VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, O. P. S., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INFORMAČNÍ SYSTÉMY A TECHNOLOGIE NA PODPORU KRIZOVÉHO ŘÍZENÍ

Autor práce: Milan Příhoda
Studijní obor: Bezpečnostně právní studia ve veřejné správě
Forma studia: Kombinované
Vedoucí práce: Antonín Čupera
Katedra: Katedra právních oborů a bezpečnostních studií

2010

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s využitím uvedených pramenů a literatury.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských regionálních studií v Českých Budějovicích a zpřístupněna ke studijním účelům.

.....

vlastnoruční podpis autora bakalářské práce

Poděkování

Děkuji vedoucímu bakalářské práce panu Antonínu Čuperovi za cenné rady, připomínky a vedení práce.

OBSAH

1 ÚVOD

Při volbě tématu bakalářské práce jsem si kladl otázku, jaké nejaktuálnější problémy, vztahující se k mému studiu, souvisí s rozvojem dnešní společnosti. Domnívám se, že právě název studijního oboru „Bezpečnostně právní studia ve veřejné správě“ dva takové přináší. Mám na mysli „bezpečnost“ a probíhající „reformu veřejné správy“. Zaujala mne myšlenka, prozkoumat tyto oblasti ve spojení se zaváděním moderních informačních a komunikačních technologií.

„Bezpečnost“ je v dnešní době hodně frekventovaný termín a zabývat se bezpečností jako problémem z jakéhokoliv úhlu se mi zdá více než žádoucí. Dnešní globální společnost klade na krizový management nové požadavky. Objevují se nové zdroje ohrožení, které ke svému odhalení a řešení již vzniklých mimořádných událostí vyžadují spolupráci a sdílení informací. Činnosti spojené s havarijní a krizovou připraveností a s řešením mimořádných a krizových situací si nelze představit bez využití informačních a komunikačních technologií a systémů. Tuto problematiku řeší zejména krizový zákon, který uvádí, že orgány krizového řízení při plánování krizových opatření a při řešení krizových situací využívají informační systémy krizového řízení.

„Veřejná správa“ a její probíhající reforma se také při zavádění informačních a komunikačních technologií stává zdrojem mnoha otázek, na které je potřeba hledat odpovědi. Myslím, že nejlépe zaměření mé práce vystihne citát z projevu bývalého předsedy vlády Mirka Topolánka na konferenci ISSS 2007 - Internet ve státní správě a samosprávě: *„Byrokracie neubylo, ba možná ještě přibylo. Dámy a pánové, my potřebujeme novou, nikoli Velkou říjnovou, ale e-govermentovou revoluci. Techniku už máme, teď potřebujeme naučit státní správu nové filozofii. Přepnout ve vztahu "úřad-občan" z režimu offline na trvalý online.“*

„Informace“. Není pochyb o tom, že se nacházíme v době převratných technologických a společenských změn. Vývoj digitálních technologií určených k vytváření, zpracování, šíření a užívání informací závažně přispěl ke vzniku nové „informační společnosti“. Proto se ve své práci zabývám problematikou zavádění informačních a komunikačních technologií a systémů do veřejné správy a jejich využitím pro podporu rozhodovacích procesů krizových orgánů.

Domnívám se tedy, že hledání souvislostí mezi ochranou obyvatelstva, reformou veřejné správy a budováním informačních systémů, v dnešní „rizikové“ společnosti, dostatečně zdůvodňuje výběr tématu pro mou bakalářskou práci.

2 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

Cílem této práce je prozkoumat problematiku zavádění informačních a komunikačních technologií do veřejné správy a nalézat vztahy k významné oblasti jejího působení, kterou je ochrana obyvatelstva, krizové řízení a havarijní plánování. Chtěl bych tímto přispět k pochopení významu budovaných informačních systémů veřejné správy a informačních systémů krizového řízení, které pracovníci veřejné správy a krizové orgány využívají pro podporu procesů krizového plánování a procesů řešení krizových situací. Dalším cílem je nalézt odpověď na otázku, na jaké kvalitativní úrovni je oblast ochrany obyvatelstva a krizového řízení v bezpečnostním systému České republiky a jakým způsobem je možné další jeho zlepšování.

Práce je členěna do třech hlavních částí, z nichž první popisuje organizační postavení ochrany obyvatelstva v bezpečnostním systému České republiky a také představuje koncepci jejího dalšího rozvoje. Druhá část se zabývá reformou veřejné správy a s ní spojené zavádění informačních a komunikačních technologií, především budování informačních systémů veřejné správy - ISVS. Ve třetí části jsou představeny současné nejmodernější informační a komunikační prostředky, které již využívají nebo zavádějí složky integrovaného záchranného systému. Vybral jsem do své práce taková dílčí témata, na kterých je možné prezentovat souvislosti poukazující na potřebu komplexního a řízeného přístupu k budování informačních a komunikačních systémů pro veřejnou správu. V částech práce, které vymezují oblast ochrany obyvatelstva, krizového řízení havarijního plánování a popisují probíhající reformu veřejné správy a již využívané informační systémy veřejné správy je použito metody literární rešerše.

Pro zaměření mé práce jsem se v některých jejích částech snažil používat především elektronických zdrojů a média budoucnosti, kterým je bezpochyby počítačová síť Internet. Jistě mnoho informací nacházejících se na internetu, má také svou tištěnou podobu. Chtěl jsem při zpracovávání této práce také ověřit svou dosavadní zkušenost, díky níž jsem nabyl přesvědčení, že vhodnou volbou klíčových slov dané problematiky a jejich vhodným zpracováním ve „fulltextovém“ internetovém vyhledávači, se ve výsledcích zobrazují také souvislosti, které pozorného čtenáře mohou dovést k zajímavým poznáním, ale především rozvíjejí jeho analytické myšlení.

„práce s informacemi je sice riskantní, ale daleko riskantnější je práce bez informací“

3 OCHRANA OBYVATELSTVA A KRIZOVÉ ŘÍZENÍ

Ochrana životů, zdraví a majetkových hodnot je spolu se zajištěním svrchovanosti, územní celistvosti a ochranou demokratických základů České republiky základní povinností, a tedy i funkcí státu. V této kapitole bych chtěl představit význam ochrany obyvatelstva a krizového řízení a popsat jejich začlenění v bezpečnostním systému České republiky způsobem, aby bylo možné uvědomit si souvislosti, které hledám ve vztazích k reformě veřejné správy a zaváděným informačním a komunikačním technologiím.

3.1 Zajištění bezpečnosti státu

Bezpečnost České Republiky je zajišťována prostřednictvím bezpečnostního systému, který musí disponovat institucionálními nástroji a strategiemi k zajištění definovaných zájmů a ke snížení nebo eliminaci všech hrozeb a rizik, které brání definované zájmy naplňovat. Zajišťování bezpečnosti ČR se děje v těchto základních oblastech: v politice vnitřní bezpečnosti a ochrany obyvatelstva, zahraniční politice a obranné politice.

Odpovědnost za zajištění bezpečnosti státu mají složky spadající do bezpečnostního systému státu. Vláda a Parlament ČR zajišťují nezbytné lidské, věcné a finanční zdroje pro vnitřní a vnější bezpečnost ČR. Řídí se principem minimální dostatečnosti v možnostech české ekonomiky a státu jako celku a sledují jejich optimální využití. Prostředky vyčleněné k zajištění vnější a vnitřní bezpečnosti musí odpovídat naléhavosti jednotlivých rizik, musí být vyvážené a vzájemně se doplňovat. Zde se promítá úloha obranného a civilního nouzového plánování v celém komplexu a využívání všech zdrojů. Zajištění bezpečnosti závisí nejenom na výši a efektivitě využití vynaložených prostředků, ale též na podílu a přístupu občanů a na jejich vůli přispět k bezpečnosti státu. Rodina a škola zde mají nezastupitelnou úlohu. Odpovědnost za zajištění bezpečnosti státu mají složky zákonodárné, výkonné, ozbrojené a soudní. Bezpečnostní systém je koncipován tak, aby každá z jeho součástí byla schopna realizovat zákonem stanovené úkoly samostatně. Za funkčnost komplexního působení celého bezpečnostního systému odpovídá vláda ČR.[1]

[1] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 10.

3.1.1 Základní povinnosti státu k zajištění jeho bezpečnosti

K zajištění bezpečnosti jsou vytvářeny státní politikou různá opatření a nástroje. Mezi základní pilíře bezpečnostní politiky k ochraně demokratických hodnot a k zabezpečení lidských a občanských práv patří tzv. „Základní funkce státu“. Mezi základní funkce státu patří zejména zabezpečení:

- ochrany obyvatelstva,
- obrany České republiky,
- základních životních podmínek a potřeb obyvatelstva,
- ochrany majetku, kulturních hodnot a životního prostředí,
- výkonu státní správy a územní samosprávy pro řešení krizových stavů,
- zákonnosti, bezpečnosti a veřejného pořádku,
- zdrojů (ekonomických, materiálních, finančních aj.) pro řešení krizových stavů,
- funkčnosti záchranných složek a orgánů krizového řízení,
- dopravní obslužnosti,
- klíčových systémů pro zachování funkčnosti a bezpečnosti státu.[2]

3.1.2 Systém řízení bezpečnosti

Základní funkcí státu je od jeho vzniku zajistit ochranu a rozvoj dané lidské společnosti, což není možné bez zajištění bezpečného prostoru, ve kterém lidská společnost žije. Proto současným nejvyšším cílem významných organizací, vlád, veřejné správy je vytvořit bezpečný prostor pro 21. století. Dnes je zcela zřejmé, že tento cíl nelze zajistit bez participace právnických a fyzických osob a bez účasti občanů, a proto se vytváří komplexní systém řízení bezpečnosti.[3]

Cílem je za každé situace zajistit ochranu životů, zdraví a bezpečí lidí, majetku, životního prostředí, infrastruktury a technologií, které jsou nezbytné pro přežití lidí, tj. mobilizaci a koordinaci využití národních zdrojů (energie, pracovní síly, výrobní schopnost, jídlo a zemědělství, suroviny, telekomunikace aj.), koordinaci činností takových jako je systém vyrozumění, systém záchrany a zdravotnické služby, které snižují dopady živelních či jiných pohrom a zajišťují kontinuitu státní správy a dodržování zákonů, a také vytvořit podmínky pro nastartování rozvoje.

---

[2] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 9.

[3] PROCHÁZKOVÁ, D. *Komplexní pohled na problematiku bezpečnosti.* [online]. 2008 [cit. 2010-01-15]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/2003/casopisy/vs/0435/konz_info.html>.

3.1.3 Nástroje pro řízení systému bezpečnosti

Jsou to nástroje státu, jeho orgánů i organizací, které zajišťují bezpečnost a rozvoj společnosti, tj. jinými slovy ochranu a rozvoj chráněných zájmů. Základní nástroje jsou následující:

- řízení / management (strategické, taktické i operativní) založené na kvalifikovaných datech, odborných hodnoceních a správných metodách rozhodování,
- výchova a vzdělávání občanů,
- specifická a odborná výchova technických a řídících pracovníků,
- technické, zdravotnické, ekologické, kybernetické a jiné standardy,
- normy a předpisy,
- inspekce,
- výkonné složky ke zvládnutí nouzových a kritických situací,
- systémy ke zvládnutí kritických situací,
- bezpečnostní, nouzové a krizové plánování,
- specifický systém řízení pro zvládnutí kritických situací (krizové řízení).[4]

3.1.4 Pozice ochrany obyvatelstva a krizového řízení v systému řízení státu

Pro správu státu i v oblasti krizového řízení jsou využívány obě úrovně veřejné správy. Jde o ***státní správu***, což je veřejná správa vykonávaná státními orgány (organizačními složkami státu). Tuto správu vykonává stát svými správními orgány. Druhou úrovní je ***samospráva***, která je u nás představována po probíhající reformě veřejné správy od r. 2002 obcemi, jako základními články samosprávy a vyššími územně správními celky, tedy kraji. Zde hovoříme o územní samosprávě, ale ochrana obyvatelstva a krizové řízení se může dotýkat také zájmové samosprávy, kterou představuje určitý okruh osob (advokáti, lékaři, myslivci apod.). Veřejná správa spočívá ve značné části v rozhodování o právech a povinnostech fyzických a právnických osob a v řízení území. To znamená, že rozhoduje o bezpečnosti a rozvoji té části lidského systému, která náleží do její působnosti. Provádí řízení strategické, taktické i operativní. Pro řádnou správu je nutné, aby příslušná rozhodnutí, která vykonává, byla založená na kvalifikovaných datech, odborných hodnoceních, správných metodách rozhodování atd.

[4] PROCHÁZKOVÁ, D. *Krizové řízení, havarijní plánování a ochrana obyvatelstva.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2009. s. 22-23.

3.2 Bezpečnostní terminologie

Význam terminologie se odráží v procesu utváření bezpečnostní politiky, kde sehrává zásadní roli diskuse, která je důležitá pro definování pojmů aktuální bezpečnostní politiky. Bezpečnostní terminologie výrazně ovlivňuje konečnou podobu bezpečnostní politiky, zejména její reálnost a efektivnost. Nejednotnost při používání bezpečnostních pojmů komplikuje jednání mezi státy, ale také uvnitř státu při řešení nejrůznějších bezpečnostních problémů.[5] Proto zde uvedu nejzákladnější pojmy a pokusím se vysvětli důležitost je rozlišovat.

3.2.1 Bezpečnost

Bezpečnostní strategie ČR chápe pojem bezpečnost jako žádoucí stav, kdy jsou na nejnižší míru snížena rizika pro ČR plynoucí z hrozeb vůči obyvatelstvu, svrchovanosti a územní celistvosti, demokratickému zřízení a principům právního státu, vnitřnímu pořádku, majetku, životnímu prostředí, plnění mezinárodních bezpečnostních závazků a dalším definovaným zájmům.

Je označována také jako stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.[6] Pro vymezení systému na podmínky státu je obsah bezpečnosti uveden v ústavním zákoně č. 110/1998 Sb. o bezpečnosti České republiky.

3.2.2 Hrozby a rizika

Hrozby a rizika jsou v teorii i praxi bezpečnostní politiky a v dalších oborech zabývajícími se bezpečností v různých směrech klíčovými pojmy. Oba dva výrazy se často používají též jako metafory. Nejen v běžném jazyce, žurnalistice, ale také v bezpečnostních dokumentech se tyto pojmy často zaměňují a také nepřesně používají. Rozdíly mezi hrozbou a rizikem lze zjednodušeně vyjádřit následovně: hrozeb se

[5] DANICS, Š. *Bezpečnostní politika ve veřejné správě.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. s. 7.

[6] *Bezpečnost* [online]. [cit. 2010-01-25]. Dostupný z WWW: <http://www.mvcr.cz/clanek/bezpecnost.aspx>.

obáváme, rizika z nich plynoucí jednak poměřujeme (kvalifikujeme), jednak je postupujeme nebo je úplně eliminujeme. Pojďme si je tedy význam slov přiblížit.

Hrozba je primární, mimo nás nezávisle existující, to znamená vnější fenomén, který může nebo chce poškodit nějakou konkrétní hodnotu. Závažnost hrozby je úměrná povaze hodnoty a tomu, jaký ji přikládáme význam. Každá hrozba může způsobit menší, větší nebo dokonce nenahraditelné škody, a tím vyvolává strach ohroženého. Ten svými opatřeními a svým chováním může hrozbu zmírnit, umocnit nebo i nechtěně vyvolat.[7]

Dále považuji za nutné ještě vysvětlit vztah mezi hrozbou, ohrožením, nebezpečím a výhrůžkou. Termín ohrožení je spjat s vojenským prostředím a překládá se anglickým slovem threats (hrozba). V tomto ohledu je možné pokládat termín „ohrožení“ za synonymum termínu „hrozba“. V literatuře a bezpečnostních dokumentech se můžeme často se spojením „hrozby a ohrožení“ setkat. Tato nadbytečnost však nezpůsobuje informační šumy ani nejasnosti a není tedy škodlivá. Termín nebezpečí můžeme také považovat za synonymum „hrozby“. Je to ale výraz méně odborný a používá se také pro vyjádření materiálního projevu hrozby např. voda při záplavách. Nutno zdůraznit, že pro „jednorázové“ fenomény typu výhrůžných dopisů vydíraným obětem nebo výhrůžka bombovým útokem je lépe používat právě onoho výrazu „výhrůžka“ než termínu „hrozba“.

Klasifikace bezpečnostních hrozeb se rozděluje do dvou kategorií jejich vnímání. První jsou nevojenské bezpečnostní hrozby a vojenské bezpečnostní hrozby. Druhou kategorií jsou hrozby spojené s používáním různých forem násilí a bezpečnostní hrozby nenásilného charakteru.[8]

Riziko je pojmem, jímž je vyjádřena určitá nejistota. Je to sekundární fenomén, odvozenou proměnnou závislou na hrozbě, která se dá kvantifikovat na základě analýzy rizik. Riziko je reakcí na hrozbu neboli stav naší připravenosti (zranitelnosti) a je spjato s lidskou činností, tedy rozhodnutím podstoupit určitou míru rizika nebo ho naopak snížit. Rizika se tudíž odvíjejí od rozhodnutí těch, kdo je činí: vláda, nadnárodní bezpečnostní společenství apod. Jinými slovy, riziko je pravděpodobnost, že vznikne událost, lišící se od toho co si přejeme. A pokud si takovouto událost nepřejeme, vyžaduje to od nás určité náklady tomuto nepříznivému stavu čelit. Riziko je opakem

[7] DANICS, Š. *Bezpečnostní politika ve veřejné správě*. 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. s. 54-55.
[8] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 11.

zájmu a při hodnocení rizik by se mělo zvažovat, jaký je v daném směru zájem, za jakou cenu je ho možné dosáhnout a co ho nejvíce ohrožuje. V české terminologii se nedávno usídlila definice. Riziko je možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí.[9] Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě tzv. analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit.

3.3 Bezpečnostní politika

Pojem bezpečnostní politika je nutno vždy chápat v kontextu bezpečnosti související s bytím a vývojem člověka jako sociální bytosti. Tím, že člověk vytváří a mění hodnoty, ovlivňuje životní prostředí pro svůj fyzicky pohodlnější život a mění tak i kritéria bezpečnosti. Obecně platí, že čím víc je člověk závislý na technologiích, tím je zranitelnější.[10] Dále platí, že čím víc jsou technologie závislé na ekonomických, energetických a dalších surovinových zdrojích a jejich teritoriální existenci, a čím víc strategických technologií daný stát vlastní v propojení na demografická a ideologická specifika národů, tím víc je nutné vynakládat prostředky a úsilí do eliminování vojensko-strategických bezpečnostních rizik. Na národní úrovni má proto vojenská (vnější) bezpečnost tu nejvyšší prioritu.

Bezpečnostní politika státu je chápána, že se jedná o společenskou činnost, jejíž základ tvoří souhrn základních státních zájmů a cílů, jakož i hlavních nástrojů k jejich dosažení, směřující k zabezpečení státní svrchovanosti a územní celistvosti státu a jeho demokratických základů, činnosti demokratických institucí, ekonomického a sociálního rozvoje státu, ochrany zdraví a života občanů, majetku, kulturních statků, životního prostředí a plnění mezinárodních bezpečnostních závazků.

[9] *Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu.* [online]. [cit. 2010-01-20]. Dostupný z WWW: <http://www.mvcr.cz/clanek/riziko.aspx>.
[10] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích*. 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 7.

Bezpečnostní politiku státu tvoří šest základních komponentů:

1. zahraniční politika v oblasti bezpečnosti státu,
2. obranná politika,
3. politika v oblasti vnitřní bezpečnosti,
4. politika v oblasti ochrany před mimořádnými událostmi,
5. hospodářská politika v oblasti bezpečnosti státu,
6. politika veřejné informovanosti v oblasti bezpečnosti státu.[11]

V této práci se dále budu zabývat čtvrtou, pátou a šestou jmenovanou bezpečnostní politikou státu. Důvodem je zaměření mé práce, kterým je nalézání vztahů mezi reformou veřejné správy, ochranou obyvatelstva a zaváděním informačních a komunikačních technologií. V těchto politikách je výkon veřejné správy zastoupen nejvíce.

