2000 Sb. o informačních systémech veřejné správy ve znění pozdějších předpisů , zákona č. 181/2014 Sb, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhlášky č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a vyhlášky 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích.

Bezpečnostní politika informačního systému MěÚ obsahuje popis bezpečnostních opatření, která MěÚ uplatňuje při zajišťování bezpečnosti IS. Požadavky na bezpečnost IS slouží k dosáhnutí dlouhodobých cílů, které chce MěÚ dosáhnout v řízení bezpečnosti IS.

Těmito cíli jsou:

- Bezpečnost dat, které jsou v IS MěÚ zpracovávány,

- Bezpečnost všech služeb, poskytovaných prostřednictvím těchto informačních systémů,
- Bezpečnost všech programových (SW) a technických (HW) prostředků potřebných pro zabezpečení informačních činností (§2 písm. a) zákona č. 365/2000 Sb.).

Základní bezpečnostní zásady a povinnosti uživatelů ISVS z nich plynoucí se uvádí v Provozním řádu MěÚ.

Pomocí bezpečnostní politiky IS MěÚ jsou stanovena základní pravidla a doporučení zaručující bezpečný provoz IS, nenarušenost uložených dat a informací a správu přístupů do IS a k datům pro oprávněné uživatele ISVS dle jejich funkčního zařazení v organizační struktuře MěÚ. Bezpečnostní politika informačního systému veřejné správy určuje právní předpisy, normy a pravidla, které specifikují způsob spravování, ochrany a distribuce citlivých informací a dalších určitých informačních zdrojů v rámci MěÚ. Určuje bezpečnostní opatření a způsob jejich realizace, stanovuje vhodné organizační postupy a určuje způsob použití, který zaručí odpovídající přiměřenou bezpečnost dle požadavků bezpečnostní politiky MěÚ. Bezpečnostní politika IS MěÚ také obecně popisuje bezpečné využívání informačních zdrojů. Správné pochopení bezpečnostních opatření dotčenými pracovníky a odpovídající obeznámenost všech zaměstnanců s bezpečností informačních systémů je nedílnou součástí systému bezpečnosti.

7.4 Základní dlouhodobé cíle bezpečnosti

Dlouhodobé cíle v oblasti bezpečnosti jsou ustanoveny v Informační koncepci kapitola 6.5.1. Bezpečnostní politika je základním obecným dokumentem pro proces systematického řešení bezpečnosti ICT MěÚ.

Základními cíle politiky bezpečnosti je zabezpečení těchto činností a stavů:

- Spolehlivé a trvalé zajištění dostupnosti, diskrétnosti a neporušenosti dat, které jsou uchovávány a zpracovány v prostředí IS MěÚ,
- Ochrana dat a softwarových či hardwarových prostředků IS MěÚ,
- Odpovědnost uživatelů za jejich jednání v IS MěÚ,
- Zajištění bezpečné vnější i vnitřní komunikace.

7.5 Požadavky na bezpečnost

Nároky na bezpečnost IS jsou uskutečněním základních bezpečnostních cílů:

Trvalé a spolehlivé zajištění dostupnosti, diskrétnosti, neporušenosti a původnosti dat

- Identifikace, přihlášení a ověření uživatelů – zajištění a aktivní řízení přístupu k IS organizace VS a k datům v IS organizace VS (prohlížení, aktualizace) pro oprávněné uživatele IS organizace na základě funkčního zařazení,
- Řízení provozu a monitorování počítačové sítě,
- Provoz systému pro pravidelné zálohování a archivaci dat,
- Vyhotovení plánu na obnovu provozu IS organizace (či kritické části IS) po havárii.
- zabezpečení soukromí uživatelů – ochrana uživatele před zjištěním, odcizením či zneužitím jeho identity ostatními uživateli IS, nebo vnějším subjektem,

Ochrana prostředků a dat IS MěÚ

- Zajištění fyzické bezpečnosti prostředků IS MěÚ: fyzické zabezpečení prostředků IS MěÚ vhodným umístěním (polohou, zábranou), zabránění neoprávněnému vstupu či přístupu, zajištění HW a SW prostředků ISVS před zneužitím či odcizením,
- Zajištění personální bezpečnosti (budování bezpečnostního vědomí uživatelů IS),
- Provoz systému komplexní ochrany před škodlivým SW (viry, malware atd),
- Ochrana IS MěÚ před napadením z externích sítí (hackeři, získání dat či porušení integrity dat, vyřazení služeb sítě, apod.),
- Vybudování bezpečnostních zábran proti napadení zevnitř (široká škála bezpečnostních pravidel od úrovně budování, administrace IS organizace, po školení zásad, jak se mají uživatelé i správci IS chovat),
- Bezpečnostní opatření znemožňující průnik do vnitřní sítě MěÚ (ochrana umístění serverů, aktivních prvků sítě a uživatelské IT),
- Ustanovení správce agendy ISVS, určení osobní odpovědnosti za data v IS organizace, nebo za určitý HW či SW IS,
- Stanovení správce IS organizace VS.

Zajištění bezpečné komunikace s okolím

- Používání zabezpečených komunikačních kanálů,
- Pravidla bezpečné komunikace mezi MěÚ a dalšími OVM,
- Používání SW a HW prostředků pro šifrování dat při komunikaci.

7.6 Role a odpovědnost

Bezpečnost ISVS MěÚ patří do provozní části úřadu, z tohoto důvodu provádí tajemník MěÚ schvalování a vyhlášení provádění bezpečnostní politiky, s personálním obsazením a stanovením role a odpovědnosti v oblasti bezpečnosti.

V souladu s požadavkem vyhlášky č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy, definuje MěÚ pro IS MěÚ vždy roli správce systému, který je zaměstnancem, nebo jinou fyzickou osobou, která zabezpečuje řízení fungování IS MěÚ. Dále bezpečnostního správce systému, který je zaměstnancem, nebo jinou fyzickou osobou, která zabezpečuje kontrolu bezpečnosti IS Městského úřadu. Zároveň úřad definuje pro každou roli soubor určených činností a potřebných oprávnění a pravomocí pro realizaci těchto činností v informačním systému Městského úřadu a souhrn příslušných odpovědností.

Pro bezpečnost IS jsou přijata organizační opatření:

- Určení bezpečnostní komise, jejich pravomocí a odpovědnosti,
- Určení povinností a odpovědnosti uživatelů ISVS MěÚ.

Bezpečnostní komise

Bezpečnostní komise se skládá z:

- Informatika MěÚ,
- Tajemníka MěÚ,
- Tajemníka krizového štábu.

Bezpečnostní komise

- Je poradním orgánem tajemníka MěÚ,
- Určuje pravidla bezpečnostní politiky,

- Upřesňuje cíle bezpečnosti a sleduje jejich plnění,
- Schvaluje důležité kroky směřující ke zvýšení zabezpečení dat a SW a HW prostředků v IS Městského úřadu,
- Schvaluje metodiku s postupy v oblasti bezpečnosti IS Městského úřadu,
- Schvaluje odpovědnosti a role v oblasti zabezpečení IS Městského úřadu v rámci celého úřadu,
- Kontroluje, zda je bezpečnost prvkem postupu plánování v oblasti informatiky,
- Koordinuje zavádění postupů v oblasti bezpečnosti IS Městského úřadu,
- Zodpovídá za průběžné sledování a kontrolu funkčnosti implementovaných bezpečnostních opatření,
- Schvaluje a podporuje podněty, které se týkají bezpečnosti IS Městského úřadu,
- Prosazuje, aby byla podpora bezpečnostní politiky vedoucími pracovníky dobře viditelná,
- Je zodpovědný za řízení přístupu k IS a informačním aktivům,
- Definuje požadavky na znalosti uživatelů a na finanční náklady,
- Prosazuje zvyšování bezpečnostní gramotnosti uživatelů IS Městského úřadu,
- Hodnotí efektivitu bezpečnostní politiky,
- Řeší disciplinární prohřešky vůči bezpečnosti.

Bezpečnostní správce

- Spolupracuje s bezpečnostní komisí a správcem informačního systému MěÚ,
- Zodpovídá za dodržování bezpečnosti IS Městského úřadu,
- Má zodpovědnost za to, že je bezpečnostní politika prvkem plánování v oblasti IT,
- Navrhuje metody a procesy v oblasti bezpečnosti IS Městského úřadu,
- Navrhuje specifické role a zodpovědnosti v oblasti bezpečnosti IS Městského úřadu v rámci celého úřadu,
- Navrhuje bezpečnostní postupy a plán jejich realizace,

- Navrhuje důležité kroky směřující ke zvýšení bezpečnosti dat a SW a HW prostředků v IS Městského úřadu,
- Řídí implementaci bezpečnostních zásad podle definovaných bezpečnostních cílů,
- Zajišťuje, že dodavatelé služeb pro úřad dodržují bezpečnostní politiku úřadu a ostatní důležité vnitřní předpisy,
- Podílí se na zlepšování bezpečnostní gramotnosti uživatelů IS Městského úřadu,
- Bezpečnostní správce IS spravuje seznam administrátorských hesel. Listinná kopie tohoto seznamu je uložena v obálce u tajemníka úřadu. Obálka je zapečetěna orazítkováním a podpisy bezpečnostní správce IS tak, aby bylo jasně patrno, zda byla či nebyla otevřena. Obálka se otevírá jen v případě nouze, o jejím otevření se následně sepíše krátký protokol, kde je uvedeno datum, důvod a osoby, které obálku s hesly otevřeli. Po nastolení normálního stavu je stejným způsobem založena a uložena nová obálka s novými administrátorskými hesly,
- Průběžně kontroluje bezpečnostní konflikty a spolehlivost bezpečnostní politiky a ověřuje důslednost zavedených bezpečnostních opatření.

Uživatelé IS Městského úřadu

- Řídí se instrukcemi Provozního řádu IS Městského úřadu,
- Chrání data a HW a SW prostředky IS MěÚ,
- Zabezpečují svěřenou výpočetní techniku proti přístupu neoprávněných osob,
- Při odchodu z pracoviště se odhlásí a ukončí spuštěné programy,
- Používají svěřenou výpočetní techniku jen k výkonu svého povolání,
- Nastavit své uživatelské heslo a nesdělovat ho dalším osobám, v pravidelných intervalech, nebo v případě podezření vyzrazení měnit své heslo,
- V případě odmítnutí povolení přístupu k IS Městského úřadu oznámí tuto skutečnost správci IS,
- Při práci v prostředí WAN sítí dodržují pravidla a bezpečnostní pokyny správců IS,

- Jsou dostatečně proškoleni z bezpečnostních opatření pro rozsah používaných IS,
- Nahlásí bezpečnostnímu správci jakýkoliv zjištěný konflikt v zabezpečení IS MěÚ,
- Nahlásí správci IS všechny závady HW a SW prostředků IS,
- Nakládají s osobními údaji a utajovanými skutečnostmi v souladu s platnou legislativou,
- Dodržovat zák. č.101/2000 Sb., o ochraně osobních údajů,
- Musí být dbalý toho, aby prostřednictvím IT úřadu nevznikla škoda jiným subjektům a nedošlo k poškození dobrého jména úřadu,
- Dodržují všechna pravidla uvedená v bezpečnostní politice.

Uživateli IS je zakázáno:

- Jakýmkoliv způsobem zasahovat do konfigurace přidělené výpočetní techniky,
- Instalovat jakýkoliv software,
- Využívat prostředky výpočetní techniky pro jiné než pracovní účely,
- Měnit nastavení aplikací a antivirových programů,
- Obcházet prostředky zabezpečující IS MěÚ,
- Provádět technické zásahy do HW zařízení IT,
- Vynášet datová média mimo prostory úřadu, pokud to nesouvisí s výkonem pracovní činnosti,
- Neoprávněně zveřejnit, zpřístupnit nebo odeslat data,
- Umožnit přístup cizí neoprávněné osoby k prostředkům IS Městského úřadu.

Vedoucí odborů, oddělení či úseků jsou odpovědní za dodržení bezpečnostních opatření v souladu s bezpečnostní politikou a dalšími předpisy. Zajišťují proškolení zaměstnanců v potřebném rozsahu tak, aby znali své povinnosti a odpovědnosti.

7.7 Základní postupy řízení bezpečnosti

7.7.1 Identifikace možných hrozeb a následků

Zde jsou uvedeny hrozby, které mohou negativně působit na provoz IS MěÚ. Úkol bezpečnostní politiky spočívá ve stanovení postupů, která tato rizika sníží na dlouhodobě přijatelnou úroveň. Můžou to být hrozby:

- Přírodní či fyzické, tj. živelná pohroma, požár, uragán, zaplavení povodní či vodou z vodovodního porubí, zemětřesení, přerušení dodávky el.energie,
- Technické, tj. porucha HW a sítí, nestandardní chování SW produktů, poškození datových úložišť či nosiče, napadení malwarem či virem,
- Personální, což je odcizení a využití cizí identity neoprávněnou osobou, neoprávněná změna dat, vyzrazení osobních údajů, či citlivých dat,
- Ostatní, tj. krádež HW, nebo nosičů dat, průnik do vnitřní sítě zvenčí.

Případná realizace některých hrozeb může mít pro MěÚ různé následky:

- Omezení provozu MěÚ,
- Finanční ztráty,
- Nedodržení právních předpisů a nařízení,
- Ztrátu citlivých či důležitých dat.

7.7.2 Bezpečnostní postupy

Zajištění fyzické bezpečnosti

Objekt |MěÚ je v pracovní době dvousměnného cyklu hlídán pracovníky městské policie, pracujícími ve veřejném aktivním víceúčelovém a přehledovém dozorovém režimu.

MěÚ je mechanicky chráněn plášťovou ochranou, která se skládá z dvouplášťového zdiva o šířce 40cm, vchodových dveří, prány pro vjezd z tepaných kovových prvků a okenních prvků. Dveře vstupů do objektu jsou dřevěné masivní osazené kováním s cylindrickými vložkami. Cylindrické vložky do vstupů budovy, a taktéž dveře do kanceláří zpracovávajících osobní údaje mají 3 stupeň zabezpečení. Stejný způsob je použit u místností, kde jsou provozovány ISVS a IS MěÚ, včetně pracoviště dohledu CCTV, navíc jsou chráněny ocelovým plechem vyztuženými dveřmi (bezpečnostní třída 5-6)

a zamřížovanými okenními prvky. Zbývající dveřní výplně, pokud jsou jejich části prosklené, mají zabezpečení ochrannou fólií.