3.3.1 Politika v oblasti ochrany před mimořádnými událostmi

Politika v oblasti ochrany před mimořádnými událostmi je členěna do několika částí, kterými jsou civilní nouzové plánování a připravenost, krizové řízení, ochrana obyvatelstva, požární ochrana, integrovaný záchranný systém, ochrana kritické infrastruktury, ochrana veřejného zdraví, ochrana před povodněmi, ochrana vnějšího ovzduší, ochrana zdraví a životního prostředí před škodlivými účinky chemických látek a chemických přípravků, ochrana osob a životního prostředí před nežádoucími účinky ionizujícího záření, prevence závažných havárií při nakládání s nebezpečnými chemickými látkami nebo chemickými přípravky, ochrana a bezpečnost komunikačních a informačních systémů, ochrana kulturních památek, sbírek muzejní povahy, předmětů kulturní hodnoty, archivnictví, příprava hospodářských opatření pro krizové stavy a další, které mají nezastupitelnou roli pro ochranu zdraví a životů obyvatelstva, majetku a životního prostředí.

3.3.2 Hospodářská politika v oblasti bezpečnosti státu

Hospodářská politika v oblasti bezpečnosti státu má ve vztahu k vnitřní a vnější bezpečnosti zajišťovat materiální předpoklady pro plnění bezpečnostních funkcí státu. Vedle toho je hospodářská politika koncipována a prováděna tak, aby eliminovala

[11] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích*. 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 7.

existující a potenciální bezpečnostní rizika, která se mohou objevovat v ekonomice České republiky a v oblasti jejích vnějších ekonomických vztahů, jakož i ta rizika, jež by mohla ohrožovat základní úkol ekonomiky ve vztahu k bezpečnosti země, tj. produkovat bezporuchově potřebné zdroje v potřebném rozsahu. Pro zajišťování bezpečnosti České republiky je nezbytná i soustava hospodářských opatření pro krizové stavy, jejichž cílem je zabezpečit poskytování nezbytných materiálních prostředků a služeb pro zajištění základních životních potřeb pro obyvatelstvo, pro fungování ozbrojených sil, ozbrojených sborů, záchranných sborů a havarijních služeb v krizových situacích. Stejnému cíli slouží i vytváření a udržování dostatečných kapacit strategických zásob podle příslušných mezinárodních závazků a obvyklých mezinárodních standardů.

3.3.3 Politika veřejné informovanosti v oblasti bezpečnosti státu

V oblasti veřejné informovanosti je nutné, aby orgány státní správy a samosprávy prováděly zejména spolupráci se sdělovacími prostředky, podporovaly tvorbu a provoz portálu veřejné správy a systém předávání informací v oblasti bezpečnosti, podporovaly budování komunikační infrastruktury k zajištění přístupu občanů k informacím určeným pro veřejnost, využívaly různých forem komunikace s občany na místní úrovni, zveřejňovaly periodicky hodnocení hrozeb a rizik, prezentovaly periodické zprávy o stavu zajišťování bezpečnosti ČR na všech úrovních, podporovaly studium v oboru bezpečnosti na univerzitách a další vzdělávací programy s bezpečnostní tematikou, prezentovaly výsledky činnosti zpravodajských služeb. Zvláštní důraz je potřeba klást především na výchovu mládeže.[12]

3.4 Koncepce zajištění bezpečnosti

Současná „riziková společnost“ musí z globálního pohledu čelit novým hrozbám a z nich plynoucím novým rizikům. Proto vznikají nové koncepty a přístupy ke krizovému řízení a k řízení bezpečnosti na národní a mezinárodní úrovni. Česká republika prožívá především pod tlakem zemí Evropského společenství období své politické, ekonomické a sociální integrace. Jedná se o složitý proces, ve kterém sehrává bezpečnostní politika státu, a tím i krizové řízení jako jeho neoddělitelná součást, klíčovou roli. Proto se hledají mezi vyspělými státy světa vhodné kvalitní a fungující

[12] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 8.

modely koncepčních přístupů ke strategii krizového řízení. Dále bych se chtěl o dvou nevýznamnějších koncepčních a strategických dokumentech zmínit.

3.4.1 Bezpečnostní strategie České republiky

Bezpečnostní politika České republiky vychází ze tří základních dokumentů. Jsou jimi Bezpečnostní strategie České republiky, Obranná strategie České republiky a Vojenská strategie České republiky. Ochrana obyvatelstva a krizové řízení pro řešení nevojenských mimořádných událostí se nejvíce týká Bezpečnostní strategie České republiky, proto zde uvedu její základní hodnoty, zájmy, postoje a ambice:

V kapitole „Východiska bezpečnostní politiky ČR“ jsou zformulovány principy, na nichž je bezpečnostní politika ČR založena.

V kapitole „Bezpečnostní zájmy ČR“ jsou definovány životní, strategické a další významné zájmy ČR.

V kapitole „Bezpečnostní prostředí“ jsou identifikovány trendy, hrozby a z nich plynoucí rizika, jež formují prostředí, v němž ČR ochraňuje a prosazuje své zájmy.

Ve stěžejní kapitole „Strategie prosazování bezpečnostních zájmů ČR“ jsou vymezeny přístupy k ochraně zájmů ČR v oblastech zahraniční, obranné a hospodářské politiky a v oblasti politiky vnitřní bezpečnosti a veřejné informovanosti.

V kapitole „Bezpečnostní systém ČR“ jsou definovány prvky bezpečnostního systému ČR, jejich struktura, a vymezeny povinnosti, kompetence a odpovědnosti jednotlivých součástí systému.[13]

3.4.2 Bezpečnostní výzkum pro potřeby státu v letech 2010 až 2015[14]

Program je zaměřen na podporu výzkumu při respektování potřeb a specifik bezpečnostního výzkumu ve smyslu aktualizovaných dlouhodobých základních směrů výzkumu v následujících subsystémech:

- Vnitřní bezpečnosti státu, zaměřené na problematiku nekontrolované migrace osob, páchané kriminality, růstu organizované zločinnosti, terorismu, vyhrocení politické, ekonomické nebo sociální situace ve státě, útoků na ústavní zřízení, náboženských a občanských střetů.

[13] *Nová Bezpečnostní strategie České republiky* [online]. 2004 [cit. 2010-02-15]. Dostupný z WWW: <http://www.revuepolitika.cz/clanky/642/nova-bezpecnostni-strategie-ceske-republiky>.

[14] *Bezpečnostní výzkum pro potřeby státu v letech 2010 až 2015* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/3-bezpecnostni-vyzkum-pro-potreby-statu-v-letech-2010-az-2015.aspx>.

- Ochrany stability hospodářské a finanční soustavy státu se zaměřením na hrozbu rozsáhlých výpadků ve fungování hospodářství státu nebo jeho produkčních schopnostech, destabilizace měny, nerespektování celních a devizových předpisů ve velkém rozsahu, hrozby možného nedostatku dovozu důležitých surovin.
- Civilního nouzového plánování zaměřeného na plánování a řešení krizových situací spojených s ohrožením životů a zdraví obyvatelstva, na problematiku ničení životního prostředí, majetkových a kulturních hodnot v souvislosti s ohrožením vnější nebo vnitřní bezpečnosti státu a dále na problematiku přírodních antropogenních pohrom a krizí, zvládání krizových situací a na dlouhodobé řešení negativních dopadů ekonomické a sociální globalizace.

Cílem programu je dosažení takové znalostní, technické a technologické úrovně, která umožní orgánům státní správy, tedy státu, získávat, osvojovat si, udržovat a rozvíjet specifické schopnosti potřebné pro zajištění bezpečnosti státu a jeho obyvatel.

Očekávanými přínosy Programu jsou:

- zvýšení úrovně bezpečnosti ČR a jeho obyvatel, zajištění jejich občanských práv, včetně přínosů pro ekonomiku, její konkurenceschopnosti pro udržitelný rozvoj společnosti, ochrany majetku, v ekonomické, sociální a ekologické oblasti,
- zkvalitnění legislativního procesu a formulaci námětů k rychlejšímu přizpůsobení bezpečnosti ČR evropským integračním procesům,
- zvyšování úrovně připravenosti bezpečnostních a záchranných složek,
- vytvoření kontrolních, represivních a preventivních opatření v případě naturogenních a antropogenních událostí,
- získání poznatků, podkladů a nástrojů pro koncepční, metodickou a rozhodovací činnost při výkonu státní správy se zaměřením na zvyšování bezpečnosti státu a to zejména v oblasti krizového řízení, civilního nouzového plánování, ochrany obyvatelstva, integrovaného záchranného systému, požární ochrany a výkonu policejní služby v exponovaných oblastech,
- eliminace nejzávažnějších hrozeb souvisejících se zabezpečením základních funkcí státu, kritickou infrastrukturou, ochranou životů, zdraví a majetku obyvatelstva ČR v případě krizových situací.

3.5 Bezpečnostní systém České republiky

Prvky bezpečnostního systému, jejich struktura, vymezení povinností, kompetencí a odpovědnosti jednotlivých součástí systému jsou definovány v jedné z kapitol Bezpečnostní strategie České republiky. Uvádím zde některé skutečnosti, vztahující se ke krizovému řízení a některé pro uvědomění si komplexnosti problému.

Bezpečnostní systém je tvořen příslušnými prvky zákonodárné, výkonné a soudní moci, územní samosprávy, ale i právnickými a fyzickými osobami, které mají odpovědnost za zajištění bezpečnosti státu. Struktura bezpečnostního systému zahrnuje zejména prezidenta republiky, Parlament, vládu, Bezpečnostní radu státu a její pracovní orgány, ústřední správní úřady, krajské a obecní úřady a jejich výkonné orgány krizového řízení, a dále ozbrojené síly, ozbrojené bezpečnostní sbory, zpravodajské služby, záchranné sbory, záchranné služby a havarijní služby.[15]

Cílem bezpečnostního systému je zajišťování bezpečnosti státu, ochraňování a prosazování životních, strategických i dalších významných zájmů. Jeho základní funkcí je řízení a koordinace činnosti jednotlivých prvků při zajišťování bezpečnostních zájmů a v době přímé hrozby nebo při vzniku krizové situace.

Pro bezpečnostní systém je žádoucí, aby byly jeho prvky schopny za všech situací stabilně reagovat a fungovat, a aby dokázal maximálně absorbovat rizikový potenciál bezpečnostního prostředí, popř. se úspěšně vyrovnával se zvládáním mimořádných událostí nebo krizových situací. Vnitřní mechanismy systému musí umožňovat rychlý a koordinovaný přechod z běžného stavu do krizového stavu.

Bezpečnostní systém je institucionálním nástrojem pro tvorbu a realizaci bezpečnostní politiky. Působí v rámci České republiky, ale současně je úzce propojen s dalšími mezinárodními organizacemi, což zabezpečuje jeho kompatibilitu a interoperabilitu s aliančními a dalšími, především evropskými bezpečnostními systémy.

3.6 Ochrana obyvatelstva a krizové řízení

V našem právním řádu je pojem ochrana obyvatelstva zaveden jako určité zastřešující pojmenování integrovaného systému. Tento systém je určen pro řešení různých druhů mimořádných událostí. Od každodenních, jako jsou dopravní nehody, havárie inženýrských sítí, přes různé druhy přírodních katastrof až po teroristické útoky

[15] *Bezpečnostní strategie České republiky 2003* [online]. [cit. 2010-02-25]. Dostupný z WWW: <http://www.mzv.cz/public/7/46/a7/14340_14945_Bezp._strategie.doc>.

a ozbrojené konflikty. Výchozím dokumentem pro rozvíjení ochrany obyvatelstva a krizového řízení je Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020, jejíž základní principy zde uvedu. Dalším důležitým dokumentem, který nemohu vynechat je Koncepce vzdělávání v oblasti krizového řízení pro svůj vztah k informovanosti obyvatelstva a pracovníků veřejné správy. Zmíním také význam terminologie a na základním přehledu legislativy představím pozici ochrany obyvatelstva a krizového řízení v bezpečnostním systému České republiky. Vzhledem k zaměření této práce se omezím na vztahy k informačním a komunikačním systémům, přesto věřím, že pohled nebude chudší.

3.6.1 Koncepce ochrany obyvatelstva do r. 2013 výhledem do r. 2020

Bezpečnou společnost ve vztahu k mimořádným událostem a krizovým situacím lze charakterizovat jako společnost, která má přijatý soubor právních, technických, organizačních, finančních, vzdělávacích a dalších ochranných opatření k minimalizaci, resp. k překonání následků mimořádných událostí a krizových situací a v praxi ho úspěšně realizuje. Musí ji vytvářet veřejná správa, která zabezpečí podmínky pro přístup občanů k informacím o rizicích vzniku mimořádných událostí, možných následcích a zároveň o přijatých opatřeních k ochraně jejich životů a zdraví, majetku a životního prostředí.

Zejména obec za pomoci složek Integrovaného záchranného systému musí více sehrávat rozhodující roli v informovanosti, resp. přípravě občanů k sebeochraně a vzájemné pomoci při mimořádných událostech a krizových situacích. Využívá k tomu hromadných komunikačních prostředků a všech dostupných prostředků propagace. Důležitou úlohu v této oblasti bude plnit podniková sféra a občané na základě budovaného systému ochrany obyvatelstva a v jeho rámci vymezených úkolů. Veřejná správa i podniková sféra musí motivovat a získat občany k aktivní účasti na zajišťování vlastní bezpečnosti, bezpečnosti svých zaměstnanců, spoluobčanů a blízkých.[16]

3.6.2 Koncepce vzdělávání v oblasti krizového řízení

Vzdělávání pracovníku veřejné správy v oblasti krizového řízení je v návaznosti na reformu veřejné správy a vstup České republiky do Evropské unie velmi důležitým krokem k zajištění podmínek pro řešení možných mimořádných událostí získáním

[16] *Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.hzscr.cz/clanek/koncepce-ochrany-obyvatelstva-do-roku-2013-s-vyhledem-do-roku-2020-503181.aspx>.

odborných znalostí, technickou a technologickou připraveností na zvládání krizových situací a také tvorbou nebo aktualizací legislativy v souvislosti s harmonizací vzájemné spolupráce mezi zeměmi Evropské unie. Z hlediska věcného zaměření vzdělávání v předmětné oblasti nová Koncepce pokrývá problematiku krizového řízení, ochrany obyvatelstva, obrany státu, ochrany ekonomiky, hospodářských a dalších opatření pro krizové stavy, vnitrní bezpečnosti a pořádku, požární ochrany a integrovaného záchranného systému.

Cílem Koncepce vzdělávání v oblasti krizového řízení je systémové řešení přípravy osob v předmětné oblasti. Dále pak stanovení cílových skupin, způsobů a zásad pro zpracování rámcových vzdělávacích programů pro tyto skupiny. Vytvoření podmínek k získávání a prohlubování kvalifikace a její zvyšování v oblasti potřebné pro činnost profesionálních pracovníků a osob dotčených oblastí krizového řízení. Realizace koordinace a výkon státní správy v oblasti činností spojených se vzděláváním v krizovém řízení v odpovědnosti Ministerstva vnitra ve spolupráci s dalšími zúčastněnými i ústředními správními úřady.[17]

3.6.3 Přehled základní legislativy

Postavení a činnosti subjektů státní správy a územní samosprávy, které jsou odpovědny za zajišťování bezpečnosti a řešení krizových situací upravují Ústava České republiky, ústavní zákony, zákony a podzákonné (prováděcí) právní předpisy. Je-li bezprostředně ohrožena svrchovanost, územní celistvost, demokratické základy České republiky nebo ve značném rozsahu vnitřní pořádek a bezpečnost, životy a zdraví, majetkové hodnoty nebo životní prostředí anebo je-li třeba plnit mezinárodní závazky o společné obraně, může se vyhlásit podle intenzity, územního rozsahu a charakteru situace nouzový stav, stav ohrožení státu nebo válečný stav.

Uvedu zde některé zákony, které obsahují ustanovení vztahující se k informačním a komunikačním technologiím, případně využívání informací potřebných k rozhodovacím procesům krizových orgánů nebo také plánování, operačnímu řízení apod.

[17] *Koncepce vzdělávání v oblasti krizového řízení* [online]. [cit. 2010-02-11]. Dostupný z WWW: <http://www.hzscr.cz/soubor/koncepce-vzdelavani-v-obl-kr-pdf.aspx>.

Zákon č. 240/2000Sb. o krizovém řízení[18]

Tento zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení. V tomto zákoně se objevuje poměrně velké množství ustanovení, vztahujících se informačním a komunikačním technologiím. Uvedu zde pouze ty nejvýznamnější.

- Správní úřady vytvářejí podmínky pro nouzovou komunikaci ve vztahu k jiným správním úřadům, obcím, právnickým a fyzickým osobám.
- Hasičský záchranný sbor kraje je oprávněn za účelem přípravy na krizové situace vyžadovat, shromažďovat a evidovat údaje vyjmenované v tomto zákoně pokud tyto údaje jsou nezbytné pro zpracování krizových plánů a pro přípravu řešení krizových situací. Dále pak koordinuje pro účely krizového řízení sběr dat od územních správních úřadů.
- Obecní úřad poskytuje hasičskému záchrannému sboru kraje podklady a informace potřebné ke zpracování krizového plánu kraje. Starosta obce odpovídá za připravenost obce k řešení krizových situací, za údržbu a provoz informačních a komunikačních prostředků a pomůcek krizového řízení určených Ministerstvem vnitra.
- Orgány krizového řízení při plánování krizových opatření a při řešení krizových situací využívají informační systémy krizového řízení. Tyto musí splňovat standardy informačních systémů veřejné správy a pravidla přenosu informací nadřízeným, podřízeným a spolupracujícím orgánům krizového řízení, technického a programového přizpůsobení pro činnost v obtížných podmínkách, bezpečnosti uchovávaných informací stanovené pro informace s nejvyšším stupněm utajení obsažené ve zpracované dokumentaci. Orgány krizového řízení při plánování krizových opatření odpovídají za dodržení zásady rovnocennosti písemných a elektronických údajů obsažených v krizovém plánu.
- Každý kdo provozuje hromadné informační prostředky včetně televizního a rozhlasového vysílání, je povinně bez náhrady nákladů na základě žádosti orgánů krizového řízení neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení krizových stavů a nařízených krizových opatřeních při krizových stavech.

[18] *Zákon č. 240/2000 Sb. o krizovém řízení* [online]. [cit. 2010-02-25]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00240&cd=76&typ=r>.

- Fyzická osoba pobývající na území České republiky má právo na nezbytné informace o připravovaných krizových opatřeních k ochraně jejího života, zdraví a majetku.

Zákon č. 239/2000 Sb. o integrovaném záchranném systému[19]

Tento zákon vymezuje integrovaný záchranný systém, stanoví složky integrovaného záchranného systému a jejich působnost. Pro účely zákona se integrovaným záchranným systémem rozumí koordinovaný postup jeho složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací. Ze zákona o Integrovaném záchranném systému vybírám tato ustanovení.

- Stálými orgány pro koordinaci složek integrovaného záchranného systému jsou operační a informační střediska integrovaného záchranného systému, kterými jsou operační střediska hasičského záchranného sboru kraje a operační a informační středisko generálního ředitelství hasičského záchranného sboru.
- Operační a informační střediska integrovaného záchranného systému jsou povinna přijímat a vyhodnocovat informace o mimořádných událostech, zabezpečovat v případě potřeby vyrozumění základních i ostatních složek integrovaného záchranného systému a vyrozumění státních orgánů a orgánů územních samosprávných celků podle dokumentace integrovaného záchranného systému.
- Ministerstvo vnitra řídí výstavbu a provoz informačních a komunikačních sítí a služeb integrovaného záchranného systému, zajišťuje a provozuje jednotný systém varování a vyrozumění, stanoví způsob informování právnických a fyzických osob o charakteru možného ohrožení, připravovaných opatřeních, způsobu a době jejich provedení.
- Ministerstvo vnitra určí způsob zajištění nepřetržité obsluhy telefonní linky jednotného evropského čísla tísňového volání.
- Prováděcí právní předpis stanoví způsob informování právnických a fyzických osob, také technické, provozní a organizační zabezpečení jednotného systému varování a vyrozumění a způsob poskytování tísňových informací.
- Ministerstvo dopravy a spojů zabezpečuje pro potřeby správních úřadů a základních složek integrovaného záchranného systému celostátní informační systém („dopravní informační systém“) pro záchranné a likvidační práce v oblasti mobilních

[19] *Zákon č. 239/2000 Sb. o integrovaném záchranném systému* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00239&cd=76&typ=r>.

zdrojů nebezpečí v dopravě. Jeho provozovatel zabezpečí ochranu poskytnutých informací a údajů.

- Hasičský záchranný sbor kraje pro zabezpečení záchranných a likvidačních prací řídí výstavbu a provoz informačních a komunikačních sítí integrovaného záchranného systému, zabezpečuje varování a vyrozumění.
- Obecní úřad zajišťuje varování. Poskytuje hasičskému záchrannému sboru kraje podklady a informace potřebné ke zpracování havarijního plánu kraje nebo vnějšího havarijního plánu.
- Při přípravě na mimořádnou událost a při provádění záchranných a likvidačních prací se použije krizová komunikace; krizovou komunikací se pro účely zákona rozumí přenos informací mezi státními orgány, územními samosprávnými orgány a mezi složkami integrovaného záchranného systému za využití prostředků hlasového a datového přenosu informací veřejné telekomunikační sítě i vybrané části neveřejných telekomunikačních sítí. Ministerstvo vnitra je povinno umožnit orgánům a složkám krizovou komunikaci v účelové telekomunikační síti Ministerstva vnitra. Poskytovatelé služeb v oblasti komunikací jsou povinni spolupracovat s Ministerstvem vnitra při přípravě a řešení způsobu krizové komunikace a jednotného evropského čísla tísňového volání. Prováděcí právní předpis stanoví zásady způsobu krizové komunikace a spojení v integrovaném záchranném systému a strukturu sdílených dat a také způsob využívání telekomunikačních sítí složkami integrovaného záchranného systému.
- Právnické osoby a podnikající fyzické osoby jsou v souvislosti se záchrannými a likvidačními pracemi a s jejich přípravou povinny strpět umístění zařízení systému varování a vyrozumění na nemovitostech, které mají ve vlastnictví, a umožnit k nim přístup hasičskému záchrannému sboru kraje nebo jím zmocněným osobám za účelem používání, kontroly, údržby a oprav.
- Fyzická osoba pobývající na území České republiky má právo na informace o opatřeních k zabezpečení ochrany obyvatelstva a na poskytnutí instruktáže a školení ke své činnosti při mimořádných událostech. Fyzických osob se týká také obsah předchozího odstavce.

Zákon č. 238/2000 Sb. o hasičském záchranném sboru České republiky[20]

Tímto zákonem se zřizuje Hasičský záchranný sbor České republiky, jehož základním posláním, je chránit životy a zdraví obyvatel a majetek před požáry a poskytovat účinnou pomoc při mimořádných událostech.

- Ministerstvo zřizuje na úrovni generálního ředitelství operační a informační středisko. Hasičský záchranný sbor kraje zřizuje operační a informační střediska jako součást hasičského záchranného sboru.

Zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy[21]

Tento zákon upravuje přípravu hospodářských opatření pro krizové stavy a přijetí hospodářských opatření po vyhlášení krizových stavů. Stanoví pravomoc vlády a správních úřadů při přípravě a přijetí hospodářských opatření pro krizové stavy. Stanoví také práva a povinnosti fyzických a právnických osob při přípravě a přijetí hospodářských opatření pro krizové stavy.

- Za nouzového stavu může vláda nařízením stanovit technické, popřípadě provozní podmínky pro výstavbu telekomunikačních sítí a zařízení, pro jejich využití při krizových situacích a podmínky pro pozastavení nebo upřednostnění telekomunikačních služeb.

Legislativa Evropské unie

Současný legislativní rámec Evropské unie v oblasti civilní ochrany, krizového řízení a plánování je tvořen třemi základními dokumenty:

- rozhodnutím Rady ze dne 23. října 2001 o vytvoření mechanismu Společenství na podporu zesílené spolupráce při asistenčních zásazích v oblasti civilní ochrany (2001/792/ES, Euratom),
- rozhodnutím Komise ze dne 29. prosince 2003, kterým se stanoví prováděcí pravidla k rozhodnutí Rady 2001/792/ES, Euratom (2004/277/ES/Euratom),
- rozhodnutím Rady ze dne 9. prosince 1999, o vytvoření Akčního plánu Společenství v oblasti civilní ochrany (1999/847/EC).

[20] *Zákon č. 238/2000 Sb. o hasičském záchranném sboru ČR* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00238&cd=76&typ=r>.
[21] *Zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00241&cd=76&typ=r>.

3.6.4 Terminologie krizového řízení

Terminologie je nutnou základnou pro komunikaci, pro sdělování myšlenek, poznatků a dalších informací mezi lidmi. Aby však tato terminologie byla skutečně potřebná, užitečná a kvalitní, je nutné si uvědomit, že unifikované termíny obsažené např. v právních předpisech, jsou nutnou základnou a jednou z hlavních podmínek pro další rozvoj. Ještě podstatnější podmínkou dalšího rozvoje je, že terminologii daná komunita přijme za svou. Správné používání odborné terminologie je důležitým aspektem sjednocující úsilí a zvyšující efektivitu výkonu veřejné správy. Správné pochopení a využívání terminologického aparátu, který je obsažen v právních předpisech, je determinujícím východiskem pro pracovníky veřejné správy v rámci zákonného přístupu při zabezpečování výkonu státní správy v oblasti krizového řízení.[22]

V termínech by se měli pracovníci veřejné správy zabývající se problematikou krizového řízení orientovat. Jde například o termíny, které se používají při různých mimořádných situacích a jsou jejich využitím vyhlašována opatření související s určitým typem ohrožení. Mohou být vyhlášeny různé „stavy" jako „Stav nebezpečí", „Stav nouze", „Stav ohrožení", „Stav pohotovosti" apod. Pro pracovníky veřejné správy, ale i pracovníky zasahujících složek IZS (hasičů, policie, zdravotníků či armády) by mělo být evidentní, o co se při vyhlášení uvedených „stavů" jedná, o jaký typ ohrožení jde a následně jaká mají být přijímána opatření. Také nepřesné nebo neúplné sdělení při řešení konkrétní mimořádné situace může mít fatální důsledky.

Vzhledem k předešlému velmi neutěšenému stavu doznal vývoj v této oblasti značného pokroku a v roce 2009 byla vydána aktualizovaná verze „Terminologického slovníku pojmů z oblasti krizového řízení a plánování obrany státu. V předešlém období došlo k řadě změn v legislativních předpisech, výkladu i chápání některých klíčových pojmů i oblastí, zavedeny byly také zcela nové pojmy a definice. Terminologický slovník je dostupný na internetových stránkách Ministerstva vnitra. Právě zde mohu myslím upozornit na jeden z cílů mé bakalářské práce, kterým je nalézání vztahů mezi informačními technologiemi a krizovým řízením. Význam spočívá v jeho dostupnosti z jakéhokoliv počítače, případně mobilního telefonu. Je zde možnost také jeho stažení do osobního počítače. Hlavní přínos však spatřuji v možnosti abecedního vyhledávání v pojmech a také jeho rozdělení do rejstříku použitých pojmových oblastí. To vše pomocí hypertextových odkazů, o kterých budu hovořit v kapitole „Internet".

[22] VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, s. 12.

4 REFORMA VEŘEJNÉ SPRÁVY

V této kapitole se pokusím najít argumenty, že reforma veřejné správy a její nové, lepší fungování, může mít významný vliv na zlepšování bezpečnostního prostředí v České republice. Vláda ve svém programovém prohlášení konstatovala, že cesta k posílení konkurenceschopnosti v mezinárodním prostředí je neodmyslitelně spjata se zvýšením efektivity výkonu veřejné správy. Proto se ve strategickém dokumentu Efektivní veřejná správa a přátelské veřejné služby[23] zavázala podniknout kroky směrem k zlepšení veřejné správy a kvality jí poskytovaných služeb, tzn. nastavit jednoznačně podmínky k tomu, aby veřejná správa byla nejen chápána, ale skutečně i fungovala, jako služba občanům.

4.1 Efektivní veřejná správa a přátelské veřejné služby (strategie)

Materiál „Efektivní veřejná správa a přátelské veřejné služby“ s podtitulem „Strategie realizace Smart Administration“ v období 2007–2015“ byl vládou přijat dne 11. července 2007 usnesením vlády č. 757.

Vizí pro rok 2015 je, že veřejná správa je primárně pojata jako služba občanovi, naplňuje principy dobrého vládnutí, funguje efektivně a výkonně. Veřejné služby jsou klientsky orientovány, naplňují očekávání občanů, flexibilně reagují na jejich potřeby a fungují hospodárně. Veřejná správa a veřejné služby přispívají ke zvyšování konkurenceschopnosti české ekonomiky a zvyšování kvality života obyvatel.

Jedním z dílčích cílů je zajistit adekvátní využívání informačních a komunikačních technologií, vytvořit centrální registry veřejné správy tak, aby bylo možné bezpečně sdílet data orgány veřejné moci a zároveň byl občanům umožněn oprávněný přístup k údajům vedeným v těchto registrech.[24]

4.2 Informační společnost

Pojem „Informační společnost“ je již několik let oficiálním termínem. V různých polohách se dostává do popředí zájmů téměř všech vyspělých států světa. Stává se předmětem veřejné politiky a součástí vládních programů. Na setkání zemí G7 v únoru 1995 byl program budování “Globální informační společnosti” deklarován dokonce

[23] *Efektivní veřejná správa a přátelské veřejné služby* [online]. [cit. 2010-03-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx>.
[24] *Cíle strategie Efektivní veřejná správa a přátelské veřejné služby* [online]. [cit. 2010-03-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/cile-strategie-efektivni-verejna-sprava-a-pratelske-verejne>.

jako mezinárodní úkol prvořadého významu. Důležitost dokazuje také vznik Rady pro informační společnost, která je odborným poradním orgánem vlády pro oblast informační společnosti. Má plnit koordinační roli místo zrušeného Ministerstva informatiky a poskytovat vládě vědomostní základnu zejména pro její rozhodování v koncepčních otázkách rozvoje informační společnosti tak, aby bylo dosaženo větší provázanosti a koordinace resortních a národních projektů.

4.2.1 Strategie rozvoje služeb pro informační společnost

Jedná se o vládní dokument, který si klade za cíl změnit veřejnou správu takovým způsobem, aby byla občanovi plnohodnotným partnerem v podmínkách moderní demokratické společnosti využívající informační a komunikační technologie pro svůj rozvoj a posílení konkurenceschopnosti. Je popisem plánu, jak změnit českou veřejnou správu, aby vyhovovala nárokům spontánně vznikající „informační společnosti“ - tedy takového hospodářského a společenského uspořádání, v němž rozhodující část ekonomických i soukromých aktivit lidí představuje nakládání s informacemi. Úkolem je vytvořit systém služeb, který bude stát informační společnosti poskytovat.[25]

Základem je transformovat a zjednodušit procesy používané dnes ve veřejné správě tak, aby využívaly moderních komunikačních a informačních technologií způsobem obdobným jejich využívání ve sféře komerční. Moderní komunikační a informační technologie totiž umožňují vytvořit zcela nové portfolio služeb veřejné správy, zjednodušující zásadním způsobem komunikaci občanů i firem s veřejnou správou i mezi subjekty veřejné správy navzájem. Současně lze výrazně zvýšit efektivitu výkonu veřejné správy bezpečným sdílením nejčastěji používaných informací v jednotlivých agendách.

Prioritními programovými oblastmi jsou:

- ***Základní registry a identifikace*** (registr územní identifikace a nemovitostí; registr obyvatel; registr osob; registr práv a povinností) spolu s organizační architekturou a technickým zázemím, které umožní propojení s agentovými registry, zabrání duplicitě dat a zachovají požadované standardy bezpečnosti.
- ***Univerzální kontaktní místo*** (asistovaná i samoobslužná komunikace s veřejnou správou, portál veřejné správy a dílčí agendové portály).

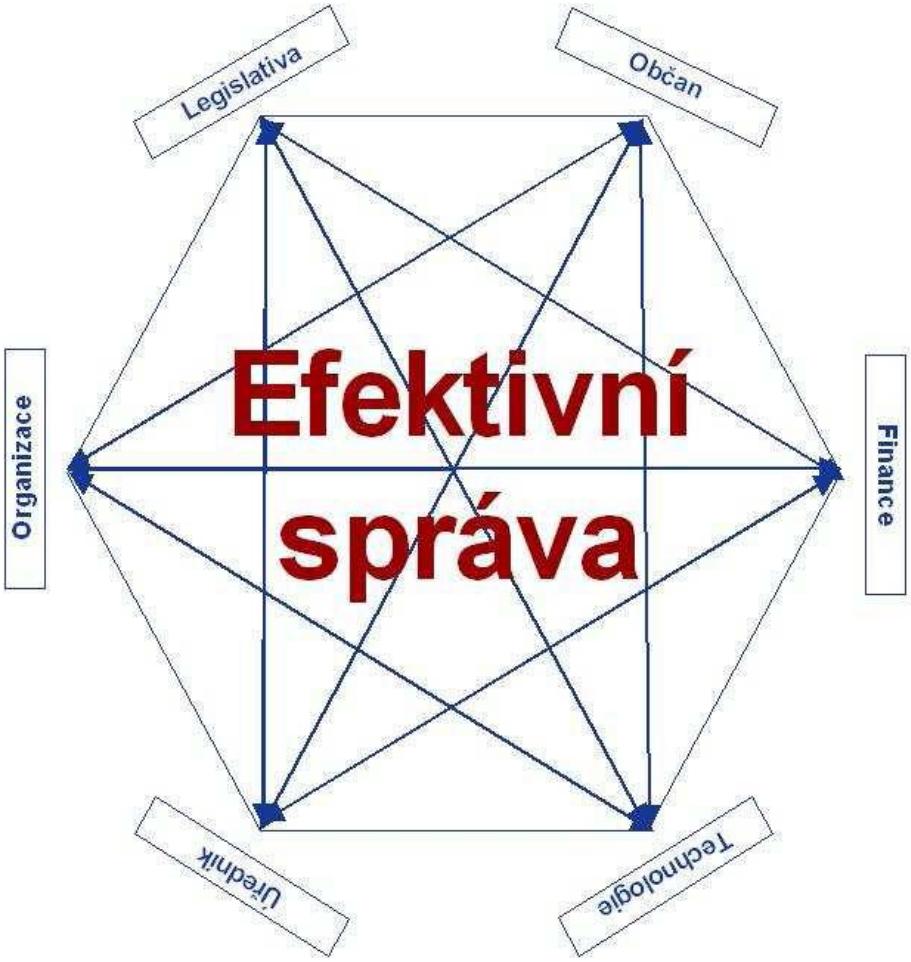
[25] *Strategie rozvoje služeb pro informační společnost* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.smartadministration.cz/files/StrategieSmartAdministration2007-2015.pdf>.

- ***Zaručená a bezpečná elektronická komunikace*** mezi úřady a stejně tak mezi občanem, firmou a úřadem využívající systém datových schránek včetně garantovaného systému autorizace a autentifikace a nezávislého dohledu nad dodržováním bezpečnostních a provozních pravidel.
- ***Vlastní služby pro informační společnost.***
- ***Zdravotnictví, důchodová a sociální péče, školství,*** v jejichž systémech se vedou ***elektronické karty*** jejich uživatelů, tedy pojištěnců, žáků, studentů atd.
- ***Veřejná správa v užším slova smyslu,*** jíž bude velmi obsáhlá skupina agend zahrnující především soudní, správní a daňové řízení, zejména vedení elektronických spisů umožňujících jednoduché předávání agendy mezi jednotlivými orgány veřejné správy a také skupina vykonávaných veřejných služeb v působnosti územních samospráv a některých státních institucí.
- ***Správa majetkových hodnot státu a samospráv***. Sem patří státní pokladna, evidence majetku, rozpočtování, zacházení s majetkem a penězi, veřejné zakázky, dotace apod.
- ***Digitalizace datových fondů a jejich archivace***, archivace a zpřístupňování kulturního bohatství v digitální podobě.[26]

[26] *Strategie rozvoje služeb informační společnosti* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/strategie-rozvoje-sluzeb-informacni-spolecnosti>.

4.3 Hexagon efektivní veřejné správy

Princip je zobrazen pomocí modelu Hexagonu veřejné správy. Hexagon má 6 vrcholů klíčových oblastí fungování veřejné správy: legislativa, organizace, občan, úředník, technologie, finance.



Obrázek č. 1: Hexagon efektivní veřejné správy.[27]

4.3.1 Legislativa jako základ kvalitní veřejné správy

Je to hlavní nástroj, který vláda používá k ochraně základních společenských hodnot a k ovlivňování chování občanů či právnických osob. Měla by ovšem být přijímána jen v případech, kdy je to nezbytné nutné, aby nezpůsobovala zbytečnou byrokratickou zátěž, zároveň by měla být co nejjednodušší a nejsrozumitelnější.

[27] *Strategie realizace Smart Administration* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/strategie-realizace-smart-administration>.

4.3.2 Organizace výkonu fungování veřejné správy

Vždy je třeba hledat rovnováhu mezi maximálním přiblížením výkonu veřejné správy občanovi a efektivním vynakládáním veřejných prostředku. Zároveň je důležité, aby bylo možné co největší množství agendy vyřídit na jednom kontaktním místě. Zásadou je, že „obíhají informace, nikoliv občan“. Organizace výkonu veřejné správy však neznamená pouze nalezení správného místa, tedy na jaké úrovni bude daná agenda vykonávána, ale také způsob, jakým je vykonávána. Důležitou roli zde hraje úroveň řízení, metody řízení kvality, sledování výkonnosti a efektivnosti vynakládaných prostředku a sledování spokojenosti „zákazníku“.

4.3.3 Využití moderních technologií ve veřejné správě

Prostřednictvím využití informačních a komunikačních technologií je nutné odstranit nadbytečné „papírování“, ulehčit styk občana s veřejnou správou, ale také komunikaci uvnitř veřejné správy. Tyto technologie je ovšem nutno vnímat pouze jako nástroj změn, nikoliv cíl sám o sobě. Při jejich zavádění se pak často stává, že administrativní zátěž je přesunuta z jednoho subjektu (občan) na subjekt jiný (úřad), cílem by ale měla být spíše minimalizace celkové zátěže pro všechny zúčastněné strany.

4.3.4 Občan je klientem veřejné správy

Je nejdůležitějším prvkem hexagonu. Je nutné mu co možná nejvíce usnadnit styk s úřady a co možná nejméně znepříjemňovat život nadbytečnou regulací. Zároveň je třeba veřejnou správu v maximální možné míře pro občana zprůhlednit, učinit ji otevřenou a umožnit tak občanům participovat na jejích rozhodnutích a kontrolovat její fungování.

4.3.5 Úředník je základním stavebním kamenem veřejné správy

A není podstatné, zda jde o úředníka ministerstva nebo úředníka vykonávající státní správu v přenesené působnosti na kraji či obci. Na úředníky by mělo být nahlíženo všude stejné, musí být vyžadována vysoká kvalita jejich výkonu a průběžné vzdělávání. Obzvlášť velký důraz je třeba klást na kvalitu řízení na všech úrovních.

4.3.6 Financování veřejné správy

Systému rozpočtování, způsobu alokace zdrojů na jednotlivé aktivity v rámci veřejné správy a provázání rozpočtu se strategickými prioritami vlády, ministerstev a zastupitelstev je proto potřeba věnovat významnou pozornost. Veškeré agendy v rámci veřejné správy je třeba přezkoumávat z hlediska nákladové efektivnosti.

4.4 eGovernment

Co to vlastně je eGovernment? OECD (Organizace pro hospodářskou spolupráci a rozvoj) definuje eGovernment jako: ***využívání informačních a komunikačních technologií a především internetu jako nástroje pro dosažení „lepší" státní správy.***[28]

Vláda České republiky chápe „eGovernment" jako transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.[29]

Hlavním cílem eGovernmentu je zvýšení výkonnosti státní správy, které by mělo přispět především ke zjednodušení činností veřejnosti při styku s veřejnou správou. Pro jeho správnou funkci je klíčová účelná elektronizace vnitřních agend ve veřejné správě, neboť jedině taková elektronizace v konečném důsledku umožní veřejnosti volbu lokality a volbu způsobu komunikace s veřejnou správou.

4.5 eGON - symbol eGovernmentu

Panáček eGON znázorněný na obrázku číslo 2., jako symbol eGovernmentu, je v přeneseném významu živý organismus, ve kterém vše souvisí se vším a fungování jednotlivých částí se navzájem podmiňuje.