Z důvodu zamezení neoprávněného vstupu do objektu MěÚ je v objektu instalováno elektronické zabezpečovací zařízení (EZS), zabezpečující prostorovou ochranu. Detektory EZS jsou umístěny na chodbách, vybraných místnostech a vstupních dveřích. Obsluhováno je přes ústřednu Digiplex 48 s ovládacími panely a poplachovými tlačítky. Zaměstnanci MěÚ mají přiděleny kódy pro ovládání EZS. Pravidla pro práci se zabezpečovacím systémem upravuje vnitřní směrnice MěÚ. Prostory, kde se nacházejí klíčové prostředky ISVS jsou prohlášeny za neveřejné, vstup do nich je povolen pouze za doprovodu informatika, popřípadě zástupce vedení úřadu. Tyto prostory jsou vybaveny prvky EZS.

Kanceláře s běžnými pracovišti počítačů uživatelů a tiskárnami jsou v případě nepřítomnosti zaměstnanců zabezpečeny uzamčením.

Vedení datové kabeláže je zabezpečeno vedením ve zdech, na nechráněných místech je zakrytováno, aby bylo dostatečně chráněno před vnějšími vlivy a byla dodržena všechna bezpečnostní opatření.

Síťové prvky a servery MěÚ jsou napojeny na systém UPS (nepřetržitého napájení), který zajistí dostatek času pro start záložního naftového generátoru s automatickým startem, kdy jakmile dojde k přerušení dodávky el.energie, automatika provede nastartování generátoru. Poté dojde k odpojení chráněného okruhu od vnější sítě a po tom co generátor dosáhne potřebného výkonu jej připojí na chráněný rozvod el.energie, což trvá přibližně dvě minuty.

O umístění počítačů, tiskáren a jiných koncových zařízení rozhoduje informatik MěÚ tak, aby byla dodržena všechna doporučení výrobce.

Reakce na přírodní či fyzické hrozby

Tuto problematiku řeší obecně směrnice MěÚ vydávaná tajemníkem MěÚ, krizové a evakuační plány a jiné. Nebezpečí je zaznamenáno buď bezpečnostním elektronickým zařízením, nebo díky lidskému faktoru a je ihned předáno krizovému štábu.

Informatik je odpovědný za informační systém MěÚ. V současné době jsou veškerá data ISVS a data ve složkách uživatelů a odborů zálohována na serveru v jiné budově. Informatik musí zajistit, aby v případě hrozby byly případné škody minimalizovány.

Prioritním úkolem je tedy odvezení serverů, které je třeba vypnout a odvést mimo dosah nebezpečí.

Protipožární ochrana

Protipožární ochrana budovy MěÚ je řešena pomocí organizačních směrnic a v souladu s platnými předpisy. Evakuační plán budovy MěÚ byl zpracován, jsou označeny únikové trasy na chodbách. Budova je vybavena hasicími práškovými přístroji a požárními hydranty. V souladu s platnými předpisy jsou prováděny pravidelné revize hasicích přístrojů, požárních hydrantů, elektrického zařízení i celé budovy. Úřad má zpracovanou dokumentaci PO a BOZP včetně revizních zpráv, provádí pravidelná školení požární ochrany a bezpečnosti a ochrany zdraví při práci.

Organizační a administrativní opatření, personální bezpečnost

Pravidla, oprávnění a zodpovědnost bezpečnosti IT jsou na pracovištích MěÚ stanovena a každý uživatel s nimi musí být seznámen a proškolen. Jde o dokumenty interních směrnic, ve kterých jsou obsaženy předpisy týkající se IS MěÚ včetně odkazů na platné legislativní nařízení. Jedná se o následující dokumenty:

- Pracovní řád MěÚ, co je závazná vnitřní směrnice o povinnosti zachovávat mlčenlivost o osobních údajích a citlivých informacích,
- Provozní řád IS MěÚ, který ustanovuje předpisy o provozu IS v provedení interní směrnice, která je závazná pro všechny osoby zaměstnané na MěÚ a případné další osoby, které využijí služeb IS,
- Havarijní plán stanovuje způsob obnovy provozu IS Městského úřadu, nebo jeho části po bezpečnostním incidentu (havárie, napadení, atd.).

Zachování důvěrnosti dat ošetříme tak, že v případě pracovních míst, kde se uživatel IS setkává nebo pracuje s daty, která obsahují osobní informace či jiné citlivé údaje, je nutné prověřit zaměstnance a do pracovní smlouvy zapracovat článek ošetřující zachování důvěrnosti.

Plán zálohování dat stanovuje přesně formu a způsob provádění procesu zálohování dat. Definuje četnost, rozsah a způsob uchovávání archivních datových sad.

Řízení přístupu do IS Městského úřadu, kdy má uživatel přístup jen k programovému vybavení, které může využít z hlediska svých bezpečnostních oprávnění, vycházejících z organizačního zařazení uživatele. O přístupu k SW vybavení rozhodne vedoucí příslušného odboru v závislosti na vykonávaných úkolech a funkčnímu zařazení uživatelů. Identifikace a přístup uživatelů do IS je spravován centrálně. Bezpečnostní komise úroveň přístupu periodicky reviduje. Po ukončení práce s programem má uživatel povinnost se co nejdříve z programu odhlásit.

Pro platnost dat v IS Městského úřadu je důležité přenesení zodpovědnosti za udržování dat v aktuálním stavu na konkrétní osoby. Provozní řád IS Městského úřadu definuje základní pravidla pro bezpečné chování uživatelů. Všem uživatelům IS jsou při nástupu do zaměstnání jasně vysvětleny bezpečnostní požadavky, je provedeno poučení a vyškolení nového zaměstnance. Jsou vyškoleni v základních bezpečnostních opatřeních (používání ISVS, antivirové ochrany IS, metody řešení komplikaci, které můžou mít za následek ohrožení bezpečnosti IS). Uživatelé jsou proškoleni o riziku při instalaci nových agend, nebo jejich aktualizací a postupech pro plnění pracovních úkolů.

Uživatel je vždy povinný oznámit bezpečnostnímu správci jakékoliv podezření na porušení bezpečnosti IS MěÚ.

MěÚ definuje způsob postihu zaměstnance, při porušení bezpečnostní politiky, či bezpečnostních postupů a metod stanovených směrnicemi MěÚ.

Incidenty, které mají za následek porušení bezpečnosti IS MěÚ, jsou povinně zadokumentovány a záznamy uchovávány. Za dokumentaci, provozní deníky, evidenci poruch atd. odpovídá bezpečnostní správce. V případě nepřítomnosti kompetentních osob, např. s administrátora ISVS, bezpečnostního správce, členů bezpečnostní komise, je nutné mít stanoveného zástupce, který bude případné bezpečnostní situace řešit.

Použití informačních technologií

Pro autentizaci uživatele k IS Městského úřadu je používán uživatelský login a heslo, které uživatel nesmí sdělovat dalším osobám. Metodika tvorby, používání, vypršení (exspirací) hesla, zamykání účtu přihlášení (login) po neúspěšných pokusech o autentizaci je důležitou součástí Provozního řádu IS Městského úřadu .

Řízení přístupu znamená nastavení bezpečného přístupu k datům, chráněného přihlašovacími hesly, při čemž dostatečná délka hesel je alespoň 8 znaků, při použití velkých a malých písmen, alfanumerických znaků a jiného znaku, při nastavení automatického odhlašování ze systému po např. 20 minutách nečinnosti, zabezpečení prostředků výpočetní techniky, hlavně se jedná o povinnost odhlašování z IS při odchodu z pracoviště.

Aktuálnost antivirových programů a jejich virových bází je zajištěna formou automatické aktualizace na lokální server dálkovým přístupem přes Internet. Koncové stanice provádějí automatický update či upgrade proti lokálnímu serveru.

Pro chráněnou komunikaci prostřednictvím internetu je používáno šifrování dat. Další uplatnění šifrování dat je na přenosných IT zařízeních jako notebooky, USB flash disky a další, jako ochrana před neoprávněným získáním a možným zneužitím dat v případě ztráty či odcizení přenosného zařízení či nosiče dat. Přístup na Internet je zabezpečen prostředky na ochranu před neautorizovaným přístupem do vnitřní sítě IS Městského úřadu (firewall).

Monitorování bezpečnosti IS Městského úřadu, je automatizované, je zaznamenáván provoz serverů, fyzických přístupů do prostor úřadu mimo pracovní dobu, záznam poruch. Přenosná zařízení znamenají další bezpečnostní rizika (notebooky, mobilní telefony, PDA, USB flash disky a další mobilní přenosná zařízení obsahují často citlivé informace. Jejich ztráta může vést k vysokým bezpečnostním či ekonomickým rizikům pro MěÚ, je nutné zabezpečení pomocí šifrování dat. Dále mobilní zařízení vystavují sítě potenciálním bezpečnostním hrozbám, jako je neoprávněný vstup do IS Městského úřadu, nebezpečí zavlečení virů, trojských koní či jiného škodlivého SW. Zásady používání a bezpečnosti přenosných ICT zařízení a nosičů dat jsou nedílnou důležitou součástí Provozního řádu IS Městského úřadu.

7.8 Analýza rizik

Aktivum znamená něco co je hodnotné pro MěÚ, co může být poškozeno působením nějaké hrozby. Jedná se například o dokumentaci, datové soubory, SW, HW či dodávku elektrické energie. Správná identifikace aktiv ISVS je důležitá pro možnost jejich ochrany.

Pro zhotovení analýzy rizika je třeba nejdřív udělat seznam aktiv, které se člení na hmotná, nehmotná (SW, softwarově zaznamenaná datová informační aktiva, know how) a služby.

Evidence aktiv (v rámci IS) se obvykle opírá o analýzu současného stavu IS, kde jsou identifikována nehmotná informační a softwarová aktiva, hmotná aktiva a služby.

Dále je provedena evidence a ohodnocení aktiv dle metodiky ČSN ISO/IEC TR 13335. Aktiva jsou členěna dle ČSN ISO/IEC 17799 na nehmotná informační aktiva, nehmotná softwarová aktiva, hmotná aktiva a služby.

Pro každé aktivum je v příslušné tabulce uveden odhad možných škod vyplývající ze ztráty důvěrnosti, integrity nebo dostupnosti aktiv. Pro posuzování těchto důsledků (dle závažnosti škody) byla zvolena následující kritéria:

A	ohrožení osobní bezpečnosti
B	ohrožení bezpečnosti prostředí
C	porušení legislativy a / nebo předpisù
D	vysoké omezení výkonu činnosti úřadu
E	střední omezení výkonu činnosti úřadu
F	nízké omezení výkonu činnosti úřadu
G	přímá finanční ztráta vetší než 1 000 000 Kč
H	přímá finanční ztráta vetší než 100 000 a menší než 1 000 000 Kč
I	přímá finanční ztráta menší než 100 000 Kč
J	porušení obchodního tajemství
K	ztráta dobrého jména/negativní vliv na dobrou pověst
X	žádné (závažné) důsledky

Tabulka 13 Kritéria posouzení důsledků [Zdroj:vlastní]

Pro posouzení obnovitelnosti aktiva byla zvolena následující kritéria:

1	velmi obtížná obnovitelnost v řádech měsíců
2	středně obtížná obnovitelnost v řádech týdnů
3	snadná obnovitelnost v řádech hodin až dnů

Tabulka 14 Kritéria obnovitelnosti aktiva [Zdroj:vlastní]

Nehmotná informační aktiva

Nehmotná informační aktiva rozdělujeme do dvou kategorií, na citlivá a veřejná.

Veřejná, či veřejně dostupná, u těchto nehmotný informačních aktiv není uplatňován požadavek důvěrnosti. Tato aktiva bývají často součástí veřejných datových služeb, které poskytuje veřejná správa veřejnosti obvykle dálkovým přístupem pomocí Internetu. Zde je

naopak důležitým požadavkem dostupnost služby. Tedy je zde velmi důležitý požadavek dostupnosti a integrity.

Citlivá nehmotná informační aktiva nejsou veřejně přístupná. Musí splňovat požadavek důvěrnosti. Citlivá nehmotná informační aktiva můžeme dále dělit na dvě podkategorie, podle síly požadavku důvěrnosti:

- Zda dojde v případě porušení důvěrnosti k trestnému činu, nebo v méně závažném případě k přestupku (dle zákona o ochraně osobních údajů a/nebo dokonce zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti),
- Porušením důvěrnosti informačních aktiv k porušení zákona nedojde, bude ale např. vyzrazeno obchodní tajemství, zaměstnanec se kompromitací aktiva dopustí porušení pracovní kázně, jsou poškozeny oprávněné zájmy, utrpí pověst úřadu či samosprávného celku.

Přehled nehmotných informačních aktiv s ohodnocením důsledků plynoucích ze ztráty důvěrnosti, integrity a dostupnosti, s ohodnocením obnovitelnosti aktiv je uveden v příloze P XI.

Seskupování aktiv

Aktiva s podobnými charakteristikami a podobností odhadu důsledků možných škod způsobených ztrátou důvěrnosti, integrity nebo dostupnosti lze sdružit a zavést seskupení aktiv:

- Zavádíme skupinu „klíčová informační aktiva“, která mají pro úřad zásadní důležitost, zahrnují data SW: ekonomický systém s účetnictvím, spisová služba, systém agend veřejné správy (administrativní a správní, analytická a zpracovatelská nástavba ekonomicko-účetních procesů), mzdový a personální systém, přestupky, matriky, volby, stavební úřad, vodoprávní úřad, silniční úřad, Správní agendy a Dopravní agendy, GIS, evidence a registry, digitální archiv dokumentů, HelpDesk, webové stránky, elektronická podatelna, elektronická pošta.
- Skupinu „další informační aktiva“, která zahrnují data SW: pasport dopravy, správa komunikací, správa zeleně, EVI (evidence odpadů), automatizovaná správa SW licencí a evidence a monitoring IT vybavení, program komunikace s bankou,

- Skupinu „anti-malware SW a firewall“, která zahrnuje data SW: Anti-Virus, Anti-Spyware, Anti-Rootkit, Anti-Spam, Firewall (na všech klientských stanicích a serverech antivirový software, ochrana elektronické pošty, ochrana před nákazou z Internetu, antivirová kontrola přenosných médií a zařízení, ochrana před spyware, adware a dalšími škodlivými programy).

Nehmotná softwarová aktiva můžeme též členit:

- Skupina „operační systémy“, která zahrnuje operační systémy, kterou můžeme členit na podskupiny:
    - Operační systémy pro servery,
    - Operační systémy pro PC,
    - Skupinu „databázové engine“, MS SQL, Oracle,,
    - Skupinu „zálohovací SW“,
- Skupinu pro „aplikace“, kterou můžeme členit na podskupiny:
    - klíčové aplikace, jejich výčet je u klíčových informačních aktiv,
    - Další aplikace, jejich výčet je u dalších informačních aktiv,
- nebo dělit na:
    - vlastní aplikace,
    - aplikace druhých stran, která zahrnuje všechny aplikace mimo vlastních.