Projekt eGON byl zahájen na konci roku 2006 a představuje komplexní projekt elektronizace veřejné správy, jehož hlavním cílem je usnadnění života občanům a zvýšení efektivity veřejné správy díky důmyslnému využití informačních a komunikačních technologií.

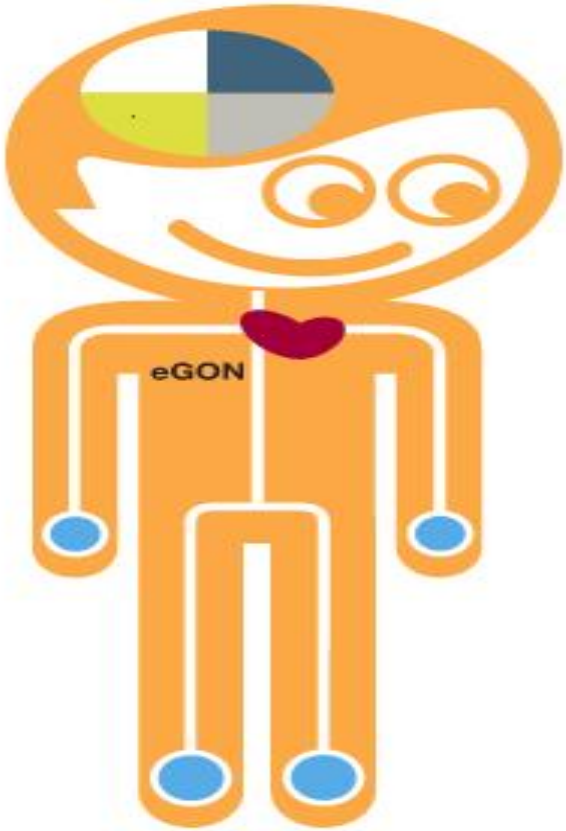
---

[28] *E-government imperative* [online]. [cit. 2010-03-15]. Dostupný z WWW: <http://www.google.com/books?hl=cs&lr=&id=E7X73oFkwV0C&oi=fnd&pg=PA11&dq=:+E+Government+Imperative&ots=zj3mySWtBt&sig=jDGfdTvOa546VN3dENQFmRRC9LM#v=onepage&q&f=false>.

[29] *Státní informační a komunikační politika e - Česko 2006* [online]. [cit. 2010-03-15]. Dostupný z WWW: <http://knihovnam.nkp.cz/docs/SIKP_def.pdf>.

Existenci a životní funkce eGONa zajišťují jeho:

- **Prsty:** Czech POINT - soustava snadno dostupných kontaktních míst.
- **Oběhová soustava:** KIVS - Komunikační infrastruktura veřejné správy, zajišťující bezpečný přenos dat.
- **Srdce:** Datové schránky - zákon o elektronických úkonech a autorizované konverzi č.300/2008 Sb.
- **Mozek:** Základní registry veřejné správy - bezpečné a aktuální databáze dat o občanech a státních i nestátních subjektech.



Obrázek č. 2: e-GON - symbol eGovernmentu

4.5.1 Czech POINT - kontaktní místa veřejné správy - eGonovy prsty

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

Cílem projektu Czech POINT je vytvořit garantovanou službu pro komunikaci se státem prostřednictvím jednoho universálního místa, kde je možné získat a ověřit data z veřejných i neveřejných informačních systémů, úředně ověřit dokumenty a listiny, převést písemné dokumenty do elektronické podoby a naopak, získat informace o průběhu správních řízení ve vztahu k občanovi a podat podání pro zahájení řízení správních orgánů. Jde tedy o maximální využití údajů ve vlastnictví státu tak, aby byly minimalizovány požadavky na občany. Tento projekt přináší značné ulehčení komunikace se státem. V některých situacích stačí dojít pouze na jeden úřad. V konečné fázi projektu by občan mohl určité své záležitosti vyřizovat i z domova prostřednictvím internetu.[30]

4.5.2 Komunikační infrastruktura veřejné správy - eGONův oběhový systém

Komunikační infrastruktura veřejné správy neboli KIVS jednoduše řečeno představuje sjednocení různých datových linek subjektů veřejné správy do jedné datové sítě. Přínosem bude jak zefektivnění služeb, tak výrazné úspory. Budování bylo zahájeno v roce 2007, v situaci, kdy paralelně vedle sebe existovaly a přibývaly další a další datové linky od jednotlivých ministerstev a úřadů. Primárním cílem zavádění KIVS bylo vytvoření jednotné datové sítě, která poskytne bezpečné připojení a vysoký standard nabízených služeb. Druhým cílem bylo odstranění monopolu poskytovatelů datových služeb. Za krátkou dobu realizace projektu KIVS přinesl systém úspory v hodnotě více než 250 milionů Kč. Úspory jsou k dispozici uživatelům systému, kteří je mohou využít pro investice do informačních systémů a získat tak kvalitnější nebo rychlejší připojení a tím pádem i zlevnění služeb díky konkurenčnímu prostředí. Komunikační infrastruktura je cestou k efektivnímu propojení mezi orgány a informačními systémy veřejné správy, umožňující jak zajištění bezpečného přenosu dat, tak nastavení jednotlivých procesů komunikace mezi zúčastněnými subjekty. Prostřednictvím KIVS jsou propojeny orgány veřejné správy například s registry nebo Czech POINTy.

Jedním z pilířů sítě je Centrální místo služeb CMS, které je potřeba zmínit ve vztahu k informačním systémům veřejné správy a také informačním systémům krizového řízení, které budou přes toto místo využívat údaje z datových skladů vytvořených příslušnými orgány veřejné správy.

[30] *Co je Czech POINT* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.czechpoint.cz/web/?q=node/22>.

Centrální místo služeb zajišťuje vzájemné řízené a bezpečné propojování subjektů veřejné a státní správy, dále zajišťuje komunikaci subjektů veřejné a státní správy s jinými subjekty ve vnějších sítích, jakými jsou Internet nebo komunikační infrastruktura Evropské unie. Zároveň tvoří jediné logické místo propojení jednotlivých operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS.

4.5.3 Základní registry veřejné správy - eGONův mozek

Vytvoření centrálních registrů veřejné správy, řeší dosavadní potíže související s nejednotností, multiplicitou a neaktuálností klíčových databází. Jsou dalším z pilířů elektronizace veřejné správy. Bez nich by celé fungování eGovernmentu v České republice bylo málo efektivní. Zásadním krokem k fungování systému základních registrů bylo přijetí zákona č. 111/2009 Sb., o základních registrech a zákona č. 227/2009 Sb. na počátku roku 2009. Tyto zákony vytvářejí předpoklad pro spuštění systému od 1. 7. 2010 ve zkušebním provozu a o rok později v ostrém provozu.

Základní registry budou celkem čtyři:

1. **Registr obyvatel - ROB**
2. **Registr práv a povinností - RPP**
3. **Registr osob - ROS**
4. **Registr územní identifikace, adres a nemovitostí - RUIAN**

Všechny čtyři základní registry budou fungovat v rámci Informačního systému základních registrů, tzv. ISZR, jehož správu bude mít na starosti nově vzniklý státní úřad (Správa základních registrů). Technologickou platformu informačního systému budou zajišťovat již zmíněné součásti eGONa – Komunikační infrastruktura veřejné správy a Centrální místo služeb. Konkrétnější rozbor základních registrů a jeho vztah ke krizovému řízení uvedu v samostatné kapitole.

4.5.4 Datové schránky - zákon o eGovernmentu - eGONovo srdce

Jedná se o zákon č.300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů. Cílem zákona o je vytvoření optimálních podmínek pro elektronickou komunikaci mezi úřady a občany i mezi úřady samotnými. Rovněž se jím umožní vedení elektronických spisů ve správních řízeních.

Klíčový institut pro provádění elektronických úkonů, tedy pro komunikaci s orgány veřejné moci, představují datové schránky, jejichž informační systém zabezpečuje doručení úředních zpráv v elektronické podobě. Druhým klíčovým prvkem

zákona o elektronických úkonech je autorizovaná konverze dokumentů, tedy převedení dokumentu v listinné podobě do dokumentu obsaženého v datové zprávě nebo převedení dokumentu obsaženého v datové zprávě do listinného a zároveň ověření shody jejich obsahu a připojení ověřovací doložky.[31]

4.6 Elektronický podpis

Elektronický podpis je jedním z hlavních nástrojů identifikace a autentizace fyzických osob v prostředí internetu. Postupně stále více právních předpisů umožňuje jeho používání v oblasti orgánů veřejné správy, a to jak při komunikaci mezi úřady navzájem, tak i při komunikaci občanů s jednotlivými úřady. V současné době občané využívají elektronický podpis vůči orgánům veřejné správy především v oblasti správy daní a v obecných správních řízeních. Nutnou podmínkou pro komunikaci občanů se státní správou s použitím elektronického podpisu jsou tzv. kvalifikované certifikáty občanů.

4.7 Informační systémy veřejné správy - ISVS

Informační systémy veřejné správy představují významný nástroj výkonu veřejné správy na všech úrovních. Bohužel zatím jednotlivé informační systémy orgánů veřejné správy rozhodně není možné považovat za funkční kooperující celek. Činnost orgánů veřejné správy je zabezpečována autonomními informačními systémy. Komunikace mezi těmito systémy je na různé úrovni, celkově ji však nelze považovat za uspokojivou, vzhledem k tomu, že řada údajů je od občanů i právnických osob vyžadována opakovaně a s následnou vzájemnou komunikací (ať už písemnou, či elektronickou) jsou problémy.[32]

V červenci 2002 Parlament ČR schválil zákon č. 365/2000 Sb., o informačních systémech veřejné správy a změně některých dalších zákonů. Základním smyslem zákona tak bylo vytvořit legislativní předpoklady pro efektivní využívání informací z jednotlivých informačních systémů veřejné správy, a postupně tak zlepšit současný stav. S ohledem na potřebu zajistit transparentnost, vzájemnou kompatibilitu, komunikaci a určitý stupeň jednotnosti všech ISVS, je kladen velký důraz na řízení této

[31] *Datové schránky* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.datoveschranky.info/o-datovych-schrankach-text/>.
[32] *Jak postupovat při plnění povinností vyplývajících ze zákona č. 365/2000 Sb.* [online]. [cit. 2010-02-25]. Dostupný z WWW: <http://www.mvcr.cz/soubor/metodicke-pokyny-jak-postupovat-pri-plneni-povinnosti-vyplyvajicich-ze-zakona-c-365-2000-sb.aspx>.

oblasti, které na nejvyšší úrovni přísluší Ministerstvu vnitra. Dlouhodobé řízení ISVS je naplňováno prostřednictvím informační koncepce a provozní dokumentace. Dlouhodobé řízení ISVS podléhá atestaci, a to na všech úrovních veřejné správy s výjimkou obcí, které vykonávají přenesenou působnost pouze v základním rozsahu.[33]

4.7.1 Terminologie ISVS

Při každé lidské činnosti je potřebné se domluvit na společných významech nezbytných pro další komunikaci. Především v této oblasti bylo nutné stanovení základních definic a pojmů. Zejména jsou to informační činnost, informační systém, správce a provozovatel informačního systému veřejné správy, standard informačních systémů veřejné správy, datový prvek, číselník, referenční sdílené a bezpečné rozhraní informačních systémů veřejné správy, dálkový přístup do informačního systému, portál veřejné správy, veřejný a provozní informační systém apod. Pro pochopení významu této kapitoly i pro krizové řízení zde některé vysvětlím.

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy definuje ***informační systémem*** jako 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, provozní údaje a dále nástroje umožňující výkon informačních činností.

Informační činnost chápe jako 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.

Datový prvek je jednotka dat, která je v daném kontextu dále považována za nedělitelnou a je jednoznačně definována.

Referenční rozhraní 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

[33] *Koncepce budování informačních systémů veřejné správy* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.isvs.cz/user_data/dokumenty/UVIS-Koncepce-ISVS-1999.pdf>.

oprávněně vyžadovaných informací mezi jednotlivými informačními systémy orgánů veřejné správy a dalšími subjekty, a to i se systémy mimo Českou republiku.

Významným pojmem je také ***dálkový přístup*** do informačního systému prostřednictvím sítě nebo služby elektronických komunikací. (například s využitím internetu)[34]

4.7.2 Data pro ISVS

Sdílení dat nejen v ISVS musí mít svá pravidla. Při elektronické výměně dat mají význam standardy, které zajišťují, aby se přenos mezi různými platformami vůbec mohl uskutečnit, a aby se obsah informace, její struktura a uspořádání na obou stranách přenosu správně interpretovaly. Standardy existují nejen pro hardware, software, komunikace, ale i pro data, tj. ***datové standardy***. Datové standardy se definují ve formě sborníků (registrů), které obsahují popisy, definice a další atributy tzv. datových prvků, případně složených datových prvků, segmentů, zpráv. Tyto datové sborníky bývají specifické pro určité oblasti použití, nebo odvětví a jejich význam vzrůstá s globální výměnou dat a dokumentů prostřednictvím sítí.

Datový prvek, jak už jsem v terminologii zmínil, je jednotka dat, která je v daném kontextu dále považována za nedělitelnou a je jednoznačně definována. Přesná a jednoznačná definice datového prvku je nezbytná pro zajištění možnosti jeho sdílení. Pro bezproblémový chod informačních systémů veřejné správy je nutné zajistit, aby datové prvky a jejich číselníky, které jsou základem jakékoli výměny dat mezi orgány veřejné správy a veřejností byly identické. V současné době proto probíhá jejich standardizace, která je řešena Metodickým pokynem pro popis datových prvků informačních systémů veřejné správy.[35]

4.7.3 Kvalita ISVS

Kvalitu i v oblasti informačních systémů a technologií je potřeba vnímat jako celkový souhrn vlastností, které dávají schopnost uspokojovat předem stanovené nebo předpokládané potřeby. Obsah řízení kvality je uveden ve vyhlášce č. 529/2006 Sb. § 2 odst. 1 písm. c), způsob naplnění v § 3. Požadavky by měly být pokud možno měřitelné a měly by být vázány na cíle kvality, k jejichž naplnění směřují. Požadavky

[34] *Zákon 365/2000 Sb. o informačních systémech veřejné správy* [online]. [cit. 2010-02-25]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00365&cd=76&typ=r>.

[35] *Metodický pokyn pro popis datových prvků* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/metodicky-pokyn-pro-popis-datovych-prvku.aspx>.

mohou být specifické, pro jeden informační systém nebo společné, pro několik informačních systémů.

Kvalita dat, která ISVS zpracovávají

Jedním z významných prvků kvality dat je jejich ***aktuálnost***. V závislosti na typu a provedení informačního systému může být aktuálnost dat značně různorodá. Od systémů, kde se změny projevují okamžitě, až po komplexní systémy, kde je např. zapotřebí replikací do prezentačních částí, které mohou mít časovou prodlevu. Důležitým prvkem je též způsob spolupráce ISVS se subsystémy či jinými spolupracujícími systémy. Zde se aktuálnost dat systému stává závislou na dodávaných datech spolupracujících zdrojů a je značně svázána s aktuálností zdrojů či způsobem, jímž jsou data ze spolupracujících zdrojů získávána.

Významnou vlastností je i ***správnost dat***, která může být zajišťována celou řadou způsobů. Počínaje pouhou vizuální kontrolou, přes kontrolu zajišťovanou administrativně či technicky.

Integrita, jako další kvalitativní vlastnost a tedy ***konzistentnost*** dat, by měla být prováděna co nejvíce na technologické úrovni. Vzhledem k tomu, že integrita je klíčovým prvkem k tomu, aby data byla vůbec použitelná, je vhodné na této úrovni minimalizovat chybu lidského faktoru.

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

Kvalita služeb, které jsou prostřednictvím ISVS poskytovány

Dostupnost služeb je velmi svázaná s kvalitou technických prostředků. Potřeba dostupnosti ISVS by měla úměrně stoupat s významem ISVS jak pro cílové uživatele, tak i pro spolupracující informační systémy. Informační systém musí zajistit, aby požadovaná informace byla přístupná ve stanoveném místě, v požadované formě a také v určeném časovém rozmezí.

Přehlednost služeb souvisí s vizuálním návrhem rozhraní ISVS. Uživatelé by se neměli "ztrácet". Naopak by měli mít jasný přehled, ve které části rozhraní se nacházejí.

Srozumitelnost služeb znamená, že všechny prvky rozhraní by měly být jednoznačné a popisky by neměly být matoucí. Rozhraní by se mělo oprostit od

používání odborného žargonu a naopak se snažit v rozumné míře přiblížit neznalému uživateli.

Kompatibilita s běžně používanými klientskými prostředími a standardy je dalším podstatným prvkem kvality služeb se týká nejen rozhraní pro uživatele, ale také pro spolupracující informační systémy. Proto je při návrhu žádoucí držet se běžně používaných standardů.

Kvalita technických a programových prostředků ISVS

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

Kvalita technických prostředků je přímo úměrná požadované kvalitě služeb. Je zajišťována jak kvalitou samotného technického vybavení, tak ale i prvky k odvrácení technických rizik. Začíná tedy volbou vhodných technických komponent systémů samotného ISVS, pokračuje přes zařízení schopná omezit rizika výpadku vnějších prvků (např. výpadek energie, výpadek připojení k internetu) a končí kompletními řešeními, schopnými snížit rizika výpadku samotného zařízení (disková pole, clustery, počítače se znásobenými komponentami pro případ jejich výpadku, apod.). Mezi prvky k zajištění kvality technických prostředků rovněž patří další podpůrné systémy, jako např. zálohovací systémy, ale i routery, firewally apod. Do prvků, určujících kvalitu technického vybavení můžeme zařadit i firmware použitého technického zařízení, ač se svou povahou spíše jedná o prvek na rozhraní technického a softwarového vybavení.

Kvalita programových prostředků je oblastí, která postihuje širokou škálu softwarového vybavení. Jedná se zejména o operační systém, certifikované ovladače, servisní balíčky či „záplaty“, databázové servery, aplikační servery, webové servery, prostředí typu Java apod. Podstatná je také kvalita konkrétního programového vybavení zajišťujícího vlastní funkčnost systému. Do této oblasti také nepřímo spadá kvalita programových prostředků spolupracujících systémů.

4.7.4 Bezpečnost ISVS

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

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

Bezpečnost dat v ISVS

Dostupnost dat by měla být zajištěna vhodnou kombinací technických a programových prostředků úměrně potřebě dat. Do této oblasti patří např. použití diskových polí, clusterů, i softwarových nástrojů, zajišťujících či posilujících datovou dostupnost. Je nutné stanovit politiku zálohování a archivací, a to nejen z hlediska pravidelnosti zálohování, způsobu zálohování, způsobu archivací dat, ale i způsobu uložení dat (např. dvojí uložení do dvou fyzicky různých lokalit pro případ požáru) apod.

Důvěrnost dat se zajišťuje aplikací základních atributů zabezpečeného přístupu, kterými jsou:

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

K datům je nutno vést řízený přístup. Je třeba, aby data byla chráněna tak, aby k nim neoprávněné osoby neměly přístup umožňující čtení či dokonce pozměňování nebo mazání.

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

Bezpečnost služeb ISVS

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

Důvěrnost služeb je opět zajišťována aplikací základních atributů zabezpečení přístupu: identifikací, autentizací a autorizací.

Tyto atributy se uplatňují jak vůči osobám, tak i vůči spolupracujícím systémům. Do této kapitoly spadá i ochrana důvěrnosti dat během přenosu sítěmi s tím,

že informace, která to svoji povahou vyžaduje, musí být v procesu přenosu mezi zdrojem a cílem chráněna odpovídajícím způsobem.

Integrita služeb je bezpečnostním cílem, který pokrývá zajištění konzistentnosti služeb samostatných a také spolupracujících systémů. Týká se např. sdílení informací o uživateli, sdílení služeb datových zdrojů apod.

Bezpečnost technických a programových prostředků ISVS

Dostupnost technických prostředků obsahuje: záložní zdroje napájení, záložní síťová připojení, zabezpečení dostupnosti hardware duplikováním či násobením důležitých prvků (clustery apod.) a umístění záložních zařízení do geograficky různých lokalit.