Nehmotná softwarová aktiva

- Operační systémy serverové, operační systémy osobních počítačů, databázové engine, SW pro ochranu před škodlivým kódem (antivirové SW, antispyware a antiadware atd.), zálohovací SW a další serverové systémy, viz příloha P XII.
- Aplikace, tj. vlastní SW, hodnocený bez dat, (nehmotná softwarová aktiva) viz příloha P XII.

Hmotná informační aktiva

Patří mezi ně HW a síťová infrastruktura, viz. příloha P XII.

Služby

U některých služeb je Městský úřad příjemcem služby, jinde je poskytovatelem služby.

Název aktiva	Důsledky plynoucí ze ztráty			Obnovitelnost
	důvěrnosti	integrity	dostupnosti	
dodávky elektrické energie	–	D	D	3
komunikační kanály pro přímé bankovnictví	G	G	F	2
připojení do sítě Internet a služby	B	E	E	3
e-podatelna, e-pošta (e-mail), WEB server	A	B	C	2

Tabulka 15 Služby [Zdroj:vlastní]

Pro stanovení relativní hodnoty aktiva se použije nejzávažnější důsledek, který plyne z porušení důvěrnosti, integrity anebo dostupnosti předmětného aktiva. Přihlédnuto bude rovněž k obnovitelnosti aktiva. Pro relativní ohodnocení aktiv byla stanovena následující stupnice:

Relativní hodnota	Zahrnuje důsledky	Zahrnuje obnovitelnost
velice vysoká	A, B, C	
vysoká	D, G	1
střední	E, H, I, J	2
nízká	F, K, X	3

Tabulka 16 Služby – ohodnocení aktiv [Zdroj:vlastní]

Relativní hodnota nehmotných informačních aktiv - tabulka viz. příloha P XIII.

Relativní hodnota nehmotných softwarových aktiv - tabulka viz. příloha P XIII.

Relativní hodnota hmotných informačních aktiv - tabulka viz. příloha P XIII.

Relativní hodnota služeb - tabulka viz. příloha P XIII.

7.8.1 Analýza rizik a identifikace hrozeb

Cílem této kapitoly je identifikovat hrozby, které mohou nepříznivě ovlivnit aktiva informačního systému Městského úřadu. Identifikace hrozeb vychází z metodiky ISVS, a je doplněna v souladu s ČSN ISO/IEC TR 13335.

Seznam hrozeb

Id hrozby	Popis hrozby
H1	předstírání identity uživatele
H2	použití softwaru neautorizovanými uživateli
H3	zneužití privilegií – použití SW neautorizovaným způsobem
H4	popření (anonymita prováděných akcí)
H5	prozrazení dat během přenosu
H6	prozrazení dat na paměťovém mediu
H7	modifikace dat na paměťovém mediu
H8	modifikace dat v databázi
H9	modifikace dat při přenosu
H10	technické selhání síťových komponent
H11	selhání hardware
H12	poškození paměťového media
H13	zemětřesení
H14	povodeň a voda z potrubí
H15	požár
H16	selhání dodávky energie
H17	selhání klimatizace
H18	krádež, násilný trestný čin
H19	škodlivý software (viry, trojské koně)

Tabulka 17 Seznam hrozeb [Zdroj:vlastní]

Odhad pravděpodobností výskytu

Označení	Pravděpodobnost výskytu hrozby
nepravděpodobné	méně než jedenkrát za 20 let
málo pravděpodobné	přibližně jedenkrát za 6 – 20 let
Příležitostné	přibližně jedenkrát za 1 – 5 let
pravděpodobné	několikrát za rok
Časté	několikrát za týden

Tabulka 18 Pravděpodobnost výskytu hrozeb [Zdroj:vlastní]

Uvedenou stupnici použijeme ke stanovení pravděpodobnosti výskytu pro každou identifikovanou hrozbu. Odhadovanou pravděpodobnost výskytu přiřadíme seznamu hrozeb, viz příloha P XIV.

Dopad hrozeb

Pro popis dopadů hrozeb na aktiva IS MěÚ použijeme následující stupnici:

Dopad hrozby	Zkratka	Popis
katastrofický	KA!	nevratná situace, porušení zákona, ztráta klíčového systému, významné škody vedoucí k výpadku v řádech měsíců
kritický	KR!	významné škody vedoucí k přerušení provozu v řádech dnů přímá finanční ztráta
vážný	V	významné škody vedoucí k přerušení provozu v řádech hodin
okrajový	O	drobná škoda napravitelná v rámci pravidelné údržby
zanedbatelný	Z	zanedbatelné následky

Tabulka 19 Popis dopadů hrozeb [Zdroj:vlastní]

7.8.2 Analýza rizik a zranitelnosti aktiv

Je možné vytvořit další vyhodnocovací tabulku:

- řádky tabulky = aktiva
- sloupce tabulky = označení (id) hrozby

V relačních polích tabulky by pak byla uvedena označení (id) popisů dopadů hrozeb - tvořená písmenem a číslem a přes id odkazují na tabulku, kde je popis hrozby. Tabulku by bylo nutné realizovat v přiměřeně velkém měřítku (cca 20 typů hrozeb = 20 sloupců tabulky, počet řádek tabulky = počtu sledovaných aktiv). Takto vzniklá tabulka by nebyla přehlednou prezentací závěrů analýzy zranitelnosti všech aktiv analyzovaných v předchozích kapitolách, ale je to možná metoda. Z tohoto důvodu použijeme zjednodušenou tabulku pro analýzu rizik.

7.8.3 Analýza rizik a posouzení výše rizika

Na základě odhadu pravděpodobnosti a dopadu hrozby pro datová aktiva stanovíme výši rizika dle následující tabulky:

Pravděpodobnost	Dopad hrozby				
	katastrofický	kritický	vážný	okrajový	zanedbatelný
časté	nepřijatelné	nepřijatelné	nepřijatelné	poškozující	poškozující
pravděpodobné	nepřijatelné	nepřijatelné	poškozující	poškozující	přijatelné
příležitostné	nepřijatelné	poškozující	poškozující	přijatelné	přijatelné
málo pravděpodobné	poškozující	poškozující	přijatelné	přijatelné	zanedbatelné
nepravděpodobné	poškozující	přijatelné	přijatelné	zanedbatelné	zanedbatelné

Tabulka 20 Výše rizika [Zdroj:vlastní]

Výsledná výše rizika je interpretována následujícím způsobem:

Id	Riziko	Popis
A!	nepřijatelné	Riziko nelze tolerovat, musí být odstraněno
B	poškozující	Riziko je vhodné odstranit, při volbě řešení je nutné zvážit náklady
C	přijatelné	Pokud je riziko monitorováno, je přijatelné
X	zanedbatelné	Riziko není významné, není třeba jej dále analyzovat

Tabulka 21 Výše rizika [Zdroj:vlastní]

Nyní by mohly následovat další vyhodnocovací tabulky, při čemž:

- řádky tabulky = aktiva
- sloupce tabulky = označení (Id) hrozby

-V relačních polích tabulky by byla uvedena označení výše závažnosti rizik - tvořená písmenem a číslem a tato tabulka by odkazovala na tabulku způsobu interpretace výše rizika, v níž je popis závažnosti rizika. Takto mohou být opět vytvořeny tabulky naznačené skladby pro všechna aktiva analyzovaná v předchozích kapitolách. Z důvodu nízké srozumitelnosti takové tabulky je použita zjednodušená tabulka pro analýzu rizik.

7.8.4 Zjednodušená tabulka pro analýzu rizik

Zde je použita zjednodušená metoda pro analýzu rizik:

U každého aktiva je uveden odhad doby obnovy provozu po havárii (D – dny, T – týdny, M – měsíce) a zároveň stanovena jeho informační hodnota (1 – nízká, 2 – střední, 3 – vysoká). V následující tabulce jsou ohodnocena aktiva podle informační hodnoty a doby obnovitelnosti. Je-li někde doba obnovitelnosti T (případně M) a hodnota aktiva 3, celý řádek je pak označen tučným písmem jako kritické aktivum.

Mezi hmotná kritická aktiva patří ponejvíce servery a aktivní prvky, viz. tabulka v příloze P XV.

V nehmotných aktivech jsou uvedeny a ohodnoceny všechny SW produkty, včetně produktů na serverech, viz. tabulka v příloze P XV.

Aktiva služeb, viz. tabulka v příloze P XV.

Některá provozovaná aktiva jsou vzhledem k jejich informační hodnotě a době obnovitelnosti označena jako kritická. Tato aktiva se v tabulkách zvýrazní.

Kritickým aktivům je zapotřebí věnovat zvýšenou pozornost s důrazem na snižování možných rizik ohrožení na co nejnižší míru.

Kritická aktiva jsou ve velké míře závislá na externích zdrojích. Je proto nutné, aby dodavatelé těchto aktiv a souvisejících služeb byli smluvně zavázáni k servisním zásahům v určitých časových termínech.

Pokud zabezpečení kritických aktiv není řešeno formou outsourcingu a je možné bezproblémový provoz určitých aktiv zvládnout vlastním personálem, musí být kladen důraz na trvalé systematické zvyšování kvalifikace těchto pracovníků.

Analýza je přínosem k poznání problému. Konečným cílem analýzy aktiv a rizik, jako součásti bezpečnostní politiky, by neměly být jen tabulky, ale pohled do problematiky hrozeb a rizik, jejich popis a odhalení, vyhodnocení stupně jejich nebezpečnosti a získání tak východiska k přípravě a tvorbě opatření, protiopatření, metodik a předpisů.

K analýze aktiv a vyhodnocení rizik je nutno se opakovaně vrátit vždy při vyhodnocení bezpečnostní politiky a informační koncepce po roce provozu IS.

7.9 Shrnutí bezpečnostní politiky

Vzhledem k dříve realizovaným a průběžně dodržovaným a kontrolovaným opatřením a zavedeným bezpečnostním pravidlům dosahuje informační systém Městského úřadu vysoké bezpečnostní úrovně a odolnosti vůči v tomto dokumentu pojmenovaným hrozbám. Zde jsou některé z nich: předstírání identity uživatele, zneužití softwaru neautorizovanými uživateli, selhání hardware, poškození paměťového média, selhání dodávky energie, krádež a škodlivý SW.

Dále jsou ohrožena aktiva provozovaná na lokálních stanicích uživatelů, která mohou být zničena poškozením HW (nebo paměťového média), pokud jsou porušena pravidla pro zálohování, např. na server.

Nejvýznamnějšími hrozbami jsou nadále prozrazení nebo modifikace dat během přenosu, odesíláním informací pocházejících z informačního systému otevřeným způsobem e-mailovou korespondencí. Dále vynesení či přímo odcizení informací pomocí nezabezpečeného notebooku nebo na datových nosičích (klasický HDD, disketa, CD, DVD, USB flash disk).

Nejvíce ohroženými aktivy jsou nehmotná informační aktiva IS Radnice VERA, a z hmotných aktiv převážně servery. Aktiva jsou nejvíce ohrožena hrozbami: škodlivý software, trojské koně a viry, prozrazení a modifikace dat na paměťovém médiu, krádež a násilný trestný čin, požár a povodeň resp. vyplavení.

Z provedené analýzy vyplývá nutnost snížení úrovně rizik u hrozeb identifikovaných jako nepřijatelné či poškozující. Vzhledem k tomu, že tato úroveň rizik je identifikována u hrozeb:

- Prozrazení a modifikace dat během přenosu,
- Použití softwaru neautorizovanými uživateli,
- Krádež, násilný trestný čin,
- Požár a povodeň,

doporučuje analýza tato bezpečnostní opatření:

- Přemístění serverů do bezpečnější lokality s bezpečnostními dveřmi, kontrolou přístupu, vyvýšenou podlahou, EZS, požárním čidlem a klimatizací,
- Šifrování přenosu dat mezi rádiovými pojítky,
- Šifrování citlivých dat na mobilních zařízeních (notebooky, USB disky, CDROM),
- Zabezpečení spojení mezi vnitřní sítí a mobilními prostředky při jejich použití mimo prostory organizace (pomocí VPN),
- Registrace MAC adres, kterým je dynamicky přidělována IP či statické přidělování IP adres,
- Stanovení pracovních předpisů popisujících postup při ukončení práce a práci s uživatelskými hesly.

ZÁVĚR

Cílem této diplomové práce bylo navržení implementace bezpečnostní politiky do informačního systému veřejné správy. Při zpracování tohoto tématu jsem využil znalosti z prostředí administrace informačních systémů veřejné správy a jejich zabezpečení.

Teoretická část práce popisuje prostředí veřejné správy a jejich informačních systémů. Postupným vývojem legislativy bylo dosaženo stanovení právního rámce nutného pro nasazení informačních systémů v oblasti veřejné správy. Na tomto základě pak probíhal vývoj jednotlivých informačních systémů, popisovaný v teoretické části, a jejich postupné propojování, tak jak rostly nároky na vlastnosti, které by měl ISVS obsáhnout.

V praktické části na základě vývoje ISVS, byla dle platných právních předpisů a norem provedena analýza současného stavu používaných informačních systémů v organizaci veřejné správy. Jako modelový příklad byl zvolen městský úřad, který svým záběrem vykonávaných činností obsáhne podstatnou část dnešních ISVS. Po vypracování analýzy v kapitolách Informační strategie a Informační koncepce byly závěry těchto analýz použity pro zpracování bezpečnostní analýzy ISVS. Shrnutím bezpečnostní analýzy je, že díky realizovaným opatřením a používaným bezpečnostním pravidlům dosahuje IS MěÚ vysoké bezpečnostní úrovně a odolnosti vůči analyzovaným hrozbám. Dále byla nalezena nejvíce ohrožená aktiva a doporučeny bezpečnostní opatření pro snížení rizik na přijatelnou úroveň. V kapitole bezpečnostní politika byl popsán návrh implementace bezpečnosti v informačním systému veřejné správy, stanovený jako hlavní cíl diplomové práce. Ve třech kapitolách praktické části byl vypracován návrh na zpracování tří klíčových dokumentů potřebných pro implementaci bezpečnostní politiky informačního systému.

Hlavním přínosem této diplomové práce je navržený popis kroků s návazností jednotlivých postupně vytvořených analýz na sestavení dokumentace informační bezpečnosti, která slouží k jako základní podklad pro provedení auditu kybernetické bezpečnosti.