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

Důvěrnost technických prostředků zahrnuje především fyzickou bezpečnost, tj. umístění technických prostředků do fyzicky zabezpečeného prostoru a také zabezpečení používané telekomunikační infrastruktury.

Důvěrnost programových prostředků se týká zejména zajištění odolnosti proti úmyslně či neúmyslně chybným vstupním datům, zajištění ochrany proti parazitním kódům, zajištění ochrany proti podvržení identity spolupracujících systémů.

Integrita technických prostředků se týká zejména ochrany proti přetížení, ochrany proti zničení či poškození.

Integrita programových prostředků zahrnuje ochranu proti smazání softwarové komponenty, ochranu proti modifikaci či podvržení softwarové komponenty a ochranu proti modifikaci konfigurace softwarové komponenty.[36]

4.7.5 Dálkový přístup k ISVS

Pro orgány veřejné správy zákon o ISVS stanoví povinnost „*postupovat při uveřejňování informací způsobem umožňujícím dálkový přístup tak, aby byly informace*

[36] *Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx>.

související s výkonem veřejné správy uveřejňovány ve formě, která umožňuje, aby se s těmito informacemi v nezbytném rozsahu mohly seznámit i osoby se zdravotním postižením ".

Formu uveřejňování informací, které souvisí s výkonem veřejné správy a jsou uveřejňovány na webových stránkách orgánu veřejné správy, je třeba uzpůsobit tak, aby byly informace pro uživatele se zdravotním postižením přístupné. Proto je nutné, aby webové stránky byly vyrobeny podle pravidel tvorby přístupných webových stránek uvedených v příloze vyhlášky o přístupnosti. Pro názornost uvádím názvy kapitol pravidel přístupnosti, kterých je celkem 33 a nachází se v metodickém pokynu k vyhlášce č. 64/2008 Sb., o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti).

Pravidla přístupného webu jsou:

A. Obsah webových stránek musí být dostupný a čitelný.
B. Práci s webovou stránkou řídí uživatel.
C. Informace musí být srozumitelné a přehledné.
D. Ovládání webových stránek musí být jasné a srozumitelné.
E. Zdrojový kód musí být technicky způsobilý a strukturovaný.
F. Prohlášení o přístupnosti webových stránek.

4.8 Celostátně provozované ISVS

4.8.1 Informační systém o základních registrech

Myslím, že jsme svědky revoluce v registrech veřejné správy. Současný stav v oblasti dat veřejné správy je, a troufám si použít slovo, žalostný. Zřejmá je roztříštěnost, nejednotnost a multiplicita vedení klíčových databází veřejné správy. Není možné sdílet nejčastěji využívané údaje v různých databázích veřejné správy. Například ještě dnes musí občan při jednání s úřady údaje vedené o jeho osobě dokládat opakovaně, v lepším případě bez správního poplatku. Praxe také dlouhodobě ukazuje, že při výkonu veřejné moci nejsou k dispozici údaje, na které se lze spolehnout.

Podstatou „revoluce" je zákon č.111/2009 Sb., o základních registrech, který vymezuje obsah základních registrů a informačního systému územní identifikace a stanoví práva a povinnosti, které souvisejí s jejich vytvářením, užíváním a provozem.

Zásadním prvkem v systému základních registrů je tzv. ***„referenční údaj"***. Je to údaj vedený v základním registru, který zákon upravující vedení příslušného registru

jako referenční údaj označuje, v daný okamžik aktuální, platný a jednotný údaj pro použití v agendách ve státní správě. Ve své podstatě jde o údaj, který bude přebírán ze systému základních registrů a v příslušných agendách se bude využívat jako údaj zaručený, platný a aktuální, bez nutnosti jeho ověření. Úřady budou povinny využívat právě data ze základních registrů a nikoli je vyžadovat po občanovi. V principu tak bude stačit jedna změna v registru, například při změně jména nebo adresy, která se promítne i v ostatních registrech.[37]

Zde vidím opět nemalý potenciál pro efektivní propojení informačních systémů krizového řízení, kdy tyto budou pracovat vždy s aktuálními „referenčními údaji" a budou minimalizovány problémy s duplicitními daty v duplicitních databázích.

Základní registry:

Registr obyvatel (ROB) - obsahující základní údaje o občanech a cizincích s povolením k pobytu. Mezi tyto údaje patří: jméno a příjmení, datum a místo narození a úmrtí a státní občanství.

Registr práv a povinností (RPP) - obsahující referenční údaje o působnosti orgánů veřejné moci, mj. oprávnění k přístupu do k jednotlivým údajům, informace o změnách provedených v těchto údajích apod. Sloužit bude také jako garance bezpečné správy dat občanů a subjektů vedených v jednotlivých registrech.

Registr osob (ROS) - obsahující údaje o právnických osobách, podnikajících fyzických osobách, orgánech veřejné moci i o nekomerčních subjektech, jako jsou občanská sdružení a církve.

Registr územní identifikace, adres a nemovitostí (RUIAN) - spravující údaje o základních územních a správních prvcích.

Ochrana osobních údajů

Důležitým prvkem systému bude převodník identifikátorů fyzických osob tzv. ORG, jež bude v gesci Úřadu pro ochranu osobních údajů. Činnost ORG je pro ochranu osobních údajů v celém systému základních registrů zcela klíčová. Zavádí se systém agendových identifikátorů fyzických osob (AIFO). ORG bude jedinou institucí, která dokáže přepočítávat agendové identifikátory z jednoho registru pro druhý. Už tedy nebude možné díky znalosti rodného čísla získat o tomto obyvateli informace

[37] *Informační systém základních registrů* [online]. [cit. 2010-04-15]. Dostupný z WWW: <http://www.szrcr.cz/file/12>.

prakticky z každého informačního systému veřejné správy, jako to lze nyní. Každá osoba bude v každé agendě vedena pod jedinečným AIFO, čímž se minimalizuje riziko zneužití osobních údajů. Důležitosti činnosti ORG bude odpovídat i jeho zabezpečení, jež bude srovnatelné se špičkovou bankou.

4.8.2 Informační systém o informačních systémech veřejné správy

Informační systém o informačních systémech veřejné správy (IS o ISVS) je informační systém, sloužící ke sběru a poskytování informací o informačních systémech veřejné správy. Jedná se o základní informace o ISVS a informace o dostupnosti ISVS. Tento systém byl vyvinut v souladu se zákonem č. 365/2000 Sb., o ISVS a příslušným navazujícím prováděcím právním předpisem - Vyhláškou Ministerstva informatiky České republiky č. 528/2006 Sb. o informačním systému o ISVS.

Orgány veřejné správy jsou povinny zpřístupňovat Ministerstvu vnitra v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi provozovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem zveřejnění v informačním systému o informačních systémech veřejné správy.

IS o ISVS je typická třívrstvá webová aplikace s datovou, aplikační a prezentační vrstvou. Pro provoz databáze IS o ISVS je vyčleněn server v příslušné konfiguraci a instalovaným programovým vybavením. Server je provozován pod operačním systémem MS Windows v databázovém prostředí MS SQL Server. Jako klientské stanice jsou použity osobní počítače se základním vybavením. Klientská stanice vyžaduje pouze webový prohlížeč. Propojení klientských stanic se serverem je realizováno prostřednictvím internetu. Pro komunikaci se využívá sady protokolů TCP/IP.[38]

4.8.3 Informační systém o datových prvcích

Informační systém datových prvků (ISDP) je informační systém veřejné správy, poskytující oficiální informace o datových prvcích informačních systémů veřejné správy. Datové prvky vyhlášené v ISDP jsou pro orgány veřejné správy a vazby jejich informačních systémů závazné. Tento systém byl vyvinut v souladu se zákonem

[38] *Informační systém o informačních systémech veřejné správy* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.asd-software.cz/clanek-142-is-o-isvs.html>.

č. 365/2000 Sb., o ISVS a Vyhláškou Ministerstva informatiky ČR č. 469/2006 Sb. o informačním systému o datových prvcích.

Orgány veřejné správy jsou povinny podle zákona předávat Ministerstvu vnitra údaje do informačního systému o datových prvcích v elektronické podobě. Dále jsou povinny zajistit, aby vazby jimi provozovaného informačního systému na informační systém jiného provozovatele byly uskutečňovány s použitím datových prvků vyhlášených v informačním systému o datových prvcích.

V ISDP jsou realizovány funkce pro podporu výkonu agendy správy datových prvků**,** tj. pro zajištění podpory životního cyklu datových prvků, používaných v informačních systémech veřejné správy. ISDP slouží k vyhlašování a evidenci datových prvků a zveřejňování číselníků. Sémanticky příbuzné datové prvky jsou seskupeny do datových slovníků. Každý datový slovník je pro účely použití v rámci komunikace informačních systémů veřejné správy prezentován ve formátu XML schématu. Ke každému datovému slovníku také existuje dokumentace v PDF formátu. Architektura informačního systému a technická infrastruktura je obdobná jako u informačního systému o ISVS. Využitím ISDP je možno získat informace o jednotlivých datových prvcích, používaných v informačních systémech veřejné správy, především informace o správci datového prvku, kontaktních osobách, povolených hodnotách, legislativních východiscích, XML reprezentaci a číselnících. ISDP bude sloužit jako generická služba komunikačního prostředí ISVS - centrální poskytovatel XML schémat datových slovníků ISVS, které budou využívat webové služby v prostředí informačních systémů veřejné správy.[39]

4.8.4 Datové schránky

Datové schránky jsou elektronickým úložištěm, na které se doručují dokumenty orgánů veřejné moci a stejně tak i vůči nim. Tento způsob komunikace nahrazuje klasické doručování v listinné podobě.

Povinně musí tento systém využívat právnické osoby a orgány veřejné moci, a to od 1. listopadu 2009. Fyzické osoby si mohou datovou schránku zřídit dobrovolně. Pokud tak učiní, orgány veřejné moci jsou povinny ji využívat i vůči nim. Fyzickým osobám žádná takováto povinnost nevyplívá, mohou nadále využívat oba typy komunikace, tedy elektronickou i listinnou. Datové schránky nejsou povinné ani pro

[39] *Informační systém o datových prvcích* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.asd-software.cz/index.php?ID=137>.

podnikající fyzické osoby. Výjimkou z této skupiny jsou však advokáti, daňoví poradci, insolvenční správci, notáři a exekutoři. Na tyto podnikatele se vztahuje přechodné období, po jehož uplynutí bude schránka zřízena automaticky. Zatím není možná komunikace mezi právnickými ani mezi fyzickými osobami navzájem.

Informační systém datových schránek vede informace o:

- datových schránkách a jejich vlastnících,
- uživatelích systému a jejich oprávněních,
- doručovaných zprávách,
- postupu doručení.

Výhodou zřízení datové schránky je nesporně přístup k obsahu datové schránky z jakéhokoli místa, kde je dostupný internet, a tedy i velká úspora času, kdy odpadá nutnost docházet na poštu a trávit dlouhé chvíle ve frontách. Nad to, všechny právnické osoby, stejně jako fyzické osoby, komunikují s orgány veřejné moci zdarma.[40]

4.8.5 Portál veřejné správy

Portál veřejné správy je elektronická brána do veřejné správy. Vznikl na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy a hlavním smyslem portálu je usnadnit občanům a firmám orientaci a komunikaci s úřady veřejné správy. Významným způsobem přispívá k potřebě kvalitních služeb při poskytování důvěryhodných a garantovaných informací širokému spektru občanů ČR, včetně poskytování relevantních informací cizincům, a zjednodušení komunikace s úřady. Cílem je přispět k modernizaci veřejné správy také prostřednictvím informačních a komunikačních technologií a tím postupně naplňovat ústřední motto „Efektivní veřejná správa a přátelské veřejné služby“. Portál veřejné správy je předurčen, v souladu s programovým cílem vlády, stát se místem, které bude *„**integrovat a zpřístupňovat všechny zveřejňované a veřejně přístupné informace veřejné správy**“,* včetně možné komunikace s úřady. Je svým zaměřením určen pro širokou veřejnost, státní správu a samosprávu, státní i soukromé organizace včetně podnikatelů, živnostníků a cizinců.[41]

[40] *Datové schránky* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.datoveschranky.info/>.
[41] *Portál veřejné správy* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://portal.gov.cz>.

4.8.6 Elektronický portál územních samospráv - ePUSA

Elektronický portál územních samospráv je informačním systémem s aktuálními kontakty na orgány veřejné správy – kraje, obce a města. Uvedený systém umožňuje vybrat potřebné údaje podle různých kritérií. Provozovatelem portálu je Ministerstvo vnitra České republiky a je společným projektem Ministerstva vnitra, krajů a ostatních samospráv. Cílem tohoto projektu je být jediným garantovaným zdrojem informací o subjektech samosprávy, a zamezit tak jejich duplicitnímu zjišťování orgány veřejné správy.[42]

4.8.7 Digitální mapa veřejné správy - DMVS

V rámci procesu dynamického zavádění principů eGovernment do oblasti veřejné správy neodkladně vyvstává potřeba mít k dispozici co největší množství dat za celé území ČR v digitální podobě, aby mohlo být co největší množství agend veřejné správy, a to i těch, které pracují s prostorovými daty, elektronizováno. Nástup digitálních technologií možnost využívání prostorových dat významně zvyšuje. Zjednodušeně lze říci, že na rozdíl od prostého zobrazování daného jevu na mapovém podkladu digitální technologie umožňují nejen snazší a přesnější práci, ale nabízejí také celou řadu nových možností v oblasti rozhodovacích a řídicích procesů. Podmínkou pro to je nejen vlastnit tato data v digitální podobě, ale také mít možnost pracovat s nimi na vhodném digitálním mapovém podkladu. A chceme-li s prostorovými (územními) jevy pracovat ve vzájemných souvislostech a vazbách, resp. řešit komplexní úkoly, (krizové situace) v nichž se celá řada územních jevů střetává, je nezbytné všechny tyto jevy zobrazovat nad jediným a jednotným digitálním mapovým podkladem. Jen tak lze totiž všechny vazby, souvislosti a vzájemné ovlivňování příslušných prostorových jevů s potřebnou přesností postihnout. Toto je základní myšlenka, která stála u zrodu projektu Digitální mapy veřejné správy. V současné době neexistuje ucelené digitální vektorové mapové dílo v rozsahu celé České republiky.

Hlavními uživateli DMVS budou subjekty veřejné správy, občané i podnikatelské subjekty, a to prostřednictvím síťových služeb i jednorázových dávkových přenosů dat. DMVS bude také hlavním zdrojem jednotných a aktuálních informací pro složky Integrovaného záchranného systému České republiky. Garantem řešení projektu budou krajské úřady, které přitom budou spolupracovat s příslušnými katastrálními úřady.

[42] *Elektronický portál územních samospráv* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.egovernment.cz/archiv/PDF%201-08/5.pdf>.

Vytvořené digitální mapové dílo bude sloužit zejména v těch oblastech výkonu veřejné správy, kde jsou dnes potřebná a využívaná mapová díla, přičemž možnosti užití se významně rozšíří jak z hlediska elektronizace příslušných agend, tak i z hlediska spektra potenciálních uživatelů, spolu se zvýšením přesnosti, spolehlivosti a výrazného zefektivnění souvisejících činností.[43]

DMVS vznikne jako mapová kompozice digitálních ortofotomap, existujících digitálních a digitalizovaných katastrálních map z produkce ČÚZK, digitálních účelových katastrálních map, které byly nebo budou vytvořeny v rámci činnosti samosprávy, a digitálních technických map, které dosud byly nebo v dalším období budou vytvořeny v rámci činnosti samosprávy nebo správců sítí. Bude nastaven pravidelný systém aktualizace DMVS subjekty veřejné správy. K uložení dat budou využity regionální datové sklady, které by měly vzniknout jako součást technologických center samosprávy.

5 INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE

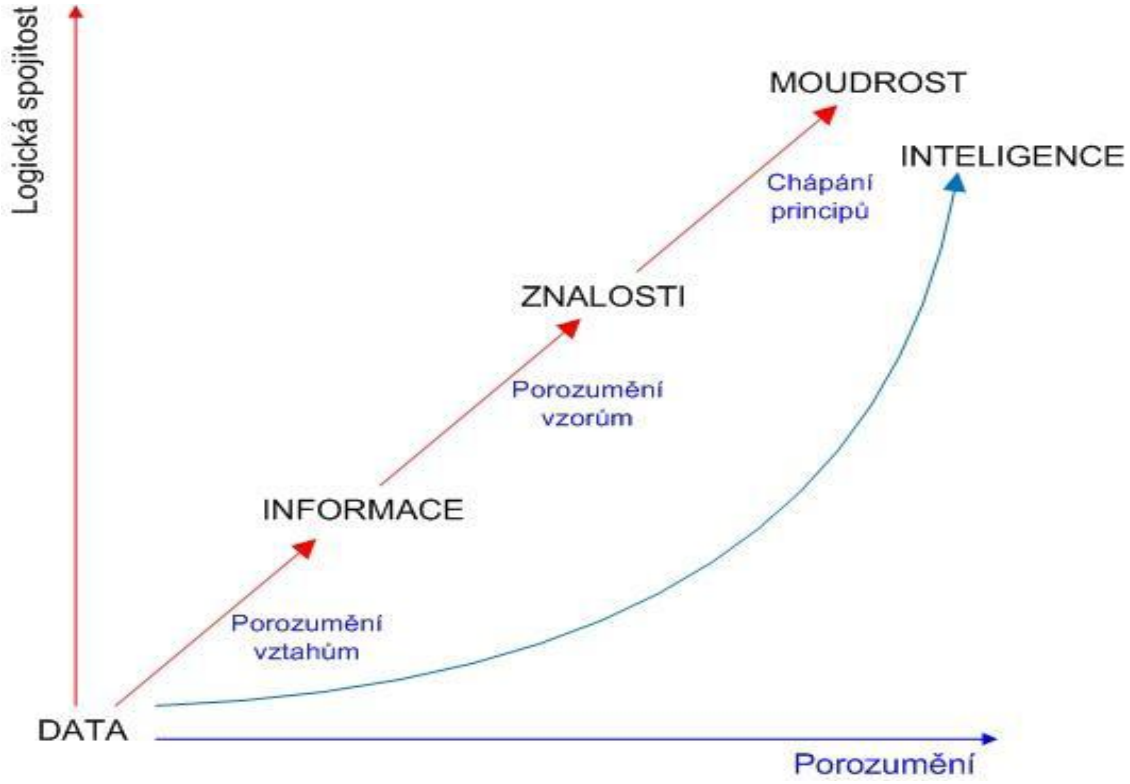
„Informační společnost“ bývá také chápána jako soubor nástrojů výpočetní a komunikační techniky a komunikačních a informačních služeb, které se stávají postupně určujícím faktorem rozvoje ekonomiky a významně ovlivňují i rozvoj celé společnosti. Je charakterizována širokým využíváním digitálního zpracování, uchovávání a přenosu informací. Chápání informačních a komunikačních prostředků jako pouhého nástroje je ale příliš úzké. Jde spíše o celkové prostředí, ve kterém se odehrává práce a i mimopracovní život lidí. Představuje i celkovou filosofii práce s informacemi, spočívající v tom, že informace nejsou chápány samoúčelně. Člověk je neshromažďuje jen proto, “aby je měl”, ale proto, aby se podle nich rozhodoval v zcela konkrétních životních situacích. V každém případě lze říci, že hlavním rysem informační společnosti není podle dnes převažujících názorů podpora produkce, ale vytvoření podmínek pro hodnotnější a spokojenější život lidí. Není účelem zvyšovat produkci prostředků informačních technologií a zavádět je překotně do všech oblastí lidské činnosti. Cílem by především mělo být život lidem usnadnit, zlepšit jeho kvalitu.

[43] *Digitální mapa veřejné správy* [online]. [cit. 2010-04-19]. Dostupný z WWW: <http://www.mvcr.cz/soubor/dmvs-informace.aspx>.

Jsem přesvědčen, že naučíme-li se dobře zacházet s informacemi a systémy pro jejich zpracovávání, dojde také ke zlepšení bezpečnostního prostředí, ve kterém žijeme.[44]

5.1 Informace

Následujícím obrázkem uvádím svůj záměr popsat postupnou proměnu dat přes informace a znalosti v moudrost a inteligenci.



Obrázek č. 3: Od dat k moudrosti a inteligenci.

5.1.1 Data

„Údaj (***data***): obraz vlastností objektu, vhodně formalizovaný pro přesnost, interpretaci nebo zpracování prostřednictvím lidí nebo automatů.“ Data sama o sobě nejsou ničím jiným než shlukem symbolů vyjadřující vlastnosti, stavy objektů či probíhající procesy ve světě kolem nás. Vyjádřena jsou pomocí znaků s využitím pravidel daného jazyka. Jsou většinou chápána jako statická fakta, časově nezávislá. Odrážejí stav reality v určitém okamžiku, a proto je nelze měnit. Lze pouze získávat nová data o realitě v jiném časovém okamžiku. Smyslem zpracování dat je vytvoření

[44] ***Strategické řízení*** [online]. [cit. 2010-02-05]. Dostupný z WWW: <http://www.bibs.cz/useruploads/files/sbornik_invex_strategicke_rizeni_is_it.pdf>.

informace.[45] Na data lze pohlížet jako na od přírody objektivní reprezentanty lidí, objektů, událostí a pojmů.

5.1.2 Informace

Termín informace je nyní velmi populární. Tímto slovem označujeme cokoliv, co se dovíme, nebo se můžeme dovědět, na první pohled to má něco společného s vědomostmi, znalostmi. Informace si sdělujeme, hledáme, rozhodujeme se podle nich, sledujeme, hodnotíme je, pracujeme s nimi, přenášíme je, ukládáme je, ztrácíme je, můžeme je i záměrně ničit. Definovat informaci je možné z několika úhlů pohledu. Jinou definici najedeme z pohledu filosofie, jinou z pohledu informatiky či ekonomie. Obecný výklad může znít, že „informace" je výsledek vyhodnocování smyslových vjemů, zpracování nebo organizace dat. Pochází z latinského *informatio / informare*, jehož význam je dát tvar, formovat, tvořit. Jinak také význam přisouzený datům. Je to vše, co vyplývá z analýz, zpracování a prezentace dat v takové formě, která bude vhodná pro rozhodovací proces. Pojem informace je subjektivní a existuje jenom ve vztahu k příjemci-uživateli. Není to tady jednoznačný pojem, ale lze se shodnout na tom, že základem pojmu informace je schopnost zvyšovat úroveň poznání lidské společnosti.

5.1.3 Znalosti

Znalost je proměnlivou směsí uspořádaných zkušeností, hodnot, do souvislostí zasazených informací, názorů expertů a podložené intuice, která vytváří prostředí a rámec pro vyhodnocování a začleňování nových zkušeností a informací. Vzniká a je používána v mysli znalostních pracovníků. V organizacích je často zabudována nejen v dokumentech a archivech, ale i v organizačních postupech, procesech, praktikách a normách.[46] Znalost je informace, která byla zorganizována a analyzována tak, aby byla srozumitelná a použitelná pro řešení problémů nebo rozhodování a učení. Znalosti jsou informace chápané ve vzájemných vztazích, souvislostech a kontextu. Vyplývají z analýzy informací na základě komplexní analýzy za použití nabytých zkušeností a již získaných znalostí. Znalosti nám pomáhají vytvářet další znalosti, a tímto procesem se formuje moudrost.

---

[45] PEKAREK, O., ČÍŽEK,. V. *Práce s agenturními a elektronickými informacemi*. 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. s. 48.

[46] *Data, informace, znalosti* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.kip.zcu.cz/kursy/KM/KM2007-8/KM2.ppt>.

5.1.4 Moudrost

Nejvyšším stupněm v popsaném procesu přerodu dat na informace a posléze znalosti je moudrost, tak jak je uvedeno výše na obrázku. Moudrost je schopnost tvorby správných soudů, propojení jednotlivých souvislostí do rozsáhlých celků či pochopení principů. Zahrnuje správu znalostí a jejich efektivní využívání a neustále rozšiřování.

5.1.5 Shrnutí problematiky významu informací

Zde bych rád upozornil, že v dalším textu ne vždy musí být údaje nazývány daty a informace informacemi, někdy mohou být data označovány jako informace. Domnívám, že vzhledem k výše uvedeným vysvětlením, co pod jakým pojmem chápeme a kontextu použití daného termínu není třeba se obávat matení pojmů. Proces rozhodování zahrnuje širokou škálu operací prováděných s daty, informacemi i znalostmi. Mnohdy jsou jednotlivé stupně lidského vědění a chápání výchozím bodem v konstrukci systémů podpory rozhodování. V této souvislosti mám na mysli rozhodovací proces orgánů krizového řízení. Každé rozhodnutí je cesta k vyřešení nějakého existujícího stavu, stavu nejistoty a neuspořádanosti, směrem k nastolení situace, jež bude pro nás příznivá či námi požadovaná. Každý den provádíme řadu rozhodnutí. Mnohdy nad jednotlivými rozhodnutími ani nepřemýšlíme a automaticky uplatňujeme naučené postupy, jindy naopak sbíráme dostupné informace, pátráme, analyzujeme, hodnotíme, abychom se posléze mohli správně rozhodnout. Mnoho rozhodnutí taktéž provedeme podle našich emocí a citů a úplně ignorujeme racionální základnu našeho jednání. Informace jednoznačně hrají v problematice rozhodování klíčovou roli. A to jak pro zmíněné racionální rozhodování, naučené postupy, tak v intuitivních a emocionálních rozhodováních jsou informace zcela nezbytné. Pro každého, kdo má činit jakékoliv rozhodnutí je práce s informacemi naprosto nezbytná záležitost.

5.2 Informační a komunikační technologie využitelné pro IZS

Termín „technologie“ by mohl pocházet řečtiny, kde výraz *techné* původně znamenal schopnost, dovednost nebo znalost řešit určitý problém. Pro účel této práce IKT slouží k výpočtům, zobrazování informací, jejich dalšímu zpracování a přenosu či sdílení mezi uživateli.

Technologie je také při ochraně obyvatelstva a v krizovém řízení pouhým prostředkem k uskutečnění kvalitativních změn. Dala by se myslím rozdělit na tři základní skupiny, ***hardware, software a komunikace***. Představím zde některé, vztahující se nebo mající významný vliv pro podporu rozhodovacích procesů v krizovém řízení.

5.2.1 Internet

Počátkem mnoha úspěšných technologií je jejich výzkum pro vojenské účely. Je tomu tak i u internetu, kdy v šedesátých letech se americká armáda snažila najít způsob, jak zajistit aby armádní počítače rozmístěné po celém území USA mohly spolu komunikovat. Zrodila se tedy síť ARPANET a poměrně brzy byla zpřístupněna i dalším pracovníkům výzkumu a vývoje pracujícím pro ministerstvo obrany USA, a ještě později byla uvolněna i pro čistě civilní výzkum a celou akademickou sféru. Přitom se k zárodečné síti ARPANET postupně připojovaly další akademické a vědeckovýzkumné sítě, až si výsledná soustava vzájemně propojených sítí zasloužila své dnešní jméno Internet.

Internet je dnes celosvětová počítačová síť. Internet je všude kolem nás a zároveň nikde. Nikomu jako celek nepatří. Je to síť velkých počítačů, takzvaných serverů, které jsou navzájem propojeny datovými kabely s vysokou průchodností. Proudí jimi informace (jedničky a nuly) opět velmi vysokou rychlostí a při cestě z jednoho počítače do druhého mohou použít různé cesty. Kromě serverů, které jsou součástí internetu a jsou neustále v provozu, tvoří internet ještě miliony dalších osobních počítačů. Ty se do internetové sítě připojují vždy jen na určitý čas. Internet je právě nyní spojení milionů počítačů pomocí analogových, digitalizovaných, optických aj. kabelů, také pomocí mikrovlnného spojení přes družice a satelity, pozemní vysílače apod. Počítače mezi sebou komunikují pomocí protokolu TCP/IP (Transmission Control Protocol/Internet Protocol) a doplňkových služeb umožňující přidělování fyzických i symbolických adres. Každý počítač v internetu musí mít svou adresu.[47]

5.2.2 Internetové služby

Internet nabízí několik služeb, z nichž některé představím. K jejich používání musí mít uživatel ve svém počítači nainstalován program, který dokáže prostřednictvím

[47] PEKAREK, O., ČÍŽEK,. V. *Práce s agenturními a elektronickými informacemi*. 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. s. 8-10.

internetu komunikovat s počítačem, který nějakou službu poskytuje. Jedná se například o webový prohlížeč, poštovní program apod. Většina operačních systémů tyto programy obsahuje a jiné speciální se musí doinstalovat.

5.2.2.1 World Wide Web - WWW

Je to nejvíce využívaná služba internetu založená na webových stránkách. Webová stránka je hypertextový dokument, který se zobrazuje pomocí webového prohlížeče (klienta) a je možné ho zobrazit na monitoru počítače či mobilního přístroje. Informace jsou prezentovány v podobě textu, multimediálních dat (obrázky, videa, zvuky, …) a hypertextu, jiným slovem odkazů, které umožňují přechod na další webové stránky.

5.2.2.2 Elektronická pošta

„E-mail“ se stává doslova novodobým fenoménem v oblasti mezilidské komunikace. Důvod je spatřován především v tom, že elektronická pošta funguje na off-line principu a tudíž nevyžaduje současnou přítomnost odesilatele i příjemce. Odesilatel může svou zprávu sestavit tehdy, kdy na to má čas, kdy se na to může soustředit, a stejně tak si i příjemce může přečíst došlou zprávu a zareagovat na ni tehdy, kdy se to hodí zase jemu. Tím se tedy individuální diskuse prostřednictvím elektronické pošty principiálně odlišuje například od telefonního hovoru. Největší výhodou přes výše uvedené je rychlost komunikace a možnost si posílat nejen text, ale i multimediální obsah. I když je elektronická pošta svou podstatou prostředkem individuální komunikace, lze ji poměrně jednoduše využít i pro komunikaci skupinovou, např. jednoduchým rozesláním jedné zprávy současně více adresátům.

5.2.2.3 Vyhledávání informací

Vyhledávání informací na internetu by se dalo rozdělit do dvou kategorií:

Katalogové vyhledávání znamená, že jsou webové stránky zařazeny do jednotlivých kategorií a podkategorií podle zaměření (např. sport, kultura, vzdělaní atd.) Do katalogů je nutné stránku zaregistrovat. Registrovaný odkaz fyzicky zkontroluje lidský editor a teprve potom je stránka do katalogu přidána. V katalogu se dá hledat buď listováním v kategoriích, nebo prohledáváním databáze zaregistrovaných stránek. Jako výsledky vyhledávání zobrazuje katalog ručně vkládané a editované popisy stránek. Součástí některých katalogových vyhledávačů občas bývají i fulltextové vyhledávače,

které nastupují v případech, kdy v katalogu není možné nalézt odpověď na žádaný dotaz.

Fulltextové vyhledávání je založeno na vyhledávacích strojích (robotech), které nepřetržitě prochází celým internetem, stránku za stránkou a výsledky své práce (hledání slov stejného významu) ukládají do připravených databází. Tyto databáze jsou uzpůsobeny tak aby mohly uživateli v co nejkratší době a co nejpřesněji „odpovědět" na jeho dotaz. Fulltextové vyhledavače (např. Google) tedy při vyhledávání nemusí procházet celý internet, ale pouze své vlastní databáze, které obsahují slova stejného nebo podobného významu. Tímto je dosahováno rychlosti vyhledání.

5.2.3 Družicové určování zeměpisné polohy

Další technologií, která má nezpochybnitelný význam pro ochranu obyvatelstva a krizové řízení je družicové určování polohy bodů v prostoru (místa požáru, dopravní nehody, zásahových vozidel, mobilního telefonu atd.). Podrobněji zde uvedu dva systémy založené na stejné technologii, jejichž význam bude v nadcházejících letech pro oblast krizového řízení zásadní. Význam bude mít především pro navigaci složek Integrovaného záchranného systému, ale i mnoho dalších. Technologie obou systémů je založená na zákonitostech šíření rádiových vln vysílaných z družic umístěných na oběžné dráze a přijímaných v mnoha druzích přijímačů, které jsou určeny pro různé účely (např. autonavigace). Hlavní výhodou těchto systémů je, že umožňují určovat polohu v jednotném souřadnicovém systému společném pro celou zeměkouli. Tyto systémy běžně pracují nepřetržitě, bez ohledu na počasí a denní nebo roční dobu.

5.2.3.1 Global Positioning System - GPS

Jedná se o vojenský polohový družicový systém provozovaný Ministerstvem obrany Spojených států amerických, s jehož pomocí je možno určit polohu a přesný čas kdekoliv na Zeměkouli nebo nad ní s přesností několika centimetrů. Pro některé civilní účely je tato přesnost záměrně snižována na několik metrů. Systém GPS se skládá ze tří segmentů: kosmického, řídícího a uživatelského. Kosmický segment tvoří soustava 24 družic, rozmístěných systematicky na oběžných drahách ve výšce zhruba 20 200km nad zemským povrchem a vysílajících navigační signály. Řídící segment je zodpovědný za řízení a kontrolu funkčnosti všech prvků systému. Tvoří ho jedna hlavní řídící stanice, pět pozemních monitorovacích stanic a tři komunikační stanice, všechny umístěné na amerických vojenských základnách. Uživatelský segment se skládá z GPS

přijímačů, které provádějí na základě přijatého signálu z družic výpočet polohy, rychlosti a času. Pro výpočet všech čtyř souřadnic (**x, y, z** a **t**) je potřeba přijímat signál alespoň ze čtyř družic. Vypočtené souřadnice jsou potom přijímačem využity k účelu, pro který byl vyroben.

5.2.3.2 Galileo

Je nezávislý, globální, evropský, satelitní navigační systém, který bude plně vyvinut a provozován Evropskou unií a jeho uvedení do provozu bylo plánováno na rok 2010, ale podle posledních informací bude posunuto na rok 2014. Bude využívat stejného principu jako nynější americký systém GPS a ruský GLONASS, se kterými se bude vzájemně doplňovat. Oba současné systémy jsou vojenské a ani jeden z provozovatelů nedává záruku, že v případě potřeby signály ze svých družic nevypne. Galileo je prvním společným projektem Evropské unie reprezentované Evropskou komisí a Evropskou kosmickou agenturou a bude zajišťovat uživatelům mnoho garantovaných služeb. Tyto služby budou poskytovány celosvětově a nezávisle na ostatních systémech, a to využíváním pouze Galileo signálů z družic.

Základní služba vychází z kombinace základních signálů, je poskytována zdarma a poskytuje určení polohy a času srovnatelné kvality s ostatními systémy.

Služba "kritická" z hlediska bezpečnosti je vylepšenou verzí Základní služby. Poskytuje aktuální varování uživateli, pokud jsou překročeny určité limity přesnosti polohy.

Komerční služba poskytuje přístup k dalším dvěma signálům, které zvyšují množství přenesených dat a zvyšují přesnost určení polohy. Zmíněné signály budou kódovány.

Veřejně regulovaná služba bude zajišťovat určení polohy a času s kontrolovanou licencí "vyvoleným" uživatelům vyžadující vysokou kontinuitu (spojitost) služby. Přístup k této službě bude kontrolován (zákazníky budou např. policie nebo armáda). V rámci této služby budou poskytovány dva navigační signály se zašifrovanými kódy (měřícími vzdálenost) a daty.

Vyhledávací a záchranná služba. Galileo družice budou také důležitou součástí tzv. MEOSAR systému (**M**edium **E**arth **O**rbit **S**earch **a**nd **R**escue systém), což je vyhledávací záchranný systém využívající navigační družice také jiných systémů. Družice budou schopny přijímat nouzové signály z lodí, letadel nebo dokonce od osob a okamžitě je posílat do národních záchranných center. Záchranná centra tak získají

přesné určení polohy místa nehody. Alespoň jedna družice Galileo bude viditelná z jakéhokoli bodu na Zemi, takže nouzový poplach bude vyhlášen téměř v reálném čase. V některých případech může být vysílači odeslána zpětná zpráva tato funkcionalita bude zajišťována pouze družicemi Galileo).[48]

5.2.4 Telekomunikace

Jsou pryč časy kouřových signálů a dnes tu máme mobilní telefony, o jejichž významu také pro krizové řízení, záchranu životů a majetku není třeba pochybovat. Pro uvědomění si zákonitostí dalšího vývoje a směřování v této oblasti zde uvedu skutečnosti významné pro výměnu, přenos, sdílení dat a informací tedy komunikaci.

Princip telekomunikace z našeho pohledu spočívá v přenosu informace, kterou přeměníme na ***elektromagnetický signál*** z bodu „A“ do bodu „B“ za využití nejrůznějších vysílačů, přijímačů a přenosových cest neboli sítí. Vývoj komunikačních technologií jde vpřed mílovými kroky a určujícími aspekty jsou především ***rychlost a bezpečnost „přepravy“ informací***. Proto jsou vyvíjeny stále nové technologie, aby stačily rychlému celosvětovému ekonomickému vývoji, nebo spíše naopak, jsou jeho katalyzátorem. V dnešní době se informace přeměněné na elektromagnetické vlny přenášejí pomocí ***metalického vedení***, které je však již dnes na ústupu. Značných přenosových rychlostí je dosahováno v ***optických sítích*** a značného rozvoje doznaly ***radiové sítě*** především proto, že radiový signál je dostupný kdekoliv a není potřeba dnes velmi drahých stavebních prací.

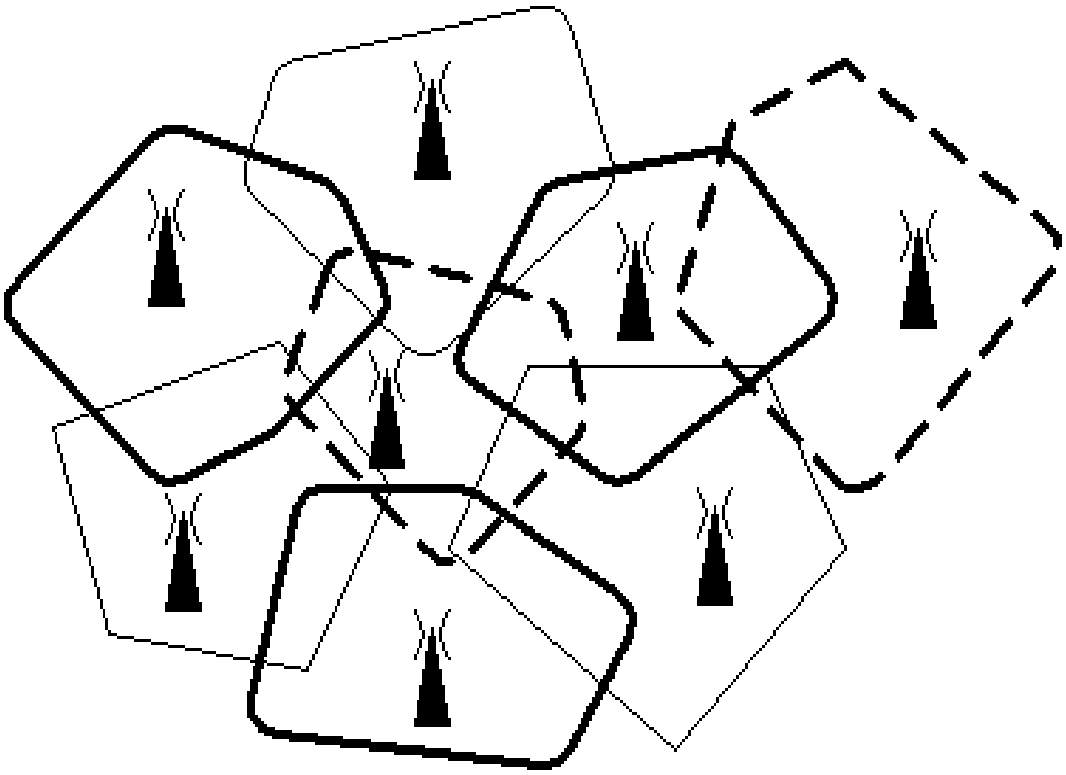
Ve své práci bych rád představil radiovou technologii s pod označením GSM, kterou také používají naši nejvýznamnější mobilní operátoři (Vodafone, T-mobile a O2). Svými možnostmi využití je pro oblast ochrany obyvatelstva a krizového řízení v dnešní době již nepostradatelná. Jedná se zejména o hlasovou komunikaci, např. mezi velitelem zásahu a operačním střediskem nebo určení zeměpisné polohy mobilního telefonu volajícího v tísni, využití pro systémy varování a vyrozumění, sběr dat z meteorologických stanic apod.