Ve státní správě je pro budoucnost předpoklad ještě větší centralizace v oblasti zdrojů dat. Postupně zřejmě dojde ke slučování dosud různorodých agendových informačních systémů na jednotnou aplikaci AIS administrovanou Ministerstvem vnitra. Logickým předcházejícím krokem bude dle zjištěných bezpečnostních rizik upuštění od rizikového využívání datových center soukromých firem k ukládání citlivých osobních dat

občanů. Pro účely ISVS budou využívána pouze datová centra ve vlastnictví státní správy a samosprávy, u kterých bude možné garantovat provoz při přijatelně nízké míře rizika pro bezpečné uložení a přenos dat mezi oprávněnými uživatelskými subjekty. Pro komunikaci mezi stanicemi uživatelů státní správy a samosprávy a rozhraním registrů veřejné správy budou využívány sítě plně oddělené od veřejných internetových sítí. Postupně bude dosaženo velmi vysokého stupně zabezpečení při daleko větších možnostech využití služeb státní správy občany, než je možné v dnešní době.

ZÁVĚR V ANGLIČTINĚ

The goal of this dissertation thesis was the design of the implementation of a security policy in the public administration information system field. In the process of this topic was used the knowledge of the administration information system of public administration and its security environment.

The theoretical part of the dissertation thesis describes the environment of the public administration and its information system. During the sequential process of legislative the determination of juridical scope essential for the placing of information system in the public administration area was achieved. On the grounds of this the development of individual information systems described in the theoretical part took place, and its gradual interconnection as the demands on the properties were rising, which the ISVS should have covered.

In the practical part was on the grounds of the ISVS development in accordance to valid legal regulations and norms analysed the current situation of the employed information systems in the organization of the public administration. As a model example was chosen the municipality which with its range of the performed activities covers the fundamental part of today's ISVS. After the preparation of the analysis in the chapters of Information Strategies and Information Concepts the conclusions of these analyses were used for the processing of security analysis of ISVS. Its conclusion is because of the realization of measures and usage of security regulations, the is MEU reaches a high safety level and resistance to analysed threats. Moreover the most threatened activity was discovered and the security regulations for the reduction of risks to the acceptable level were recommended. In the chapter of the security policy the design of the implementation of security in the information system in public administration was described, which was the main aim of the dissertation thesis. In three chapters of the practical part the design of the making of three key documents required for the implementation of the security policy of information system was covered.

The main contribution of this dissertation thesis is considered the proposition of the steps and connection to individual analyses for the composition of documentation of information safety, which serves as the essential foundation for the execution of the cybernetic safety audit.

The supposition in the state administration is for the future even bigger centralization in the area of the data sources. Gradually apparently there will be unification of up to now diverse agenda information systems for united application AIS administration of Ministry of the Interior. Logical preceding step was be the abandonment of the security risk use of data centre of private companies for depositing delicate personal data of citizens. For the purposes of ISVS the data centre in the ownership of state administration and self-government will be only used, in which will be possible to guarantee the operation of acceptable low risk measurement for the safety placing and transfer of data among authorized user entity. For the communication between state and local administration users stations and the boundary of public administration registry will be making use of network fully separated from the public internet networks. Gradually will be reached a high level of security in bigger opportunities for usage of services in the public administration, than is possible in these days.

SEZNAM POUŽITÉ LITERATURY

[1] **Svoboda, Ivo a Schelle, Karel.** *Základy organizace veřejné správy.* Ostrava : KEY Publishing s.r.o., 2006. ISBN 80-239-8011-4.

[2] **Horzinková, Eva a Novotný Vladimír.** *Základy organizace veřejné správy v ČR.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2010. ISBN 978-80-7380-263-9.

[3] **Atlas consulting spol. s r.o.** *Právní systém Codexis.* Praha : Atlas consulting spol. s r.o., 2015.

[4] **Provazníková, Romana a Sedláčková, Olga.** *Financování měst, obcí a regionů: teorie a praxe.* Praha : Grada, 2009. stránky 26, 304. ISBN 978-80-247-2789-9.

[5] **Jašek, Roman a Malaník, David.** *Bezpečnost informačních systémů.* Zlín : UTB ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978 - 80 - 7454 - 312 - 8.

[6] **Hronek, Jiří.** *Informační systémy.* Olomouc : Univerzita Palackého, Přírodovědecká fakulta, Katedra informatiky, 2007. učební text.

[7] **Špaček, David.** *eGovernment - cíle, trendy a přístupy k jeho hodnocení.* Praha : C. H. Beck, 2012. ISBN 978-80-7400-261-8.

[8] **Pomahač, Richard a a kolektiv.** *Veřejná správa.* Praha : C. H. Beck, 2013. ISBN 978-80-7400-447-6.

[9] **Peterka, Jiří.** Quo vadis, KIVS? *lupa.cz.* [Online] Internet Info, s.r.o., 9. 1 2012. [Citace: 20. 4 2015.] Dostupné z: http://www.lupa.cz/clanky/quo-vadis-kivs/.

[10] **Ministerstvo vnitra ČR.** mvcr.cz. *eGON a Klaudie - symboly eGovernmentu.* [Online] Ministerstvo vnitra ČR, 2015. [Citace: 20. 4 2015.] Dostupné z: http://www.mvcr.cz/egon-a-klaudie-symboly-egovernmentu.aspx.

[11] **Národní centrum kybernetické bezpečnosti.** govcert.cz. *Národní centrum kybernetické bezpečnosti.* [Online] Národní centrum kybernetické bezpečnosti, 19. 12 2014. [Citace: 26. 04 2015.] Dostupné z: http://www.govcert.cz/cs/legislativa/legislativa/.

[12] **Felix, Ondřej.** *Kyberbezpečnost = architektonická bezpečnost. Egevernment, č.2* Praha : info.com s.r.o., 2014, stránky 20-22. ISSN 18019420.

[13] **Správa základních registrů.** *Správa základních registrů.* [Online] Správa základních registrů, 04 2015. [Citace: 03. 05 2015.] Dostupné z: http://www.szrcr.cz/co-jsou-to-zakladni-registry.

[14] **Úřad pro ochranu osobních údajů, Talandová, Jana**. *Kick off projektu uoou.cz.* [Online] 2013. [Citace: 28. 04 2015.] Dostupné z: https://www.uoou.cz/ke-stazeni/ds-1969/archiv=0&p1=1933.

[15] **Správa základních registrů.** Podmínky pro připojení AIS do ISZR. *szrcr.cz.* [Online] 02. 01 2015. [Citace: 28. 04 2015.] Dostupné z: http://www.szrcr.cz/file/170/.

[16] **Peterka, Jiří.** *Báječný svět elektronického podpisu.* Praha : CZ.NIC, z. s. p. o., 2011. ISBN: 978-80-904248-3-8 .

[17] **Dostálek, Libor a kolektiv.** *Velký průvodce protokoly TCP/IP: Bezpečnost.* Praha : Computer Press, 2001. ISBN 80-7226-513-X.

[18] **Doseděl, Tomáš.** *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, a.s., 2004. ISBN 80-251-0106-1.

[19] **Ministerstvo vnitra ČR.** mvcr.cz. *Informace k přechodu k bezpečnějším kryptografickým algoritmům v oblasti elektronického podpisu.* [Online] 27. 1 2010. [Citace: 29. 04 2015.] Dostupné z: http://www.mvcr.cz/soubor/informace-k-prechodu-k-bezpecnejsim-kryptografickym-algoritmum-v-oblasti-elektronickeho-podpisu.aspx.

[20] **Mates, Pavel a Smejkal, Vladimír.** *E-government v České republice: Právní a technologické aspekty.* 2.podstatně přepracované a rozšířené vydání. Praha : Leges, 2012. ISBN 978-80-87576-36-6.

[21] **Ministerstvo vnitra České republiky.** Aktuální statistiky Czech POINT. *czechpoint.cz.* [Online] Ministerstvo vnitra České republiky, 1. 5 2015. [Citace: 2. 5 2015.] Dostupné z: http://www.czechpoint.cz/web/?q=node/488.

[22] **Software602 a.s.** Download Form Filler. *602.cz.* [Online] Software602 a.s., 27. 4 2015. [Citace: 27. 4 2015.] Dostupné z: http://www.602.cz/produkty/form_filler/download.

[23] **Svoboda, Jaroslav.** Elektronický portál územních samospráv ePUSA. *inforum.cz.* [Online] 25. 5 2006. [Citace: 27. 4 2015.] Dostupné z: http://inforum.cz/pdf/2006/Svoboda_Jaroslav.pdf.

[24] **Tesař, Pavel. Seznam orgánů veřejné moci**. *institutpraha.cz.* [Online] 27. 6 2011. [Citace: 26. 4 2015.] Dostupné z: http://www.institutpraha.cz/obj/obsah_fck/seminar_eGON/elektronizace_VS/SOVM_prezentace_20110627.pdf.

[25] **Tesař, Pavel; Ministerstvo vnitra ČR;.** Provozní řád ISDS. *datoveschranky.info.* [Online] 15. 12 2014. [Citace: 22. 4 2015.] Dostupné z: https://www.datoveschranky.info/documents/1744842/1746058/provozni_rad_isds.pdf/a49d0691-d02d-44fd-8068-c158599de574.

[26] **Ministerstvo vnitra ČR.** Služby pro informační systémy veřejné správy ČR. *sluzby-isvs.cz.* [Online] Ministerstvo vnitra ČR, 2015. [Citace: 28. 4 2015.] Dostupné z: http://www.sluzby-isvs.cz/.

[27] **Ministerstvo vnitra ČR.** O informačním systému o státní službě. *mvcr.cz/sluzba.* [Online] Ministerstvo vnitra ČR, 4 2015. [Citace: 2. 5 2015.] Dostupné z: http://www.mvcr.cz/sluzba/docDetail.aspx?docid=21894157&doctype=ART.

[28] **Ministerstvo pro místní rozvoj ČR.** Informační systém o veřejných zakázkách. *www.portal-vz.cz.* [Online] Ministerstvo pro místní rozvoj ČR, 2015. [Citace: 29. 03 2015.] Dostupné z: http://www.portal-vz.cz/cs/Informacni-systemy-a-elektronicke-vzdelavani/Information-System-on-Public-Contracts.

[30] **Odbor strukturálních fondů Ministerstva vnitra České republiky.** osf-mvcr.cz. *Portál strukturálních fondů Ministerstva vnitra ČR.* [Online] QCM s.r.o., 2015. [Citace: 2. 4 2015.] Dostupné z: http://www.portal-vz.cz/cs/Informacni-systemy-a-elektronicke-vzdelavani/NIPEZ.

[31] **Odbor strukturálních fondů Ministerstva vnitra České republiky.** http://www.osf-mvcr.cz. *Národní infrastruktura pro elektronické zadávání veřejných zakázek - manažerské shrnutí.* [Online] 18. 6 2010. [Citace: 03. 04 2015.] Dostupné z: http://www.osf-mvcr.cz/file/1959_1_1.

[32] **Ministerstvo pro místní rozvoj ČR.** NEN. *portal-vz.cz.* [Online] [Citace: 02. 04 2015.] Dostupné z: http://www.portal-vz.cz/cs/Informacni-systemy-a-elektronicke-vzdelavani/NIPEZ/NEN.

[33] **Ministerstvo pro místní rozvoj ČR.** Shrnutí informací k monitorovacímu systému MS2014+. *http://www.strukturalni-fondy.cz.* [Online] 7. 4 2015. [Citace: 12. 04 2015.]

Dostupné z: http://www.strukturalni-fondy.cz/cs/Informace-a-dokumenty/Novinky/Shrnuti-informaci-k-monitorovacimu-systemu

[34] **ČTK.** Spouštění monitorovacího systému evropských fondů nabírá zpoždění. *zpravy.e15.cz.* [Online] 12. 04 2015. [Citace: 15. 04 2015.] Dostupné z: http://zpravy.e15.cz/domaci/udalosti/spousteni-monitorovaciho-systemu-evropskych-fondu--zpozdeni-1179860#utm_source=rubrika-domaci&utm_medium=selfpromo&utm_campaign=e15rss.

[35] **European Business Enterprise a.s.** www.ebe.cz. *Výzkumné projekty.* [Online] 2015. [Citace: 28. 3 2015.] Dostupné z: http://www.ebe.cz/ebe/redakce.nsf/i/vyzkum.

[36] **European Business Enterprise, s.r.o.** www.zive.cz. *Databáze dodavatelů na serveru www.statnisprava.cz.* [Online] 30. 7 2001. [Citace: 28. 03 2015.] Dostupné z: http://www.zive.cz/zpravy-z-firem/databaze-dodavatelu-na-serveru-wwwstatnispravacz/sc-5-a-102183/default.aspx.

[37] **European Business Enterprise a.s.** www.dodavatele.statnisprava.cz. *Server statnisprava.cz.* [Online] European Business Enterprise a.s., 2015. [Citace: 28. 3 2015.] Dostupné z: http://dodavatele.statnisprava.cz/ebe/redakce.nsf/i/server_statnisprava_cz.

[38] **Jašek, Roman.** *Ochrana znalostí a dat v podnikových informačních systémech.* Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. ISBN 80-7318-095-2.

[39] **AutoCont CZ a .s.** Povinnosti pro organizace. *kybernetickyzakon.cz.* [Online] AutoCont CZ a .s., 12 2014. [Citace: 26. 04 2015.] Dostupné z: http://www.kybernetickyzakon.cz/?gclid=COedyeXCtsUCFcjnwgodR4EADg.

[40] **Risk Analysis Consultants.** Řada norem ISO/IEC 27000. *iso27000.cz.* [Online] Risk Analysis Consultants, 2015. [Citace: 28. 4 2015.] Dostupné z: http://www.iso27000.cz/.

[41] **TECHNOR. TECHNOR.** *technicke-normy-csn.cz.* [Online] Technor, webdesign eStudio, 3 2010. [Citace: 25. 4 2015.] Dostupné z: http://www.technicke-normy-csn.cz/technicke-normy/elektrotechnika-36/identifikacni-karty-a-ochrana-dat-3697/.

[42] **Tobolka, Martin.** Změny a dopady nové normy ISO/IEC 27001:2013. *systemonline.cz.* [Online] CCB spol. s r.o., 8 2014. [Citace: 26. 04 2015.] Dostupné z: http://www.systemonline.cz/clanky/zmeny-a-dopady-nove-normy-iso-iec-27001-2013.htm. ISSN:1802-615X.

[43] **Risk Analysis Consultants, s. r.o.** RAMSES: Řízení bezpečnosti informací organizace. *rac.cz.* [Online] Risk Analysis Consultants, s. r.o., 04 2015. [Citace: 29. 4 2015.] Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/Ramses.

[44] **ADVICE.CZ.** Atestace IS. Praha : ADVICE.CZ, 2010. Dostupné z: http://www.advice.cz/.