5.2.4.1 Komunikační systém GSM

Základním principem mobilní komunikace je pokrytí území radiovými vlnami, pomocí kterých mezi sebou mobilní telefony komunikují. Území je rozdělené do

[48] Galileo [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.czechspace.cz/cs/galileo>.

systému buněk. Každou z nich svým signálem pokrývá základnová stanice tzv. BTS (Base Ttransciever Station). Schéma je znázorněno na obrázku níže.



Obrázek č. 4: Pokrytí území radiovým signálem.

Jejím úkolem je komunikovat s mobilními telefony, které se nachází v jejím dosahu. Pokud se mobilní telefon pohybuje a přemístí z jedné buňky do druhé, dojde k tzv. handover-u (předání) a aktualizaci záznamu v databázi, kde se daný mobilní telefon nachází. Jednotlivé základnové stanice jsou mezi sebou propojeny a řízeny nadřízenými stanicemi. Celá soustava všech základnových stanic je napojena na centrální ústřednu, která zabezpečuje směrování hovorů k jednotlivým příjemcům s využitím již zmíněné databáze, která obsahuje záznamy o tom kde se mobilní telefon nachází.

Významnou funkcionalitou pro krizové řízení je především možnost určení zeměpisné polohy mobilního telefonu ze kterého je voláno na linku tísňového volání 112. K lokalizaci mobilního telefonu se používá několika metod. Všechny vycházejí z informací, které lze získat z komunikace mobilu se základnovými stanicemi (BTS). Nejpřesnější metodou je ***lokalizace triangulací*** z více BTS. V principu jde o nalezení průsečíku oblouků kružnic, které určují místo, kam svým signálem zasahují tři nejsilnější základny v okolí hledaného telefonu, jak je uvedeno na obrázku č. 4. Metoda je poměrně přesná a v závislosti na konkrétním řešení může dosahovat přesnosti

na stovky metrů. Ve městech, kde je síť základnových stanic nejhustší, může být mobilní telefon lokalizován s přesností několika metrů.[49]

Obrázek č. 5: Určení polohy mobilního telefonu v síti GSM.[50]

5.3 Informační a komunikační projekty IZS

5.3.1 Komunikace v síti PEGAS

Systém PEGAS je celostátní radiokomunikační systém výhradně určený pro složky Integrovaného záchranného systému. Je to buňková, digitální síť založená na technologii standardu TETRAPOL, umožňující využití hlasových a datových služeb. Je částečně obdobou mobilních sítí GSM s řadou speciálních vlastností umožňujících například:

- utajený digitální přenos hlasu vysoké kvality,
- přímou komunikaci mezi dvěma účastníky bez účasti sítě,
- hromadnou, skupinovou, konferenční a individuální komunikaci v síti,
- volání mimo síť propojením do veřejných i neveřejných sítí,
- tísňové volání s nejvyšší prioritou,

[49] *Jak určit polohu mobilního telefonu* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.mobilmania.cz/default.aspx?article=1107567>.
[50] *Lokalizace volajícího při tísňovém volání z mobilního telefonu* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.zachrannasluzba.cz/odborna/0306_lokmt.htm>.

- utajený přenos dat, dotazování do databází,
- krátké datové zprávy,
- větší dosah a odolnost proti rušení apod.

Pokrytí území rádiovým signálem je optimalizováno s ohledem na potřeby IZS a na finanční náklady realizace celoplošné ***Národní radiokomunikační sítě***. Národní síť tvoří vzájemně propojené ***regionální sítě***. Regionální síť tvoří prvky infrastruktury, kterými jsou ***hlavní rádiová ústředna***, několik ***podřízených rádiových ústředen, základnové radiostanice*** v počtu dle požadavků rádiového pokrytí a provozu a ***řízení sítě*** sestávající z ***pracoviště technického dohledu*** a ***pracoviště taktického řízení.*** Tato pracoviště jsou určena k řízení veškerých služeb, účastníků a skupin uživatelů.

Komunikace v systému je zabezpečena šifrováním "konec - konec", které zabezpečuje ***středisko klíčového hospodářství,*** které slouží k vytváření a distribuci šifrovacích klíčů využívaných všemi regionálními sítěmi systému.

Společná infrastruktura radiokomunikačního systému PEGAS a systémové vlastnosti standardu TETRAPOL zabezpečují pro každou složku IZS vlastní komunikační prostředí na zájmovém teritoriu (okres, region, jiné) a pro vzájemnou komunikaci mezi složkami pro případy spolupráce složek i komunikační prostředí společné.

V případě potřeby je možné základní nastavení komunikačního prostředí dynamicky měnit a přizpůsobovat ho aktuální situaci. Komunikační prostředí je pro každou složku IZS autonomní a záleží na jejím rozhodnutí o případném povolení vstupu jiným uživatelům do něj. Provoz v tomto prostředí si řídí každá složka samostatně (dispečink, operační středisko, jiná řídicí stanice apod.).[51]

5.3.2 Telefonní centrum tísňového volání - TCTV 112

V roce 1991 Rada Evropských společenství vydala rozhodnutí č. 91/396/EEC ze dne 29. července 1991 o zavedení jednotného evropského čísla tísňového volání pro všechny členské státy. Stalo se tak především z důvodu usnadnění komunikace s tísňovými službami v rámci Evropské unie. Pro přístup k tísňovému volání bylo stanoveno telefonní číslo **112.** V České republice byl vybudován, a v roce 2005 předán do provozu, v Evropě dosud nejmodernější systém pro odbavování tísňových volání. Základní funkcionality zde uvádím.

[51] *Radiokomunikační systém PEGAS* [online]. [cit. 2010-03-10]. Dostupný z WWW: <http://www.pramacom.cz/cz/projekt-detail.php?projectId=4>.

Technologie TCTV 112 propojuje základní složky Integrovaného záchranného systému: Hasičský záchranný sbor České republiky, Policii České republiky a Zdravotnickou záchrannou službu. To umožňuje rychlé vyhodnocení vzniklé situace a okamžitou reakci záchranných složek.

V rámci projektu bylo vybudováno 14 Telefonických center tísňového volání v operačních střediscích jednotlivých Krajských ředitelství Hasičského záchranného sboru ČR a zajištěna jejich hlasová i datová konektivita do sítí navazujících systémů a složek. Komunikační platformu tvoří tři pobočkové ústředny, které jsou umístěny v Praze, Plzni a Olomouci a na které je napojeno 11 vzdálených bloků (tzv. remote TCTV) těchto ústředen ve zbývajících krajích ČR. V současnosti je celková kapacita systému dimenzovaná pro více jak 100 operátorů tísňové linky pracujících na hlavních a záložních pracovištích. Tato pracoviště jsou vybavena digitálními telefony s náhlavními soupravami a dalšími komunikačními a IT prostředky.

Všichni operátoři využívají jednotný informační systém, který umožňuje zobrazovat informace o stavu aktuálně řešených událostí a profilech aktivních operátorů přihlášených do systému. To umožňuje, společně se systémem lokalizace a GIS podpory, rychlé odbavení události kterýmkoliv operátorem z jakéhokoliv místa ČR a předání do působnosti místně příslušné výkonné složky IZS. Pro primární předávání zpracovaných informací operátorem TCTV 112 byla v rámci projektu kodifikována datová věta obsahující veškeré informace získané v systému. Veškerý hlasový provoz v systému je nahráván a umožňuje on-line přístup k nahrávkám jak operátorům TCTV 112 tak i operačním střediskům složek IZS pro případ zpětného vyhodnocení určité krizové situace nebo upřesnění informací o události. Hovory jsou archivovány a na každém krajském pracovišti je možné je s pomocí speciálního softwaru vyhledat, případně exportovat pro další využití, např. složkami činnými v trestním řízení.

Naprosto unikátní funkcionalitou TCTV 112 je automatická lokalizace volajících, kdy se operátorům TCTV 112 současně příjmem tísňového volání zobrazí na monitoru počítače v GIS aplikaci místo, kde se volající nachází. Tato funkcionalita zajišťuje bezproblémové odbavení tísňového volání v kterémkoliv místě České republiky, ať již pochází z mobilní nebo fixní telefonní sítě.[52]

[52] *Tísňová volání v České republice* [online]. [cit. 2010-03-05]. Dostupný z WWW: <http://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice.aspx?q=Y2hudW09MQ%3d%3d>.

5.3.3 Jednotný systém varování a vyrozumění - JSVV

Varování, tísňové informování obyvatelstva a vyrozumění je nedílnou součástí všech opatření na ochranu obyvatelstva. Základní a společnou podstatou varování, tísňového informování a vyrozumění jsou informace. Celý systém je tedy možno chápat jako vznik, tok a zpracování informací. Jestliže reálně hrozí, nebo již nastala mimořádná událost, musí o tom vzniknout informace, která se od místa vzniku události šíří k řídícím orgánům složek IZS, orgánům územní samosprávy, státní správy a dalším orgánům a organizacím, podílejícím se na řešení situace a mezi nimi navzájem. Takto předávané informace se nazývají vyrozumění. Příslušný orgán informaci přijme, zpracuje a vyhodnotí. Pokud rozhodne, že situace vyžaduje realizaci opatření na ochranu obyvatelstva, informaci přepracuje do vhodné formy a předá ji obyvatelstvu. Takto zpracované a předávané informace se nazývají varování, případně varování a tísňové informování.

Jednotný systém varování a vyrozumění je technicky, provozně a organizačně zabezpečen vyrozumívacími centry, telekomunikačními sítěmi a koncovými prvky varování a vyrozumění. Základní technologickou infrastrukturu tvoří Systém selektivního radiového návěštění (SSRN). Umožňuje varování a tísňové informování obyvatelstva dálkovým ovládáním koncových prvků varování a vyrozumění předáváním zpráv na osobní přijímače (pagery). SSRN využívá digitálních technologií, což umožňuje efektivní činnost všech částí systému, pružné změny konfigurace systému a jeho částí úpravami řídících programů a řídících komponentů podle skutečné potřeby uživatelů systému. Zároveň to přináší možnost průběžné modernizace systému a zařazování nových částí a prvků.[53]

Pro šíření varovných signálů a tísňového informování se vychází ze zásady, že varování je věc veřejná a že každý občan má právo být varován. Z tohoto pohledu je možno využít, s ohledem na charakter mimořádné situace, její rozsah a časový průběh i na aktuální dostupnost prostředků a kanálů:

- Koncových prvků varování jednotného systému varování a vyrozumění.
- Místních informačních systémů.
- Mobilních rozhlašovacích prostředků.
- Osobního vyhlášení.
- Rozhlasu a televize.

[53] *Vyhláška č. 380/2002 Sb. k přípravě a provádění úkolů ochrany obyvatelstva* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.hzscr.cz/soubor/vy-380-2002-pdf.aspx>.

- Mobilních telefonů, internetu a dalších technologií.

Pro vyrozumění lze využít širokého spektra komunikačních prostředků:

- Telefonního spojení v pevné i mobilních sítích (včetně jejich služeb - SMS, fax…).
- Rádiového spojení v sítích složek IZS a dalších zúčastněných organizací.
- Osobních svolávacích přijímačů (pagerů) používaných v JSVV.
- Sirén a MIS pro svolání jednotek požární ochrany sboru dobrovolných hasičů.
- Elektronické pošty, datových přenosů a dalších komunikačních systémů a prostředků.
- V případě rozrušení komunikačních systémů je možno použít i spojek.

5.3.4 Krizová telefonní čísla

V krizovém řízení se vyskytoval problém v podobě důvěryhodné integrální komunikace mezi účastníky při řešení krizových operací. Z tohoto důvodu byl v České republice realizován projekt ***„krizových mobilních telefonů“***, provozovaný do 30. června 2008.

Od 1.7 2008 je komunikace zajištěna na základě smlouvy se společností Telefónica O2 Česká republika, a.s., jejímž předmětem je ***zabezpečení přednostního spojení*** pro krizová telefonní čísla účastníků krizové komunikace a další plnění související se zabezpečením fungování krizových telefonních čísel při mimořádných událostech, krizových stavech a při přípravě na mimořádné události a krizové stavy, kdy může docházet k přetížení telefonní sítě. Účastníky krizové komunikace jsou složky integrovaného záchranného systému, ministerstva, jiné ústřední správní úřady, správní úřady s krajskou působností nebo působností ve správních obvodech obcí s rozšířenou působností, orgány krajů, orgány obcí a další orgány či právnické osoby, které určí GŘ HZS. Také požadavky na zabezpečení přednostního spojení podléhají schválení a lze je nastavit u libovolných telefonních čísel s O2 paušálním tarifem. Telefonním číslům s přednostním spojením je nastavována priorita (v hodnotách 1+, 1, 2 a 0) upřednostnění volání. Získání hodnoty je závislé na tom, do jaké skupiny je účastník krizové komunikace zařazen a v jakém stavu se nachází síť operátora. Účastníky krizové komunikace dělíme do tří skupin (VIP, Velký starosta, Malý starosta). Stav sítě dělíme na stav „Krize“ a „Bez krize“. Do stavu „Krize“ přechází síť mobilního operátora na základě žádosti GŘ HZS a znamená to navýšení priorit pro účastníky krizové komunikace.

Smlouva také za krizového stavu a na základě požadavku zajišťuje nasazení ***mobilních základnových stanic***, které jsou určeny pro pokrytí zájmové lokality signálem operátora.[54]

5.3.5 Informační systém ARGIS

Informační systém pro plánování civilních zdrojů ARGIS je vytvářen, rozvíjen a provozován v gesci Správy státních hmotných rezerv (SSHR) k zabezpečení informační podpory plánovacích a rozhodovacích procesů orgánů krizového řízení od úrovně určených obcí, přes orgány krajů až po ústřední správní úřady včetně SSHR v oblasti zajišťování věcných zdrojů pro řešení krizových situací v souladu se zákonem č.241/2000 Sb. o hospodářských opatřeních pro krizové stavy.

Do systému mohou vstupovat rovněž vybrané právnické a podnikající fyzické osoby, které poskytují požadované údaje včetně informací o svých schopnostech dodat předmět nezbytné dodávky.

Je realizován jako centrální systém s modulární strukturou, kde nad společnou servisní částí (správa číselníků a registrů, nástroje pro práci s mapovými podklady, komunikační subsystém se správou účtů a práv) jsou vytvářeny moduly jednotlivých aplikací.

Centrální systém umožňuje řízený sběr dat a následně práci s nimi podle územní nebo resortní příslušnosti. S využitím stejné technologie zpracování je realizován i systém formulářového sběru dat od právnických a podnikajících fyzických osob. Výsledkem je jednak naplnění požadavku jednotného principu pořizování dat a současně vyloučení jejich duplicity.

Uživatelé systém využívají pomocí dálkového přístupu prostřednictvím bezpečné komunikace v prostředí Internetu s rozdílnými přístupovými právy a zabezpečením. Práva uživatelů jsou odvozena od působnosti správního úřadu a přidělené role konkrétního uživatele.[55]

Informační systém ARGIS byl atestován v roce 2005 a tím byla splněna zákonná podmínka pro jeho provozování jako informačního systému veřejné správy.

---

[54] *Zabezpečení krizové komunikace* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.cz.o2.com/izs/cz/site/home/index.html>.

[55] *Informační systém ARGIS* [online]. [cit. 2009-12-18]. Dostupný z WWW: <http://www.argis.cz/>.

5.3.6 Informační systém integrovaného záchranného systému (IS IZS) - projekt

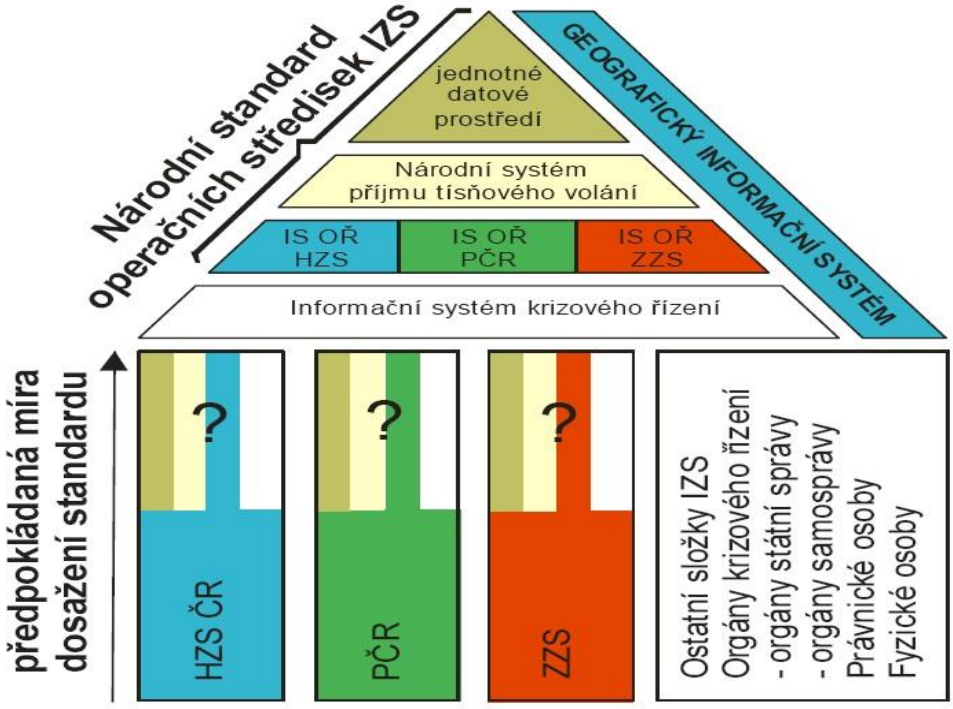
Projekt se nachází v přípravné fázi a je zaměřen na vybudování jednotné systémové a technologické platformy pro příjem tísňového volání na všech tísňových číslech a efektivní výměnu dat operačního řízení jednotlivých základních složek IZS. Projekt zajistí propojení technologií, které jsou dosud společně využívány všemi základními složkami IZS na úseku operačního řízení a tísňového volání.

Hlavními přínosy informačního systému bude snížení následků mimořádných událostí v případě společných akcí složek IZS díky rychlejším a provázanějším zásahům, které umožní plně dostupné tísňové volání, přesnější určení místa mimořádné události v mapovém podsystému a rychlejší přeprava na místo události díky využití navigačních systémů vozidel IZS přímo spojených s mapovou technologií.

Současný projekt IS IZS, dá se říci, nahrazuje před rokem ukončený projekt budování Informačního systému krizového řízení, který byl zastaven, a budou využity pouze některé jeho segmenty.

Následující obrázek vystihuje ideové řešení projektu IS IZS. Základní myšlenkou je provázanost celkového řešení a základní struktura založená na:

- Národním systému příjmu tísňového volání.
- Jednotném datovém prostředí.
- Jednotném geografickém informačním systému.



Obrázek č. 6: Projektové schéma IS IZS.[56]

V rámci projektu IS IZS bude tedy základním složkám IZS prostřednictvím střechového projektu NIS IZS dodána technologie pro příjem tísňového volání tzv. Národní systém příjmu tísňového volání, technologie jednotného geografického systému (GIS), technologie vizualizace operační situace a výměny dat (Integrační platforma). Informační systém IZS je vyvíjen pro operační střediska Policie ČR, Hasičského záchranného sboru ČR a Zdravotnickou záchrannou službu krajů, která jsou určena pro komunikaci s občanem v tísni a pro rychlé nasazení sil a prostředků. Projektem bude také nastaven a budován dosud nejednotný koncept operačních středisek základních složek IZS. Nasazením nejmodernějších informačních a komunikačních technologií bude zajištěna vyšší úroveň koordinace operačních středisek a bude dosaženo jednotné úrovně informačních systémů operačního řízení.

[56] *Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému* [online]. [cit. 2010-04-10]. Dostupný z WWW: <http://www.hzscr.cz/soubor/prezentace-projekt-isizs-pdf.aspx>.

6 ZÁVĚR

Závěrem své práce konstatuji, že činnosti spojené s ochranou obyvatelstva, havarijním plánováním, jakož i s řešením mimořádných a krizových situací si nelze představit bez využití informačních a komunikačních technologií a na jejich základě budovaných informačních a komunikačních systémů. O jaké systémy by se mělo jednat, resp. jaké požadavky by na ně měly být kladeny, je předmětem diskuse odborníků v bezpečnostní komunitě již několik let. Věřím, že se mi podařilo zmapovat současnou situaci v této části společenské praxe a nastínit směry jejího dalšího vývoje. Jedním z cílů mého úsilí bylo rovněž odpovědět na otázku, na jaké kvalitativní úrovni je oblast ochrany obyvatelstva a krizového řízení v bezpečnostním systému České republiky. Ukázalo se, že také díky zkušenostem z minulého období, především dob „studené války“, je náš systém ochrany obyvatelstva, dříve civilní obrany, na velmi vysoké úrovni. Důkazem kvalitní práce krizového managementu, právě v zavádění moderního způsobu řízení v oblasti organizační i technologické je uznání, kterého se dostalo České republice díky projektu SIPROCI – „Mezinárodní odezva na přírodní a člověkem způsobené katastrofy“, jenž byl realizován již v letech 2004-2007. Systém krizového řízení v České republice byl zástupci z několika evropských států vyhodnocen jako nejlepší operační příklad pro účelné užití IKT v civilní ochraně.[57]

Doufám, že také forma zpracování mé práce umocnila apel na potřebu vzdělávání pracovníků veřejné správy a to nejen v oblasti krizového řízení. Zvyšování kvalifikace profesionálů zachraňujících životy a značné majetkové hodnoty vyžaduje systémová řešení jejich přípravy. Myslím, že i tímto směrem by se mohlo do budoucna orientovat vzdělávání na Vysoké škole evropských a regionálních studií.

Je nutné si uvědomit, s jakou rychlostí dochází k rozvoji informačních a komunikačních technologií. Je proto nezbytné koncipovat informační systémy krizového řízení jako otevřené a přístupné změnám, které zmíněný vývoj přináší. Každý informační systém vyžaduje kvalitní databázi, která obsahuje pravdivé údaje, má svého správce zajišťujícího její aktualizaci a umožňuje své sdílení různými informačními systémy vylučující zneužití dat nepovolanými osobami.[58]

V práci se zabývám řadou technologií využitelných v oblasti ochrany obyvatelstva a krizového řízení. Tento závěr si však zaslouží vyzdvižení několika

[57] *Projekt SIPROCI a jeho výsledky* [online]. [cit. 2010-02-15]. Dostupný z WWW: <http://www.kraj-jihocesky.cz/file.php?par%5Bid_r%5D=24491&par%5Bview%5D=0>.

[58] *Zákon č. 101/2000 Sb. o ochraně osobních údajů* [online]. [cit. 2010-02-19]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>

technologií a systémů, o kterých jsem přesvědčen, že také do budoucna budou ovlivňovat i organizační oblast krizového řízení. Komunikace představuje nejdůležitější součást krizového řízení a v našich podmínkách je to komunikace především pomocí mobilních telefonů, která se pro svou všeobecnou rozšířenost a řadu doplňkových služeb systému GSM již mnohokrát osvědčila. Další dnes již nepostradatelnou technologií je určování zeměpisné polohy bodů v prostoru tzv. GPS. Díky ní mají krizové orgány při operačním řízení přehled o nasazených silách a prostředcích. Navíc ve spojení s mobilní komunikační technologií jsou tyto informace zobrazovány online na monitorech operačních a informačních středisek nebo kapesních komunikátorech velitelů zásahů přímo na místě mimořádné události. Pro lidské vnímání je nejsrozumitelnější prezentace těchto prostorových dat zobrazením v geografických informačních systémech. Pro tyto systémy bude mít zásadní význam projekt, kterým je budování digitální mapy veřejné správy. Dosud totiž neexistuje ucelené mapové dílo celé České republiky. Bude tak také, jak doufám, odstraněno i dosavadní plýtvání veřejnými prostředky, protože podle mých zjištění snad každý větší orgán veřejné správy dosud budoval pro své potřeby GIS tak zvaně na vlastní pěst.

Věřím, že se mi v bakalářské práci podařilo dosáhnout cílů, které jsem si vytyčil. Problematice, které jsem se v ní věnoval, bych rád zasvětil následující studium. V budoucnosti bych zejména rád analyzoval možnosti využití informačních systémů a služeb, které provozuje, a ke komerčním účelům poskytuje, internetová společnost Google. Již dnes jsem přesvědčen, o širokých možnostech jejich využití ve veřejné správě a s tím spojených značných úsporách veřejných prostředků.

SEZNAM ZKRATEK

AIFO	Agendový identifikátor fyzických osob
BTS	Base Ttransciever Station
CMS	Centrální místo služeb
ČR	Česká republika
ČÚZK	Český úřad zeměměřický a katastrální
DMVS	Digitální mapa veřejné správy
DP	Datový prvek
eGON	Symbol eGovernmentu
ePUSA	Elektronický portál územních samospráv
ES	Evropské společenství
EU	Evropská unie
GIS	Geografický informační systém
GPS	Global Positioning System
GŘ	Generální ředitelství
GSM	Globální Systém pro Mobilní komunikaci
HOPSK	Hospodářská opatření pro krizové stavy
HZS	Hasičský záchranný sbor
IKT	Informační a komunikační technologie
IP	Internet Protocol
IS	Informační systém
IS DP	Informační systém o datových prvcích
IS IZS	Informační systém integrovaného záchranného systému
ISKŘ	Informační systém krizového řízení
ISSS	Internet ve státní správě a samosprávě
ISVS	Informační systémy veřejné správy
ISZR	Informační systém základních registrů
IZS	Integrovaný záchranný systém
JSVV	Jednotný systém varování a vyrozumění
KIVS	Komunikační infrastruktura veřejné správy
KŘ	Krizové řízení
MEOSAR	Medium Earth Orbit Search and Rescue systém
MIS	Místní informační systém
MS	Microsoft

MS SQL	Relační databázový systém
MV	Ministerstvo vnitra
NIS IZS	Národní informační systém integrovaného záchranného systému
O2	Telefónica O2 Česká republika, a.s.
OECD	Organizace pro hospodářskou spolupráci a rozvoj
ORG	Identifikátor fyzických osob
PDF	Datový formát (Portable Document Format)
POINT	Podací Ověřovací Informační Národní Terminál
ROB	Registr obyvatel
ROS	Registr osob
RPP	Registr práv a povinností
RUIAN	Registr územní identifikace, adres a nemovitostí
SMS	Short message service
SSHR	Správa státních hmotných rezerv
SSRN	Systém selektivního radiového návěštění
TCP	Transmission Control Protocol
TCTV	Telefonní centrum tísňového volání
VIP	Very important person
WWW	World Wide Web
XML	Datový formát (eXtensible Markup Language)

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÉ LITERATURY

Literární zdroje

1. DANICS, Š. *Bezpečnostní politika ve veřejné správě.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. 99 s. ISBN 978-80-86708-38-6.
2. HORÁK, R., KRČ, M., ONDRUŠ, R. *Průvodce krizovým řízením pro veřejnou správu.* 3. Vydání Praha : Linde, 2004. 408s. ISBN 80-7201-471-4.
3. MARTÍNEK, B., LINHART, P. *Ochrana obyvatelstva.* 1. Vydání Praha : MV-GŘ HZS ČR, 2006, 128 s.
4. PEKAREK, O., ČÍŽEK,. V. *Práce s agenturními a elektronickými informacemi.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2007. 140 s. ISBN 978-80-86708-40-9.
5. PROCHÁZKOVÁ, D. *Bezpečnostní plánování.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2009. 200s. ISBN 978-80-86708-80-5.
6. PROCHÁZKOVÁ, D. *Krizové řízení, havarijní plánování a ochrana obyvatelstva.* 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2009. 111s. ISBN 978-80-86708-86-7.
7. PROCHÁZKOVÁ, D. *Monitoring zdrojů ohrožení v území*. 1. Vydání Č. Budějovice : Vysoká škola evropských a regionálních studií, 2009. 108s. ISBN 978-80-86708-87-4.
8. RAPANT, P. *Družicové polohové systémy.* 1. Vydání Ostrava : VŠB Technická univerzita, 2002. 200 s. ISBN 80-248-0124-8.
9. RAPANT, P. *Geoinformatika a geoinformační technoligie.* 1. Vydání Ostrava : VŠB Technická univerzita, 2006. 513 s. ISBN 80-248-1264-9.
10. *Sborník konference* : *Současnost a budoucnost krizového řízení 2006*. Praha : T-soft, 2007. 48 přednášek. ISBN 80-239-7296-2.
11. *Sborník konference* : *Současnost a budoucnost krizového řízení 2007*. Praha : T-soft, 2009. 47 přednášek. ISBN 978-80-254-0726-4.
12. *Sborník konference* : *Současnost a budoucnost krizového řízení 2009*. Praha : T-soft, 2010. 27 přednášek. ISBN 987-80-254-5912-6.
13. VALÁŠEK, J., KOVAŘÍK, F. *Krizové řízení při nevojenských krizových situacích.* 1. Vydání Praha : MV-GŘ HZS ČR, 2008, 104 s. ISBN 978-80-86640-93-8.

Elektronické zdroje

1. *Bezpečnost* [online]. 2010 [cit. 2010-01-25]. Dostupný z WWW: <http://www.mvcr.cz/clanek/bezpecnost.aspx>.
2. *Bezpečnostní výzkum pro potřeby státu v letech 2010 až 2015* [online]. 2008 [cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/3-bezpecnostni-vyzkum-pro-potreby-statu-v-letech-2010-az-2015.aspx>.
3. *Bezpečnostní strategie České republiky* [online]. 16.12.003 [cit. 2010-02-25]. Dostupný z WWW: <http://www.mzv.cz/public/7/46/a7/14340_14945_Bezp._strategie.doc>.
4. *Cíle strategie Efektivní veřejná správa a přátelské veřejné služby* [online]. 2010 [cit. 2010-03-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/cile-strategie-efektivni-verejna-sprava-a-pratelske-verejne>.
5. *Co je Czech POINT* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.czechpoint.cz/web/?q=node/22>.
6. *Data, informace, znalosti* [online]. 02.10.2001 [cit. 2010-02-15]. Dostupný z WWW: <http://www.kip.zcu.cz/kursy/KM/KM2007-8/KM2.ppt>.
7. *Datové schránky* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.datoveschranky.info/o-datovych-schrankach-text/>.
8. *Digitální mapa veřejné správy* [online]. 12.11.2009 [cit. 2010-04-19]. Dostupný z WWW: <http://www.mvcr.cz/soubor/dmvs-informace.aspx>.
9. *Efektivní veřejná správa* a přátelské veřejné služby [online]. 21.01.2008 [cit. 2010-03-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/modernizace-dokumenty-strategie-pdf.aspx>.
10. *Elektronický portál územních samospráv* [online]. 28.02.2008 [cit. 2010-02-15]. Dostupný z WWW: <http://www.egovernment.cz/archiv/PDF%201-08/5.pdf>.
11. *Galileo* [online]. 20.04.2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.czechspace.cz/cs/galileo>.
12. *Informační systém ARGIS* [online]. 2010 [cit. 2009-12-18]. Dostupný z WWW: <http://www.argis.cz/>.
13. *Informační systém o datových prvcích* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.asd-software.cz/index.php?ID=137>.
14. *Informační systém o informačních systémech veřejné správy* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.asd-software.cz/clanek-142-is-o-isvs.html>.
15. *Informační systém základních registrů* [online]. 12.04.2010 [cit. 2010-04-15]. Dostupný z WWW: <http://www.szrcr.cz/file/12>.
16. *Jak postupovat při plnění povinností vyplývajících ze zákona č. 365/2000 Sb.* [online]. 09.09.2009 [cit. 2010-02-25]. Dostupný z WWW: <http://www.mvcr.cz/soubor/metodicke-pokyny-jak-postupovat-pri-plneni-povinnosti-vyplyvajicich-ze-zakona-c-365-2000-sb.aspx>.
17. SNAŠEL, J. *Jak určit polohu mobilního telefonu* [online]. 26.02.2004 [cit. 2010-02-15]. Dostupný z WWW: <http://www.mobilmania.cz/default.aspx?article=1107567>.

18. *Jednotná úroveň informačních systémů operačního řízení a modernizace technologií pro příjem tísňového volání základních složek integrovaného záchranného systému* [online]. 22.03.2010 [cit. 2010-04-10]. Dostupný z WWW: <http://www.hzscr.cz/soubor/prezentace-projekt-isizs-pdf.aspx>.
19. *Koncepce budování informačních systémů veřejné správy* [online]. 29.06.2007 [cit. 2010-02-15]. Dostupný z WWW: <http://www.isvs.cz/user_data/dokumenty/UVIS-Koncepce-ISVS-1999.pdf>.
20. *Koncepce ochrany obyvatelstva do roku 2013 s výhledem do roku 2020* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.hzscr.cz/clanek/koncepce-ochrany-obyvatelstva-do-roku-2013-s-vyhledem-do-roku-2020-503181.aspx>.
21. *Koncepce vzdělávání v oblasti krizového řízení* [online]. 22.12.2009 [cit. 2010-02-11]. Dostupný z WWW: <http://www.hzscr.cz/soubor/koncepce-vzdelavani-v-obl-kr-pdf.aspx>.
22. *Lokalizace volajícího při tísňovém volání z mobilního telefonu* [online]. 22.07.2003 [cit. 2010-02-15]. Dostupný z WWW: <http://www.zachrannasluzba.cz/odborna/0306_lokmt.htm>.
23. *Metodický pokyn pro popis datových prvků* [online]. 10.09.2009 [cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/metodicky-pokyn-pro-popis-datovych-prvku.aspx>.
24. *Nová Bezpečnostní strategie České republiky : politicko-společenská revue* [online]. Brno : RevuePolitika, 20.02.2004 [cit. 2010-02-15]. Dostupný z WWW: <http://www.revuepolitika.cz/clanky/642/nova-bezpecnostni-strategie-ceske-republiky>. ISSN 1803-8468
25. *Portál veřejné správy* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://portal.gov.cz>.
26. PROCHÁZKOVÁ, D. *Komplexní pohled na problematiku bezpečnosti : článek* [online]. Ministerstvo vnitra : Týdeník veřejná správa, 2008 [cit. 2010-01-15]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/2003/casopisy/vs/0435/konz_info.html>.
27. *Projekt SIPROCI a jeho výsledky* [online]. 06.04.2007 [cit. 2010-02-15]. Dostupný z WWW: <http://www.kraj-jihocesky.cz/file.php?par%5Bid_r%5D=24491&par%5Bview%5D=0>.
28. *Radiokomunikační systém PEGAS* [online]. 2010 [cit. 2010-03-10]. Dostupný z WWW: <http://www.pramacom.cz/cz/projekt-detail.php?projectId=4>.
29. *Státní informační a komunikační politika e - Česko 2006* [online]. 31.03.2004 [cit. 2010-03-15]. Dostupný z WWW: <http://knihovnam.nkp.cz/docs/SIKP_def.pdf>.
30. *Strategické řízení* [online]. 30.09.2003 [cit. 2010-02-05]. Dostupný z WWW: <http://www.bibs.cz/useruploads/files/sbornik_invex_strategicke_rizeni_is_it.pdf>.
31. *Strategie realizace Smart Administration* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/strategie-realizace-smart-administration>.

32. *Strategie rozvoje služeb informační společnosti* [online]. 2010 [cit. 2010-02-15]. Dostupný z WWW: <http://www.osf-mvcr.cz/strategie-rozvoje-sluzeb-informacni-spolecnosti>.
33. *Strategie rozvoje služeb pro informační společnost* [online]. 19.06.2007 [cit. 2010-02-15]. Dostupný z WWW: <http://www.smartadministration.cz/files/StrategieSmartAdministration2007-2015.pdf>.
34. *Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu.* [online]. 2010 [cit. 2010-01-20]. Dostupný z WWW: <http://www.mvcr.cz/clanek/riziko.aspx>.
35. *Tísňová volání v České republice* [online]. 17.03.2009 [cit. 2010-03-05]. Dostupný z WWW: <http://www.hzscr.cz/clanek/tisnova-volani-v-ceske-republice.aspx?q=Y2hudW09MQ%3d%3d>.
36. *Vyhláška č. 380/2002 Sb. k přípravě a provádění úkolů ochrany obyvatelstva* [online]. 21.08.2008 [cit. 2010-02-15]. Dostupný z WWW: <http://www.hzscr.cz/soubor/vy-380-2002-pdf.aspx>.
37. *Vyhláška č. 529/2006 Sb., o dlouhodobém řízení informačních systémů veřejné správy* [online]. 06.02.2006.[cit. 2010-02-15]. Dostupný z WWW: <http://www.mvcr.cz/soubor/vyhlaska-c-529-2006-sb-o-dlouhodobem-rizeni-informacnich-systemu-verejne-spravy.aspx>.
38. *Zabezpečení krizové komunikace* [online]. 2010[cit. 2010-02-15]. Dostupný z WWW: <http://www.cz.o2.com/izs/cz/site/home/index.html>.
39. *Zákon 365/2000 Sb. o informačních systémech veřejné správy* [online]. 1996 [cit. 2010-02-25]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00365&cd=76&typ=r>.
40. *Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů* [online]. 1996 [cit. 2010-02-19]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00101&cd=76&typ=r>
41. *Zákon č. 238/2000 Sb. o hasičském záchranném sboru ČR* [online]. 1996 [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00238&cd=76&typ=r>.
42. *Zákon č. 239/2000 Sb. o integrovaném záchranném systému* [online]. 1996 [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00239&cd=76&typ=r>.
43. *Zákon č. 240/2000 Sb. o krizovém řízení* [online]. 1996 [cit. 2010-02-25]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00240&cd=76&typ=r>.
44. *Zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy* [online]. 1996 [cit. 2010-02-15]. Dostupný z WWW: <http://www.sagit.cz/pages/sbirkatxt.asp?zdroj=sb00241&cd=76&typ=r>.

ABSTRAKT

PŘÍHODA, M. *Informační systémy a technologie na podporu krizového řízení : bakalářská práce*. České Budějovice : Vysoká škola evropských a regionálních studií, o. p. s., 2010. 76 s. Vedoucí bakalářské práce: Antonín Čupera.

Klíčová slova: Bezpečnost, ochrana obyvatelstva, krizové řízení, veřejná správa, informační společnost, informační a komunikační technologie, jednotné evropské číslo tísňového volání, internet, Integrovaný záchranný systém.

Práce vymezuje oblast ochrany obyvatelstva a krizového řízení v bezpečnostním systému České republiky. Zabývá se směry dalšího vývoje za využití informačních a komunikačních technologií. Popisuje probíhající reformu veřejné správy, zavádění informačních systémů veřejné správy a filosofii moderní veřejné správy jako služby občanovi. Představuje informační a komunikační technologie, které jsou již v systémech veřejné správy a krizového řízení využívány. Nalézá vztahy mezi těmito systémy a snaží se poukázat na naléhavost jednotného přístupu k datům, se kterými tyto systémy pracují. Vyzdvihuje projekt Digitální mapa veřejné správy, který by měl být základem geografického informačního systému, využívaného pro podporu rozhodování krizových orgánů. Apeluje na vzdělanost pracovníků veřejné správy a orgánů krizového řízení v oblasti informačních a komunikačních technologií, tak aby bylo možné naplňovat cíle budování bezpečné společnosti, popsané v Koncepci ochrany obyvatelstva do roku 2013 s výhledem do roku 2020.

ABSTRACT

PŘÍHODA, M. *Information Systems and Technology for Support of Crisis Management :* Bachelor Thesis. České Budějovice : The College of European and Regional Studies, o. p. s., 2010, 76 p. Supervisor: Antonín Čupera.

Key words: Security, protection of the population, crisis management, public administration, Information Society, Information and Communication Technologies, the single European emergency call number, Internet, Integrated safety system.

The bachelor thesis defines areas of population protection and crisis management in the security system of the Czech Republic. It deals with the further development guidelines in applying information and communication technologies. The bachelor thesis describes a running process of public administration reform, the implementation of its information systems and explains modern public administration based on the principal of public service. It introduces the information and communication technologies already used in the public administration and the crisis management systems. Founding relations between these two systems, it tries to demonstrate the urgency of uniform access to data the systems work with. It highlights the Digital Public Administration Map project that should be the basis of geographical information system used to support the crisis authorities' decisions. The bachelor thesis appeals to the public administration and crisis management authorities to be well educated as to Information and Communication Technologies usage and so possible to achieve the aims of safe society creation as described in the Conception of Population Protection until 2013 with future development expectations until 2020.