[45] **Nortcutt, Stephen, a další.** *Bezpečnost počítačových sítí.* Brno : CP Books, a.s., 2005. ISBN 80-251-0697-7.

[46] **COMPACT OFFICE, s.r.o.** Atestace ISVS. *compact-office.cz.* [Online] COMPACT OFFICE, s.r.o., 2015. [Citace: 28. 04 2015.] Dostupné z: http://www.compact-office.cz/atestace-isvs/.

[47] **TAYLLOR & COX s.r.o.** Co je Atestace ISVS? *tayllorcox.cz.* [Online] TAYLLOR & COX s.r.o.,, 2015. [Citace: 28. 4 2015.] Dostupné z: http://www.tayllorcox.cz/atestace-isvs.html.

[48] **Risk Analysis Consultants, s. r.o.** RAMSES: Řízení bezpečnosti informací organizace. *rac.cz.* [Online] Risk Analysis Consultants, s. r.o., 04 2015. [Citace: 29. 4 2015.] Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/SS/$FILE/RAC%20Rizeni%20bezpecnosti%20informaci_Datasheet_CZ_100521%20Screen.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IS	Informační systém.
ISVS	Informační systém veřejné správy.
VS	Veřejná správa.
NKÚ	Nejvyšší kontrolní úřad.
ČSÚ	Český statistický úřad.
SIS	Státní informační systém.
ÚSIS	Úřad pro státní informační systém
SIP	Státní informační politika.
ICT	Informační a komunikační technologie.
KIVS	Komunikační infrastruktura veřejné správy.
NCKB	Národní centrum kybernetické bezpečnosti.
CERT	Computer Emergency Response Team.
CSIRT	Computer Security Incident Response Team.
NBÚ	Národní bezpečnostní úřad.
MěÚ	Městský úřad.
OÚ	Obecní úřad.
HW	Hardware.
SW	Software.
IT	Informační technologie.
AIS	Agendový informační systém.
eGON	Symbol elektronizace veřejné správy.
ROB	Registr obyvatel.
ROS	Registr osob.
RPP	Registr práv a povinností.

ORG	Převodník identifikátorů fyzických osob.
OVM	Orgán veřejné moci.
SZR	Správa základních registrů.
AIFO	Agendový identifikátor fyzické osoby.
ZIFO	Základní identifikátor fyzické osoby.
RÚIAN	Registr územní identifikace, adres a nemovitostí.
ISZR	Informační systém základních registrů.
ÚOOÚ	Úřad pro ochranu osobních údajů.
IDM	Identity Manager, kategorie SW nástrojů k řízení a správě identit.
ESB	Egon Service Bus, sběrnice pro komunikaci AIS a ZR.
JIP	Jednotný identitní prostor, součást centrály Czech POINT.
KAAS	Katalog autentizačních a autorizačních služeb, součást eGovernmentu.
DS	Datová schránka.
e-PUSA	Portál územních samospráv.
Seznam OVM	Seznam orgánů veřejné moci.
IS o ISVS	Informační systém o informačních systémech veřejné správy.
IS DP	Informační systém o datových prvcích.
JeDP	Jednoduchý datový prvek.
SIDP	Složený datový prvek.
IS VZ	Informační systém o veřejných zakázkách.
NIPEZ	Národní infrastruktura pro elektronické zadávání veřejných zakázek.
NEN	Národní elektronický nástroj pro zadávání veřejných zakázek.
IEN	Individuální elektronické nástroje.
TED	Tendered Electronic Daily – el.verze dodatku k úřednímu věstníku EU.
MS2014+	Monitorovací systém evropských strukturálních a investičních fondů pro programové období 2014–2020.

ESIF	Evropské strukturální a investiční fondy.
CMS	Systém pro správu obsahu, redakční systém.
BP	Bezpečnostní politika.
IK	Informační koncepce.
ISMS	Systém řízení bezpečnosti dat a informací.
PHA	Preliminary Hazard Analysis (předběžná analýza ohrožení).
QRA	Process Quantitative Risk Analysis (analýza kvantitativních rizik procesu).
HAZOP	Hazard Operation Process (analýza ohrožení a provozuschopnosti).
FMEA	Failure Mode and Effect Analysis (identifikace závažnosti a četnosti poruch).
UMRA	Universal Matrix of Risk Analysis (univerzální matice rizikové analýzy).
SWOT	Strengths, Weaknesses, Oportunities, Threats (Analýza silných a slabých stránek, příležitostí a hrozeb).
PDCA	Demingův cyklus, plánuj, dělej, kontroluj, jednej.
NAS	Network Attached Storage, síťové úložiště.
TPS	Řízení na taktické úrovni.
MIS	Strategické řízení.
EIS	Podpora kancelářských prací a týmové práce.
OIS	Podpora kancelářských prací a týmové práce.
EDI	Zajištění komunikace s okolím.
EZS	Elektronické zabezpečovací zařízení.
PO	Požární ochrana.
BOZP	Bezpečnost a ochrana zdraví při práci.
UPS	Uninterruptable Power Supply, nepřerušitelný zdroj napájení.
CCTV	Systém průmyslové televize, kamerový systém.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: PRÁVNÍ PŘEDPISY A TECHNICKÉ NORMY PRO ISVS [3]

Zákon č. 365/2000 Sb., ze 14. září 2000, o informačních systémech veřejné správy ve znění zákonů č. 517/2002 Sb., č. 413/2005 Sb., č. 444/2005 Sb., č. 70/2006 Sb., č. 81/2006 Sb., č. 230/2006 Sb., č. 110/2007 Sb., č. 269/2007 Sb., č. 130/2008 Sb., č. 190/2009 Sb., č. 223/2009 Sb., č. 227/2009 Sb., č. 281/2009 Sb., č. 263/2011 Sb., č. 18/2012 Sb., č. 167/2012 Sb. a č. 64/2014 Sb.

Zákon č. 148/1998 Sb., z 11. července 1998, o ochraně utajovaných skutečností, ve znění zákonů č. 164/1999 Sb., č. 18/2000 Sb., č. 29/2000 Sb., č. 30/2000 Sb., č. 363/2000 Sb., č. 60/2001 Sb., nálezu Ústavního soudu č. 322/2001 Sb., zákonů č. 151/2002 Sb., č. 310/ 2002 Sb., č. 320/2002 Sb., č. 436/2003 Sb., č. 257/2004 Sb., č. 386/2004 Sb., č. 190/2005 Sb., nálezu Ústavního soudu č. 220/2005 Sb., zákonů č. 290/2005 Sb., č. 413/2005 Sb., č. 250/2008 Sb., č. 41/2009 Sb. a č. 255/2012 Sb.,

Zákon č. 106/1999 Sb., z 11. května 1999, o svobodném přístupu k informacím, ve znení dalších předpisů,

Zákon č. 101/2000 Sb., ze 4. dubna 2000, o ochraně osobních údajů, ve znění pozdějších předpisů,

Zákon č. 128/2000 Sb., ze 12. dubna 2000, o obcích (obecní zřízení), ve znění pozdějších předpisů,

Zákon č. 227/2000 Sb., z 29. června 2000, o elektronickém podpisu, ve znení dalších předpisů a v duchu prováděcích vyhlášek,

Zákon č. 240/2000 Sb., z 28. června 2000, o krizovém řízení a o změně některých zákonů, ve znění pozdějších zákonů ,

Zákon č. 412/2005 Sb., z 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti,

Zákon č. 499/2004 Sb., z 30.června 2004, o archivnictví a spisové službě a o některých zákonů, ve znení dalších předpisů,

Zákon č. 500/2004 Sb., z 24. června 2004, správní řád, ve znění pozdějších předpisů,

Vyhláška č. 523/2005 Sb.,z 5.prosince 2005, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor

Vyhláška č. 528/2005 Sb., z 14. prosince 2005, o fyzické bezpečnosti a certifikaci technických prostředků,

Zákon č. 137/2006 Sb., ze 14. března 2006, o veřejných zakázkách, ve znění pozdějších předpisů,

Vyhláška č. 442/2006 Sb., z 31. srpna 2006, kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup, ve znění vyhlášky č. 416/2008 Sb.,

Vyhláška č. 469/2006 Sb., z 3. října 2006, o informačním systému o datových prvcích,

Vyhláška č. 529/2006 Sb., z 23. listopadu 2006, o dlouhodobém řízení informačních systémů veřejné správy,

Vyhláška č. 378/2006 Sb., z 19. července 2006, o postupech kvalifikovaných poskytovatelů certifikačních služeb,

Vyhláška č. 52/2007 Sb., z 13. března 2007, o postupech atestačních středisek při posuzování způsobilosti k realizaci vazeb informačních systémů veřejné správy prostřednictvím referenčního rozhraní,

Vyhláška č. 53/2007 Sb., z 13. března 2007, o referenčním rozhraní (mezi ISVS),

Vyhláška č. 64/2008 Sb., ze 7. února 2008, o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti),

Zákon č. 300/2008 Sb., ze 17. července 2008, o elektronických úkonech a autorizované konverzi dokumentů,

Zákon č. 301/2008 Sb., ze 17. července 2008, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.

Zákon č. 111/2009 Sb., z 26. března 2009, o základních registrech, ve znění pozdějších předpisů,

Vyhláška č. 193/2009 Sb., ze 17. června 2009, o stanovení podrobností provádění autorizované konverze dokumentů,

Vyhláška č. 194/2009 Sb., ze 23.června 2009, o stanovení podrobností užívání a provozování informačního systému datových schránek, ve znění vyhlášky č. 422/2010 Sb.,

Nařízení vlády č. 432/2010 Sb., z 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb., z 8. prosince 2014,

Nařízení vlády č. 161/2011, z 25. května 2011, o stanovení harmonogramu a technického způsobu provedení opatření podle § 64 až 68 zákona o základních registrech,

Zákon 181/2014 Sb., z 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů.

Zákon č. 234/2014 Sb., z 1. října 2014, o státní službě,

Vyhláška č.316/2014 Sb., z 15. prosince 2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti.

Vyhláška č.317/2014 Sb., z 15. prosince 2014, o významných informačních systémech a jejich určujících kritériích.

PŘÍLOHA P II TECHNICKÉ NORMY PRO ISVS [40] [41]

ČSN ISO/IEC 27000 (369790) Informační technologie, Bezpečnostní techniky, Systémy řízení bezpečnosti informací, Přehled a slovník

ČSN ISO/IEC 27001 (369797) Informační technologie, Bezpečnostní techniky, Sytém řízení bezpečnosti informací, Požadavky.

ČSN ISO/IEC 27002 (369798) Informační technologie, Bezpečnostní techniky, Soubor postupů pro management bezpečnosti informací.

ČSN ISO/IEC 27003 (369790) Informační technologie, Bezpečnostní techniky, Směrnice pro implementaci systému řízení bezpečnosti informací.

ČSN ISO/IEC 27004 (369790) Informační technologie, Bezpečnostní techniky, Řízení bezpečnosti informací, Měření.

ČSN ISO/IEC 27005 (369790) Informační technologie, Bezpečnostní techniky, Řízení rizik bezpečnosti informací.

ČSN ISO/IEC 27006 (369790) Informační technologie, Bezpečnostní techniky, Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

ČSN ISO/IEC 15408-1 (369789) Informační technologie, Bezpečnostní techniky, Kritéria pro hodnocení bezpečnosti IT, Část 1: Úvod a obecný model.

ČSN ISO/IEC 15408-2 (369789) Informační technologie, Bezpečnostní techniky, Kritéria pro hodnocení bezpečnosti IT, Část 2: Bezpečnostní funkční komponenty.

ČSN ISO/IEC 15408-3 (369789) Informační technologie, Bezpečnostní techniky, Kritéria pro hodnocení bezpečnosti IT, Část 3: Komponenty bezpečnostních záruk.

ČSN ISO/IEC 17799:2005 (369790) Informační technologie, Bezpečnostní techniky, Soubor postupů pro management bezpečnosti informací. ISO/IEC 17799 byla zveřejněním dne 13.8.2007 začleněna do nové řady série 27000 a to jako ISO/IEC 27002.

PŘÍLOHA P III: VÝZNAMNÉ INFORMAČNÍ SYSTÉMY DLE PŘÍLOHY Č.1 VYHLÁŠKY Č. 317/2014 SB [3]

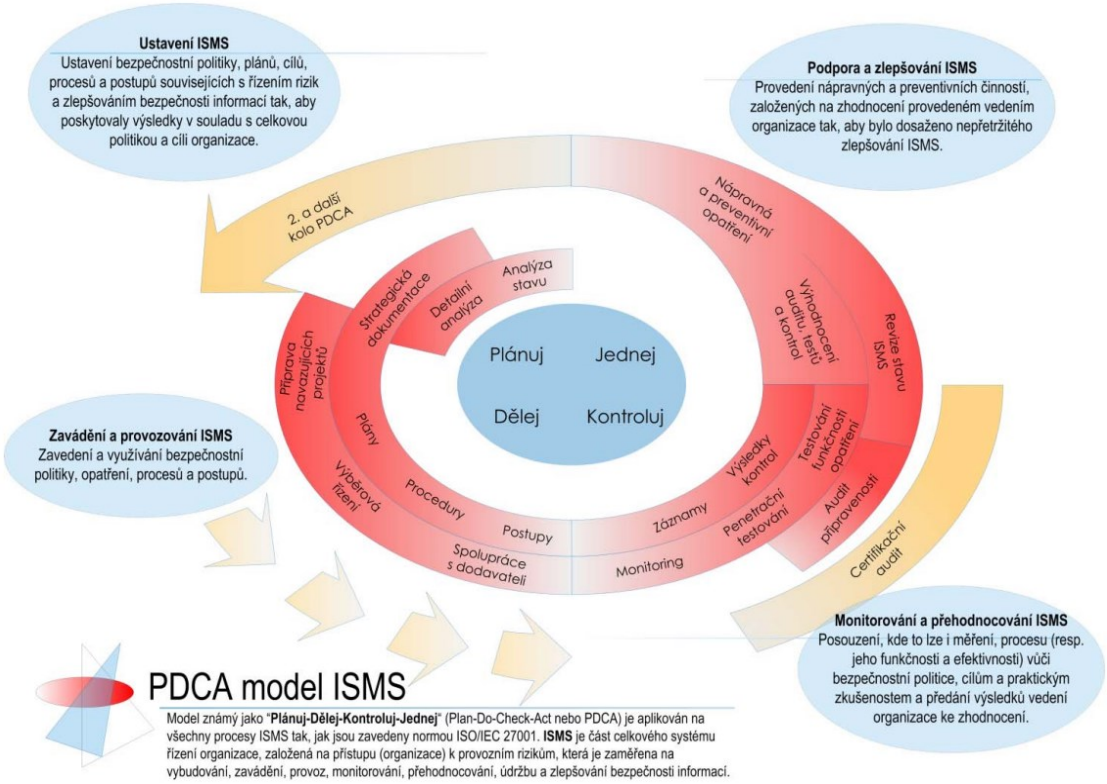
PČ	Správce	Název
1	Česká inspekce životního prostředí	Centrální informační systém (CIS)
2	Český statistický úřad	Integrovaný agendový informační systém registru osob (IAIS – ROS)
3	Český statistický úřad	Soustava statistických registrů (SSREG)
4	Český telekomunikační úřad	Automatizovaný systém monitorování kmitočtového spektra (ASMKS)
5	Český telekomunikační úřad	Systém pro podporu správy kmitočtového spektra (Spectra)
6	Český telekomunikační úřad	Modulární správní systém (MOSS)
7	Český úřad zeměměřický a katastrální	IS územní identifikace (ISÚI)
8	Český úřad zeměměřický a katastrální	Informační systém katastru nemovitostí (ISKN)
9	Energetický regulační úřad	Jednotný informační systém ERÚ
10	Generální finanční ředitelství	Automatizovaný daňový informační systém (ADIS)
11	Generální ředitelství cel	Centrální registr subjektů (CRS)
12	Generální ředitelství cel	Informační systém agendy celního a daňového řízení
13	Ministerstvo dopravy	Aplikace pro testování nových řidičů a dopravců v rámci autoškol (eTesty)
14	Ministerstvo dopravy	Centralizovaný informační systém STK (CIS STK)
15	Ministerstvo dopravy	Centrální registr dopravců (CRD)
16	Ministerstvo dopravy	Centrální registr řidičů (CRŘ)
17	Ministerstvo dopravy	Centrální registr vozidel (CRV)
18	Ministerstvo dopravy	Informační systém o silniční a dálniční síti ČR (ISSDS ČR)
19	Ministerstvo dopravy	Informační systém pro podporu při schvalování technické způsobilosti vozidel (ZTP)
20	Ministerstvo dopravy	IS Digitální tachograf (ISDT)
21	Ministerstvo dopravy	Databáze vozidel (DAVOZ)
22	Ministerstvo dopravy	Přeprava nebezpečných věcí (ADR)

PČ	Správce	Název
22	Ministerstvo dopravy	Přeprava nebezpečných věcí (ADR)
23	Ministerstvo dopravy	Systém elektronického mýta (MÝTO)
24	Ministerstvo financí	Evidenční dotační systém/Správa majetku ve vlastnictví státu (EDS/SMVS)
25	Ministerstvo financí	Integrovaný informační systém státní pokladny (IISSP)
26	Ministerstvo financí	Informační systém programového financování (ISPROFIN)
27	Ministerstvo financí	VIOLA
28	Ministerstvo obrany	Biologický a monitorovací informační systém
29	Ministerstvo obrany	Informační systém mobilizačních příprav
30	Ministerstvo obrany	Informační systém o službě a personálu
31	Ministerstvo obrany	Informační systém Vojenské policie
32	Ministerstvo obrany	LETVIS
33	Ministerstvo obrany	Síť včasného zjištění armádní radiační monitorovací sítě (SVZ ARMS)
34	Ministerstvo obrany	Štábní informační systém AČR
35	Ministerstvo obrany	Zdravotnický informační systém
36	Ministerstvo práce a sociálních věcí	Informační systém pomoci v hmotné nouzi
37	Ministerstvo práce a sociálních věcí	Informační systém registr poskytovatelů sociálních služeb
38	Ministerstvo práce a sociálních věcí	Informační systém v oblasti zaměstnanosti
39	Ministerstvo práce a sociálních věcí	Informační systém o dávkách státní sociální podpory
40	Ministerstvo práce a sociálních věcí	Informační systém o příspěvku na péči
41	Ministerstvo práce a sociálních věcí	Informační systém o dávkách pro osoby se zdravotním postižením
42	Ministerstvo práce a sociálních věcí	Informační systém sociálně–právní ochrany dětí
43	Ministerstvo práce a sociálních věcí	Jednotný informační systém práce a sociálních věcí

PČ	Správce	Název
43	Ministerstvo práce a sociálních věcí	Jednotný informační systém práce a sociálních věcí
44	Ministerstvo průmyslu a obchodu	IS Registru živnostenského podnikání
45	Ministerstvo spravedlnosti	Centrální evidence stíhaných osob
46	Ministerstvo spravedlnosti	Evidence znalců a tlumočníků – prezentační část
47	Ministerstvo spravedlnosti	Informační systém Rejstříku trestů (RT)
48	Ministerstvo spravedlnosti	Informační systém registru obchodního rejstříku (ISROR)
49	Ministerstvo spravedlnosti	Informační systém insolvenčního rejstříku (ISIR)
50	Ministerstvo školství, mládeže a tělovýchovy	Informační systém uznávání kvalifikací (ISKA)
51	Policie České republiky	Informační systém cizinců
52	Policie České republiky	Informační systém ZBRANĚ
53	Policie České republiky	Informační systém Policie ČR
54	Ministerstvo vnitra	Czech POINT – systém kontaktních míst veřejné správy
55	Ministerstvo vnitra	Informační systém datových schránek (ISDS)
56	Ministerstvo vnitra	Informační systém evidence cestovních dokladů (ISECD)
57	Ministerstvo vnitra	Informační systém evidence občanských průkazů (ISEOP)
58	Ministerstvo vnitra	Informační systém evidence obyvatel (ISEO)
59	Ministerstvo vnitra	Portál veřejné správy (PVS)
60	Ministerstvo vnitra	Rejstřík politických stran a politických hnutí
61	Ministerstvo vnitra	Ústřední evidence nabytí a pozbytí státního občanství České republiky
62	Ministerstvo zahraničních věcí	Víza ČR (EVC2)
63	Ministerstvo zahraničních věcí	Systém na pořizování, přenos a zpracování žádostí o cestovní doklad s biometrickými prvky (ePasy)

PČ	Správce	Název
64	Ministerstvo zdravotnictví	Ochrana veřejného zdraví
65	Ministerstvo zemědělství	Informační systém VODA
66	Ministerstvo zemědělství	Informační systém vodovodů a kanalizací (ISVaK)
67	Ministerstvo zemědělství	Integrovaný zemědělský registr (IZR)
68	Ministerstvo zemědělství	Evidence využití půdy podle uživatelských vztahů (LPIS)
69	Ministerstvo zemědělství	Společný zemědělský registr (SZR)
70	Ministerstvo životního prostředí	Integrovaný registr znečišťování životního prostředí
71	Ministerstvo životního prostředí	Integrovaný systém plnění ohlašovacích povinností
72	Ministerstvo životního prostředí	Informační systém SEA
73	Ministerstvo životního prostředí	Informační systém EIA
74	Nejvyšší kontrolní úřad	Kontrolní informační systém
75	Probační a mediační služba	Agendový informační systém AIS PMS
76	Správa státních hmotných rezerv	Informační systém pro plánování civilních zdrojů Argis (ISARGIS)
77	Správa státních hmotných rezerv	IS Krizkom
78	Správa základních registrů	Formulářový agendový informační systém (FAIS)
79	Správa základních registrů	Systém řízení přístupů do základních registrů (RACS)
80	Státní zemědělský a intervenční fond	Informační systém platební agentury (IS PA)
81	Státní úřad pro jadernou bezpečnost	Registr externích adres (REA)
82	Státní ústav pro kontrolu léčiv	Centrální úložiště elektronických receptů
83	Státní ústav pro kontrolu léčiv	Registr léčivých přípravků s omezením
84	Úřad pro civilní letectví	IS úřadu pro civilní letectví (IS ÚCL)
85	Úřad pro ochranu osobních údajů	Informační systém Úřadu pro ochranu osobních údajů (IS ÚOOÚ)
86	Úřad pro zastupování státu ve věcech majetkových	Informační systém majetku státu (ISMS)
87	Úřad průmyslového vlastnictví	Informační systém duševního vlastnictví (ISDV)
88	Úřad vlády České republiky	Elektronická knihovna legislativního procesu (eKLEP)
89	Ústav zdravotnických informací a statistiky České republiky	Národní zdravotnický informační systém (NZIS)
90	Vězeňská služba České republiky	Vězeňský informační systém (VIS)
91	Všeobecná zdravotní pojišťovna České republiky	Centrální registr pojištěnců
92	Zeměměřický úřad	IS veřejné správy zeměměřictví

PŘÍLOHA P IV: PCDA MODEL ISMS [48]



Pramen: **Risk Analysis Consultants, s. r.o.** RAMSES: Řízení bezpečnosti informací organizace. *rac.cz.* [Online] Risk Analysis Consultants, s. r.o., 04 2015. [Citace: 29. 4 2015.] http://www.rac.cz/rac/homepage.nsf/CZ/SS/$FILE/RAC%20Rizeni%20bezpecnosti%20informaci_Datasheet_CZ_100521%20Screen.pdf

PŘÍLOHA P V: SERVERY ISVS A JEJICH CHARAKTERISTIKA [ZDROJ: VLASTNÍ]

Název serveru	**HP**
Účel, funkce	Informační systém MěÚ, virtualizace
Operační systém	VMware vSphere 6
SW	Virtualizované servery
HDD	RAID 10 4x 300GB
CPU	Intel Xeon E5-2620v3 (2.4GHz/6-core/ 15MB Level 3 cache)
RAM	16 GB

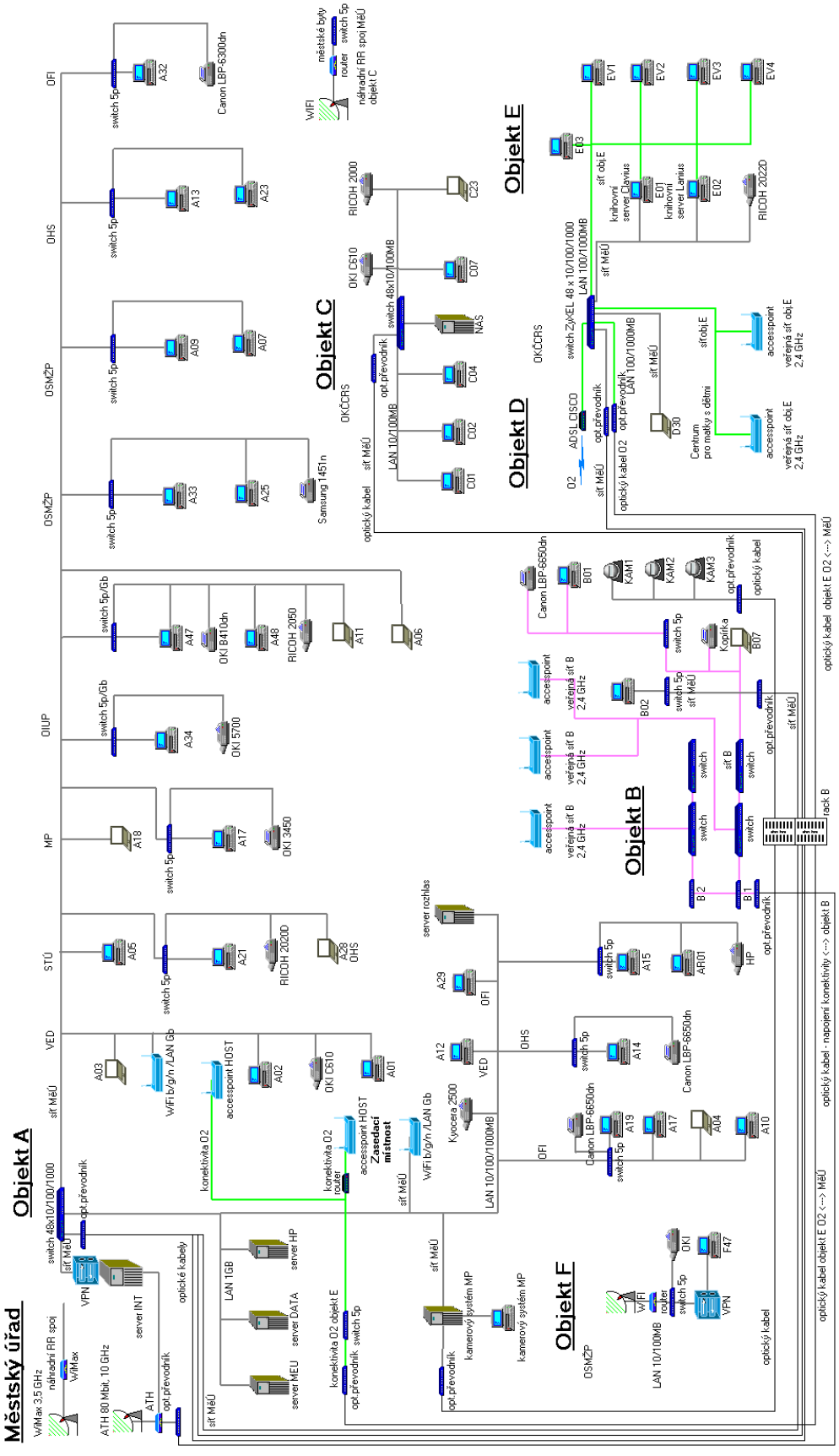
Název serveru	**MEU**
Účel, funkce	Informační systém MěÚ
Operační systém	Virtualizovaný RED HAT Enterprise Linux server v.6.6
SW	IS Radnice VERA, Informix
HDD	RAID 10 4x 300GB
CPU	Intel Xeon E5-2620v3 (2.4GHz/6-core/ 15MB Level 3 cache)
RAM	8 GB

Název serveru	**Rozhlas**
Účel, funkce	Rozhlas, protipovodňový systém
Operační systém	MS Windows Server 2012
SW	Rozhlas, výstražný systém
HDD	RAID 1 2 x 300GB
CPU	Intel Xeon E5- 2,4GHz
RAM	2,5 GB

Název serveru	**Kamerový systém**
Účel, funkce	Digitální bezpečnostní rekordér
Operační systém	Linux
SW	Aplikace kamerového systému
HDD	2 TB
CPU	Specifikace není k dispozici
RAM	Specifikace není k dispozici

Název serveru	**NAS**
Účel, funkce	Zálohovací úložiště
Operační systém	RED HAT EL server v.5.5
SW	IS Radnice VERA, Informix
HDD	RAID 1 2 x 3 TB
CPU	Intel Atom Dual Core D2700 2,13GHz
RAM	1 GB

PŘÍLOHA P VI: SCHÉMA SÍTĚ MĚÚ [ZDROJ: VLASTNÍ]



PŘÍLOHA P VII: FAKTORY SWOT ANALÝZY [ZDROJ: VLASTNÍ]

Faktory seřazené dle důležitosti.

číslo	faktor	důležitost	síla
6	vysoké využití IT v činnostech MěÚ	4	4
1	podpora rozvoje ICT od vedení MěÚ	4	4
5	zaměstnanci vyškolení v IT	4	4
2	dobrý základ infrastruktury sítí	4	3
15	nedostatek finančních prostředků pro rozvoj IT	4	2
10	koordinované řízení rozvoje informatiky (globální strategie města, informační strategie úřadu)	3	4
3	velký počet PC na zaměstnance MěÚ	3	4
4	použití stejného kancelářského SW (MS Office)	3	4
7	definice základních pravidel v IT	3	4
9	Vlastní provoz a rozvoj IS	3	4
14	systém školení uživatelů IT	3	3
13	Komunikace mezi odbory MěÚ	3	3
11	malý podíl agendového přístupu v aplikacích IS (nízká duplicita a nekonzistence dat)	3	3
18	omezené možnosti odměňování zaměstnanců v oblasti IT ve srovnání s komerční sférou	3	1
8	internetové stránky jako prostředek komunikace	2	4
12	projektové řízení	2	3
17	různorodost aplikačního SW	2	2
16	absence metadat (dat o datech) – nepřehlednost dat používaných na MěÚ	0	3

Faktory seřazené dle síly:

číslo	faktor	důležitost	síla
6	vysoké využití IT v činnostech MěÚ	4	4
1	podpora rozvoje ICT od vedení MěÚ	4	4
5	zaměstnanci vyškolení v IT	4	4
10	koordinované řízení rozvoje informatiky (globální strategie města, informační strategie úřadu)	3	4
3	velký počet PC na zaměstnance MěÚ	3	4
4	použití stejného kancelářského SW (MS Office)	3	4
7	definice základních pravidel v IT	3	4
9	vlastní provoz a rozvoj IS	3	4
8	internetové stránky jako prostředek komunikace	2	4
2	dobrý základ infrastruktury sítí	4	3
14	systém školení uživatelů IT	3	3
13	komunikace mezi odbory MěÚ	3	3
11	malý podíl agendového přístupu v aplikacích IS (nízká duplicita a nekonzistence dat)	3	3
12	projektové řízení	2	3
16	absence metadat (dat o datech) – nepřehlednost dat používaných na MěÚ	0	3
15	nedostatek finančních prostředků pro rozvoj IT	4	2
17	různorodost aplikačního SW	2	2
18	omezené možnosti odměňování zaměstnanců v oblasti IT ve srovnání s komerční sférou	3	1

PŘÍLOHA P VIII: INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY POUŽÍVANÉ MĚÚ [ZDROJ: VLASTNÍ]

Úplný název ISVS:	IS Radnice – E-podatelna
Zkratka názvu:	EPOD
Právní předpisy:	Zákon č. 227/2000 Sb., o elektronickém podpisu
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Aplikace pro zajištění provozu elektronické podatelny s využitím kvalifikovaných certifikátů
Zpracovávaná data:	Údaje o elektronických podáních.
Technické a programové prostředí:	Server MeU
Současný stav:	ISVS je v běžném provozu.
Předpokládané změny:	Pro ISVS nejsou plánovány žádné změny.

Úplný název ISVS:	IS Radnice – Spisová služba
Zkratka názvu:	EVP
Právní předpisy:	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Komplexní vedení spisové služby, automatizovaná evidence a oběh písemností v celém jejich životním cyklu
Zpracovávaná data:	Údaje o písemnostech
Technické a programové prostředí:	Server MeU
Současný stav:	ISVS je v běžném provozu.
Předpokládané změny:	Pro ISVS nejsou plánovány žádné změny.

Úplný název ISVS:	EVI 9 – Evidence odpadů, zařízení
Zkratka názvu:	EVI
Právní předpisy:	Evidence odpadů při každém vzniku, zneškodnění, nebo předání odpadu, generování hlášení a statistických výkazů.
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Zákon č. 185/2001 Sb., o odpadech, vyhláška č. 381/2001 Sb., vyhláška č. 383/2001 Sb.
Zpracovávaná data:	Data o odpadech.
Technické aprogramové prostředí:	Intel Core i5-4590, 3.30GHz, 8GB RAM, SSD 120GB, HDD 1TB, Microsoft Windows 8.1 Professional
Současný stav:	ISVS je v běžném provozu.
Předpokládané změny:	Pro ISVS nejsou plánovány žádné změny.

PŘÍLOHA P IX: PROVOZNÍ AGENDY S VAZBOU NA ISVS [ZDROJ: VLASTNÍ]

Úplný název ISVS:	IS Radnice – Registr obyvatel
Zkratka názvu:	ZEO
Právní předpisy:	Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Evidence obyvatel, změny dat
Současný stav:	V běžném provozu.
Vazba na ISVS:	Sesouhlasení dat s Registrem obyvatel

Úplný název ISVS:	UCR – Účetnictví a rozpočet
Zkratka názvu:	UCR
Právní předpisy:	Zákon č. 563/1991 Sb., o účetnictví
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Účetní agenda, výkaznictví
Současný stav:	V běžném provozu.
Vazba na ISVS:	Předávání finančních výkazů MFČR.

Úplný název ISVS:	PERM
Zkratka názvu:	PAM
Právní předpisy:	Zákon č. 262/2006 Sb., zákoník práce, nařízení vlády č. 564/2006 Sb.
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Personální a mzdová agenda
Současný stav:	V běžném provozu.
Vazba na ISVS:	Aplikace poskytuje data do IS o platech

Úplný název ISVS:	Czech POINT
Zkratka názvu:	Czech POINT
Právní předpisy:	Zákon č. 565/2000 Sb., vyhláška 364/2009 Sb.
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Výdej dat z registrů přístupných z aplikace Czech POINT
Současný stav:	V běžném provozu.
Vazba na ISVS:	Registry MVČR

Úplný název ISVS:	ISDS
Zkratka názvu:	Informační systém datových schránek
Právní předpisy:	Zákon č.365/2000 Sb., 300/2008 Sb.,301/2008 Sb., vyhláška č.194/2009 a 193/2009
Provoz zajišťuje:	Informatik MěÚ
Charakteristika:	Elektronické úložiště, které je určeno k doručování orgány veřejné moci a k provádění úkonů vůči orgánům veřejné moci.
Současný stav:	V běžném provozu.
Vazba na ISVS:	MVČR, Česká pošta s.p.

PŘÍLOHA P X: TERMINOLOGIE PRO BEZPEČNOSTNÍ POL. [44]

Aktivum (asset) je cokoliv, co má pro organizaci nějakou (nepominutelnou) hodnotu.
Analýza rizik (risk analysis) je systematické používání informací k odhadu rizika a k určení jeho zdrojů.
Anonymním údajem (z.č.101/2000Sb.) se rozumí takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů.
Autentizace /autentifikace, autentikace, ověřování/ (authentication), proces ověření identity uživatele je ověření toho, že uživatel je skutečně tou osobou, za kterou se vydává. Ověření uživatele je provedeno pomocí uživatelského hesla, USB tokenu iKey („klíčenka"), čipovou kartou, kartou s magnetickým proužkem, ve vyšším stupni pomocí metod biometrie. Doporučuje se kombinovat např. token iKey nebo kartu s použitím hesla.
Autorizace (authorization) je přidělování práv, která uživateli umožňují v informačním systému provádět definované operace, např. přistupovat k určitým systémovým zdrojům. Autorizace je založena na právech, která přiděluje uživatelským účtům správce systému. U neanonymních účtů musí autorizaci předcházet autentizace. Nejčastěji jde o přiřazení práv (oprávnění) již ověřené (autentizované) entitě, tj. obvykle uživateli. Každý uživatel je oprávněn k úkonům odpovídajícím roli, kterou zastává. Nastavení přístupových práv uživatele provádí správce IS na základě schválené matice funkčních míst a uživatelských rolí jednotlivých aplikací provozovaných v IS. Žádný uživatel pak nemá přístup k datům, které nejsou relevantní k jeho funkčnímu zařazení.
Bezpečnost informací (information security) znamená zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
Bezpečnostní incident (information security incident) je jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.
Bezpečnostní událost (information security event) je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostních opatření. Může se také jednat o jinou situaci, která dříve nenastala a může být z pohledu bezpečnosti informací důležitá.
Blokováním osobních údajů (z.č.101/2000Sb.) se rozumí vytvoření takového stavu, při kterém je osobní údaj určitou dobu nepřístupný a nelze jej jinak zpracovávat.
Citlivým údajem (z.č.101/2000Sb. o ochraně osobních údajů) se rozumí osobní údaj vypovídající 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 subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.
Číselníkem (z.č.365/2000Sb.) je seznam přípustných hodnot datového prvku obvykle ve formě dvojic, to znamená kódovaného údaje a hodnoty jeho kódu.
Dálkovým přístupem (z.č.365/2000Sb.) je přístup do informačního systému prostřednictvím sítě nebo služby elektronických komunikací (například s využitím internetu).
Datovým prvkem (z.č.365/2000Sb.) je jednotka dat, která je v daném kontextu dále považována za nedělitelnou a je jednoznačně definována.
Dostupnost dat, Dostupnost **služeb**, Dostupnost **technických a programových prostředků** – znamená zajištění přístupu k aktivům (do požadované nebo stanovené doby), aktiva mají být autorizovaným subjektům dostupná. Jedná se též o odolnost proti odmítnutí služby.
Důvěrná data (confidential data), **důvěrná informace** (confidential information) jsou neveřejné informace, které jsou chráněné před neoprávněným přístupem a zveřejněním (odhalením), zpravidla tak, že s nimi má oprávnění pracovat pouze určitá skupina uživatelů určená přístupovými právy. Též **citlivá data**, **citlivé informace**. Vyšší formou jsou informace obsahující utajované skutečnosti. Nakládání s těmito informacemi a přístup k nim určuje legislativa příslušného státu.
Důvěrnost dat znamená zajistit, že informace nemůže být zjištěna nebo zneužita neautorizovanou osobou.
Důvěryhodnost dat znamená, že uživatel přistupující k požadovaným datům musí mít jednak jistotu, že zpracovává opravdu ta data, o která má zájem (zpravidla lze řešit aplikační logikou), jednak jistotu, že data nebyla neoprávněným způsobem měněna, že se jedná o platná data. Bývá často požíváno jako synonymum k pojmu integrita dat.
Evidencí nebo **datovým souborem osobních údajů** (z.č.101/2000Sb.) se rozumí jakýkoliv soubor osobních údajů uspořádaný nebo zpřístupnitelný podle společných nebo zvláštních kritérií.
Hodnocení rizik (risk assessment) je celkový proces analýzy a vyhodnocení rizik. Riziko zanedbatelné, běžné, katastrofické.
Hrozba (threat) je označení pro potenciální příčinu nežádoucího incidentu, která může vyústit v poškození IS nebo úřadu. Hrozba představuje možnost útoku. Hrozba existuje díky zranitelnosti systému, který obhospodařuje aktiva úřadu.
Identifikací rozumíme určení (zjištění, zadání) uživatelovy identity, například tím, že vloží (zapíše nebo potvrdí) své uživatelské jméno nebo kód (username, user-ID), („bez jeho ověřování", to bývá až v dalším kroku).

Informační bezpečnost je chápána jako nedílný celek složený z jednotlivých bezpečnostních opatření jak v oblasti bezpečnosti ICT, tak i personálních opatření, zabezpečení fyzické bezpečnosti s cílem ochrany aktiv a pro zajištění dostupnosti, integrity a důvěrnosti informací, jež pokrývají celé spektrum činností úřadu.
Informační činnosti (z.č.365/2000Sb.) je 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.
Informační koncepce (z.č.365/2000Sb.) je dokument, v němž 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.
Informační systémy veřejné správy (z.č.365/2000Sb.) jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Jsou jimi i informační systémy zajišťující činnosti podle zvláštních zákonů (např. zákon č. 455/1991 Sb., o živnostenském podnikání /živnostenský zákon/, zákon č. 117/1995 Sb. o státní sociální podpoře, zákon č. 111/2006 Sb., o pomoci v hmotné nouzi, a další).
Informačním systémem (z.č.365/2000Sb.) 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.
Integrita dat znamená zabezpečit ochranu dat před neautorizovanou záměrnou či nezáměrnou modifikací.
Likvidací osobních údajů (z.č.101/2000Sb.) se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání, nebo jejich trvalé vyloučení z dalších zpracování. Pozn.: postup spolehlivého a zaručeného vymazání zapsané informace z nosiče (harddisk, disketa, atd.) musí být popsáno přesnou metodikou. Pouhé smazání informace z nosiče je častou příčinou kompromitace (nechtěného zveřejnění) osobních, ale i citlivých údajů.
Management rizik (risk management) jsou koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika. Management rizik zpravidla zahrnuje hodnocení rizik, zvládání rizik, akceptaci a seznámení s rizikem.
Metodický postup, **doporučení**, postup (guideline) je popis, který objasňuje co a jak má být uděláno k dosažení cílů stanovených v jednotlivých politikách úřadu.
Odhlášení (logout, logoff) je proces odhlášení uživatele od víceuživatelského systému, počítačové sítě, online služby apod.
Opatření (control), (bezpečnostní opatření), (protiopatření), je prostředek managementu rizik, zahrnuje politiky, směrnice, metodické pokyny, praktiky nebo organizační struktury, které mohou být povahy administrativní, technické, řídící nebo legislativní.
Osobním údajem (z.č.101/2000Sb. o ochraně osobních údajů) se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.
Politika (policy) představuje celkový záměr a směr formálně vyjádřený vedením úřadu.
Provozní dokumentací (z.č.365/2000Sb.) je dokumentace informačního systému veřejné správy, která popisuje funkční a technické vlastnosti informačního systému. Provozní dokumentaci ISVS tvoří tyto dokumenty (dle vyhlášky č. 529/2006 Sb.): a) bezpečnostní dokumentace ISVS, (Bezpečnostní politika ISVS a Bezpečnostní směrnice pro činnost bezpečnostního správce systému), b) systémová příručka, c) uživatelská příručka.
Provozním informačním systémem (z.č.365/2000Sb.) je informační systém zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy. Některé integrované IS mohou spadat do obou kategorií, pak je na ně nutno pohlížet jako na ISVS.
Provozovatelem informačního systému veřejné správy (z.č.365/2000Sb.) je 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.
Přihlášení (login) je proces přihlášení do systému, kdy uživatel zadává uživatelské jméno a heslo. Každý uživatel, který používá víceuživatelský operační systém nebo používá lokální počítačovou síť, musí mít svůj uživatelský účet, který je identifikován uživatelským jménem.
Příjemcem (z.č.101/2000Sb.) je každý subjekt, kterému jsou osobní údaje zpřístupněny; (za příjemce se nepovažuje subjekt, který zpracovává osobní údaje podle § 3 odst. 6 písm. g). z.č.101/2000Sb.)
Přístupové /uživatelské/ heslo (password, user password) je znakový řetězec používaný jako autentizační informace pro rozpoznávání uživatelů oprávněných používat ve stanoveném rozsahu určitý výpočetní prostředek nebo datový zdroj.
Přístupové právo (access right) je oprávnění uživatele používat daný objekt předem definovaným způsobem.
Referenčním, sdíleným a bezpečným rozhraním informačních systémů veřejné správy (dále jen "**referenční rozhraní**") (z.č.365/2000Sb.) je 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.
Riziko (risk) je kombinace pravděpodobnosti, že dojde k nežádoucí události a následků, které by z takové události mohly vzniknout. Pravděpodobnost uplatnění hrozby, důsledky uplatnění hrozby, velikost škody.
Řízení přístupu (access control) je vymezení práv uživatelů při přístupu k prostředkům sítě. Jeho cílem je umožnit přístup autorizovaného uživatele, zabránit přístupu neautorizovaného uživatele, případně zabránit využití zdroje neautorizovaným způsobem.
Sdílením dat (z.č.365/2000Sb.) je umožnění přístupu (tj. poskytování příslušné služby) k daným datům prostřednictvím referenčního rozhraní více subjektům současně.
Shromažďováním osobních údajů (z.č.101/2000Sb.) se rozumí systematický postup nebo soubor postupů, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací pro jejich okamžité, nebo pozdější zpracování.
Službou (z.č.365/2000Sb.) je činnost informačního systému uspokojující dané požadavky oprávněného subjektu spojená s funkcí informačního systému.
Souhlasem subjektu údajů (z.č.101/2000Sb.) je svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů.
Správcem /(evidence, nemusí být podporována prostředky ICT) osobních údajů nebo IS s osobními údaji (z.č.101/2000Sb.) je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.
Správcem informačního systému veřejné správy (z.č.365/2000Sb.) je subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá. Správci informačních systémů veřejné správy jsou ministerstva, jiné správní úřady a územní samosprávné celky (dále jen "orgány veřejné správy").
Subjektem údajů (z.č.101/2000Sb.) je fyzická osoba, k níž se osobní údaje vztahují.
Škoda vzniká ztrátou nebo snížením hodnoty aktiva. Škoda může být zanedbatelná, akceptovatelná, významná, katastrofická.
Uchováváním osobních údajů (z.č.101/2000Sb.) se rozumí udržování údajů v takové podobě, která je umožňuje dále zpracovávat.
Útok bývá příčinou ztráty nebo snížení hodnoty aktiva, útok je realizací hrozby.
Uživatelské jméno (username, user-ID) je symbolické jméno osoby, která má právo využívat prostředky sítě, nebo určitou službu. Zpravidla se pro identifikaci uživatele používá v kombinaci s heslem.
Vazbou mezi informačními systémy veřejné správy (z.č.365/2000Sb.) je vzájemné nebo jednostranné poskytování služeb a informací, například sdílení dat.
Veřejným informačním systémem (z.č.365/2000Sb.) je informační systém vedený správci tzv. "orgány veřejné správy" (ministerstva, jiné správní úřady a územní samosprávné celky), nebo jiný informační systém poskytující služby veřejnosti, který má vazby na informační systémy veřejné správy.
Vyhodnocení rizik (risk evaluation) je proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu. Např. vyhodnocení nákladů na eliminaci rizika, předchání událostem proti nákladům finančním, materiálním a personálním.
Vytvářením informačních systémů veřejné správy (z.č.365/2000Sb.) je proces zavádění informačních a komunikačních technologií, včetně jeho právního, organizačního, znalostního a technického zajištění. (Každé z těchto zajištění má i své bezpečnostní prvky, součásti, složky).
Zpracováním osobních údajů (z.č.101/2000Sb.) se rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.
Zpracovatelem (z.č.101/2000Sb.) je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.
Zranitelnost (vulnerability) je označení pro vlastnost, slabé místo aktiva nebo skupiny aktiv, které může být využito jednou nebo více hrozbami. Zranitelnost je též daná existencí zranitelných (slabých) míst systému a existencí potenciálních útočníků.
Zveřejněným osobním údajem (z.č.101/2000Sb.) je osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu.
Zvládání rizik (risk treatment) znamená proces výběru a přijímání opatření pro změnu rizika.

PŘÍLOHA P XI: PŘEHLED NEHMOTNÝCH INF. AKTIV ZDROJ:VLASTNÍ]

Název aktiva	Důsledky plynoucí ze ztráty			Obnovitelnost
	Důvěrnosti	Integrity	Dostupnosti	
operační systémy	C	B	E	3
Anti-malware SW a Firewall – AVG Business Ed.(AVG)	B	B	B	3
databáze	C	D	D	2
zálohovací systémy	C	C	B	3
e-mailová korespondence uživatelů	A	A	E	2
CzechPoint (MV ČR)	C	C	C	3
ePUSA (Marbes Consulting, Plzeň)	X	C	F	3
webové stránky Města	X	K	C	2
UCR – účetnictví a rozpočet (Gordic)	C	G	E	3
GIS MISYS (Gepro Praha)	X	E	F	3
Registr střetu zájmů (Zlínský kraj/VERA)	C	C	C	3
FISO (AQE Brno)	X	F	F	3
Registr pozemků (Ing. Řezníček, Brno)	X	G	E	3
EVI9 - evidence odpadů (Inisoft, Liberec)	X	C	F	3
PERM3 - Mzdy a personalistika (Kvasar, Zlín)	A	C	F	3
ISKN - (ČUZK)	X	C	F	3
Adresy (VERA)	K	H	F	3
Banka (VERA)	C	G	E	3
Doprava a komunikace (VERA)	C	E	F	2
Evidence majetku (VERA)	C	G	D	3
Evidence písemností (VERA)	C	D	D	2
Evidence psů (VERA)	X	C	F	3
Evidence smluv (VERA)	B	C	D	2
Evidence účtů (VERA)	X	F	F	3
Evidence úkolů (VERA)	X	F	F	3
Export do účetnictví (VERA)	X	F	F	3
Fakturace (VERA)	C	G	E	3
Hrací automaty (VERA)	X	C	F	3
Hřbitovní agenda (VERA)	X	C	F	3
Komunální odpad (VERA)	C	G	E	3
Městská policie (VERA)	C	G	E	3
Občanské průkazy a pasy (VERA)	B	C	D	2
Objednávky (VERA)	X	C	F	3
Organizace voleb (VERA)	A	C	K	2
Pokladna (VERA)	C	E	E	2
Pronájem nemovitého majetku (VERA)	X	G	E	3
Přestupkové řízení (VERA)	C	E	E	2
Registry - OB, ES, NEM, UIR (VERA)	C	D	D	2
Rozpočtové účetnictví (VERA)	C	G	E	3
Správa databáze (VERA)	X	F	F	3
Stavební úřad (VERA)	C	E	E	2
Stížnosti a petice (VERA)	A	F	F	3
Struktura úřadu (VERA)	X	F	F	3
Tvorba rozpočtu (VERA)	C	G	E	3
Volební agendy (VERA)	A	C	K	2
Výdaje (VERA)	C	G	E	3
Vymáhání pohledávek (VERA)	A	G	F	3
Změny obyvatel z centrální evidence (VERA)	A	C	K	2
e-Podatelna (VERA)	A	B	C	2

PŘÍLOHA P XII: NEHMOTNÁ A HMOTNÁ SOFTWAROVÁ AKTIVA [ZDROJ: VLASTNÍ]

Nehmotná aktiva

Název aktiva	Důsledky plynoucí ze ztráty			Obnovitelnost
	Důvěrnosti	Integrity	Dostupnosti	
operační systémy serverové	C	B	E	3
operační systémy PC	C	B	E	3
anti-malware SW a firewall	B	B	B	3
databázové engine	C	D	D	2
zálohovací SW	C	C	B	3
systém elektronické pošty	A	A	E	2

Název aktiva	Důsledky plynoucí ze ztráty			Obnovi-telnost
	Důvěrnosti	Integrity	Dostupnosti	
klíčové aplikace	C	D	D	2
další aplikace	C	F	F	3
webové stránky	X	K	C	2

Hmotná aktiva

Název aktiva	Důsledky plynoucí ze ztráty			Obnovitel-nost
	Důvěrnosti	Integrity	Dostupnosti	
síťová infrastruktura a přepínače	B	B	D	3
kritické síťové servery	B	B	D	3
ostatní síťové servery	B	B	E	2
uživatelské stanice (osobní počítače PC)	B	B	F	3
ostatní hardware (HW)	–	F	F	3

PŘÍLOHA P XIII: RELATIVNÍ HODNOTA AKTIV A SLUŽEB [ZDROJ: VLASTNÍ]

Relativní hodnota nehmotných informačních aktiv

Název aktiva	Relativní hodnota
operační systémy serverové	velice vysoká
operační systémy PC	vysoká
Anti-malware a Firewall	velice vysoká
databáze	velice vysoká
zálohovací systémy	velice vysoká
e-mailová korespondence uživatelů	velice vysoká
klíčová informační aktiva	velice vysoká
další informační aktiva	vysoká
webové stránky	velice vysoká

Relativní hodnota nehmotných SW aktiv

Název aktiva	Relativní hodnota
operační systémy serverové	velice vysoká
operační systémy PC	vysoká
anti-malware SW a firewall	velice vysoká
databázové engine	velice vysoká
zálohovací SW	velice vysoká
Systém elektronické pošty	velice vysoká
klíčové aplikace	velice vysoká
další aplikace	vysoká
webové stránky, publikační a redakční systém	vysoká

Relativní hodnota hmotných aktiv

Název aktiva	Relativní hodnota
síťová infrastruktura a přepínače	velice vysoká
kritické síťové servery	velice vysoká
ostatní síťové servery	vysoká
uživatelské stanice (osobní počítače PC)	vysoká
ostatní hardware (HW)	nízká

Relativní hodnota služeb

Název aktiva	Relativní hodnota
dodávky elektrické energie	velice vysoká
komunikační kanály pro přímé bankovnictví	střední
připojení do sítě Internet + služby	velice vysoká
e-podatelna, e-pošta (e-mail), WEB server	velice vysoká

PŘÍLOHA P XIV: PRAVDĚPODOBNOST VÝSKYTU HROZEB [ZDROJ: VLASTNÍ]

Id hrozby	Popis	Pravděpodobnost
H1	předstírání identity uživatele	pravděpodobné
H2	použití softwaru neautorizovanými uživateli	příležitostné
H3	zneužití privilegií – použití SW neautorizovaným způsobem	příležitostné
H4	popření (anonymita prováděných akcí)	pravděpodobné
H5	prozrazení dat během přenosu	příležitostné
H6	prozrazení dat na paměťovém mediu	pravděpodobné
H7	modifikace dat na paměťovém mediu	pravděpodobné
H8	modifikace dat v databázi	pravděpodobné
H9	modifikace dat při přenosu	příležitostné
H10	technické selhání síťových komponent	pravděpodobné
H11	selhání hardware	pravděpodobné
H12	poškození paměťového media	pravděpodobné
H13	zemětřesení	nepravděpodobné
H14	povodeň a voda z potrubí	málo pravděpodobné
H15	požár	málo pravděpodobné
H16	selhání dodávky energie	pravděpodobné
H17	selhání klimatizace	pravděpodobné
H18	krádež, násilný trestný čin	málo pravděpodobné
H19	škodlivý software (viry, trojské koně)	časté

PŘÍLOHA P XV: ZJEDNODUŠENÁ TABULKA PRO ANALÝZU RIZIK [ZDROJ: VLASTNÍ]

Hmotná aktiva

Název aktiva	Hodnota	Obnovitelnost
kritické síťové servery	3	T
ostatní síťové servery	2	T
centrální prvky sítě	3	T
infrastruktura sítě	3	D
osobní počítače	2	D
ostatní hardware	1	D

Nehmotná aktiva

Název aktiva	Hodnota	Obnovitelnost
operační systémy	3	D
Anti-malware SW a Firewall – AVG Business Edition (AVG)	3	D
databáze	2	D
zálohovací systémy	3	D
e-mailová korespondence uživatelů	2	D
CzechPoint (MV ČR)	3	D
ePUSA (Marbes Consulting, Plzeň)	3	D
webové stránky města	2	T
UCR – účetnictví a rozpočet (Gordic)	3	T
GIS MISYS (Gepro Praha)	3	D
Registr střetu zájmů (Zlínský kraj/VERA)	3	D
FISO (AQE Brno)	3	D
Registr pozemků (Ing. Řezníček, Brno)	3	D
EVI9 - evidence odpadů (Inisoft, Liberec)	3	D
PERM3 - Mzdy a personalistika (Kvasar, Zlín)	3	D
ISKN - (ČUZK)	3	D
Adresy (VERA)	3	D
Banka (VERA)	3	D
Doprava a komunikace (VERA)	2	D
Evidence majetku (VERA)	3	D
Spisová služba (VERA)	2	T
Evidence psů (VERA)	3	D
Evidence smluv (VERA)	2	D
Evidence účtů (VERA)	3	D
Evidence úkolů (VERA)	3	D

Export do účetnictví (VERA)	3	D
Fakturace (VERA)	3	D
Hrací automaty (VERA)	3	D
Hřbitovní agenda (VERA)	3	D
Komunální odpad (VERA)	3	D
Městská policie (VERA)	3	D
Občanské průkazy a pasy (VERA)	2	D
Objednávky (VERA)	3	D
Organizace voleb (VERA)	2	D
Pokladna (VERA)	2	D
Pronájem nemovitého majetku (VERA)	3	D
Přestupkové řízení (VERA)	2	D
Registry - OB, ES, NEM, UIR (VERA)	2	T
Rozpočtové účetnictví (VERA)	3	T
Správa databáze (VERA)	3	D
Stavební úřad (VERA)	2	D
Stížnosti a petice (VERA)	3	D
Struktura úřadu (VERA)	3	D
Tvorba rozpočtu (VERA)	3	T
Volební agendy (VERA)	2	D
Výdaje (VERA)	3	D
Vymáhání pohledávek (VERA)	3	D
Změny obyvatel z centrální evidence (VERA)	2	D
e-Podatelna (VERA)	2	D

Aktiva služeb

Název aktiva	Hodnota	Obnovitelnost
připojení do sítě Internet	3	D
e-podatelna, e-pošta (e-mail), WEB server	3	T
komunikační kanály pro přímé bankovnictví	2	D